Analysis of IoT Platform Security: A Survey

Jin-Yong Yu
Dept. of Computer and Information Security
Sejong University
South Korea
instrument_u@naver.com

Young-Gab Kim*
Dept. of Computer and Information Security
Sejong University
South Korea
alwaysgabi@sejong.ac.kr

***Abstract*—- Because the IoT (Internet of Things) is emerging as the next generation growth engine that leads the IT (information technology) industry, many developed countries and companies are developing IoT based technologies to preoccupy the IoT market. Among the core technologies that make up IoT, IoT platform can have a huge impact on future devices. It is attracting attention as one of the most promising technologies of IoT technology, but at the same time concerns about platform security are also increasing. In response to this, Korea (domestic) and international IoT platforms adopt diverse security technologies according to the developed purpose and environment. For most domestic IoT platforms are developed based on platforms on which standardization is underway like oneM2M and OCF. For the international IoT platforms, they were developed in a proprietary method. Not only this, the security method also adopted their own method. But, even though the security methods of domestic and international IoT platforms have a distinct difference like this, studies comparing and analyzing the security elements of domestic and international IoT platforms are not enough. Therefore, in this paper, we analyze and compare security elements of domestic and international IoT platforms so that more secure domestic IoT growth can be achieved. Finally, we propose the development direction of future IoT platform security.**

Keywords—Internet of Things; IoT platform; Security

I. INTRODUCTION

Recently, the IoT (Internet of Things) is emerging as the next generation growth engine that leads the IT (information technology) industry. For this reason, many developed countries are actively supporting the IoT industry, and Korea is also setting up strategies for fostering IoT. Earlier, well-known companies such as Gartner, Cisco, and IDC have selected IoT as one of the promising technologies of the future [1], and IDC predicts that the IoT market will grow by 14.4% per annum from 2017 to 2021 [2]. On the strength of this trend, global companies such as Google, Amazon, Samsung, and Cisco are developing technologies, standards, and devices related to IoT in order to take the lead in the IoT market. Among them, the platform is especially recognized as the core technology of IoT because it can directly or indirectly affect the devices that are expected to grow exponentially in the future by providing the devices with various functions that the platform has [3]. Due to these characteristics, the platform technology of IoT is attracting attention as the most promising technology in the future, but there are also a lot of concerns about security. In response to this, the IoT platform security technologies are developing in Korea, and being expanded on the basis of platforms on which standardization is underway like oneM2M (one machine to machine) and OCF (open connected foundation) to supplement the security vulnerabilities. Not only this, it is being developed focusing on interoperability with various devices. However, despite these efforts, the domestic IoT platforms are considered to have lower security reliability than the international IoT platforms. However, despite awareness of this problem, there is not enough analysis and comparison on security factors with international IoT platforms. Also, since all of the currently domestic and international IoT platforms were developed independently, security for interoperability was not considered sufficiently. Therefore, in this paper, we analyze and compare the security factors of domestic and foreign IoT platforms and suggests future direction of IoT platform security.

The rest of this paper is structured as follows. In section 2, we analyzed the security of IoT platform based on oneM2M because most domestic platform security development are based on it. We also dealt with the analysis of various elements for IoT platform security, and guideline studies to make secure IoT environment. In section 3, we analyzed the security factors of the selected domestic and international IoT platforms. In section 4, we compared the security elements of each IoT platform. Through this, we pointed out the problem of security of domestic IoT platforms as well as analyzed common problems of existing IoT platforms. We also proposed the development direction of IoT platform security in the future to make secure environment of IoT platform. Finally, in section 5, conclusion is drawn from the above.

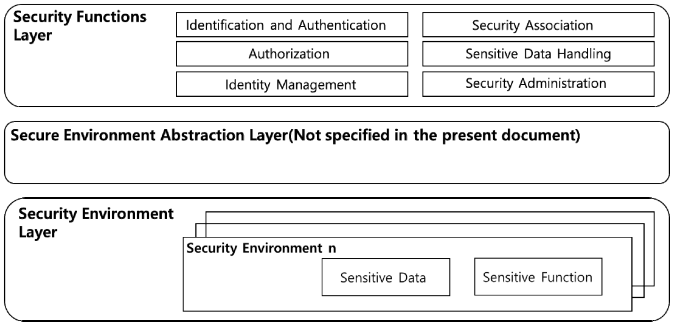

Fig. 1. Security Architecture of oneM2M [6]

II. RELATED WORK

Heo et al. [4] analyzed the overall security technology and security structure of oneM2M. Fig. 1 schematizes oneM2M's security architecture, and shows oneM2M security architecture

* Corresponding Author

978-1-7281-1288-6/19/$31.00 ©2019 IEEE

that consists of Security Function layer, Secure Environment Abstraction layer, and Security Environment layer. The security function layer provides the functions of identification, authentication, authorization, identity management, security association, sensitive data management, and security management [5]. They were focusing on analyzing the security service provided by the security layer.

As an analysis of the security elements of various IoT platforms, Ammar et al. [7] referred to the IoT framework as a set to simplify the implementation of IoT applications. This IoT framework explains that security mechanisms are designed to protect sensitive data including security and personal information. They analyzed the security factors (i.e., IoT framework) of eight currently active IoT platforms, and also specified the proposed architecture for the framework, the essential elements of app development, compatible hardware, and security features.

As IoT security study of International Organization for Standardization, Hwang et al. [8] emphasized that heterogeneous interoperability is an essential process in the IoT environment, and pointed out that there were no studies related to IoT security standards although IoT standards were being published by international organizations. Therefore, they provided guidelines for establishing a secure IoT environment.

III. DOMESTIC AND INTERNATIONAL IOT PLATFORM SECURITY ANALYSIS

As the IoT market grows rapidly, growing concerns about security are growing. Especially, interest in IoT platform security, which is the core of IoT security, is increasing. In Korea, they are developing platforms based on platforms on which standardization is underway like oneM2M and OCF. ARTIK, which is discussed in this paper, is developed based on OCF authentication technology. In the case of Thingplug and GiGA IoTmakers are developed based on oneM2M. On the other hand, the international IoT platforms (AWS IoT, Azure IoT, and Google Cloud IoT) protect themselves by using its own security service, and various security solutions were still being studied. In this section, IoT platforms of domestic conglomerate and international IoT platforms, which are commercialized, are selected, and security elements of them are analyzed.

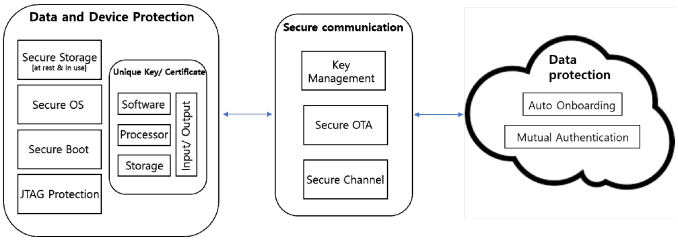

Fig. 2. Security Architecture of ARTIK [9]

A. ARTIK

ARTIK, which is developed by Samsun, is an integrated IoT platform. This platform includes OCF-based authentication technology and IoT elements, such as hardware, software, cloud, security and ecosystem. And also, it is a typical cloud-based IoT platform that performs security procedures including information exchange and authentication using ARTIK cloud from devices to applications and 3rd party cloud. First, the REST API is supported to access the resources of ARTIK. The MQTT (Message Queue for Telemetry Transport), CoAP (Constrained Application Protocol) and Websocket are supported as the application protocol. And the transport protocol adopts the TLS, thereby establishing a secure communication environment. The AES (advanced encryption standard) and RSA (Rivest, Sharmir, Adleman) cryptography algorithms are supported for data confidentiality. And the ARTIK module provides a cryptographic engine for encryption and decryption. In secure communication, not only confidentiality but also authentication is important. Therefore, ARTIK uses PKI (public key infrastructure) to create and apply unique certificates and key pairs to each module in the manufacturing process. In addition, by adopting the ECDH (elliptic-curve Diffie-Hellman) algorithm as a method of generating the session encryption key, it provides a high level of security environment even in a low power environment which is a restriction characteristic of IoT. Also, OAuth and OAuth2 are used to authenticate clients using access token, and various access token issuance methods are provided in ARTIK. Not only this, as shown in Fig. 2, ARTIK offers a variety of other security services. Secure OS manages the entire system to create secure execution environment of ARTIK. Secure boot enables only proven software to be executed. And sensitive data is stored in the database by applying secure element and Trustzone based TEE (trusted execution environment) security technology. In addition, it supports JTAG (joint test action group) services for platform debugging and secure OTA (over the air) services for secure update or installation of the platform.

B. Thingplug

SKT's Thingplug is the first open IoT platform developed by the telecommunication company based on international standard oneM2M. Since it was developed by a telecommunications company, this platform requires a wide communication network, such as LPWA (low-power long distance communication) and LoRa (long range) network which is well established nationwide. In the LoRa network, various security functions such as MAC (message authentication code), AES, and ADR (adaptive data rate) are provided for secure communication [10]. To receive these security services, Thingplug supports HTTP and MQTT protocol to be possible to access oneM2M standard based REST API from outside. However, it does not support CoAP which is a standard protocol of short range and low power device, because it uses their proprietary GMMP (global M2M protocol). There are not many commercial cases of CoAP, but GMMP protocol has been already actively used in various services [11]. As transport protocol, TLS is adopted and data encryption method for data confidentiality protects data by supporting AES, ECC (elliptic curve cryptosystem) and ARIA, which is a domestic standard cryptography algorithm. Thingplug also establishes PKI environment so that only authorized terminals of SKT can be connected. It also

contributes to Thingplug's secure authentication environment by providing authentication value of dKey and uKey. However, Thingplug does not provide information other than the security functions mentioned above. Further, users can not find any information about the security architecture by using it. Since it was just developed based on oneM2M, Thingplug security architecture follows the oneM2M security architecture as shown in Fig. 1. Thingplug explains that basic security functions as well as security policies are based on oneM2M's standard rule TS-0003 security solutions.

C. GiGA IoTMakers

GiGA IoTMakers, is an open IoT platform based on oneM2M developed by telecommunications company KT. This platform is selectively implemented by using the functions of layers. It expands its security function based on the security service provided by oneM2M like Thingplug. GiGA IoTMakers and Thingplug are developed based on the same IoT standard and have similar development motivation. So, they have many common security elements, but the network is different. Thingplug uses LoRa network, while GiGA IoTMakers uses NB (narrow band)-IoT network. Compared to LoRa networks that uses non-license frequency band, NB-IoT network uses the licensed frequency band. It is affected relatively little interference from other frequencies. Besides, GiGA IoTMakers is supported by the AES and RSA cryptography algorithms for data confidentiality and provides security solutions verified by international standard organizations, such as 3GPP (3rd Generation Partnership Project) and ETSI (European Telecommunication Standards Institute). Like other platform, to utilize platform resources, GiGA IoTMakers supports REST API and various industrial protocols, such as HTTP, MQTT, CoAP, TCP (transmission control protocol). All communication uses TLS transport protocol, and AES is adopted as encryption methods to protect confidentiality of data. Each cryptography algorithm supports CBC (cipher block chaining) mode and CTR (counter) mode according to the characteristics of data. The consideration about authentication, which is the core of communication security, is supplementing through applying PKI environment, which guarantees not only authentication but also integrity and non-repudiation to make secure communication environment. Authentication and authorization for clients is verified by OAuth like ARTIK. However, like Thingplug, it does not provide any more security information, even though it provides many security services.

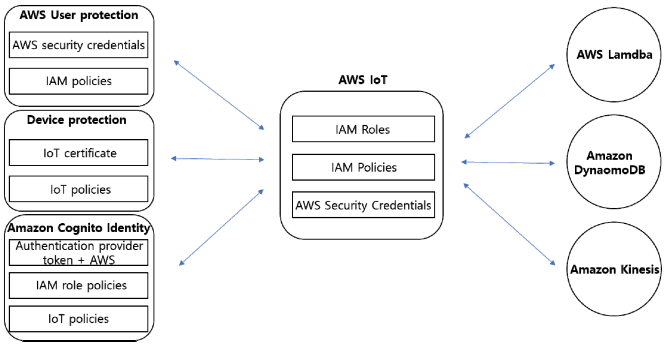

Fig. 3. Security Architecture of AWS IoT [12]

make secure communication environment. Authentication and authorization for clients is verified by OAuth like ARTIK. However, like Thingplug, it does not provide any more security information, even though it provides many security services.

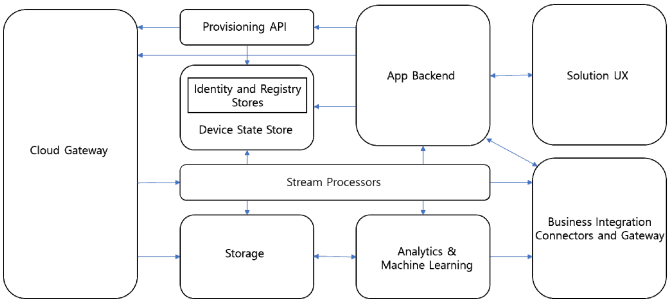

Fig 4. Architecture of Azure [13]

D. AWS IoT

AWS IoT is a cloud-based IoT platform that provides bi-directional communications developed by Amazon and enables devices connected to AWS IoT to easily and securely interoperate with applications and other devices. As shown in Fig. 3, in AWS IoT, each connected device must have security credentials to access the service and security credentials must be kept safely to communicate securely. This role is handled by AWS IoT. These security functions have been implemented because AWS IoT has been developed steadily for a long time. Among these security technologies, AWS IoT Core plays a key role in AWS IoT security and performs device connection and management, data security, processing and operation, and controls only authorized devices to communicate. The REST API is supported as an access method to use the resources of the platform in the authorized client. The application protocols are extended to support a variety of industry standard and user-defined protocols besides MQTT, HTTP, CoAP, and Websocket. AWS IoT adopts TLS transport protocol to ensure more secure data communication and uses AES and RSA cryptography as encryption method to keep confidentiality of data. Furthermore, the PKI system can be applied to ensure authentication as well as integrity verification and non-repudiation prevention. OAuth is adopted as client authentication, and also applies various authentication policies (e.g., x.509 certificates, AWS IAM (identity& access management), AWS cognito, AWS STS (security token service) to secure the platform. Not only this, AWS IoT provides security services such as API traces, AWS cloudtrail tracking which resources clients have used, and negative access attempts.

E. Azure IoT

Azure IoT, which is developed by Microsoft, is a platform designed to assist in the creation of IoT applications. This platform offers a variety of features to build from SaaS (software as a service) solutions to PaaS (platform as a service) and intelligent Edge. According to the REST API which is supported to access the resources of the platform providing these various functions and HTTP, MQTT and AMQP

(advanced message queuing protocol) are adopted as application protocols. TLS is adopted as a transport protocol to ensure data security. AES and RSA are used as data encryption method to protect data by double encryption. Besides, Azure IoT has its own security framework that performs threat modeling. Fig. 4 shows how to find threats through the Azure IoT reference architecture and resolve identified threats. The Azure IoT Hub is a key component of Azure IoT security and enables secure communication between the platform and devices using device-specific security credentials and access controls. In the communication environment with devices, PKI system is introduced basically to ensure data integrity, authentication, and non-repudiation. In addition to authentication method x.509 certificates and HMAC-SHA256, there is OAuth method to authenticate and authorize clients using access token. Not only this, Azure IoT can specify the authorization level for resources based on the token (SAS: sharing access signature) generated by the device ID. Azure includes active directory to manage access control, Azure cosmos DB, a globally dispersed database service, and stream analytic to detect data changes in real time to protect availability.

F. Google Cloud IoT

Google's Google Cloud IoT is a platform for intelligent IoT services that manages data distribution, management, internal data processing, and IoT devices distributed across the globe. As shown in Fig. 5, Cloud IoT Core is the core technology of Google Cloud IoT. It ensures and manages secure connections to devices. Client uses the REST API to access the platform's resources and support MQTT, HTTP application protocol. TLS is adopted by transport protocol for secure communication. To prevent connections to malicious devices, it uses JWT (JSON web token) as a method for authenticating devices. It is signed

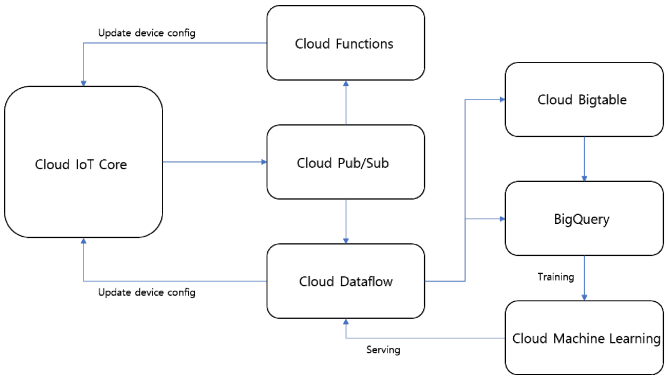

Fig. 5. Architecture of cloud IoT core [14]

by the private key among the public key/private key that key pairs generated on each device to authenticate the JWT. This approach can limit the impact on a single device without affecting the entire device. Besides, Google Cloud IoT supports RSA and ECC cryptography algorithms to provide a strong signature key size while simultaneously enforcing security by registering keys and expiring credentials. Data is encrypted with AES-128 or AES-256, but some data requiring authentication is used in CBC mode with AES and HMAC (HASH message authentication code). Also, some replicated files are used in CTR mode with AES and HMAC. Another key security technology is PKI and OAuth. PKI technology is applied to ensure data integrity, authentication, and non-repudiation. OAuth technology using access token is applied to authenticate and authorize clients, and creates a secure access control environment. Not only this, there are cloud IAM policy for access control and cloud IPA, GCP (google cloud platform) armor, cloud DLP (data loss prevention) API and cloud

TABLE I. COMPARISON OF IOT PLATFORM SECURITY ELEMENTS

	Samsung ARTIK	**SKT Thingplug**	**KT GiGA IoTMakers**	**Amazon AWS IoT**	**Microsoft Azure IoT**	**Google Google Cloud IoT**
Based Platform	OCF	oneM2M	oneM2M	N/A	N/A	N/A
Open Source	Supported	Supported	Supported	Supported	Supported	Supported
Application Protocol	MQTT CoAP Websocket	HTTP MQTT GMMP	TCP HTTP MQTT CoAP	HTTP MQTT CoAP Websocket	HTTP MQTT AMQP	HTTP MQTT
Transport Protocol	TLS	TLS	TLS	TLS	TLS	TLS
Cryptography Algorithm	AES RSA ECC	AES RSA ARIA	AES RSA ECC	AES RSA ECC	AES RSA ECC	AES RSA ECC
Authentication Protocol	X.509 certificates OAuth	X.509 certificates uKey dKey	X.509 certificates OAuth	x.509 certificates OAuth JWT AWS IAM AWS Cognito	x.509 certificates OAuth SAS token HMAC	X.509 certificates OAuth JWT
Other Security Features	Secure OTA Secure storage Secure boot Secure JTAG	oneM2M's standard rule TS-0003 security solutions		IAM roles IAM policy AWS security credentials AWS policy AWS STS	Azure IoT hub Azure active directory Azure cosmos DB Azure stream analytics	Cloud IoT core Cloud IAM policy Cloud IPA GCP armor Cloud DLP API Cloud security scanner
		LoRa network	NB-IoT network			

security scanner to prevent with various attacks.

IV. Comparison of Domestic and International IoT Platform Security

Table 1 shows security elements of each platform based on the analysis in Section 3. In case of domestic IoT platforms, they are developed based on IoT platforms on which standardizations are underway, and security functions are extending according to these standardizations. On the other hand, international IoT platform has developed its own security technology and utilized them. Domestic and international IoT platforms are expanding their ecosystem based on open source to attract more users. They also support standard protocols (e.g., HTTP, MQTT, CoAP), industrial protocols, and user-defined protocols to use platform resources. The reason for supporting such a large number of protocols is to communicate smoothly. For secure communication, domestic and international IoT platforms use TLS transport protocol in common, and use cryptography algorithms, such as AES, RSA and ECC, as an encryption method for securing confidentiality. Not only this, the analyzed platforms guarantee integrity and non-repudiation prevention including authentication through PKI environment. As one of the core technologies of IoT platform security, authentication is the universal use of x.509 certificates or OAuth. There is also an IoT platform that implements authentication by introducing proprietary technology concepts. Although the domestic and international IoT platforms seem to support similar security functions, the international IoT platforms provide a lot of additional security services compared to the domestic IoT platforms. The reliability of international IoT platforms is also excellent by providing security related data. On the other hand, most domestic IoT platforms tend to be limited to the security services and reliability because they do not provide security related data. However, not only the domestic but also the international IoT platforms are independently developed, and each platform has a vulnerability. Therefore, there are threats that can have a fatal impact on the system. It will also have limitations in interworking with other platforms in the hyper-connected society where all future resources can be shared, and the IoT industry will become a deadly evil to develop. Therefore, an integrated standard IoT platform should be established so that the currently developed IoT platforms can interoperate with all platforms. In addition, comprehensive countermeasures and solutions reflecting the security situation of various IoT platforms are required.

V. Conclusions and Future Work

In this paper, we discuss the reasons why IoT platform security is becoming increasingly important according to the rapidly growing IoT industry. Therefore, we analyzed and compared the security factors by selecting IoT platforms of conglomerate which is most commercialized abroad. Each IoT platform supports security technologies that match the platform characteristics according to the purpose and environment of development. However, the security data of domestic IoT platforms is not much considered as compared with the international IoT platforms. The biggest problem is that most of the currently developed platforms are developed independently and have various vulnerabilities, threats on each platform, and limitations in interworking with other platforms. This is a fatal detriment of the hyper-connected society in which all the resources are shared in the future. Therefore, an IoT standard platform that can interoperate with all IoT platforms is needed. In addition, a solution that can integrate the vulnerabilities and threats of each platform is required. In this paper, we propose the development direction of the IoT platform by analyzing and comparing the influential domestic and international IoT platforms and expect the development of a secure domestic IoT platform through analysis of the data.

Acknowledgment

This work was supported by Institute for Information & communications Technology Promotion (IITP) grant funded by the Korea government (MSIP) (No.2016-0-00498, User behavior pattern analysis-based authentication and anomaly detection within the system using deep learning techniques).

References

[1] IDC, http://www.idc.com/getdoc.jsp?containerId=prUS25658015
[2] IDC (International Data Corporation), "Forecasts Worldwide Spending on the Internet of Things to Reach $772 Billion in 2018," https://www.idc.com/getdoc.jsp?containerId=prUS43295217
[3] Se-Ra Oh, Young-Gab Kim "Interoperable Security Framework for Heterogeneous IoT Platform," KIPS Tr. Comp. and Comm. Sys, Vol.7, No.3 pp.81~90
[4] S. W. Heo, H. W. Kim "An Analysis of IoT Security Requirements And oneM2M Security Technology," Communications of the Korean Institute of Information Scientists and Engineers 2017.1, 16-22
[5] NIST, "Security Requirements for Cryptographic Modules", NIST FIPS PUB 140-2, Dec. 2002
[6] oneM2M technical specification "TS-0003-V2.4.1" oneM2M, Aug 2016
[7] M. Ammar, G. Russello, B. Crispo "Internet of Things: A survey on the security of IoT frameworks," Journal of Information Security and Application Volume 38, Pages 8-27, February 2018,
[8] Intae Hwang, Young-Gab Kim "Analysis of Security Standardization for the Internet of Things," IEEE 2017 Platform Technology and Service(PlatCon), pp.1-6, February 2017
[9] ARTIK, https://www.artik.io/overview/samsung-artik-iot-security/secure-storage/
[10] Lina Yi, Garam Lee, Howon Kim "A Study on the Lora Systems," KICS Proceedings of Symposium of the Korean Institute of communications and Information Sciences, 2017.6, 217-218
[11] Garam Ko, Hong-bum Ahn, Gyu-Byeong Kim, Jong Eun Lee, Sang-Min Lee, Lee Jae-han "IoT service development starting with Thingplug," pageblue, Korea, Nov 2015
[12] AWS (Amazon Web Service) "AWS IoT Developer Guide," https://docs.aws.amazon.com/iot/latest/developerguide/iot-security-identity.html
[13] Azure, https://docs.microsoft.com/en-us/azure/iot-fundamentals/iot-security-architecture
[14] Google cloud IoT, https://cloud.google.com/iot-core/