Journal of Digital Convergence
Vol. 17. No. 11, pp. 195-200, 2019

ISSN 1738-1916
https://doi.org/10.14400/JDC.2019.17.11.195

IoT Environment and Security Countermeasures in 4th Industrial Revolution

Sunghyuck Hong
Baekseok University, Divison of ICT, Information Security Major, Associate Professor

4차 산업혁명 시대의 사물인터넷 현황 및 보안 대응책

홍성혁
백석대학교 ICT학부 정보보호전공 부교수

Abstract The role of the Internet of Things in the Fourth Industrial Revolution is in the era of collecting data at the end and analyzing big data through technology to analyze the future or behavior. Therefore, due to the nature of the IoT, it is vulnerable to security and requires a lightweight security protocol. The spread of things Internet technology is changing our lives a lot. IT companies all over the world are already focusing on products and services based on things Internet, and they are going to the era of all things internet that can communicate not only with electronic devices but also with common objects. People, people, people and objects, things and things interact without limitation of time and space, collecting, analyzing and applying information. Life becomes more and more smart, but on the other hand, the possibility of leakage of personal information becomes greater. Therefore, this study proposed security threats that threaten the protection of personal information and countermeasures, and suggested countermeasures for building a secure IoT environment suitable for the Fourth Industrial Revolution.

Key Words : IoT(Internet of Things), IoE(Internet of Everything), Big Data, Hacking, Personal information protect

요 약 4차 산업혁명시대에 사물인터넷의 역할은 엔드단에서 데이터를 수집하여 빅데이터를 기술을 통하여 분석하여 미래나 행동을 분석하는 시대에 있다. 따라서 사물인터넷의 특성상 보안에 취약하여 경량화된 보안 프로토콜이 필요한 실정이다. 또한 사물인터넷의 보급은 우리 생활을 많이 변화시키고 있다. 전 세계 IT 기업들은 이미 사물인터넷 기반의 제품과 서비스에 주력하고 있으며 전자기기를 통한 통신 뿐 아니라 일반 사물과의 통신이 가능한 만물인터넷 시대로 가고 있다. 사람과 사람, 사람과 사물, 사물과 사물이 시간과 공간의 제약을 받지 않고 상호작용하면서 정보를 수집하고 분석해서 적용하고 있다. 생활은 점점 스마트해 지지만 이에 반해 개인정보 유출의 가능성은 더욱 커져서 이를 악용할 경우 사생활 침해를 넘어 생명을 위협하는 경우도 생길 것이다. 따라서 본 연구에서는 개인정보 보호를 위협하는 보안 위협과 이에 대응하는 방안을 제안하여 4차산업혁명시대에 걸맞는 안전한 사물인터넷 환경을 구축하는데 필요한 대응책을 제시하였다.

주제어 : 사물인터넷, 만물인터넷, 빅데이터, 해킹, 개인정보 보호

*This paper was supported by 2019 Baekseok University Research Fund.
*Corresponding Author : Sunghyuck Hong(sunghyuck.hong@gmail.com)
Received August 12, 2019 Revised September 16, 2019
Accepted November 20, 2019 Published November 28, 2019

1. Introduction

If IBM and Xerox simply manufactured and sold a PC based on a microprocessor, HP, Dell and Verizon made wireless communication technology available for a variety of services and online transactions. Since 2010, the era of the Fourth Industrial Revolution, products that combine tangible and intangible services have emerged, and APPLE and Google are the leaders [1]. In line with these trends, online-based communities such as facebook and instagram became active, and virtual banks such as Cacao Pay and Google Pay appeared. The Internet of Things (IoT), which connects people with things and objects through communication with people, is a time when the world of things becomes reality, which can seriously affect our lives and threaten our safety. I do not know. With the development of IoT, the importance of security has been emphasized as a result of hacking and infiltration of information leakage [2]. This research paper is organized as follows. In Chapter 2, IoT definition, market status of IoT industry and various use cases are examined. In Chapter 3, IoT security threats and security measures are constructed. Finally, Section 4 describes the conclusions of this study report.

2. IoT

2.1 What is IoT?

IoT is an abbreviation of Internet of Things, which means connecting all things through the Internet. IoT technology together with AI and Big Data are key technologies leading the fourth industrial revolution era. Not only do people interact with devices or objects over the Internet, but they also involve the generation, collection, sharing and utilization of data [3]. Once the information using the sensor is generated, it can be called technologies and services including the ability to collect the generated information using various devices and share it in the cloud environment to reproduce large data and various hardware and software. Unlike traditional M2M machines that collect information and process information through human commands, IoT allows objects to collect, process, share, and interact with information on their own.

The IoT industry, which was limited to the B2C market such as consumer-oriented Internet shopping malls, is being actively promoted as B2B e-commerce, and it must cope with and cope with these changes. In addition, IoT connected objects must have IPs that are identifiable and all objects can be hacked, so security technology should be developed along with the development of IoT.

2.2 Phase of IoT development

IBM has identified three stages of IoT development [4].

Step 1 is a level of device connection, which is a level that connects data to the Internet and inquires collected data in real time. Phase 2 is the stage of infrastructure construction, which allows objects to be connected to other objects by sensing the surrounding environment. This is an exponential increase in the number of devices connected to the Internet, a big data platform for collecting and analyzing large amounts of data. Predictive analysis through the use of a variety of infrastructure technologies. The last three stages are the stages of developing innovative solutions for each industry, creating solutions for innovation in each industry by utilizing the ability of automatic execution of objects and inter-connectivity. During this period, services can be implemented in a wider area, including automotive, transportation, smart home, healthcare, energy, utilities, security, finance and manufacturing.

2.3 IoT core technology

IoT core-based technologies include sensing, networking, interfaces, and low-power networking.

2.3.1 Sensing technology

Intelligent sensor technology such as MEMS sensor, NANO sensor and System on Chip is utilized as a function to remotely detect using sensors such as temperature, humidity, heat, gas, and illumination, and to collect information by tracking position and movement.

2.3.2 Networking technology

It uses 4G, WiFi, Bluetooth, satellite, etc. as a function to connect environmental elements such as human, object, and service, and 5G service is started.

2.3.3 Interface technology

IoT is a technology that connects services that perform certain functions with the capability of IoT, such as detection information based technology, location information based technology, and web service technology that detect, process and process information.

2.3.4 Low Power Networking Technology

The power consumption of the terminal increases for frequent data transmission by connecting a large number of terminals, so it is important to efficiently transmit data with low power.

2.4 IoT Market Status

As the IoT industry got into full swing, our life became smarter. The word "smart" is connected to almost every product, and things that I imagined in science fiction movies or movies that portray the future of decades later are becoming reality. In fact, new products and services such as smart cars, smart homes and smart grids continue to evolve.

The number of devices connecting IoT is exploding and consumers are expected to use more than half of IoT devices. Just as we do not feel that there is air, our lives are all connected and we will not need to recognize the Internet. According to Cisco forecasts, in 2030, more than 50 billion objects will be connected to the Internet through the Internet of Everything (IoE) era, or the Internet age [4]. This view is only a shame, and given the current pace of growth, the times when all things and people are connected and communicated will come sooner than predicted.

2.5 Examples of using IoT

The various fields of application of IoT are as follows.

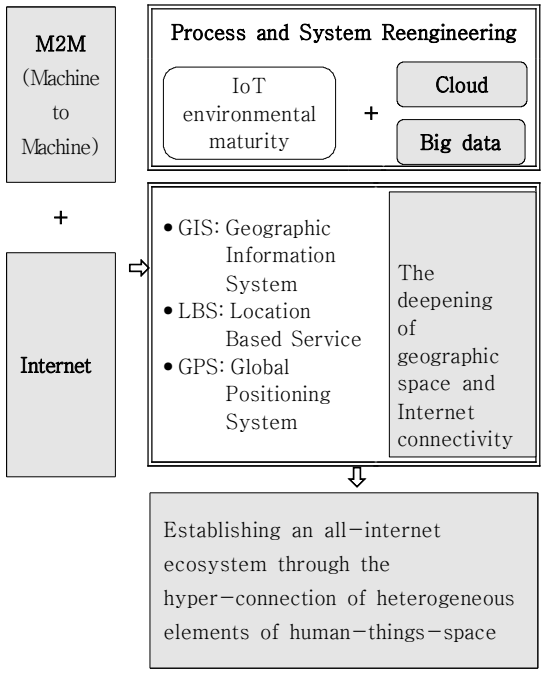

Fig. 1. IoE : Internet of Everything

Table 1. IoT Application fields

Field	Application example
Medical	U-health, Telemedicine
Car	Unmanned vehicle, Remote control
Logistics	RTLS, Smartrucking

Public protection	CCTV Security, Disaster management
Environment	Weather forecasting, Environmental monitoring
Office	Smart Office, U-Work
Home Appliances	Smart Home, Remote meter reading system

2.5.1 Utilization of health sector

The doctor monitors the patient through the monitor, uses the collected data, diagnoses and treats it, and operates the robot while operating the robot while watching the monitor, which is difficult for the doctor to visually check in the operating room. By using sensors that detect light, temperature, humidity, vibration, etc., it is possible to control the state of the refrigerator that stores the vaccine or medicine and keep it in the optimal condition. It is possible to have a system that allows the situation to be immediately acknowledged.

n the future, smart devices equipped with various sensors will collect not only respiration, pulse, body temperature, sleep, but also various metabolism of the body. By analyzing and collecting the data of patients collected by using big data of objects, Exercise, diet, medication and prescription system will be introduced. Recently, an MOU has been signed with the fire department, community security council, and local medical institutions in Jincheon-gun, Chungcheongbuk-do, and an IoT sensor is installed in a residential area such as severely handicapped people and elderly people to detect biological information such as breathing, heartbeat, The 'One-person Safe Care Monitoring' project is being implemented [5] to allow managers to immediately inform the manager through the control cloud [6].

2.5.2 Connected car

It means a car that can be operated safely and comfortably by connecting the information and communication technology to the car to enable two-way internet and mobile service. It can be connected remotely by connecting to a smart phone, turning on a heater or air conditioner, and allowing the driver to receive information such as weather, news, and traffic conditions in real time. In addition, various contents such as video and music can be used in real time, navigation can be operated by searching for location information by voice, and dialing is possible [7]. Autonomous parking and autonomous freeways have become possible. In the future, if you call a car like in a movie, you will be able to drive yourself from the parking lot to the driver 's place, or to detect the danger yourself and inform the driver.

2.5.3 Unattended Store

Amazon, the largest e-commerce company in the United States, operates unmanned convenience stores and is testing a technology for realizing unattended stores without cash registers and cashiers by installing thousands of cameras and sensors in large offline stores. The introduction of unattended stores minimizes the expense of labor costs and allows consumers to receive better quality goods at lower prices. Thousands of sensors detect the weight of a selected food and send it to the customer's account linked to the automatic calculation system [8].

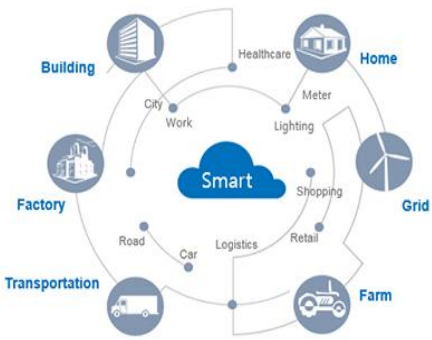

Fig. 2. IoT Application fields

3. IoT security threats and security measures

3.1 IoT Security Threat

As the IoT industry develops, security and privacy infringement are the issues that must be overcome. The vulnerability of security in the transportation and medical field is a more important issue because it may lead to a life threat. Most of the IoT devices are transmitted using a web interface that does not encrypt the information gathered by security. Therefore, not only professionals but also general people are very concerned about the risk of information disclosure. The most serious problem as well as the possibility of hacking the smart home system to steal the house entirely, or to hack the smart key of the car to manipulate the steering wheel or brakes, is the most serious problem. Recently, Google Plus has shut down its personal information leak service. [9] Shodan's search engine is being threatened by security as a hacker's playground and should pay more attention to its countermeasures.

Table 2. IoT security threat

division	threat situation
Platform	Vulnerabilities in Public Platform traceability of information
Network	interconnection Network Vulnerability Network Traffic Attack
Device	Hacking low-spec devices Management Vulnerabilities

3.2 IoT Security Infringement Cases

3.2.1 Hacking the gas station pump

You can hack the password associated with the Internet to manipulate the pump at will and change the price, or you can skip the customer card information of the loaned customer. The pressure and temperature of the pump can also be controlled, which can lead to an explosion [10,11].

3.3 IoT Security Measures

IoT is a fusion of various factors. In addition to the vulnerability of each element, there is a new vulnerability that occurs due to convergence. These IoT products need to be concerned with security from the manufacturing process. Consumers should also use genuine safety-certified products and care about security. Also, in order to identify the secure data when communicating with the device, an authentication method using Public Key Infrastructure (PKI) is introduced in addition to ID and PW. It is a relatively secure method of security, though it is a hassle to manage the certificate separately.

Wi-Fi, which is most commonly used, is a security weakness as it is a wireless communication. In order to secure the data, it is possible to prevent hacking if the authentication procedure is used to access the network using WEP (Wired Equivalent Privacy) and WPA (Wi-Fi Protected Access). IoT service In the Iot-A project, AuthZ (Authorization) component is responsible for introducing a system that grants access rights through authentication process [12]. Since IoT is a system in which people and objects exchange data, there is a possibility that personal information should be input in the course of authentication, which may lead to leakage. Therefore, we use Privacy Preserving Data Mining to transform and distribute collected data.

To maintain security while using IoT-related services, you must use secure hardware and software that is secure, reset the initial password, and update the security patches constantly. There is also a need for strong legislation against hackers at the national level [13-15].

4. Conclusion and Discussion

Examples of the problems of the Internet of Things are as follows. Suppose a worm crawls

into a temperature and humidity sensor installed on a farm. The temperature and humidity information sent to the farmer is then the body temperature and humidity of the worm. That does not help farming. Bad data can also be generated if dust or factory contaminants cover the sensor or if someone damages the sensor.

There are also IoT devices that generate bad data or stop reporting data due to malfunctions. In many cases, human error is the cause. Incorrect settings can cause the device to generate incorrect data. One way to reduce this bad data is to set up and configure the device correctly. As the computer network developed, the IoT industry also developed and our lives got smarter. It is possible to enjoy a convenient life at a small cost with the technology of analyzing and applying a lot of collected big data by oneself, but the infringement of privacy is serious because of leakage of personal information. It is also important to internalize security during the IoT infrastructure creation phase. However, users themselves need software updates and ongoing PW management. Above all else, the infringement of the personal privacy of others is a very serious crime, and it is necessary to have an ethical consciousness that should be kept on the basis of mutual trust.

REFERENCES

[1] G. Kortuem & F. Kawsar. (2010). Market-based user innovation in the Internet of Things. *2010 Internet of Things (IOT).* DOI:10.1109/iot.2010.5678434

[2] B. Haughian. (2018). IoT Industries. Design, *Launch, and Scale IoT Services, 163-183.* DOI:10.1007/978-1-4842-3712-0_8

[3] Y. S. Jeong. (2019). An Efficient Personal Information Collection Model Design Using In-Hospital IoT System. *Journal of Convergence for Information Technology, 9(3),* 140-145.

[4] B. Haughian. (2018). The Current and Future Status of the IoT. Design, *Launch, and Scale IoT Services, 193-202.* DOI:10.1007/978-1-4842-3712-0_10

[5] Infinity Acute Care System Monitoring Solution. (2012). *Biomedical Safety & Standards, 42(2),* 9-10. DOI:10.1097/01.bmsas.0000411012.71323.29

[6] Y. S. Jeong. (2019). Efficient Patient Information Transmission and Receiving Scheme Using Cloud Hospital IoT System. *Journal of Convergence for Information Technology, 9(4),* 1-7.

[7] *North American Economic Integration: Trial by Fire.* (n.d.). North American Economic Integration. DOI:10.4337/9781840647693.00020

[8] M. Hirota, H. Mizuochi & S. Kakegawa. (2006). A Demonstrational Test of Pressurization Smoke Control System at A Large-scale Shopping Store. *Fire Science and Technology, 25(3),* 213-237. DOI:10.3210/fst.25.213

[9] Unintentional and Involuntary Personal Information Leakage on Facebook from User Interactions. (2016). *KSII Transactions on Internet and Information Systems, 10(8).* DOI:10.3837/tiis.2016.07.024

[10] *Netherlands Antilles - Cybercrime, Data Protection, Information & Internet.* (n.d.). Foreign Law Guide. DOI:10.1163/2213-2996_flg_com_141095

[11] H. M. Jung, K. M. Jeong & H. J. Cho. (2017). A Design for Security Functional Requirements of IoT Middleware System. *Journal of the Korea Convergence Society, 8(11),* 63-69.

[12] J. S. Lee. (2018). A Study of protective measures of the source program for the development of the Internet of Things (IoT) : Protection of the program as well as plagiarism research. *Journal of the Korea Convergence Society, 9(4),* 31-45.

[13] M. J. Lee. (2015). A Study on IoT Service for Game Development. Journal of Digital Convergence ,13(2), 291-297.

[14] C. D. Lee. (2017). An Adaptive Traffic Interference Control System for Wireless Home IoT services. *Journal of Digital Convergence, 15(4),* 259-266

[15] C. W. Park & J. W. Kim. (2016). An Empirical Research on Information Privacy Concern in the IoT Era. *Journal of Digital Convergence, 14(2),* 65-72.

홍 성 혁(Hong, Sunghyuck) [정회원]

- 2007년 8월 : Texas Tech University, Computer Science (공학박사)
- 2012년 3월 ~ 현재 : 백석대학교 ICT학부 부교수
- 관심분야 : 블록체인, 사물인터넷 보안, 경량보안프로토콜
- E-Mail : sunghyuck.hong@gmail.com