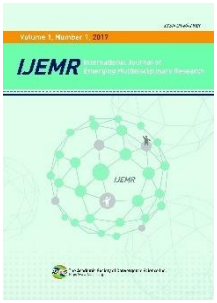


International Journal of
Emerging Multidisciplinary Research

ISSN : 2546-1583
Volume 4, Number 1, March 2020
https://doi.org/10.22662/IJEMR.2020.4.1.001

Technology Trends and Policies for IoT Security

Sunghyuk Hong[1]
[1]Division of Information & Communication Technology, Baekseok University, Cheonan, 31065, KOREA

Abstract

Background/Objectives: In this research, we have explored to the concept and the element of the IoT technology, and some attacking factors to the IoT security. Methods/Statistical analysis: Things and security threats and also examined the security technology and policy contents. Findings: The most important issue for security was security technology and policy on the threat of personal information leakage, and it was found that each country is aware of its importance and is making efforts to research and prepare policies. Improvements/Applications: We will look at some security technology and other supporting policies to suggest some solutions for the direction for the currently improving IoT security.

Index Terms

IoT, Internet of Things, Security, Trends, Policies

Corresponding author : Sunghyuck Hong
shong@bu.ac.kr

•Manuscript received December 6, 2019.
•Revised January 5, 2020; Accepted January 25, 2020.
•Date of publication March 31, 2020.

© The Academic Society of Convergence Science Inc.
2546-1583 © 2017 IJEMR. Personal use is permitted, but republication/redistribution requires IJEMR permission.

I. INTRODUCTION

A. Purpose of Research

Starting with the 4th Industrial Revolution, technologies using the network such as the Internet of Things, Blockchain, and Cloud technologies have attracted attention as its core technologies. Among them, the IoT is currently used in real life. For example, IoT technology is integrated into home appliances such as refrigerators, TVs, and vacuum cleaners to enable overall control with a smartphone. In addition, the technology is being used for smart factories, health care, and automobiles [1].

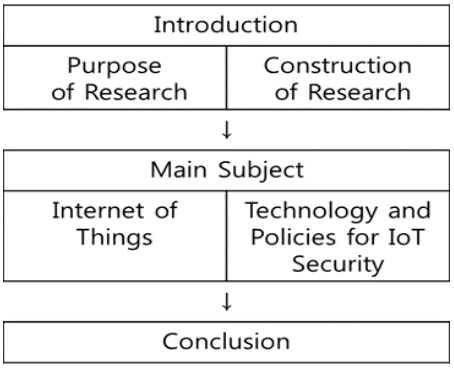
As mentioned above, as network-based technologies are getting closer and more widely used, the importance of security is also increasing. In particular, the Internet of Things is likely to be directly harmed to security when security problems arise in that it is integrated with real things [2]. Kang Nam-hee (2015) discusses security vulnerabilities in IoT technology, reveals threat cases in areas where IoT is applied, and explains the importance of security in IoT technology [3]. Therefore, this study examines the trends of security technology trends and policies centering on the Internet of Things, and hopes that these will be used as basic data on security in the future development of IoT security technology.

B. Research composition

The purpose of this study is to proceed as follows.

First, in Chapter 1, the purpose and composition of this study will be explained, and in Chapter 2, the exact concept of the Internet of Things will be examined to improve understanding of the contents of the study. We will look at technologies, policies, and so on. Third, based on the contents of Chapter 2, we will look into the problems or implications of the current IoT security situation and suggest suggestions.

Fig. 1. Research organization



II. MAIN SUBJECT

A. Internet of Things: IoT

a. Internet of Things

The concept and term of the Internet of Things was first used by Kevin Ashton in 1999, and since then it has been of great interest in industry and academia [9]. All these devices are referred to [4]. In other words, it can be defined as "a technology that processes information by itself based on existing wired / wireless communication." In this regard, ITU-U Y. 2060 defines it as “a foundation technology for the information society that makes advanced services possible by connecting existing or evolved objects based on interactive information and communication technology” [5]. .

The IoT is largely a device composed of data collection sensors, communication modules, a network composed of wireless communication, wired communication technology, a service platform implemented by intelligent information technology, and services implemented by IoT such as healthcare, smart home, and remote management. This is composed of four. In other words, the IoT has many technologies in that people, things, and services must be connected and realized, have an unstructured network structure, require self-organization and management functions, and interface between things is also important [6]. In other words, since information processing / extraction and service provision are based on atypical networks, economic damage, personal information, and company confidential information may be leaked depending on the service, and threats may occur depending on the IoT applied objects. Security is an essential technology in the Internet of Things [3].

b. Security of Internet of Things

The IoT can be attacked by malware, DDoS, etc., through physical components, IoT devices, or software, compared to other technologies. Thus, Table 1 shows the attack paths that the IoT can be attacked, that is, the weak security [8].

Table 1. Potential attack path to the OWASP attack surface

Attack Surface	Potential Attack Path
Ecosystem Access Control	trust exploitation attack, access control system attack
Device Memory	password attack, credentials-based attack, encryption key attack
Device Physical Interfaces	firmware extraction, attack by using CLI, privilege escalation, storage media integrity attack

Device Web Interface	SQL injection, cross-site scripting, cross-site request forgery, user information disclosure
Device Firmware	sensitive information and URL disclosure, encryption key attack, firmware information disclosure
Device Network Services	information disclosure, attack by using CLI, injection, denial of service, service information disclosure, buffer overflow
Administrative Interface	SQL injection, cross-site scripting, cross-site request forgery, user information disclosure, IoT Botnet attack, spoofing attack
Local Data Storage	data confidentiality and integrity attacks
Cloud Web Interface	SQL Injection, cross-site scripting, cross-site request forgery, user information disclosure, pass word attack, spoofing attack
Third-party Backend APIs	personal information disclosure, device and location information leak
Update Mechanism	update mechanism attack
Mobile Application	user information disclosure, password attack, storage data attack, spoofing attack
Vendor Backend APIs	trust exploitation attack, spoofing attack, injection attacks
Ecosystem Communication	IoT healthcare security attack, ecosystem commands attack
Network Traffic	routing attack, DoS attack, Sybil attack

As such, there are various threat possibilities, and IoT security needs to establish security modeling by setting criteria according to the threat. In a related study, Arbia Riahi et. al., (2014) have a holistic approach to IoT security, and Sachin Babar et. al., (2010) discuss the issues of security and privacy and propose a model for trust and privacy. And Orestis Mavropoulos et. al., (2017) present a model using a structure-oriented approach and show security analysis by way of example [8].

Taken together, the IoT basically needs to independently complement and manage all security areas (see Table 2), including three elements: confidentiality, integrity, and availability. In addition, the security level should be applied differently according to the information. In this process, additional security functions are required in addition to the basic security functions based on high-level algorithms and lightweight security solutions (see Table 3.).

Table 2. Security sector for the Internet of Things

Item	Security requirements
System reliability	Service availability
	Infrastructure availability
	Infrastructure integrity
	Infrastructure Reliability
	Non repudiation (user in service)
	Account management
Communication stack Service layer	Service Access Control / Permission Management
	Service certification
	Service reputation measurement
	Service reliability
Communication stack Network layer	Network level anonymization
	Confidentiality
User service privacy	User privacy protection when using infrastructure
	User privacy protection when using the service
	Privacy protection of your targeted services

Table 3. Security features for the Internet of Things

Internet of Things Security features	Description of security features
IoT devices Boot support for Windows	To ensure a safe and secure computing environment for each device operating on the Internet of Things, secure booting technology is required to verify the integrity by verifying the authentication value of the firmware when the switch is first turned on. To do this, cryptographic operations such as digital signatures can be operated by a separate device outside the operating system..

Support lightweight passwords and distributed voluntary security settings	Privacy protection and encryption methods require lightweight encryption solutions that are simple and can be applied to small devices. Since at least 26 billion things are connected to the network, it is impossible for security administrators to properly manage security parameters for all things. Therefore, it is necessary to make the setting for authentication and security voluntarily without administrator..
Virtual between things Private network setup and management support	When transferring sensitive data over public networks, it should be possible to establish and release a virtual private network between things. In addition, mechanisms for delivering software updates and security patches must also be configured while maintaining the limited bandwidth allocated to each device and the intermittent network connectivity characteristics of embedded devices..
For big data analytics Privacy protection	Big data analysis is applied to the information collected from many sensors on the IoT, and privacy protection must be provided. Appropriate privacy protection and anonymization can also be applied to IoT data.
In-depth packet information monitoring Function support	Firewalls and intrusion prevention systems capable of deep packet inspection (DPI) should be configured. If necessary, a DPI solution should be applied for traffic destined for a particular device.

B. IoT security technologies and policies

a. IoT security technology

The Internet of Things is a fusion of technologies, and there are vulnerabilities that arise from physical or technical convergence [9]. In recognition of the importance of the security of the IoT, the Ministry of Science, ICT and Future Planning launched the IoT Security Alliance in June 2015 to examine and supplement potential threats and vulnerabilities in consideration of the operating and life cycle of IoT devices and services. Seven common security principles (hereinafter referred to as 'security principles') with emphasis have been published [3].

Based on this, this study classifies security technology of IoT into four categories: device, network, service / platform, data / privacy, and examines security technology.

① Device security

Device security technologies include authentication / identification, access control, OS security, and lightweight crypto / security protocol technologies. The most basic authentication / identification methods use ID / PW-based, PKI, SIM, and Biometric-based technologies. Their commonality is that they must keep separate keys or cards needed for authentication, and their security is vulnerable to SW threats. The result is a security chipset, which allows hackers to be highly secure against attacks, minimizing device degradation and battery consumption [9].

Looking at the trend of domestic and international research on device security, D.I.Y security devices are being developed in foreign countries, and researches on hardware security, security OS, and device security are being conducted in Korea [10].

② Network security

Commonly used network technologies include Wi-Fi, Radio Frequency Identification (RFID), Zigbee, Bluetooth, and CoAP. Their commonality is the use of wireless networks [9]. Therefore, threats to external communication exist. Accordingly, researches are being conducted mainly on wireless and mobile devices in foreign countries, and researches are focused on hyper-connection security, security management, and intrusion surveillance [10].

③ Service / Platform Security

Since the IoT provides new services through convergence technology, various security techniques such as authentication / authorization, access control / authorization control, etc. are required [9]. The security of service / platform is classified into two categories, password and authentication / authorization. Researches conducted from abroad first discuss low-power / lightweight password, hash, and key management technologies. For example, authentication / authorization focuses on lightweight user authentication protocols and device-to-device authentication technologies, and cryptography research in Korea is similar to that of overseas research. However, research on T2T technology is also underway [10].

④ Data / Privacy Security

An attacker can attack by simply intercepting and forging data and passing the authentication procedure. As such, security of data and privacy is essential in the Internet of Things. In particular, the need for enhanced security against privacy invasion is highlighted because personal information is likely to be leaked [9].

However, the IoT is not easy to solve security and privacy breaches because of the various actors involved [11]. In this regard, both domestic and international progress is underway. At the Twente University in the Netherlands, the QoC-Aware Privacy Policy framework technology was researched in 2008. A study was made [10].

b. IoT Security Policy

In order to grow and spread the IoT market, the Korean government formed an Information and Communication Strategy Committee to resolve regulations against the market [11]. He began to show a positive attitude. In 2015, the three-year plan established the Internet of Things (IoT) Information Security Roadmap, enabling the IoT to be used safely and conveniently [9].

However, current norms of IoT privacy still have limitations, and there is a need to present norms considering IoT for reliability and safety of IoT use [12]. Details of each countermeasure are shown in Table 4.

Table 4. Policies for Internet of Things Security

Division	Contents
National Cyber Security Measures	① Cyber threat information sharing system ② Expand key information and communication infrastructures, including integrated information and communication facilities (IDCs) and medical institutions, and operate national infrastructures separately from the Internet network and conduct crisis response training. ③ Promote various manpower training programs such as expanding the training of the best information security experts and establishing the gifted education center.
Internet of Things (IoT) Security Roadmap	① IoT product and service design considering information protection and privacy ② Application and verification of safe software and hardware development technology ③ Provide safe initial security setting ④ Security protocol compliance and safe parameter setting ⑤ Continue to implement vulnerability patches and updates for IoT products and services ⑥ Establish information protection and privacy management system for safe operation and management ⑦ Plan to secure IoT infringement incident response system and traceability
Current Code of IoT Privacy	Current Code: According to the Personal Information Protection Act Limitations: The question arises whether the owner or user of an IoT device should be a personal information processor, the limitation of consent-based application principle, the notification and consent of Article 17 (3) of the Personal Information Protection Act, Article 26 (Article 26) of the Cloud Computing Act There is a validity for the request for notification of storage country in paragraph 1.

III. CONCLUSION

As the Fourth Industrial Revolution began, network-based technology is developing. Detailed technologies are also developing accordingly, and the Internet of Things will converge to provide services.

Therefore, in this study, I looked into the definition of Internet of Things and security threats and also examined the security technology and policy contents. The most important issue for security was security technology and policy on the threat of personal information leakage, and it was found that each country is aware of its importance and is making efforts to research and prepare policies. However, with the introduction of 5G, new security issues also began to emerge.

This is why we are not aware of the importance of security despite the ongoing development of security technology. This can have a negative impact on the growth of the IoT industry, so a new perspective should be taken to address security issues [9]. In particular, since security issues for privacy have many limitations due to the current law, it is necessary to expand the scope to include security issues of IoT through the revision of current laws. For example, by adding the contents of the person who owns the IoT device even if it is not intended for work, the personal information processor that is the subject of the Personal Information Protection Act can protect the personal information of the users who use the IoT.

As technology continues to evolve, new security issues will continue to emerge. In light of these issues, research on security should be continued in the future, and the government should spare no efforts to secure policies and support for corporate growth and market growth.

ACKNOWLEDGMENT

This research is supported by 2020 Baekseok University Research Fund.

REFERENCES

[1] Hong, S. (2017). Secure and light IoT protocol (SLIP) for anti-hacking. Journal of Computer Virology and Hacking Techniques, 13(4), 241–247. doi: 10.1007/s11416-017-0295-5

[2] S. W. Heo, H. W. Kim (2017). An Analysis of IoT Security Requirements And oneM2M. Communications of the Korean Institute of Information Scientists and Engineer, 35(1), 16-22

[3] Hong, S. (2017). Research on IoT International Strategic Standard Model. Journal of the Korea Convergence Society, 8(2), 21–26. doi: 10.15207/jkcs.2017.8.2.021

[4] S. Y. Kim (2015). Cyber Physical System Security Technology Trends in the Internet of Things Era. Magazine of the IEEK, 42(8), 16-25

[5] J. Y. Lee, B. G. Kim, S. K. Park, J. W. Jang (2014). Encryption of Routing Path for Internet of Things. Journal of the Geological Society of Korea. Type: Academic journal, 730-732
[6] H. W. Kim (2014). Security Issues in IoT Services. Communications of the Korean Institute of Information Scientists and Engineer, 32(6), 37-41
[7] Hong, S. (2019). P2P networking based internet of things (IoT) sensor node authentication by Blockchain. Peer-to-Peer Networking and Applications. doi: 10.1007/s12083-019-00739-x
[8] S. T. Bae, J. K. Kim (2016) Paradigm Shift in the Development of the Internet of Things and Security, 14. 44-57
[9] J. N. Kim, S. H. Jin (2017). Research on Internet of Things (IoT) security technology for coping with security threats in hyper-connected environments. Korean Institute of Communication Sciences), 34(3), 57-64
[10] H. J. Lee, K. G. Kim (2015). Domestic and foreign market and policy trends of the Internet of Things. Information Communication Technology Promotion Center.
[11] B. C. Oh (2016). IoTA Study on Privacy Protection in the Environment. NAVER Privacy White Paper
[12] Key Policy Insights. (2020). doi: 10.1787/df3aed65-en