International Journal of Innovative Research in Technology & Science

Received 11 September 2018, Accepted 20 September 2018, Available online 30 September 2018

ISSN: 2321-1156 Volume VI Issue V, September 2018

A STUDY ON SECURITY ENHANCING MEASURES IN APPLICATION ENVIRONMENT WITH IOT TECHNOLOGY

Eun Young Choi, Korea Internet & Security Agency; Haeryong Park, Korea Internet & Security Agency; SEUNGHO AHN
Chonnam National University

Abstract

The Internet of Things (IoT) has been increasing in recent years. Under the IoT technology, all things are connected based on the internet and the exchange of information is possible with the Fourth Industrial Revolution. This technology can be applied to various service fields including smart home, healthcare and the transportation system. Standardization is necessary to widen its application to industry fields and many companies such as QUALCOMM and Samsung have participated in developing an open platform such as oneM2M, AllJoyn, and IoTivity. Given that IoT is in a wireless environment, security can be threatened in the form of privacy invasion from cyber-attack and information leakage from an unauthorized access to major facilities. So, we investigate the development status of an IoT open platform and the IoT applications technology status in this paper. We also analyze security under the open platform and suggests considerations to strengthen safety service by application environments where IoT technologies can be applied.

I. Introduction

Recently, according to the market research firm Gartner, the global number of IoT devices - excluding PCs, tablets, and smartphones - will reach 20.8 billion by 2020 [3]. The IoT technology has been applied to various fields such as smart home, healthcare, transportation system, environments, disaster control, manufacturing, construction and energy. So it is deeply related to our daily lives. While all devices are connected in IoT environments, information leakages as well as system damages from an unauthorized access and the breach of personal information could take place.

Various security techniques including data encryption and access authority have been applied in order to reinforce security to establish a safe internet-based service infrastructure. For the purpose of establishing and managing security, recommendation (plans) and standardizations on safe management of an encryption key have been introduced by NIST, ISO/IEC and OASIS [2, 7-13, 15]. An open platform has been developed and activated such as OneM2M and IoTivity with the aim of establishing the IoT technology at both the global company (i.e., QUALCOMM) and national levels. However, establishing a platform is so urgent that possible security issues in the process of utilizing the system are insufficiently dealt with. To activate IoT technologies, it is necessary to investigate security vulnerabilities and offer alternatives to cope with them.

This paper is consisted as follow. In Section 2, we provide the status on an open platform development such as OneM2M, IoTivity and smart things and sectoral technologies. In Section 3, we analyze the security related to oneM2M and IoTivity. Also, we suggest sectoral considerations in order to safely establish IoT environments in Section 4. Finally, we conclude in Section 5.

II. Introduction of IOT Technologies

In this section, we describe Open Platforms and sectoral technologies status on IoT.

2.1 IoT Open Platforms

The IoT open platform involves OneM2M, IoTivity and AllJoyn, etc. Their functions and security are as follow:

OneM2M [14]:

OneM2M, the global standards partnership for M2M, was launched in July 2012 by seven major standardization organizations including TTA (Korea), ATIS (North America), TTC (Japan), CCSA (China) and ETSI (Europe). Eight standardization organizations are active after TSDSI (India) is included. Machine to machine (commonly abbreviated as M2M) means that devices directly communicate with each other using any communications channel, including wired and wireless. OneM2M specifications provide a framework to support a wide range of applications and services such as smart cities and connected cars. The TLS (Transport Layer Security)/DTLS (Datagram Transport Layer Security) protocol aims to establish a safe security channel and then provide confidentiality and data integrity for identification, authentication and communications messages [17, 18].

AllJoyn [1]:

AllJoyn developed in 2011 is an open source platform after upgrading DLNA (Digital Living Network Alliance) by Qualcomm, the technology which shares media contents among appliances in smart home. Spearheaded by Qualcomm, it is the

IoT platform developed by 100 All Seen Alliance members. The AllJoyn framework consists of apps and routers. The App communicates with the router. The communications among apps can only be available by routers. The AllJoyn platform supports Window, iOS/OS X and Linux and a smartphone operating system such as Android. It also supports Thin-Linux, Thin-Windows and Arduino embedded in IoT devices. The TLS 1.2 version is used for communications security. In case of establishing the security function of IoT system through Security 2.0 architecture, it offers the architecture, configuration and the method of authentication as well as key exchanges among devices.

IoTivity [4]:

It is developed by the Open Connectivity Foundation OCF (Open alliance for IoT standard) where 400 technology companies, research organizations and manufacturers such as CISCO and Intel have participated. They have developed the technology enabling the control from inside and outside of a local by connecting the IoT devices. IoTivity supports Ubuntu, Windows, Tizen, Android and IOS. In case of an open source platform, it supports Arduino. The platform aims to realize IoT on devices and supports DTLS RFC 6347[18] and TLS RFC 5246[17] to ensure data safety.

Android Things [20]:

Android Things is a platform that brings the power of Android development to embedded devices and IoT use case and then Android frameworks can be applied to develop IoT devices. It is able to reuse Android API which developers already have known because all Android frameworks can be used.

Smart Things [21]:

It is an IoT platform that Samsung Electronics takes over to make smart electronic devices open and acceptable. It is an open platform for smart home appliances and serves as a hub mobile application enabling interoperability with many platforms.

2.2 Sectoral application status of IoT

The IoT technologies can be applied to home automation, healthcare, transportation, disaster control, manufacturing, construction and energy. In this section, we are going to look into the status of application of IoT technology in each field.

2.2.1 Smart home field

A smart home means the housing or home with IoT system applied which monitors and controls various things and environments remotely or controls automatically. This field has grown rapidly in the field of smart appliance control, air conditioning and heating, energy use, HVAC control, security, child care. The smart home based on IoT technology has getting attention in annually held CES (Consumer Electronics Show) since 2015.

A smart controller has been in the spotlight in this field. It is the device which embeds the IoT technology to an existing home appliance by attaching a smart controller to home appliances such as a refrigerator or an air conditioner. Then things are connected to the Internet and can be controlled. A smart TV can be connected to the Internet and interaction is available unlike an existing TV which only focuses on transmitting simple broadcastings. So, various contents including a VOD, a game, searches and the weather can be used in user-friendly environments (UI/US). A smart refrigerator is about detecting the type of items stored in it and managing groceries with the use of IoT technology. Various technologies applied to housing, robots, lightings and energy have been introduced. Apple’s Home kit and Google’s Nest Labs Thermostat are case in point.

HomeKiT: HomeKit is a software framework that connects household items and can be operated by Apple’s device. Home Kit’s ID is based on a public key (Ed25519) and a private key. These keys are created between iOS devices and HomeKit users. They are only saved by key chains and an encrypted key chain backup. With iCloud keychain, the key can be synchronized [23].

Nest Labs Thermostat: The Nest Labs Thermostat, the intelligent thermostat, is an IoT device that is responsible for controlling a home's heating and/or air conditioning. Users can check home temperatures by having access to the Nest Cloud Service from a mobile device or website [25].

2.2.2 Healthcare field

The connected medical devices supported by big data enhance monitoring capabilities and good results when caring patients with the IoT technology linking to healthcare solutions. This offers remote monitoring and treatment, customized healthcare, preventive treatment and more efficient treatment. For example, the connected medical devices with the use of IoT can monitor insulin levels and heart rates of chronic patients and prevent them from visiting again and then help reduce unnecessary medical costs. Moreover, smart health care services equipped with healthcare functions in mobile devices such as wearable devices have appeared. This makes it possible to provide the tailored service thanks the spread of mobile devices amid the paradigm shift of medical service which is from treating diseases to checking health on a regular basis. Wearable devices are mostly used for checking health conditions by measuring and transmitting the bio-information via connecting the devices wirelessly.

2.2.3 Transportation field

Major leaders of the smart transportation system are mainly in the U.S. Three major automakers such as GM, Ford and Chrysler have studied the vehicle cooperation system on the road by cooperating with US-DoT since the early 1990s. MIT has engaged in ITS (Intelligent Transportation System) R&D. Europe, Japan and China also have developed the technology as follows:

U.S.: Google- Self-Driving system, GM-Security Solution, IBM-Connected Car Technology Intelligent City
Japan: Toyota –Toyota Safety Sense (TSS), Denso – Electronic Toll Collection system, Toshiba – Digital Transmission Content Protection
EU: BMW – ParkNow (mobile parking service), Siemens – Telematics
China: ZTE – Traffic Information Collecting Device, Unitedsoft. – Traffic Information detector, Wisesoft – tTraffic Information Collecting System

2.2.4 Environment and disaster control field

The disaster includes natural disasters, environment degradation and industrial disasters. As disasters and accidents have become various and complicated as well as unpredictable, other management system different from the past are needed. The IoT technology of disaster and safety manages environments and disasters in the areas of monitoring a dam, managing wastes and checking the safety of a bridge. These areas are gradually expanding due to the development of low-cost, high definition and reliable sensors, communications, big data processing and platform technology. Furthermore, global companies such as Libelium, Echelon and Battelle have developed the products to embody a smart city.

2.2.5 Manufacturing and construction field

In the manufacturing field, it is able to sense, store and process the information of order, inventory and process. It preforms manufacturing processes in faster and efficient ways. When it comes to the MDS technology, it provides smart factory and industrial IoT solution. The MDS technology provides the IoT solution for a smart factory and industry and then offers the solution to realize a smart factory such as sizes and communications modules as well as a software detection device for industry communications and machine data conversion [24]. In case of the construction field, it is able to construct a building with the help of sensing information by monitoring buildings and bridges and checking maintenance as well as workers' safety.

III. Security technology of an open platform for OneM2M and IoTivity

This section, we analyze the security technology of an open platform for OneM2M and IoTivity.

3.1 Security technology of an open platform for OneM2M

We analyze the security technology provided by TS-0003 Security Solutions which is a security standard [22]. OneM2M adopts both TLS 1.2 and DTLS 1.2 versions for the security of communications. DTLS (Datagram Transport Layer Security) is based on TLS (Transport Layer Security) protocol which provides the security to TCP protocol of a transport layer, making it possible to transmit an encrypted datagram. The security structure of OneM2M is shown in Figure 1 below.

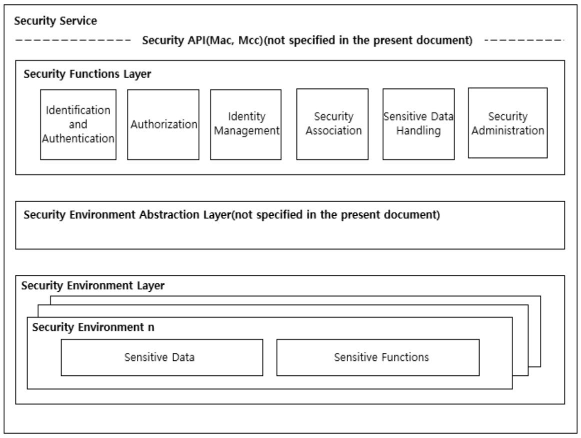

Security Service
Security API(Mac, Mcc)(not specified in the present document)
Security Functions Layer
Identification and Authentication
Authorization
Identity Management
Security Association
Sensitive Data Handling
Security Administration
Security Environment Abstraction Layer(not specified in the present document)
Security Environment Layer
Security Environment n
Sensitive Data
Sensitive Functions

Figure 1 Security structure of OneM2M

The security structure of OneM2M consists of Security Functions Layer, Secure Environment Abstraction Layer and Secure Environments Layer. The layer has the security functions layer via Mac and Mcc which are reference points. It supports six functions such as identification and authentication, authorization, ID management, security association, sensitive data handling and security administration.

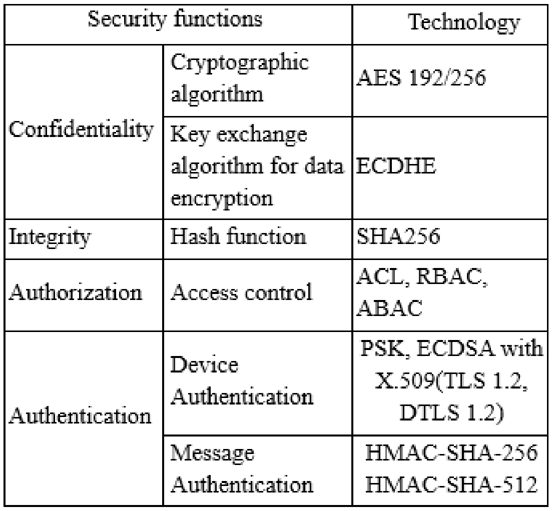
Identification and authentication: The authentication is the process of verification provided by the identification process. The identification is different in accordance with the purpose of the authentication. In case of a resource access, it is recommended to check whether AE (Application Entity) and CSE (Common Service Entity) are registered as a local CSE (Common Service Entity).

Authorization: It plays a role in allowing the service and data to have access to authorized organizations. It is needed to evaluate various access control policies. The authentication evaluation process (ACL, RBAC) allows to sign up for the service after joining an authentic object according to an access control policy related to protection support.

Identity management: It is also referred to as ID management. If the ID is stored under the security environments, the ID is to provide to an independent object necessary for identifying oneM2M and identification. It is used in an independent way without any role related to ID verification.

Security association: It is about physical relations between two nodes connecting with the communications node. It aims to connect safely with the help of safe section settings and security of things.

Table 1 Cryptographic technology for OneM2M



Security functions		Technology
Confidentiality	Cryptographic algorithm	AES 192/256
	Key exchange algorithm for data encryption	ECDHE
Integrity	Hash function	SHA256
Authorization	Access control	ACL, RBAC, ABAC
Authentication	Device Authentication	PSK, ECDSA with X.509(TLS 1.2, DTLS 1.2)
	Message Authentication	HMAC-SHA-256 HMAC-SHA-512

Sensitive data handling: It offers three functions to application layers: 1) functions to safely save data 2) to support encryption features 3) the way for bootstrapping minimum keys.

Security administration: It is about independent environments of security (independent hardware module, reliable integrated execution environments or software protection).

The Secure Environment Layer includes multiple protection environments. Each protection environment contains sensitive data and sensitive functions. The sensitive data involves SE (Security Entity), capability, a security key, a local authentication, and the identification information. This platform employs the key exchange algorithm of TLS 1.2 and DTLS 1.2 versions and exchanges an encryption key. Table 1 shows detailed information.

3.2 Security technology of an open platform for IoTivity

The Open Connectivity Foundation (OCF) is an industry group whose stated mission is to develop specification standard and develops the platform for IoTivity. The platform layer of IoTivity consists of a transfer layer, a framework layer and a profile layer. The OCF is based on a RESTful architecture model and expresses all objects as resources and then provides CRUDN (Create, Read, Update, Delete and Notify) functions. It is designed based on CoAP (Internet Engineering Task Force Constrained Application Protocol) and it can be applied to the light device with low specification and low power [16].

Transports layer: It is partly scalable about various network technologies used in IoT such as Bluetooth, WI-Fi and Zigbee.
Framework layer: It supports data transmission, device handling and data management for various IoT applications.
Profiles layer: It means the application filed of IoT.

The security structure of IoTivity developed by the OCF protects the resource and resource-supporting hardware and software. The OCF describes the way of configuring the existing IoT network or new IoT network with the use of reliable initial settings such as OBT (Onboarding Tool) in order for various devices which use different encryption functions to establish the network. Security standardizations provide security requirements in order to load OCF software on various operation systems or platforms. Table2 offers detailed information [19]. Figure 2 shows the security structure of IoTivity as follows [19]. IoTivity devices consist of the OIC client who uses the service, the client server which provides the service and OIC intermediaries which are responsible for service intermediaries.

IoTivity devices have application resources and application profiles are defined toward each application. Application profiles are composed of SRM (Secure Resource Manager) responsible for access controls and Security Resources. Session Protection can be included to establish a security channel. The OIC client is responsible for an access request action for OIC resources and the access control on resources is executed in accordance with the access control model of an OIC server. The OIC client connects the network with the OIC server which has resources. In order to identify OIC devices, a device ID is used in IoTivity and the network address is mapped as a device ID and then they are connected with the network address.

The security policy of IoTivity is described with the use of a device ID and a security channel is established with the help of DTLS. Mutual authentication and security communications are performed by using an encryption key stored in a local platform. In order for OIC client to access resources, an OIC server identifies and authenticates an OIC client. The SRM (Secure Resource Management) is responsible for the access control in accordance with an access control model. Generally, hardware security functions and data encryption functions are employed to save important resources. In case of using DTLS for the purpose of the data transfer security in IoTivity, data can be saved through encryption by establishing mutual authentication and security channels. The IoTivity platform adopts a key exchange algorithm with TLS 1.2 and DTLS 1.2 versions and shares security keys with each other and then supports encryption algorithms such as AES, SHA and ECDHE. Given Table 3 offers detailed information:

Table 2. OCF Security Features and Descriptions

OCF Security Features	Description
Access Control	Provides a method to manage access control of resources using ACL(Access Control List) and ACE(Access Control Entry)
Onboarding and Security Provisioning	OBT(Onboarding Tool) and initial entry method of OCF device of existing IoT network
Bootstrap process and Security bootstrapping	Provides a way to protect the bootstrap process and bootstrap
Secure Resource Manager	SRM (Secure Resource Manager) plays a key role in providing security. It consists of Resource Manager (RM), Policy Engine (PE), and Persistent Storage Interface (PSI), and includes functions such as resource management, policy enforcement and secure repository management.
Security Credential Management	Provides a way to protect data during identification and communication between OCF devices using public/private keys.
Device Authentication	Provides a way for a server to authentication access to a client.
Message Integrity and Confidentiality	Provides the use of security mechanisms that provide confidentiality and integrity to protect message from attacks such as eavesdropping, tampering, or message repetition that can occur in communication between a server and a client.
Security Resources	Define security resources needed to provide security functions.

IV. Security considerations to establish safe IoT environments

In case of establishing the service based on an open platform as described in Section 3, security could be ensured. However, things to consider would be different in accordance with situations and circumstances where IoT technologies are applied. Therefore, it is required to define security requirements field by field where IoT technologies are applied and draw up the suitable authentication method. In this section, we suggest sectoral security considerations where IoT technologies can be applied such as smart home, healthcare and construction.

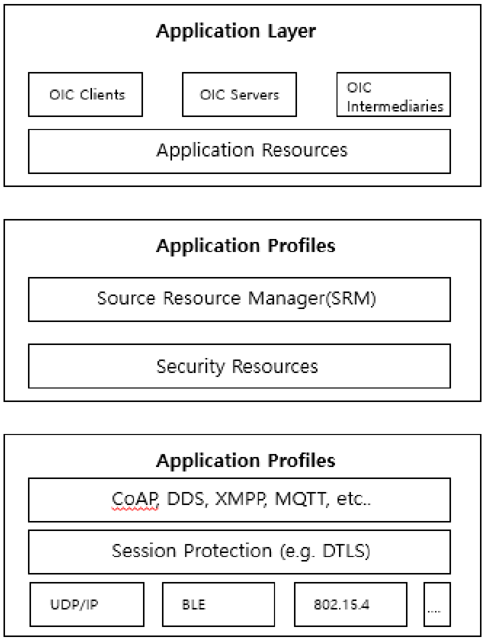
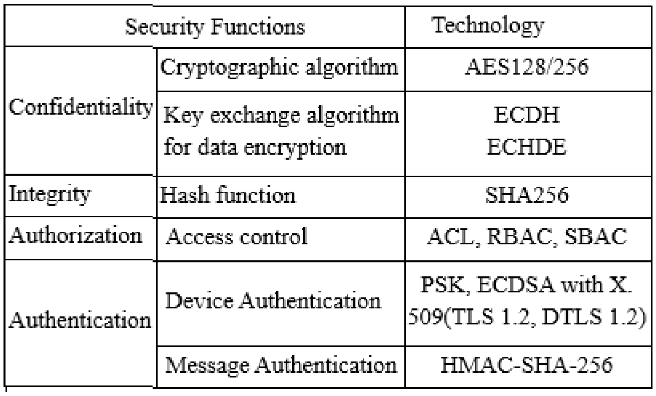


Figure 2 IoTivity Security Structure

Table 3 Cryptographic technology for IoTivity



Security Functions		Technology
Confidentiality	Cryptographic algorithm	AES128/256
	Key exchange algorithm for data encryption	ECDH ECHDE
Integrity	Hash function	SHA256
Authorization	Access control	ACL, RBAC, SBAC
Authentication	Device Authentication	PSK, ECDSA with X. 509(TLS 1.2, DTLS 1.2)
	Message Authentication	HMAC-SHA-256

Smart home field: The smart home service needs to authenticate an authorized user in order to have access to its service and provide a suitable service. The information collected by smart devices can be stored in the Internet or Cloud. In the process of it, the function of confidentiality and integrity via encryption communications shall be provided to ensure a safe channel. The function of protecting personal information in order not to reveal the user's living patterns at home shall be offered. With this in mind, smart home and electronics need to mandatorily conduct the check of security before their launch. After their launch, it is required to apply and distribute a security patch. As to the device where personal information and voice as well as visual information are stored, a user authentication and access control features to protect information shall be applied.

Smart home and electronics built in remote control features shall apply a user authentication and encryption communication features to prevent an unauthorized access. Consistent security checks and update shall be performed for smart applications to be used in a safe manner.

Healthcare field: As smart healthcare deals with personal information and disease history, managing and transmitting data in a safe manner shall be at the top priority. Medical devices which store and process personal information and disease history as well as data processing devices which are interlocked with this shall adopt authentication and encryption function. It is required to regularly check vulnerabilities of medical devices and apply security management system in consideration international norms and manage software safely to prevent illegal forgery. It is also recommended to set up a plan to protect personal information collected and shared by the smart medical service.

Transportation field: The IoT technology can be applied to the transportation system by sharing information on traffic accidents and traffic flows rapidly with the help of the Internet network and controlling vehicles. To ensure safety, following things should be considered. In the process of transmitting the sensing information, in order to prevent traffic accidents due to tampered traffic information, data integrity shall be offered. It is required to support a user authentication and authorization only for an authorized user to be able to have access to a vehicle and control speeds and functions. Data from a vehicle could reveal a user's location and then privacy protection technologies are also needed to prevent the breach of privacy.

Environment and disaster control field: In the environment and disaster fields, integrity is more important than confidentiality of the sensing data generated by a sensor device. Integrity is for preventing artificial forgery from outside. When controlling a sensing device from a control center, integrity and confidentiality on the control command are important. The integrity on sensing information, a command for controlling a device and access control is more important than confidentiality. To this end, encryption technologies need to be used in accordance with the feature of a device and protocols.

Manufacturing field: Sensing and utilizing the information on order, inventory and process is conducted in the manufacturing field. Since a company's secret could be leaked, integrity, confidentiality and privacy protection are important. Existing manufacturing environments are vulnerable to integrity, confidentiality and authentication as well as approval due to the use of each device's protocol. So, security technologies that an existing standardization does not provide shall be offered.

Construction and energy field: The construction field needs to acquire accurate sensing information from unforged or unaltered sensors rather than ensuring confidentiality information sensed by construction/bridge status monitoring and maintenance. Therefore, it is required to provide integrity on sensing data as well as authentication and authorization. The sensors in the construction field are used for a long time and batteries cannot be exchanged frequently. So, light encryption algorithms and protocols need to be considered.

In the energy field, data collection and service are provided based on AMI. Therefore, it is recommended to support data confidentiality and authentication and authorization between a device and a user in consideration of possible information leakage via a device.

V. Conclusion

In this paper, we investigate open platform technologies related to IoT and the application status by field, and analyze the security technology in oneM2M, IoTivity. However, circumstances and situations are different field by field such as smart home and healthcare where IoT technology are applied. So, an open platform can be applied or not. Therefore, we suggest sectoral security considerations in the section 4. Currently, the value of IoT technology has been recognized and the infrastructure to apply various fields has been established. To establish a safe IoT environment, it is necessary to develop and apply technologies considering security consideration in the long term.

Acknowledgments

This work was supported by Institute for Information & communications Technology Promotion (IITP) grant funded by the Korea government (MSIT) (No.2017-0-00267)

References

[1]. AllJoyn, https://allseenalliance.org/

[2]. CRYPTREC, List Guide 2010(Key management), 2012.

[3]. Garnter.Inc, http://www.gartner.com/newsroom/id/ 3165317

[4]. Iotivity, https://www.iotivity.org/

[5]. IETF RFC 5246, the Transport Layer Security (TLS) Protocol Version 1.2, IETF, 2008.

[6]. IETF RFC 6347, Datagram Transport Layer Security Version 1.2, IETF, 2012,

[7]. ISO/IEC 11770-1, "Information technology-Security techniques-Key management", ISO/IEC, 2010.

[8]. ISO/IEC 11770-3, Information technology-Security techniques-Key management-Part 3: Mechanisms using asymmetric techniques, 2015.

[9]. NIST SP 800-57, Recommendation for Key management Part 1: General (Revision 3), 2012.

[10].NIST SP 800-57, Recommendation for Key management-Part 2: Best Practices for Key Management Organization, MIST, 2016.

[11].NIST SP 800-57, Recommendation for Key management-Part 3: Application-Specific Key Management Guidance, NIST, 2017.

[12].NIST SP 800-130, Framework for Designing Cryptographic Key Management Systems, NIST, 2013.

[13].NISTIR 7628, Guidelines for Smart Grid Cyber security, NIST, 2014.

[14].OneM2M, http://www.onem2m.org/

[15].OASIS, Key Management Interoperability Protocol Specification Version 1.2, 2015.

[16].Subash, Ashok, IoTivity-Connecting Things in IoT, TIZEN Development summit, 2015.

[17].IETF, the Transport Layer Security Protocol Version 1.2, RFC 5246.

[18].IETF, Datagram Transport Layer Security Protocol version 1.2. RFC 6347.

[19].OCF Security, OCF Security Specification v.1, OCF, 2016.

[20].Dave Smith, Just Android Things, realm, 2017.

[21].SmartThings Developer Documentation. https://docs.smartthings. com /en/latest/architecture/

[22].TS-0003 Security Solutions-onem2m, www.onem2m.org

[23].Apple iOS-Home. http://www.apple.com/ios/home/

[24].MDS technology, http://www.hancommds.com.

[25].Google nest, https://nest.com

Biographies

EUNYOUNG CHOI received the B.S. degree in Mathematics from Korea University, Korea in 2001, the M.S degree in Information Security from Korea University, Korea, in 2003, and the Ph.D. degree in Information Security from Korea University, Korea, 2009, respectively. Currently, she is a general researcher at Korea Internet & Security Agency in Korea. Her research areas include mobile security, cyber financial security, cryptography and information security. Dr. Eunyoung Choi may be reached at bluecey@kisa.or.kr

HAERYONG PARK RECEIVED the B.S. degree from Chonnam National University in 1999, Chonnam, Korea, the M.S. degree from Seoul University in 2001, Seoul, Korea, and the Ph.D. degree from Chonnam National University in 2006, Chonnam, Korea. Currently, he is a general researcher at Korea Internet & Security Agency in Korea. His research areas include cryptographic algorithm design analysis, cyber black box technology development and cloud service security. Dr. Haeryong Park may be reached at hrpark@kisa.or.kr.

SEUNGHO AHN received the B.S degree from Chonnam National University in 1977, M.S degree from Chonnam National University in 1981, Gwangju Korea, the Ph.D. degree from Cheonbuk National University in 1985, Jeonju Korea. Currently, he is a professor at Department of Mathematics of Chonnam National University, Gwangju, in Korea. His research areas include transformation group and combinatorial topology. Professor Seungho Ahn may be reached at shahn@jnu.ac.kr. He is a corresponding author of this paper.