Authentications for Internet of Things Security: Threats, Challenges and Studies

Seo Yeon Moon[1], Jin Ho Park[2], Jong Hyuk Park[1]

[1] Department of Computer Science and Engineering Seoul National University of Science and Technology (SeoulTech), South Korea

[2] Department of Computer Science, School of Software, SoongSil University, South Korea

moon.sy0621@seoultech.ac.kr, j.park@ssu.ac.kr, jhpark1@seoultech.ac.kr

Abstract

The Internet of Things (IoT) is attracting attention as the core technology with the development of the wireless network and the universal use of portable terminals. IoT provides high quality service to the user through various technology convergences that are based on smart devices to high performance. However, due to the vulnerabilities connected with complex technologies and problems with implementation methods, there are various security threats. Therefore, to provide the best service, it is necessary to construct a secure environment for security threats in the IoT. It also must be protected and managed the device via authentication or secure policies. In this paper, we describe the security threats, issue and consideration in IoT, and we examine authentication structure, lightweight technology, and key management. We also propose an authentication service scenario based on existing authentication technology and research. Finally, we present the development and research direction of Internet security technology to provide secure service.

Keywords: Authentication, Internet of things, Security threat, Computer security

1 Introduction

Recently, Wi-Fi, LTE, and other wireless internet usage rates have increased significantly through the universal use of mobile devices, such as Smartphone and tablet. It is possible to easily use the network communication connection without the restrictions of space and time via the development of various kinds of wireless network technology. As such, the network communication range is becoming more diverse and narrower between people, things, and people and things based on wireless networks without being bound to a specific space and time [1-3]. This environment is called the Internet of Things (IoT), and it is becoming a core technology that is leading the industry into the fourth industrial revolution. It provides services by collecting and processing a lot of information via things that have a close relationship with people, such as smart car, smart home, smart wearable, etc. IoT technology and services are attracted the most attention IT due to the potential of various content development and its wide range of usability.

By influencing the IoT environment, computing technology is being integrated into small-sized objects to form a network for all connectable elements. In addition, various technologies are being fused together to form a specific service. Accordingly, there are various security threats due to the weakness of the technology itself or various implementation methods. Therefore, IoT security challenges include existing security threats and new security threats, such as infringement of data integrity, infringement of confidentiality of signals and data, unauthorized service, user access, authentication interception, personal information leakage, and retransmission attacks. The economical damage is also serious with these security vulnerabilities. The IoT needs to solution from the perspective of new information and communication services and industries. From amongst these areas, internet security technologies and services will have a significant impact on other related industries in the future.

IoT security should first consider whether the data exchanged through network communication is normal and whether there are any problems with integrity. Therefore, authentication is essential to ensure a normal network connection, and key management is very important to keep this authentication secure. As a result, authentication provides a security service between objects to confirm that the data is secure [4]. IoT security should be based on a technical and lightweight cryptography algorithm for low-power device authentication. For optimal performance, the authentication process should not be complex. The authentication procedure should be designed to be optimized for various smart environments based on IoT

*Corresponding Author: Jong Hyuk Park; E-mail: jhpark1@seoultech.ac.kr
DOI: 10.3966/160792642018031902004

technology and security the requirements of each environment [5].

In this paper, we describe the security threats and requirements of the IoT. In addition, we examine authentication structure, lightweight technology, and key management. We propose an authentication service scenario based on existing authentication technology and research, and then we present the development and research direction of internet of things security technology in order to provide secure service.

2 IoT Security

The IoT environment is likely to generate security vulnerability due to the integration of many technology elements. In addition, it has the problems of high security/privacy and integrated security due to various reasons [6]. Furthermore, there are other reasons, such as physical equipment supplier, telecom/network provider, IoT services developer, platform provider, and data owner. It is very difficult for all of these elements to guarantee the same security/privacy. This section describes security threats, issue and considerations in the IoT environment.

2.1 Security Threat

IoT service is used by combining various technologies for the purpose of gathering information and processing, processing and storing data, and communicating with people, services, and objects. That is, IoT uses smart sensor technology and collected information to collect more information. Various types of technologies are applied in order to provide smooth network communication technology and service functions, such as chip technology, platform technologies, big data processing of mass sensing data technology, mining technology for useful information extraction, web services for the IoT services, the autonomous and intelligent behavior of objects for operating system, embedded system technologies, utilizing IoT devices, and application development [7].

IoT services based on complex technologies may have various security vulnerabilities due to the problems of technology convergence itself or implementation methods. IoT security threats can occur in the form of attacks, such as data forgery and tampering, unauthorized service and user access, authentication tampering, confidentiality and integrity breach of signals and data, information leakage, replication attacks, etc [8]. In addition to these security vulnerabilities, personal privacy violation is also a serious issue. Therefore, in order to provide secure and reliable IoT service, it is necessary to first examine IoT security requirements and technology.

In terms of space, a smart home is an example of a small case of security threat. A smart home is a system that controls home appliances, energy consumption devices, such as water, electricity, heating and cooling, and door locks; and security devices, such as CCTV, through a communication network. Devices in a residential smart home setting can be easily disabled by hacking programs. If the vulnerability of a commonly used product is found the damage could be quite significant when a security threat occurs. IoT services in relatively small spaces (smart home, smart car, etc.) are exposed to security threats, such as malicious device control and the leakage of personal information [9].

IoT security can be divided into three types: smart terminal security, user authentication and access control, and various application service layer securities for things such as the internet, PC, Smartphone, IoT devices, and sensors. Convenience of smart devices mainly provides functions by utilizing user information. In addition this requires a variety of other information for greater productivity [10]. Therefore, there is a risk that the user's personal information and related information will be exposed to the attacker. IoT threats and types of damage are shown in Figure 1 below.

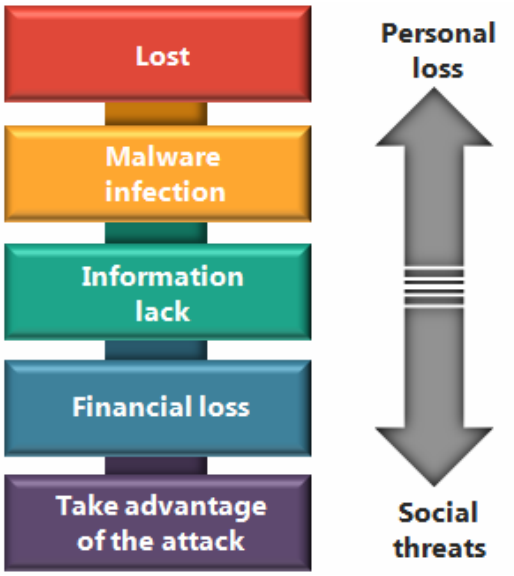

Figure 1. IoT threats and types of damage

Threats to smart devices include lost, malware infection, information leakage, and financial losses. "Lost" is the possibility of data leakage about individuals and businesses occurring. Malware infections are similar to malicious code infections and are an attack threat that can be exploited over a wireless network between web services or devices, such as the internet, Bluetooth, and Wi-Fi. It is mainly used for data takeover and devices access control through the use of Trojans. Information leakage can result in secondary security attacks because the call log, SIM card information, location information, etc. are indirect information of the user. Financial losses are fee manipulation and charged content billing. This

occurs through control, such as middleware, smart devices, application programs, etc., and causes direct damage to the user. Advantage of the attack' means high level security threat, such as APT (Advanced Persistent Threat), DoS (Denial of Service) attack and DDoS (Distributed Denial of Service) attack. Listed below are some of the security threats per IoT component.

2.2 Issue and Considerations

A key challenge of device placement and network communication configuration in IoT is to coordinate multiple networks with a common all-IP system [11]. This can ensure both the quality and versatility of the network communication system. However, due to complex technology convergence, other issues should be taken into consideration in order to build a stable system.

IoT security issues can be summarized as described below [12-16]:

(1) Objects and devices that are not related to internet access at all are connected to the internet in the IoT environment. Because of the variety of services available, IoT can present all the risks and vulnerabilities that can occur in the existing Internet environment. In other words, in a network with limited resources and low-power communication technologies, various threats that currently exist in the internet can occur.

(2) Because program code is open, an attacker can easily find open platform source vulnerabilities. This can increase the likelihood of attack threats using security vulnerabilities. In an IoT environment consisting of multiple devices, the threat of an attack will significantly augment via the part of connected infection devices.

(3) Some research suggests that smart home devices lack password strength, mutual authentication, or account protection against enterprise attacks. Recently-used smart home appliances and devices are still vulnerable to security threats, such as the inability to meet complex cryptographic configuration requirements.

(4) IoT security threat can create physical damage and even pose risks to human life. In a variety of medical devices (including smart healthcare), autonomous vehicles, and smart transportation systems, malfunctions due to hacking can lead to accidents. It can be seen as a direct problem with human life.

Table 1 lists described the secure requirements for the security threats.

Table 1. Requirements for security threats on IoT

Layer	Requirements
Device	• Development and application of lightweight encryption technology (vaccine, encryption, authentication) • Develop security patch technology for reliability and integrity verification • Sensor device monitoring technology
Network	• Protocol interoperability criteria • Development of low security network technology • Network monitoring and monitoring technology
Platform/ Service	• Secure open platform guidelines • Device - service cross-certification and key management • Personal information collection / tracking prevention and identification information filtering technology

First it is the sensor device. As devices become more diverse and more sophisticated, the use of low-power devices increases. Currently, there are many cases where it is difficult to apply security for certain areas, such as vaccines, encryption, and authentication, to low-power devices with security technology. As the number of devices increases, it becomes more difficult to apply security patches, and security vulnerabilities will increase due to the difficulty in monitoring communication contents. To solve this problem, it is necessary to develop and apply lightweight security technology (vaccines, encryption, authentication, etc.) that reflects various device characteristics, including low-end devices. In addition, it is necessary to develop sensor and device security patches by applying technology and sensors and device monitoring systems in order to ensure the reliability of the operation of the apparatus and to verify its integrity.

Second, interworking communication is performed between mobile wireless networks, such as Zigbee, Wi-Fi, and Bluetooth, in the network. This communication is exposed and this means that a malicious user is easy to access. In other word, it is difficult to maintain a constant level of security. In addition, since inter-device communication can be supported, device authentication is supported on a limited basis. Attackers can infect devices by used malware, such as large-scale mass production of zombies PC via the cloud, virtualization services, refrigerator, cleaning robots, and medical equipment. At the same time, traffic explosion attacks are possible. To solve this problem, it is necessary to develop an interoperability protocol standard for dual network interworking and a security technology that is suitable for a heterogeneous low-end connection communication network environment. Security status monitoring and the monitoring of large scale equipment and networks will also be required.

Third it is platform / service. Attacks, such as false data transmissions/malfunctions between devices and open platform services, are a common occurrence. The centralization and combination of fragment information collected by an IoT device can result in the leakage of user identity information. Technology, such as a secure, open platform using the instructions provided mutual authentication and key management between devices / user services, trust management, collecting / tracking personal information, and personally identifiable device etc., are all needed to solve this problem.

3 Authentication for IoT security

Authentication is a security procedure that verifies the subject's ability to access arbitrary information or the subject's credentials [17]. Authentication in IoT is the process of restricting access to non-operation devices and identified users between users and devices in network communications [18]. In this section, we discuss authentication requirements, Existing scheme, technologies, and key management in IoT.

3.1 Requirements

Authentication requires that when a user requests access to an information asset, systems and administrators go through a series of identification and authorization processes, such as the user's presence, user identification, and authorization. In the course of this process, the identification and authentication of users, authorization of usage rights, and ensuring accountability are required [19]. Access control requirements for authentication are controlled by user authentication and authorization policies according to identification, authentication, authorization, and accountability.

- *Identification*: This is the process of requesting the system for the expression ID of the subject. Users of each system have a unique identifier (e.g., Login ID) that the system can identify. Since these identifiers represent the identity of each individual, they are also important in the analysis of the user's accountability.
- *Authentication*: This is the step of verifying the subject's ability to access arbitrary information or the subject's qualification. This prevents unauthorized use of the system or the improper transmission of information.
- *Authorization*: This means the permission granted to the user, program, or process. Authorization is the process of granting something that can do a certain act or have a certain resource.
- *Accountability*: This is a foundation for recording who, what, and when, and some actions were taken in a multi-user, multi-tasking network environment and making it possible to trace the actors when necessary.

When these requirements are met, a security environment with a basic user authentication policy is established. Also, the more the associations between the elements are combined, the greater the stability of secure will be.

3.2 Existing Scheme on Authentication

Table 2 shows the existing schemas for authentication in the IoT described above. Muhamed Turkanovic et al. proposed a new user authentication and key agreement for different ad-hoc wireless sensor networks [20]. Their proposed model provides mutual authentication, password protection, free password selection, password change, and dynamic node addition between all parties. The system is very light and is effective in responding to common network security attacks. Such as reply attack, verification attack, smart card violation attack, impersonation attack, authorized insider attack, GWN bypass attacks, password attack, DoS attack, etc. In the research Ruhul et al. it shows some security weaknesses of the protocol [21].

The researcher also noted that they were not efficient in terms of the authentication and security parameters created by Turkanovic et al. To overcome the security vulnerabilities mentioned above, they designed a new architecture for the WSN environment and proposed schemes for user authentication and key contract schemes. In addition, our proposed method is simulated using the well-known AVISPA security tool. The simulation results show that this protocol is secure under OFMC and CL-AtSe models.

In addition, we confirmed that some security problems and proposed protocols are adequately protected from the viewpoint of related security attacks including the security vulnerabilities we've already listed. Huansheng Ning et al. described the security problem of ubiquitous objects. They designed an integrated proof-based hierarchical authentication scheme (APHA) for layered networks with an emphasis on the existing U2 IoT architecture (unit IoT and ubiquitous IoT) [22].

The 4th study shows the resource requirements for adopting DTLS handshake public key encryption in peer authentication and key contracts. The delegated structure acts as the center of the delegation server in the initial connection setup.

IoT provides a comprehensive and concise solution for authentication, authorization, and secure data transfer over IP [23]. IP-based security solutions include real-time detection of IP data traffic, SSL / TLS handshaking, open port analysis, clear text keyword matching analysis, and endpoint information (location, domain name). The IoT authentication service requires that clients (connected devices, server applications, mobile applications or users) use strong authentication (X.509 certificates, credentials or external security authority authentication). All

Table 2. Summary of existing scheme on Authentication for IoT

Reference	Scheme	Basic theory	Description	Other feature
[20]	A novel user authentication and key agreement scheme based on IoT	lightweight key agreement protocol, password-change option	It enables a remote user to securely negotiate a session key as well as it ensure ensures mutual authentication between the user, sensor node, and the gateway node (GWN)	Tackle the IoT risk and challenges, ensure high security and performance feature.
[21]	A secure lightweight scheme for user authentication and key agreement scheme	BANlogic, AVISPA security tool, OFMC and CL-AtSemodels	The scheme provides the security validation of the proposed protocol has done by using BANlogic. Paper ensures that the protocol achieves mutual authentication and session key agreement property securely between the entities involved	Energy efficiency, user anonymity, mutual authentication and user-friendly password change phase
[22]	Aggregated-Proof based hierarchical authentication scheme for the IoT	homomorphism functions, Chebyshev chaotic maps, dynamically hashed values, BAN logic	Paper focus on existing U2IoT- unit and ubiquitous IoT architecture design an aggregated-proof based hierarchical authentication scheme (APHA) for the layered networks.	Establishes trust relationships via the lightweight mechanisms
[23]	Delegation-based Authentication and Authorization for the IP-based IoT	DTLS handshake, public-key cryptography	When using public key cryptography for peer authentication and key agreement purposes, it identifies critical resource requirements of the DTLS handshake. It provides a comprehensive and compact solution for authentication, authorization, and secure data transmission with IP based IoT.	authorization functionality, network transmissions, reduces the memory overhead
[24]	Security Analysis and Improvements of Authentication and Access Control in IoT	Role Based Access Control, ECC algorithm.	Paper analyses the authentication and access control method using in the Internet of Things presented by Jing et al (Authentication and Access Control in the Internet of Things	Confidentiality, integrality and authenticity and achieves better efficiency at a lower communication cost.
[25]	An Efficient Authentication and Access Control Scheme for perception layer of IoT	Elliptic Curve Cryptography (ECC), Attribute-based Access Control	An efficient ECC-based authentication and the attribute-based access control policy are proposed in order to achieve mutual authentication between user and nodes and fine-grained access control.	flexible fine-grained access control, Mutual authentication security of the communication between user and nodes

communications provide encryption and granular authorization to isolate and protect authenticated client-to-client communications.

Bruce Ndibanje et al. provided various aspects that could be addressed and improved the security gaps found in the protocol [24]. They analyzed and improved Jing et al. 's protocol for IoT. They used the decryption methodology to find problems in the proposed protocol. We have reviewed and analyzed the work in detail and found that the protocol is vulnerable to device attacks and replay attacks. Sensor data should be encrypted for use by intended recipients only, and static encryption should be avoided so that it can not be easily analyzed externally and reused. Some devices use fixed encryption and may be subject to reuse attacks without the need for decryption. For example, an attacker can stop a device at any time through reuse by simply acquiring a device stop command passphrase. Ye Ning et al. proposed an efficient ECC-based authentication and attribute-based access control policy for mutual authentication and granular access control between users and nodes [25]. This method can solve the resource limitation problem of the perceptual layer of IoT. other improvements rather than mitigating authentication and authorization issues.

3.3 Existing Authentication Technology

Sanaz Rahimi Moosavi's work developed a secure and efficient authentication and authorization architecture for healthcare services in the IoT environment [26]. Due to the resource constraints of medical sensors, it is not feasible to use existing encryption in IoT-based medical care.

The existing IoT gateways insist on focusing on other improvements rather than mitigating authentication and authorization issues. In the proposed architecture, the authentication and authorization of a remote end user is performed by a distributed smart

electronic health gateway. It therefore prevents the medical sensor from performing any work on its own.

C. Schmitt's WSN optimized a two-way authentication solution for a small device (TinyTO) that combines end-to-end secure communications [27]. TinyTO provides confidentiality and integrity in a fast and secure handshake. It uses public key encryption and elliptic curve encryption (ECC) for message encryption and authentication. Sheetal Kalra investigated the widespread use of IoT in many industry and government organizations due to the integration of embedded devices and cloud servers [28]. The authors proposed a mutual authentication protocol to ensure communication between the embedded device and the cloud server. This protocol is based on ECC and Hyper Text Transfer Protocol (HTTP) cookies.

The security analysis of the proposed protocol has a robust advantage over multiple security attacks. Namje Park et al. proposed symmetric key based inter-device authentication and session key agreements for an IoT environment [29]. Unlike the existing sensor network environment in which the key distribution center distributes keys, each sensor node is involved in generating a session key. For efficient performance, the session key can only be calculated for an authenticated device. Sravani Challa al. an IoT device remotely accesses and controls the network infrastructure that enables the integration of physical infrastructure and computing. The authors proposed a new signature-based authenticated key establishment scheme for the IoT environment. [30]

Among the existing authentication technologies, there are methods, such as login procedure and one-time-pad (OTP) through object information [31]. In IoT, mutual authentication procedures are required before various devices can exchange information, which is an important procedure for the mutual identification. Technically, object-based login authentication is the simplest, but the password itself can be easily exposed. Since the unique identification ID of the device is easy to duplicate, it is necessary to use it in conjunction with other authentication methods. OTP, which is known as the most powerful authentication method, should be automatically authenticated between devices due to the nature of the IoT environment. Therefore, it is difficult to use it in IoT.

Biometrics is not a perfect authentication method, but it is very effective as one of the authentication technologies to complete transactions by providing secure and convenient authentication [32]. The biometrics of these devices provide a secure ecosystem that keep biometric data private by using an integrated hardware channel, allowing the user to conveniently and securely use the most personal devices such as Smartphone. This makes biometrics one of the safest mobile device authentication methods [33]. The information available for biometric technology is owned by the individual and is only required to be personally identifiable, not reproducible. While biometric technologies can provide greater security than traditional password-based security systems, there are still many limitations due to high technology barriers [34]. For instance, since the recognition rate of biometric information is unstable and it is much more expensive, it still needs more time until it is used more easily in various fields. Because biometric information also has sensitive personal data, there is a systematic system and management cost to manage that information. Therefore, in order to use biometric information as a security measure, a management system to prevent personal information infringement should be considered.

4 Use-case Scenario

4.1 Sound Recognition-based Authentication

Sound recognition is called speaker recognition, and it is a field that has been actively researched because it has a higher error rate than other biometrics, but it excludes the ability to imitate. In particular, unlike other biometric devices, the microphone, which is a sound acquisition device, is inexpensive and is generally installed in PC, PDA, Smartphone. In addition, it can be used in a remote area using a telephone or the internet, and can be used in an application field in which other biometric methods, such as telephone banking, cannot be applied.

In order to correctly process the sound of the user, high recognition performance and noise processing are required. Speech recognition requires consideration of language models, vocabulary dictionaries, and pronunciation rules. In addition, it is necessary to recognize the language model and key words considering various pronunciation variations. If you take advantage of the large voice DB and sub-word units in the form of process models considering the context, it will be more accurate and handle a variety of commands.

Sound recognition can be applied to authenticate locks, user identifications, etc. in small networks owned by individuals, such as smart car and smart home. The user authenticates the service through a specific voice command or pattern, and uses a device equipped with various microphone functions and voice recognition functions, such as Smartphone, template, and portable PC. Successful authentication is for ensuring that owners of small networks and services are eligible to receive services. In general, a device with a microphone and voice recognition function is a network communication device, whereby a user can remotely authenticate to another person via a voice message and transfer small network rights. Figure 2 shows the sound recognition-based authentication

process for smart car.

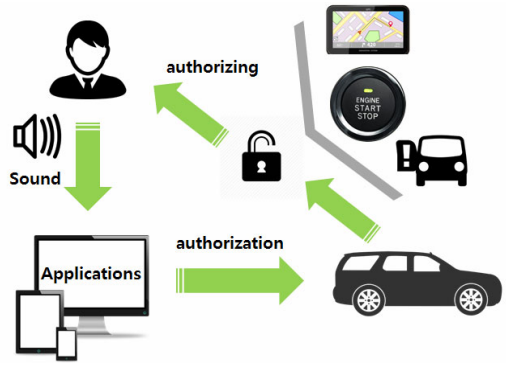

Figure 2. Sound recognition-based authentication

4.2 Location-based Authentication

Location-based services (LBSs) are services that use location determination technology (LDT) to find and provide related technologies. This technique can be applied to various types of users, devices, vehicles, etc. through the acquired location information. This universal technology provides navigation, identification of the location of human finders, and identification of traffic congestion. LBSs is largely divided into positioning technology, platforms, and application services. Positioning technology is GPS (Global Positioning System) and Cell-ID (Cellular-ID) system. Users can also measure their location using RFID, terrestrial radio beacons, and wireless LAN.

The user is authorized to use the smart home service through the location information of the device. Devices that are available for positioning technology include Smartphone, RIFDs, and beacons. Smart home services utilize a wide variety of devices and some services include a high risk. Therefore, when a user is authenticated at home, a smart service with high risk (locks, specific device, personal information transmission, etc.) should be provided, and the usual smart home services will continue to be provided. The location-based security authentication scenario using the location-based technique in the smart home network is shown in Figure 3.

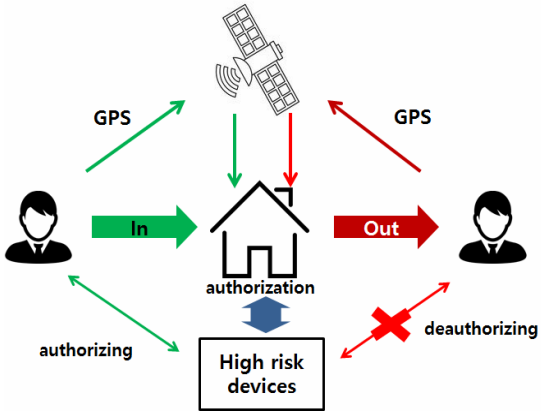

Figure 3. The location-based authentication scenario

The user is authorized to use the smart home service through the location information of the device. Devices that are available for positioning technology include Smartphone, RIFDs, and beacons. Smart home services utilize a wide variety of devices and some services include a high risk. Therefore, when a user is authenticated at home, a smart service with high risk (locks, specific device, personal information transmission, etc.) should be provided, and the usual smart home services will continue to be provided

Figure 4 shows the location-based authentication flowchart. In order for a user to be recognized at a specific place (house, company, etc.), a terminal registration is necessary. It performs physical security role, primarily, and can be an effective defense against indiscriminate attacks.

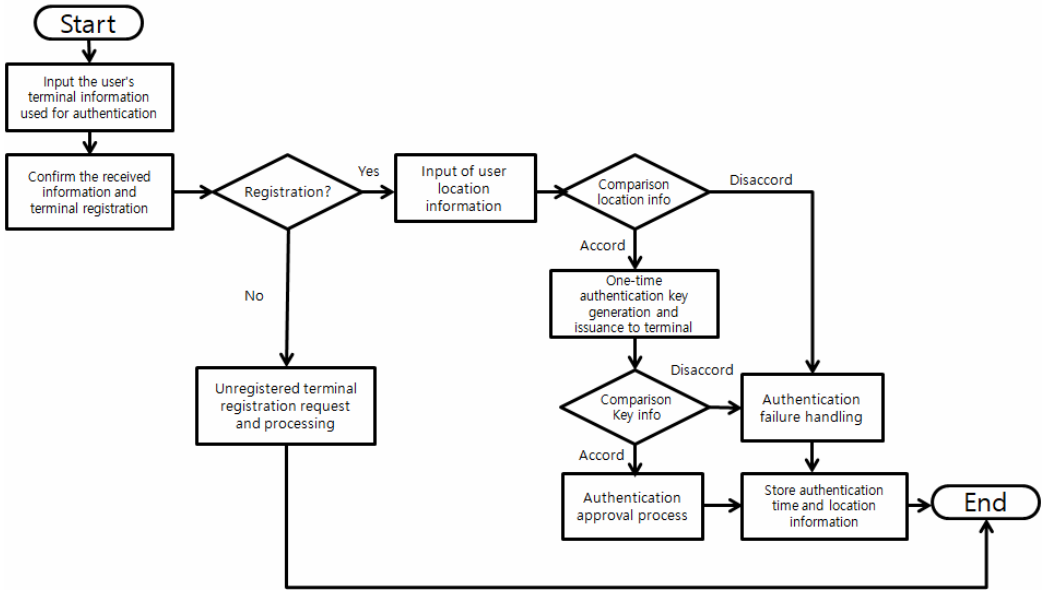

Figure 4. Flowchart of location-based authentication

After the registration confirmation of the terminal, it requests the location information collection. The user transmits location information of the terminal. If the received location information is an appropriate distance for authentication, the authentication process is performed. If the user's location is farther or worse than the authentication location, the authentication process fails.

The authentication process first generates a one-time authentication key. The authentication point delivers the one-time authentication key to the user via the online service system or application. The user transmits the issued authentication key. It compares the received key with the issued key at the authentication point. If the authentication keys curret, it process authentication acknowledgment. It saves time and location information to record authentication log. It sends authorization and processing results to the user. Otherwise, it handles the authentication failure.

5 Conclusion

In order for IoT technology to expand into the industry, challenges, such as security and privacy protection and the establishment of global standards, must be proactively solved along with the development of related technology. In IoT, security technology is as essential as sensor or network technology because security threats in IoT devices can threaten users' lives and safety and cannot be commercialized. In particular, authentication, which is regarded as a primary technology in security, must be built and strengthened in the IoT environment because it primarily protects access. As the IoT evolves, IoT security becomes increasingly important, as current security threats spread more rapidly through IoT devices and various types of attacks are expected to shift.

IoT security should be approached from a new point of view, such as the scope of protection, target characteristics, subject of security, and protection methods. This is unlike it is for the cyber environment, which is centered on existing PCs and mobile devices. In the past, the scope of protection was limited, but in the IoT era, everything connected to the IoT, such as wearables, home appliances, automobiles, and medical devices, is expanded and existing high-power / high-performance protection targets are greatly expanded to ultra-lightweight, low-power, and low-performance objects. In the past, security principals were limited to Internet Service Providers (ISPs), security vendors, and users. However, in the IoT era, it extends to manufacturers and the above-listed security principals. In the case of protection methods, the protection object has been protected by separate security equipment.

In this paper, IoT analyzes security threats through Lost, malware infection, information leakage, and financial loss. We explained the requirements and the security platform. We also described the authentication system, which is the primary security procedure for secure smart services, and the lightweighting technology and cryptosystem for implementing it. We studied the existing IoT authentication scheme and its technology and proposed a scenario using it. In the future, as the range of IoT increases, the scope of security threats will expand and the importance of protecting information will also increase. As a result, based on our authentication study of IoT in this paper, a more secure IoT environment should be constructed by developing concrete and systematic security frameworks and solutions. We hope that this paper can be used as useful data for security accident prevention, certification technology, and security technology utilization.

Acknowledgments

This study was supported by the Research Program funded by the SeoulTech (Seoul National University of Science and Technology).

References

[1] A. Whitmore, A. Agarwal, L. D. Xu, The Internet of Things: A Survey of Topics and Trends, *Information Systems Frontiers*, Vol. 17, No. 2, pp. 261-274, April, 2015.

[2] D. Sopori, T. Pawar, M. Patil, Roopkala Ravindran, Internet of Things: Security Threats, *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)* Vol. 6, No. 3, pp. 263-267, March, 2017.

[3] J. Pescatore, G. Shpantzer, *Securing the Internet of Things Survey*, SANS Institute, 2014.

[4] M. Yoon, J. Baek, A Study on Framework for Developing Secure IoT Service, *Advances in Computer Science and Ubiquitous Computing*, Singapore, 2015, pp. 289-294.

[5] A. Furfaro, L. Argento, A. Parise, A. Piccolo, Using Virtual Environments for the Assessment of Cybersecurity Issues in IoT Scenarios, *Simulation Modelling Practice and Theory*, Vol. 73, No. 1, pp. 43-54, April, 2017.

[6] W.-T. Cho, Y.-W. Ma, Y.-M. Huang, A Smart Socket-Based Multiple Home Appliance Recognition Approach over IoT Architecture, *Journal of Internet Technology*, Vol. 16, No. 7, pp. 1227-1238, December, 2015.

[7] M. P. Andersen, G. Fierro, D. E. Culler, Enabling Synergy in IoT: Platform to Service and Beyond, *Journal of Network and Computer Applications*, Vol. 81, No. 1, pp. 96-110, March, 2017.

[8] O. Bello, Sherali Zeadally, Mohamad Badra, Network Layer Inter-operation of Device-to-Device Communication Technologies in Internet of Things (IoT), *Ad Hoc Networks*, Vol. 57, No. 15, pp. 52-62, March, 2017.

[9] W. M. Kang, S. Y. Moon, J. H. Park, An Enhanced Security Framework for Home Appliances in Smart Home, *Human-centric Computing and Information Sciences*, Vol. 7, No 6, pp. 1-12, March, 2017.

[10] J. Kim, S.-C. Choi, I. Yep Ahn, Nak-Myoung Sung, Jaeseok Yun, From WSN towards WoT: Open API Scheme Based on oneM2M Platforms, *Sensors*, Vol. 16, No. 10, pp. 1-23, July, 2016.

[11] M. F.-C. Tiago, F.-L. Paula, S.-A. Manuel, L. Castedo, Reverse Engineering and Security Evaluation of Commercial Tags for RFID-Based IoT Applications, *Sensors*, Vol. 17, No. 1, pp. 1-31, December, 2016.

[12] M. F. Alam, S. Katsikas, O. Beltramello, S. Hadjiefthymiades, Augmented and virtual reality based monitoring and safety system: A prototype IoT platform, *Journal of Network and Computer Applications*, Vol. 89, No. 1, pp. 109-119, July, 2017.

[13] S. Pirbhulal, H. Zhang, M. E. Alahi, H. Ghayvat, S. C. Mukhopadhyay, Y.-T. Zhang, W. Wu, A Novel Secure IoT-Based Smart Home Automation System Using a Wireless Sensor Network, *Sensors*, Vol. 17, No. 1, pp. 1-19, December, 2016.

[14] H.-K. Kong, M. K. Hong, T.-S. Kim, Security Risk Assessment Framework for Smart Car Using the Attack Tree Analysis, *Journal of Ambient Intelligence and Humanized Computing*, Vol. 27, No. 1, pp. 1-21, January, 2017.

[15] T. Winkler, Security and Privacy Protection in Visual Sensor Networks: A Survey, Journal*, ACM Computing Surveys (CSUR)*, Vol. 47, No. 2, pp. 1-13, July, 2014.

[16] W. Wang, Z. Lu, Cyber Security in the Smart Grid: Survey and Challenges*, Computer Networks*, Vol. 57, No. 5, pp. 1344-1371, April, 2013.

[17] G. P. Hancke, K. Markantonakis, K. E. Mayes, Security Challenges for User-Oriented RFID Applications within the "Internet of Things", *Journal of Internet Technology*, Vol. 11, No. 3, pp. 307-313, May, 2010.

[18] M. Bilal, S.-G. Kang, An Authentication Protocol for Future Sensor Networks, *Sensors*, Vol. 17, No. 5, pp. 1-29, April, 2017.

[19] G. Abdelkader, H. S. Naima, A. P. Adda, Secure Authentication Approach Based New Mobility Management Schemes for Mobile Communication, *Journal of information processing systems*, Vol. 3. No. 1, pp. 152-173, January, 2017.

[20] M. Turkanović, B. Brumen, M. Hölbl, A Novel User Authentication and Key Agreement Scheme for Heterogeneous Ad Hoc Wireless Sensor Networks, Based on the Internet of Things Notion, *Ad Hoc Networks*, Vol. 20, No. 1, pp. 96-112, September, 2014.

[21] R. Amin, G. P. Biswas, A Secure Light Weight Scheme for User Authentication and Key Agreement in Multi-gateway Based Wireless Sensor Networks, *Ad Hoc Networks*, Vol. 36, No. 1, pp. 58-80, September, 2016.

[22] H. Ning, H. Liu, L. T. Yang, Aggregated-proof Based Hierarchical Authentication Scheme for the Internet of Things, *IEEE Transactions on Parallel and Distributed Systems*, Vol. 26, No. 3, pp. 657-667, March, 2015.

[23] R. Hummen, H. Shafagh, S. Raza, T. Voig, K. Wehrle, Delegation-based Authentication and Authorization for the IP-based Internet of Things, *Sensing, Communication, and Networking (SECON), 2014 Eleventh Annual IEEE International Conference*, Singapore, 2014, pp. 284- 292.

[24] B. Ndibanje, H.-J. Lee, S.-G. Lee, Security Analysis and Improvements of Authentication and Access Control in the Internet of Things, *Sensors*, Vol. 14, No. 8, pp. 14786-14850, December, 2014.

[25] N. Ye, R. C. Wang, Q. Lin, *An Efficient Authentication and Access Control Scheme for Perception Layer of Internet of Things*, Repository of the UP, July, 2014.

[26] S. R. Moosavi, SEA: A Secure and Efficient Authentication and Authorization Architecture for IoT-based Healthcare Using Smart Gateways, *Procedia Computer Scienc*, Vol. 52, No. 1, pp. 451-459, June, 2015.

[27] M. N. Corinna, B. Stiller, *TinyTO: Two-way Authentication for Constrained Devices in the Internet of Things*, Internet of Thing (Elsevier), 2015.

[28] S. Kalra, S. K. Sood, Secure Authentication Scheme for IoT and Cloud Servers, *Pervasive and Mobile Computing*, Vol. 24, No. 1, pp. 210-223, March, 2015.

[29] N. Park, M. Kim, C. Bang, Symmetric Key-Based Authentication and the Session Key Agreement Scheme in IoT Environment, *Computer Science and its Applications*, Springer, Berlin, Germany, 2015, pp. 379-384.

[30] S. Challa, A. K. Das, N. Kumar, A. G. Reddy, E. J. Yoon, K. Y. Yoo, Secure Signature-Based Authenticated Key Establishment Scheme for Future IoT Applications, *IEEE Access*, Vol 5. No1, pp. 3028-3043, December, 2017.

[31] Y.-S. Kim, Implementation of a MTM-based Secure OTP Generator for IoT Devices, *Journal of Embedded Systems and Applications*, Vol. 10, No. 4, pp. 199-206, March, 2015.

[32] C. Ziegler, E. von Zezschwitz, Implicit Authentication 2.0: Behavioural Biometrics in Smart Environments, *Human Computer Interaction in the Internet of Things Era*, Munich, Germany, 2015, pp. 100-107.

[33] H. Khan, U. Hengartner, Towards Application-centric Implicit Authentication on Smartphones, *Proceedings of the 15th Workshop on Mobile Computing Systems and Applications*, Santa Barbara, CA, 2014. pp. 1-10.

[34] A. Mosenia, S. Sur-Kolay, A. Raghunathan, N. K. Jha, CABA: Continuous Authentication Based on BioAura, *IEEE Transactions on Computers*, Vol. 66, No. 5, pp. 759-772. May, 2017.

Biographies

Seo Yeon Moon received bachelor's degree of Computer Engineering in Kumoh National Institute of Technology, and master degree of Computer Science and Engineering from Seoul National University of Science and Technology. His current research interests include IoT, computer security and machine learning, etc.

Jin-Ho Park received his doctor's degree of Computer Science in Soongsil University. Now he is a professor in the School of Software, Soongsil University, Seoul, Korea. His research interests focus on Software Engineering, SW Safety/QA /Testing, SW Convergence/Power, IoT, National Defense ISR, IT Service, etc.

Jong Hyuk Park received Ph.D. degrees in Graduate School of Information Security from Korea University, Korea and Graduate School of Human Sciences from Waseda University, Japan. He is now a professor at the Department of Computer Science and Engineering, Seoul National University of Science and Technology (SeoulTech), Korea. His research interests include IoT, Ubiquitous Computing, Information Security, Digital Forensics, etc.