Enhancement of Security Monitoring Model for a Safe Internet of Things (IoT) Environment*

WonHyung Park[1], Gwanghyun Ahn[2], Jin-won Kim[3], Jang-Mook Kang[3], and Young-joon Lee[3†]

[1]Department of Information Protection Engineering, Sangmyung University, Cheonan, South Korea
whpark@smu.ac.kr

[2]Department of Computer Engineering, Sejong University, Seoul, South Korea
rhkdgus8781@sju.ac.kr

[3]Department of A.I. Security, FarEast University, South Korea
frkjw15@gmail.com, {2021035, 2020032}@kdu.ac.kr

Received: December 29, 2021; Accepted: March 14, 2022; Published: April 17, 2022

Abstract

Recently, hacking accidents and Distributed Denial of Service (DDoS) attacks are increasing in the Internet of Things(IoT) environment, and various cyber threats are increasing. In particular, threats from various services such as webcams and telemedicine provided by mobile communication operators such as LGU+ and KT olleh through IoT services are increasing in korea, so it is necessary to strengthen the security control system for a safe Internet of Things environment. In this paper, IoT technology, security incident trends, and standardization of the IoT were collected and analyzed. Through this, we propose a security control model that is strengthened in the analyzed IoT environment. Through the proposed security control model, it is divided into 'pre-response-incident response-post-response', and the IoT environment is classified into IoT devices, IoT networks/communications, and IoT services/platforms according to strategic directions. It is hoped that this paper will contribute to the rapid detection and response of new cyber threats and attacks.

Keywords: IoT, Cyber Threat, Security Platforms, Integrated Security Control

1 Introduction

Cybercrime has evolved at a rapid pace and is likely to become more serious in the future. Kevin Mitnick, a hacker who began to uncover loopholes in Windows servers and other platforms in the 1990's purely for pranks, was soon imprisoned for five years, inflicting millions of dollars in malicious damage. Since then, cybersecurity awareness has grown, and the antivirus industry has grown into a multi-million dollar industry. Later came the so-called script kiddie, rudimentary hackers who use malicious code

Research Briefs on Information & Communication Technology Evolution (ReBICTE), Vol. 8, Article No. 2 (April 17, 2022)
DOI:*10.22667/ReBiCTE.2022.04.17.002*

*This paper has been revised and expanded from "A Study on the Next Generation Security Control Model for Cyber Threat Detection in the Internet of Things (IoT) Environment" [1] that was presented at the 21st ACIS International Winter Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, (SNPD-Winter'21) in January 2021 (DOI: 10.1109/SNPDWinter52325.2021.00053). Compared to [1], this paper not only deals with ITU-T IoT international standardization technology and security matters for cloud environment, but also describes based on the US NIST SP 800-61 document that the IoT security control system can be systematically enhanced using the NCISS of the National Security Communication Information Center (NCCIC) under the US Department of Homeland Security (DHS).

†Corresponding author: 6-32, Daehak-gil, Gamgok-myeon, Eumseong-gun, Chungcheongbuk-do, South Korea, Tel: +82-(0)43-880-3875

written by others to do damage, mainly because they want to look good. But unfortunately, it didn't stop there. In the 21st century, a tremendous transformation has taken place. Accidental hacking has developed into a full-fledged cybercrime. According to Verizon's 2018 Data Breach Investigation Report1, organized criminals accounted for half of all data breaches in the past year, and most of them belonged to organized criminal groups. According to the report, 76% of data breaches were for financial gain, and these criminal activities include stealing intellectual property, embezzling cash, extorting cryptocurrencies such as Bitcoin, or encrypting organizational data to attack This can take a variety of forms, including making the data unusable by the target organization or individual and then demanding monetary compensation in return for its use. The cost of cybercrime has increased significantly. The Center for Strategic and International Studies (CSIS) recently estimated that the cost of cybercrime worldwide in 2017 was between $450 billion and $608 billion, an increase of more than $100 million from the lowest estimate in 2014 [2]. IoT (Internet of Things) refers to the formation of an intelligent relationship through sensing, net working, and service information processing through mutual cooperation without artificial intervention between human and object components, and the connection of object configuration spaces, In the IoT era, most devices It is expected that new products and services will emerge based on the self-information and network connection function. One of the big challenges for the introduction of IoT is security-related issues, and the connection of the Internet to most things that exist everywhere requires the steps of generating, collecting and distributing a large amount of information, and managing and utilizing it. The system faces two classes of risks: a significant threat to public safety and a privacy breach. It is the time when IoT security control is needed to reinforce such IoT security. Until now, the term "security control" has not been defined as a legal regulation, but in recent years, it is an early stage in which the concept definition has begun. Security control is used as 'Security Monitoring & Control' in English. In the dictionary definition of Monitoring, it is described as monitoring activities to prepare for various possible errors during the performance of a computer program'. In the Korean dictionary, 'control' is defined as 'forced management and control required by the state, airport, etc.' In addition, cyber attack techniques through malicious code production and distribution are changing and developing rapidly, and it is difficult to completely detect and block new cyber attacks at the current level of security system because it utilizes more advanced and intelligent methods such as applying double cryptography techniques that are not easily detected by security control and vaccine. Especially, in IoT environment where all objects are connected to the network, it is necessary to prepare more than security control strategy through existing pattern matching or simple inspection, and it is time to implement security control through advanced strategy.

2 Related Work

2.1 Service using IoT

LG U+ Physical Security: LG U+'s LTE national network and M2M technology combined with physical security are expected to be a chance to advance security services and M2M technology based in Korea such as ADT Caps by one step, and plans to expand its market dominance by developing video control technologies that are used with vast amounts of data in the future.

Safe Home: KT's Safe Home Zone detects an emergency situation occurring in the home of the elderly and provides prompt action, emergency caregiver service, and a service that enables simple health check through a communication module in a portable urine analyzer. It presented an IoT technology model for an aging society.

Global Logistics Security M2M Module: It can effectively deal with the 2014 Port Security Act in-

troduced in the United States. The law mandates the installation of security equipment in all containers brought into the U.S. after the Sept. 11 terrorist attacks. It is a security control solution that allows container tracking, and all cargo in use can be passed without inspection, enabling quick clearance procedures. KT is currently providing services that can check container information (temperature, humidity, shock, and seal) and location through telecommunication modules.

2.2 IoT Security Threat

Telemedicine Services Vulnerabilities: The scale is connected to online, and it is showing examples of product development service of Internet of things through various analysis reports, services, and mutual linkage. Weight data, which users agree and want to measure directly, is sent to the service provider's server, that is, to the cloud, and users can typically check the results by running the app through their smartphone terminals. This flow of weight data seems simple with services, but personal weight data can be used for many different types of services. For example, a weight scale that can be connected to a specific Internet of Things can share measured personal weight data on SNS according to personal consent and choice. However, personal weight data stored through service providers can be used for malicious purposes, and it is also possible for service providers to analyze and process their profits and convert them into useful information with high value added in the company. In any case, since the data is used contrary to the intention of the original data owner (user), serious privacy invasion occurs [3]. Figure 1 is a schematic diagram of the usage status of major security products.

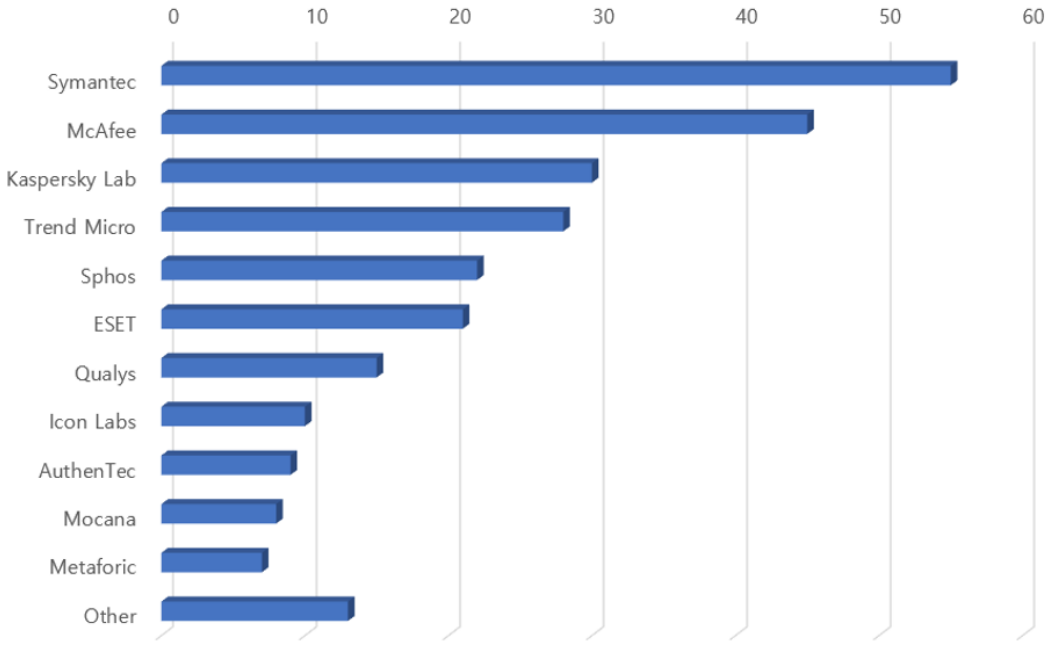

Figure 1: Security Product Usage Status

Wireless sharing device vulnerability: Recently, it has emerged as a serious part of the security problem of wireless sharing devices. Unlike PCs that could be supplemented with security patches and vaccines that correct security vulnerabilities, sharing device have no clear countermeasures and are clearly exposed to cyber attacks. Cyber attacks via wireless sharing devices have soared [4]. Recently, there have been cases where hackers impersonate major carriers' Wi-Fi networks to create wireless networks and steal personal information. When the hacker creates a fake SSID that is the same as the Wi-Fi network

installed by the mobile operator using a wireless router, Users may inadvertently try to access public Wi-Fi that lacks security settings such as “T wifi zone” and “ollehWifi”, and then personally owned data stored on laptops and smartphones may be stolen.

2.3 IoT Security Technology Requirements

Customized device security technology: There is a need for customized device security technology for each loT device with different types of performance such as drones and sensors [5]. Figure 2 is a schematic diagram of the structure in which the web cloud and IoT are connected.

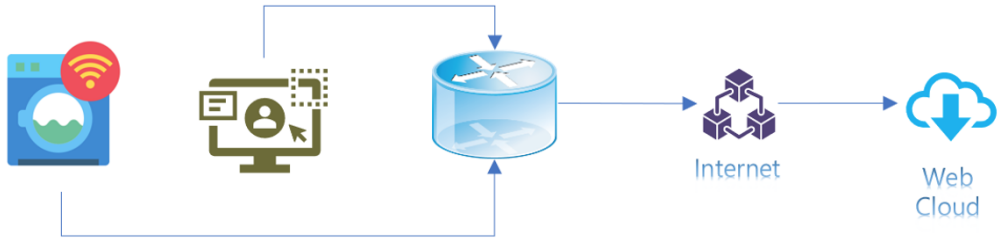

Figure 2: IoT Web Cloud

IoT devices that have strong restrictions on the performance of the central processor, the size of memory, and power consumption cannot use the previously used encryption technology, so a lightweight and low-power encryption technology is required that considers the device performance and security level. It is also necessary to prevent modulation of the operating system by malicious code infection and external hacking, and to prevent the device from being stopped or malfunctioned. There is also a need for hardware security technology to prevent illegal copies due to theft of IoT devices, leakage of important data through theft or hacking. IoT network security: Network security technology is needed to detect and block hacking and malicious code attacks targeting IoT networks where heterogeneous devices are interconnected. Figure 3 is a diagram of a security control system on an IoT device.

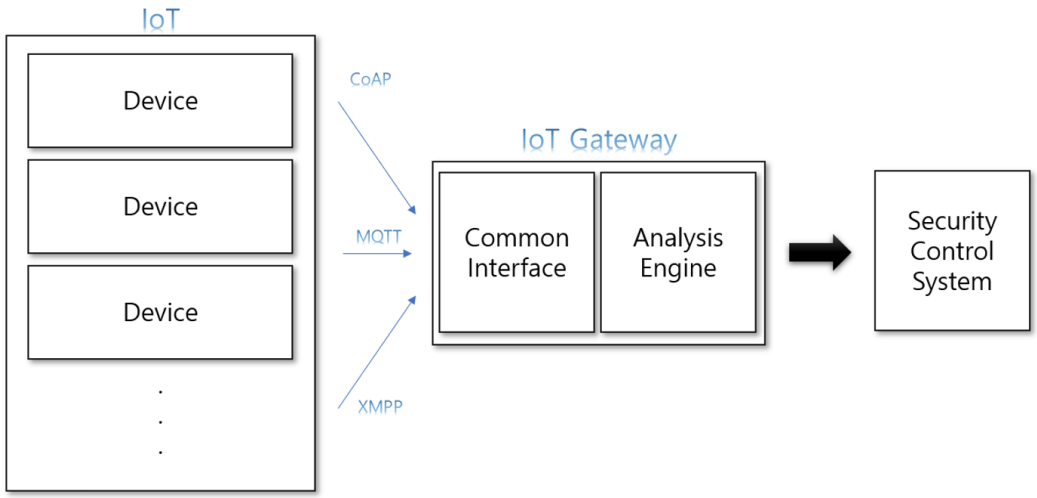

Figure 3: IoT Interface

In order to perform different functions based on networks where different devices such as communication methods (Bluetooth, WiFi, ZigBee, etc.) and security characteristics (certification methods, password types, etc.) are interconnected through sensors, authentication between terminals is required for integrated networking between IoT devices. Devices connected to IoT network should be able to detect and respond to hacking attacks in the IoT service environment, which consists of gateways with different security functions. Monitoring and management technology of the network is needed to prevent distributed denial-of-service attacks (DDoS) by object bots infected with malicious codes [6]. IoT Platform Security: IoT service also needs to provide mutual authentication and access control between components (services and devices, users), and privacy (data, location, ID) protection. Figure 4 shows the structural diagram of IoT integration platform implementation.

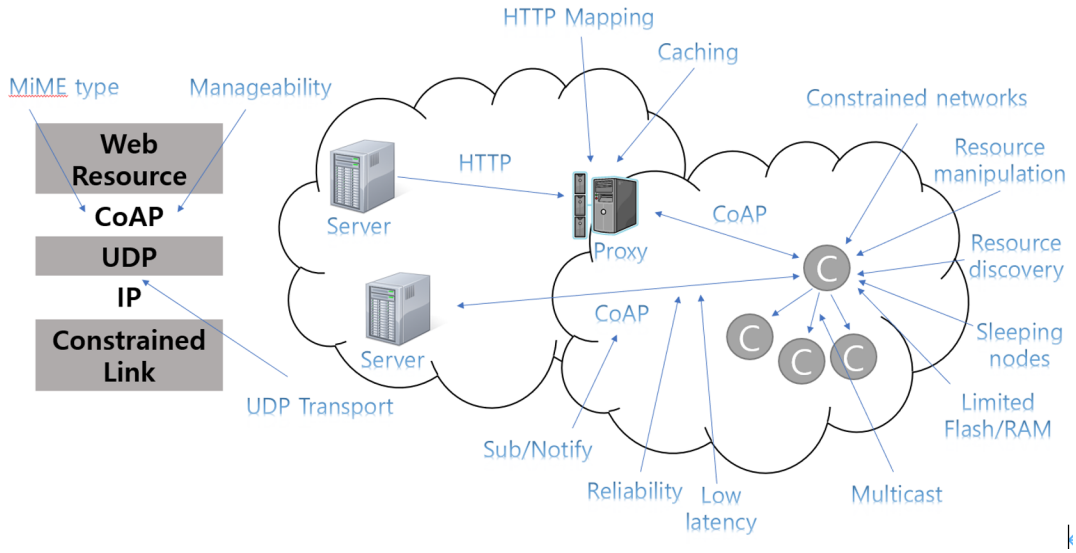

Figure 4: IoT Working Group

Services of camouflage and functional modulated objects also require inter-device authentication for unauthorized access blocking, key management and access control. There is a need for technology to prevent privacy violations (tracking and personal identification) caused by data collection and analysis in IoT environments [7]. IoT services require data and development of security platforms specialized for embedded, wearable, and mobile operating environments such as home/home appliances, medical care, and transportation. When multiple IoT services are mixed and operated (access to home, home appliances, and medical services from a car), an integrated platform that links common and specialized functions is required for cost efficiency [8].

3 Proposed IoT Security Monitoring & Control Plan

3.1 Components of the IoT Environment

In the process of establishing a security control strategy on IoT (Internet of Things), it is also necessary to understand the components of IoT environment due to the introduction of IoT devices. Since IoT environment is different from the security control environment that was limited to existing computers and mobile devices, it is necessary to summarize each component and the newly needed security requirements [9]. As shown in the figure data above, the IoT environment can be divided into three main components. First, let's look at the bottom of the picture data above. The bottom part is marked in red, and this

is the part about the IoT device. IoT device refers to equipment that adds a new function of Internet connection to ordinary home appliances or objects that were not previously connected to the Internet and the network [10]. That is why access should be made from a different perspective than computers, mobile devices, etc., which used to serve as traditional end nodes. Generally, IoT devices are difficult to apply uniform security solutions. The reason is that the roles of various appliances and other objects were different and the original purpose was not to connect to the Internet. Therefore, it is necessary to keep in mind that most of the heterogeneous devices are difficult to apply uniform security. Next, the parts marked in blue are the contents of IoT network and communication. In this network/communication field, the most important part is the standardization. Earlier, when briefly mentioned IoT device, he mentioned that IoT device is not standardized and that its operation, information processing.
Functions are all different. In this regard, assuming that there are several IoT devices connected to a network, it is difficult to secure reliability due to different communication methods and security structures for each IoT device and it is difficult to expect smooth security control. And another problem is that there is a concern that there is a risk of occurrence of a denial of service attack (DDoS, Distributed Denial of Service) using a thing bot. In the IoT environment, the number of devices connected to the network or the Internet rapidly increases. But if you look at this from a different perspective, it also means that the number of terminating nodes that can be used as zombie PCs in a typical DDoS is increasing. In this regard, it is also necessary to allow this point to be reflected in IoT security control in the future. Finally, the top part is about 'IoT Service/Platform'. This part is understood as the destination to transmit the information generated by IoT Device through the network [11]. Here, it is considered that it is the part that plays the role of brain of IoT as a part of processing the information collected by IoT Device and constructing data in the form of Database to analyze various Big Data. The characteristics of this part are that it does not support authentication/authorized user interworking between domains and that a high cost security service which is relatively difficult to use in low-end devices is mainly used.

3.2 Security Monitoring & Control Plan Considering IoT Environment

The scheme plots that basically constitute the security control strategy are not much different from the conventional security control strategy. The flow of security control strategies made up of proactive response-accident response-post response is similar, and the detection equipment used is similar to those used in traditional security control strategies. The reason for this is that the basic change in terms of security control strategy as IoT becomes more common is mostly the connected equipment at the end of the network. Therefore, for detection equipment that exists within the network, there is basically no need for much variation. Figure 5 shows the flow of the security monitoring center.
There is something to consider when there are more IoT devices connected to the network. The point is that it becomes difficult to collect and manage log information for each device in the central security control system. As the number of objects to supervise log information increases, the number of log records and detection information that occur increases, which results in the central security system being overloaded. Therefore, it is necessary to have an alternative to this environment, and the concept of IoT Gateway is the alternative to this. The reason why IoT gateway should be used is because the central security control system cannot supervise all IoT devices one by one, so it wants to combine several IoT devices into one internal network using a single IoT gateway. In this way, let's assume that four to five wired IoT devices are configured into one small LAN using one IoT gateway. At this time, by installing Network IDS (Network Intrusion Detection System) or Packet Filtering Firewall on the path leading to the IoT Gateway, packets flowing into 4 to 5 IoT devices connected to the internal network or from internal IoT devices Inspect outgoing packets. In addition, attempts to threaten security are blocked and related records are logged. In other words, four to five IoT devices that exist on the internal local area network (Local Area Network) based on the IoT gateway are all integrated into one by the

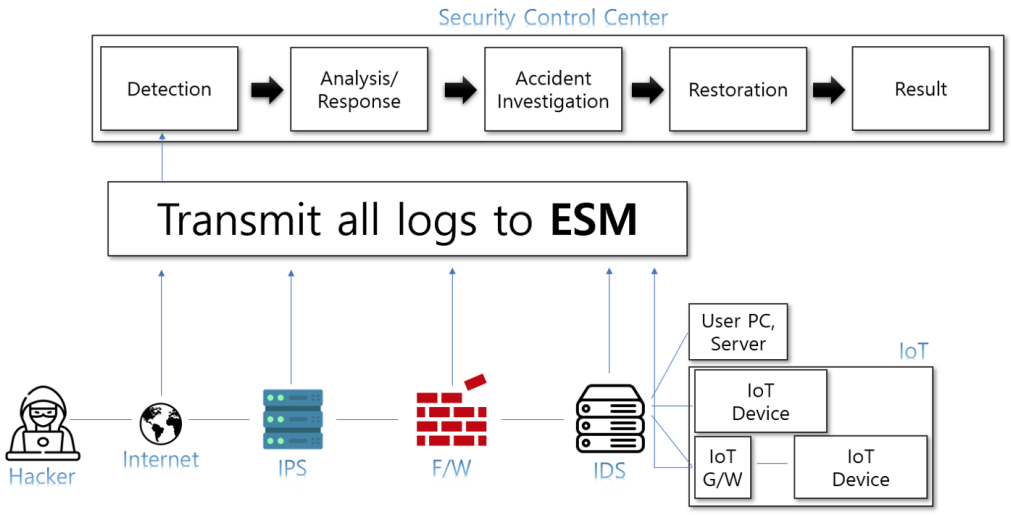

Figure 5: IoT Security Monitoring & Control Model

IoT gateway and become security control. In this case, the central security control system only needs to implement the security control strategy by accepting log packets and detection information from one IoT gateway without having to pay attention to each IoT device. This naturally reduces the load on the central security system as well. It presents a technical overview of the Internet of Things. A physical thing may be expressed in the information world through an association relationship with one or more related virtual things, and virtual things that do not have a relationship with a physical thing may also exist. Figure 6 shows the IoT ITU-T network between the physical world and the information world.

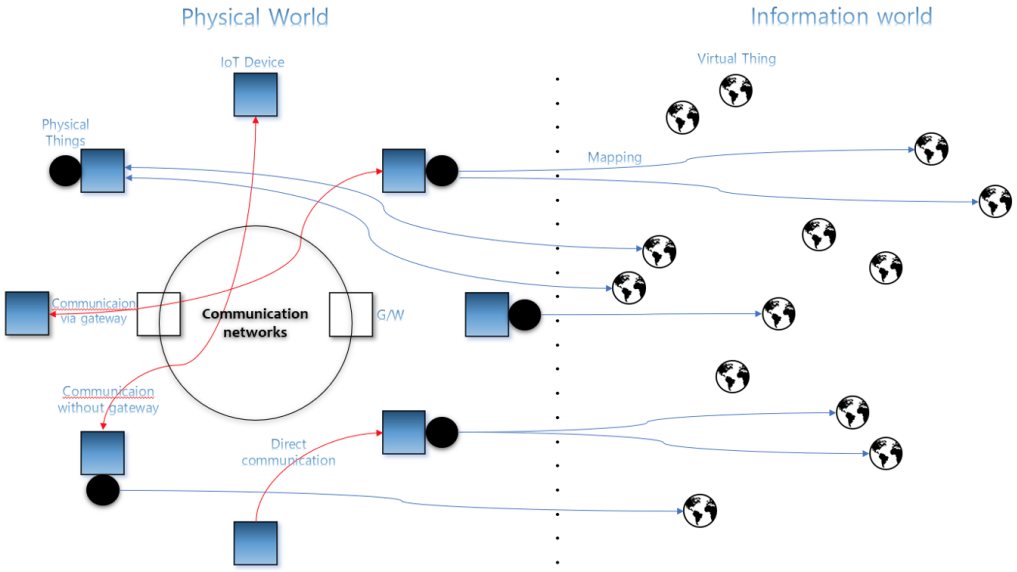

Figure 6: ITU-T Internet of Things Technology

The device of the IoT is a device having a communication function and may have sensing and driving, information acquisition, information storage, and processing functions. This device collects various information and transmits it to the communication network for further processing, and can execute com-

mands received from the communication network. It expresses only communication in the physical world, but communication between virtual objects in the information world and communication between physical objects and virtual objects are also possible. Figure7 shows IoT ITU-T layer systematized.

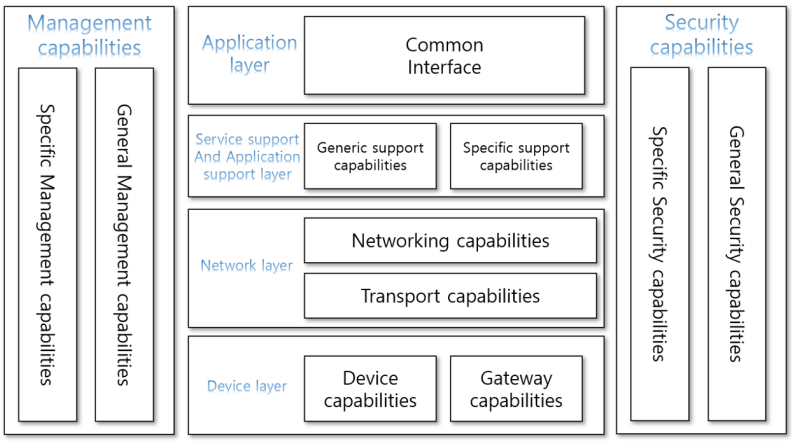

Figure 7: IoT Reference Model of ITU-T

JCA-IoT is in the process of coordinating IoT standardization activities not only within ITU-T but also other standards development: organizations (SDOs), and is preparing an IoT standardization roadmap for this purpose. In this roadmap, each standardization body Information on IoT-related standards that have been developed or are under development are included. IoT-GSI establishes and manages IoT-related standardization plans within ITU-T, and this standardization plan includes IoT-related standards that require future development. Information on standardization items is included. According to this standardization plan in IoT-GSI, 10 core working groups (Questions) such as Q2/13 and Q25/16 are in the process of developing IoT-related standards. Figure 8 is and 802.16-based M2M service diagram.

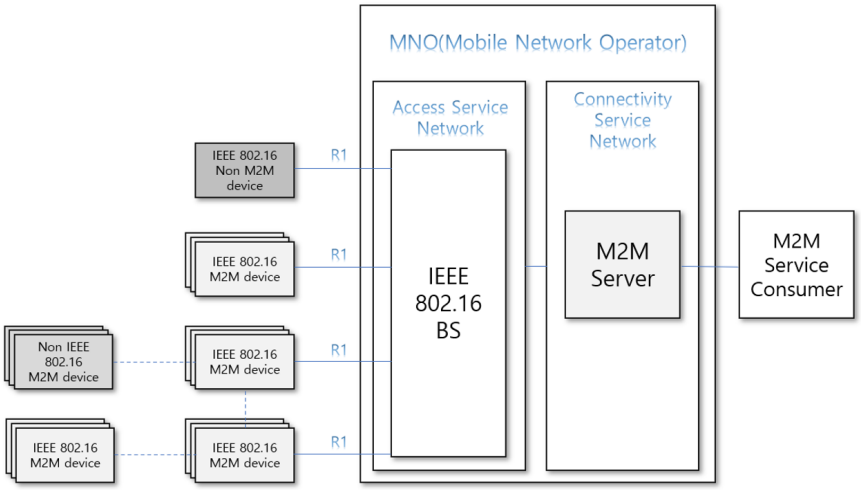

Figure 8: IEEE 802.16p Advanced M2M Service System Architecture

The IEEE 802.16 M2M task group, which developed a standard for Machine-to-Machine (M2M) communication that can be usefully used for communication of the Internet of Things, among various IoT-related standards within the IEEE, and the standards carried out by the group in a little more detail do. O

In IEEE 802.16, which is used as a standard for WiMAX technology, the 802.16p group is in charge of standards related to the Internet of Things. 802.16p is the M2M task group of 802.16, It was approved in January and until December 2012, activities were carried out to develop a wireless access standard to support M2M/IoT application applications in IEEE 802.16-based mobile communication systems.
In 802.16p, the requirements document for M2M application service support and standard specifications satisfying the requirements for M2M application service were developed. The standard developed in 802.16p supports low power of terminals, efficient control of a very large number of terminals, and efficient small size. It includes contents such as MAC improvement and OFDMA physical layer change for device data transmission support and improved device authentication support. IEEE-SA considered smart home & building, e-health, smart grid, next-generation manufacturing and smart city as emerging industries and smart applications, and saw the Internet of Things as a key factor for the success of these industries and services. Most of the IoT-related standardization activities currently in progress or in the past have produced limited standards limited to specific industries and services. do. Heterogeneous IoT structures and standards also cause problems such as overlapping development of the same function. IEEE-SA decided to standardize the Internet of Things reference structure model in order to prevent the fragmentation of the Internet of Things service and market, and eventually hindering the environment in which new industries of the future can be created flexibly. As a group, P2413 was approved in July 2014. The IoT reference structure standard to be developed in P2413 has the purpose of enhancing the interaction between the IoT cross-domains, enhancing the compatibility between systems and adaptability of functions, and thereby contributing to the revival of IoT-related industries and services. The scope of work of IEEE P2413 is to establish standards for the structural framework of the Internet of Things. The structural framework describes various IoT domains, defines the abstraction of IoT domains, and derives commonalities between different IoT domains. including contents such as The IoT architecture framework defined by IEEE deals with standards for the following details. Reference models (data abstraction, information protection, security, privacy, safety, basic structural building blocks and multi-tier systems) that define the relationships among various IoT verticals (transportation, healthcare, smart home, etc.) and common structural elements [12]. There are plans to strengthen cooperation with various IoT-related activities within and expand relationships with external standards organizations. In particular, it plans to strengthen cooperation with the International Electronical Commission (IEC) in fields related to smart manufacturing and smart grid, and with the International Standards Organization (ISO) in the fields of intelligent transportation systems and e-health.

3.3 IoT Security Control Score Suggestion

Figure 9 shows the NCISS score in color stages. The NCCIC Cyber Incident Scoring System (NCISS) of the National Cybersecurity and Communications Integration Center (NCCIC) under the Department of Homeland Security (DHS) in the U.S. designed to estimate the risk of NCISS is a National Institute of Standards and Technology (NIST) special publication 800-61 Rev. 2 Based on the 'Computer Security Incident Handling Guide', it is designed to be scored in consideration of the characteristics of each institution, and it is designed so that NCCIC staff can assign priorities to cyber incidents nationwide and accordingly. . NCISS blends the individually analyzed evaluation values. Although individual bias is minimized through training and practice, various graders inevitably have slightly different views in answering some grading questions. NCISS uses several individually verified values to reduce the impact of individual analysis and increase the overall stability of the system. According to the NCISS Demo, there are eight possible responses in the Functional Impact category: No Impact, No Impact to services, Minimal Impact to Non-Critical Services, Significant Impact to Non-Critical Services Impact), Denial of Non-Critical Services, Significant Impact to Critical Services, Denial of Critical Services/Loss of Control loss) is the item. In IoT security control, most of the country's major services depend on communication

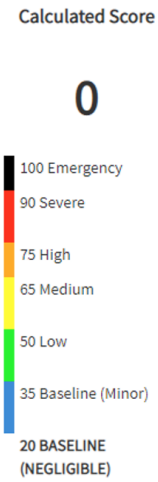

Figure 9: Responsive Items in Observed Activity in NCISS Demo

and cyber networks, so it becomes the mission of the National Cyber Security and Communication Integration Center, requiring information sharing and emergency response coordination at the national level. Therefore, each country proposes scoring to IoT security control.

3.4 Future-Oriented IoT Security Monitoring & Control Strategy

Previously, the details related to security control were summarized and the points for establishing a future-oriented Internet of Things security control strategy were summarized. In order to establish a future-oriented IoT security control strategy, we were able to reach the conclusion that we should first follow the security control strategy framework under the big framework of 'pre-response (prevention), accident response (detection, response, analysis) and post-action (reporting and sharing). Considering security threats and security requirements, we will divide into strategic stages of security control, and each component (IoT Device, IoT Network and Communication, IoT Service/Platform) to discuss the security control strategy in preparation for the time when future IoT technology is universalized. As a security infringement prevention and detection strategy, the SoC(System on Chip) method for preventing forgery and alteration of devices is a strategic measure in the preventive dimension and is a measure to implement the function to prevent forgery and alteration of devices using SoC. Because it is true that there are many lightweight/low power based devices due to the nature of IoT devices, it is necessary to consider a method of embedding SoC, which contains falsification of devices, into lightweight equipment/objects. SoC (System on Chip) refers to a structure that processes a number of functions through a single chip and integrates individual semiconductors such as memory semiconductors, microprocessors, digital signal processing circuits (DSPs), and MCUs into a single chip edge. In other words, the system implemented on several semiconductor chips on the circuit board (PCB) is integrated into one chip, thereby solving the change of the calculation function, data storage, and signal between analog and digital with one chip. It is an equipment integrated with various functions. The reason why SoC is used is that it is difficult to apply security technology directly to lightweight/low power equipment and it can have basic function to cope with information asset security threat from the security control strategy point of view [13]. This can be seen as the embedded Tamper Proof technology. The second strategy is to design a new IoT security operating system based on Micro-Kernel. The reason for presenting these strategic measures is to take into account the characteristics of Micro-Kernel. In the case of micro kernels, only the most basic

services are mounted on the core kernel of the system level, and the other functions are implemented in each process at the user level. In the case of such a micro kernel, it is said that low-level address space management and task management are included. It has the characteristic that when trying to modify a specific function, only the process containing the function needs to be recompiled. In contrast, the Monolithic Kernel puts all the capabilities required by the system at the kernel level, unlike the micro-kernel method, which uses the process to split the rest of the operating system's functional elements into the process and mount multiple simultaneously at the user level. Figure 10 shows the post-system call steps of the user mode and the kernel mode.

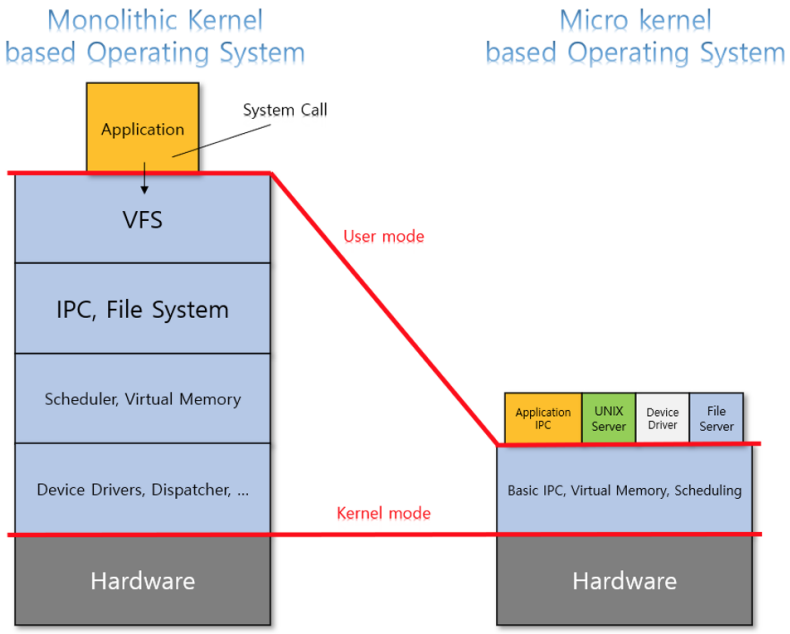

Figure 10: Monolithic Kernel and Micro Kernel

In the case of a monolithic kernel approach, the entire kernel code must be recompiled and rebooted if the kernel parts need to be modified to perform certain functions mounted at the system level. In other words, it means that all kernel codes that are not related to the modified part must also be recompiled. In view of this, it can be easily found that the monolithic kernel has no flexibility compared to the micro-kernel type operating system. Therefore, this inflexible feature is not good in terms of security control. Assuming that there has been an attempt to falsify certain functions, the damage is likely to spread to other kernels than to the kernels that correspond to the functions that received the forgery attempt. Therefore, it is considered desirable to apply an operating system designed with a micro kernel to IoT devices. The third strategy is various methods using artificial intelligence in the security area. The development of IT technology is continuously trying new or variant cyber attacks as the environment changes. According to the development of the technology, security control has developed in the order of unit security control, integrated security control, big data security control, and artificial intelligence security control. Artificial intelligence security control (Zero trust), which has recently attracted attention, is a generation that uses artificial intelligence such as machine learning and SOAR (Security Orchestration Automation and Response) to respond organically to increasingly intelligent cyber attacks [14]. Artificial intelligence security controls enable rapid analysis of vast amounts of data automated with limited time and resources and active response to highly intelligent security threats. Intelligent integrated security control system that implements artificial intelligence security control can collect various information from secu-

rity system using big data technology and analyze high-risk events intensively through machine learning to respond to security threats in real time, and it can also expect detection of unknown threats. A general intrusion detection system mainly detects patterned attacks, and this method shows relatively high efficiency, but it requires a lot of cost and manpower to respond quickly after recognizing and analyzing the ex- act pattern of the attack. In addition, pattern-based detection is difficult to detect by bypassing existing patterns or modified attacks. Therefore, IoT security system needs IoT network artificial intelligence intrusion detection algorithm to identify threats and process them in real time using artificial intelligence Typically, it is possible to analyze and manage packets generated in real time through various machine learning algorithms such as DBSCAN (Density-Based Spatial Clustering of Applications with Noise), thus overcoming limitations of existing real-time analysis [15]. On the other hand, as artificial intelligence technology developed, it began to be used for network attacks. Artificial intelligence technology is expected to continue to develop in the future, and cyber attacks using artificial intelligence will continue to increase. Therefore, there is a limit to responding with existing security technology in IoT environment, and artificial intelligence technology is expected to be an essential element for information protection in IoT environment and network to overcome such limitations [16].

4 Conclusion

This paper, above all, analyzed the trend related to commercialization and universalization of IoT technology and the degree of standardization of IoT. Based on the actual conditions of IoT analyzed through this process, research and analysis were conducted on what is required for IoT security control and the IoT security control strategy was presented. In this strategy, the IoT environment was divided into IoT device, IoT network/communication, and IoT service/platform in line with the basic strategic framework of 'Pre-response-accident response-post-response,' and the strategic direction of security control was established suitable for each of them. The IoT security control strategy can induce a quick and effective response to events that are detected and judged as illegal infringement and harmful traffic, and it is possible to minimize damage by responding after early detection of the inflow of malicious traffic flowing into the control target system. It can contribute to the creation of a solid industrial foundation by increasing the effectiveness of IoT and reducing the cost of responding to IoT security breaches. Cybersecurity professionals are already overloaded with thousands of threats added every day, variants being created and evolving to evade detection. Additionally, as cybercriminals and attacks become more sophisticated, a higher level of threat prevention and response is imperative.

References

[1] W. Park and G. Ahn. A study on the next generation security control model for cyber threat detection in the internet of things (iot) environment. In *Proc. of the 21st ACIS International Winter Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD-Winter'21), Ho Chi Minh City, Vietnam*, pages 213–217. IEEE, January 2021.

[2] S.J. Park and J.H. Park. Current status and analysis of domestic security control system. *Journal of the Electronic Communications Association of Korea*, 9(2):261–266, February 2014.

[3] List of information security incidents in south korea. Wikipedia, June 2021. `https://ko.wikipedia.org/wiki/%EB%8C%80%ED%95%9C%EB%AF%BC%EA%B5%AD%EC%9D%98_%EC%A0%95%EB%B3%B4_%EB%B3%B4%EC%95%88_%EC%82%AC%EA%B3%A0_%EB%AA%A9%EB%A1%9D`[Online; Accessed on March 31, 2022].

[4] J.H. Park and H.G. Kim. A study on the automatic information gathering and management system of the wireless devices for reinforcing wireless intrusion detection and prevention. In *Proc. of the 2010 Korean Information Science Society Conference, Jeju, South Korea*, volume 37, pages 30–35. Korean Institute of Information Scientists and Engineers, June 2010.

[5] J.Y. Ko, S.G. Lee, J.W. Kim, and C.H. Lee. Technologies analysis based on iot security requirements and security operating system. *The Journal of the Korea Contents Association*, 18(5):164–177, 2018.

[6] S.Y. Min and J.S. Lee. Authentication and group key management techniques for secure communication in iot. *Journal of the Korea Academia-Industrial cooperation Society*, 20(12):76–82, November 2019.

[7] O.H. Ha. A study on conversion security control system for industrial security. *Convergence Security Journal*, 9(April):1–6, November 2009.

[8] G.H. Koh, S.R. Lee, and S.J. Ahn. A study on the direction of security control of iot environment. *Journal of the Korea Convergence Security Association*, 15(May):53–59, 2015.

[9] H.W. Kim. Security/privacy issues in the internet of things environment. *Communications of the Korean Institute of Information Scientists and Engineers*, 32(6):37–41, June 2014.

[10] S.J. Ahn. Security control, 2014.

[11] W.Y. Yoo. An analysis of domestic and foreign research trends on iot security. *Korea convergence Security Association*, 18(1):61–67, March 2018.

[12] D. Kim, K.M. Kim, and J.S. Cho. Discussions on iot security requirements. *Journal of Computing Science and Engineering*, pages 1072–1074, June 2015.

[13] W.C. Ahn. Trends and utilization of internet of things (iot). *Korean Railroad Society*, 18(2):74–78, April 2015.

[14] M.S. Gong, H.J. Chae, and K.H. Yoo. Internet of things (iot) technology trends and prospects. *Korean Society of Mechanical Technology*, 56(2):32–36, February 2016.

[15] K. Khan, S.U. Rehman, K. Aziz, S. Fong, and S. Sarasvady. Dbscan: Past, present and future. In *Proc. of the 5th International Conference on the Applications of Digital Information and Web Technologies (ICADIWT'14), Bangalore, India*, pages 232–238. IEEE, May 2014.

[16] S.Y. Lee. Trend of information protection on the internet of things(iot). 16(2):28–35, February 2015.

Author Biography

WonHyung Park is a professor in Department of Cyber Security, Sangmayung University, South Korea. He received Ph.D. degree in Department of Information Security from the Kyonggi University, South Korea, in 2009. he co-authored more than 50 technical papers in the area of information security. Also, he has been reviewer for International Journal(Computer-Journal) of Oxford Univ. press and IEEE Conference.

GwangHyun Ahn received a B.S. degree in cybersecurity from Far East University, Chung-cheong bukdo, South Korea, in 2018. He is currently pursuing a Ph.D. degree with the Department of Computer Engineering, Sejong University, South Korea, Since 2020. He was commissioned as an officer specializing in cyber security in the Republic of Korea and served in the military for three years before moving to a state civil service. His research interests include cybersecurity, industrial security, Incident Response, Forensic, Self-driving car hacking, Profiling of major hacking groups and Dark Web.

Jin-Won Kim received a B.S. and M.S. degree in Department of AI Computer Engineering from Far East University, South Korea. He is currently pursuing a Ph.D. degree in Department of AI Security, Far East University, South Korea, Since 2021. His research interests include the prevention of industrial secret leakage, IoT and security monitoring model, security audit for internal information leakers and diagnosis of vulnerabilities using Artificial Intelligence.

Jang-Mook Kang received a Ph.D. in Information security from Korea University, Korea, in 2005. He is currently a Professor in the Department of Hacking Security at Far East University in Korea. From 2010 to 2017, he worked in the Dept. of computer science and research lab., where he has researched BigData as a Research Official and research Professor. From 2017 to 2020, he worked in the Namseoul University and Global Cyber University, where he has researched AI and Security as a professor. From 2020 to now, he worked in the Department of Hacking Security at Far East University in Korea, where he has researched industrial technology security as a professor. His research interests have been focused on issues of AI and Cyber Security.

Yong-Joon Lee received a Ph.D. in Computer Science from Soongsil University, Korea, in 2005. He is currently a Professor in the Department of Hack- ing Security at Far East University in Korea. From 2016 to 2020, he worked in the Defense Security Institute(DSI), where he has researched insider threat program as a Research Official. From 2010 to 2015, he worked in the Korea Internet & Security Agency(KISA), where he has researched cyber security as a Principal Researcher. From 2006 to 2009, he worked in the LG CNS, where he has researched industrial technology security as a Senior Researcher. His research interests have been focused on issues of cyber incidents detection.