Authentication Techniques in the Internet of Things Environment: A Survey

Sunghyuck Hong
Division of Communication and Information, Baekseok University
Chungcheongnam-do, Cheonan-si, Dongnam-gu, Anseo-dong 115, Korea
(Email: sunghyuck.hong@gmail.com)

(Received Nov. 2, 2017; Revised and Accepted July 7, 2018; First Online Jan. 30, 2019)

Abstract

The Internet of Things (IoT) enables the offering of services specialized for each client in real time by processing and analyzing the sensor information concerned after storing the sensor information collected from numerous things on the Internet through wired/wireless communications technology. The IoT technology currently applies to various industrial fields including home, medical service, transportation, environmentdisaster, manufacturing, construction, and energy and has been actively researched. The IoT technology closely combined with real life can cause monetary and physical damages to clients by malicious clients through the seizure and falsification of information. Unlike computes and mobile devices, the IoT technology uses micro devices, and therefore lightweight cryptographic techniques with limited storing space are needed. In this regard, this report aims to examine security threatening factors that may occur in the IoT environment and service and to guide authentication techniques by which safe IoT service can be realized. Through this, this research presents a reference guide that can be used by companies or security protocol developers.

Keywords: IoT; Light-Weight Protocol; Secure Authentication; Secure IoT

1 Introduction

1.1 Overview of IoT

IETF, ITUT (MOC), 3GPP (MTC), and ETSI (M2M) defined the security IoT, respectively. Many definitions on the IoT exist, and the IoT concept defined in the CERT-IoT 2009 seems to be most comprehensive and clear. According to it, the IoT is the integrated part of the futuristic Internet and can be defined as a dynamic global network infrastructure equipped with a self-setup function as a mutually compatible communications protocol with standards. Also, CERT-IoT 2009 defines that the IoT consists of self-identifiers, physical things having different characteristics, and virtual things. Upon looking at the definition, things represent a concept containing both physical and virtual things. Here, the examples of virtual things can be software service, software object, and actor as a main player of an act.

Figure 1 shows the concept of IoT [5]. Things, a main component of the IoT, include not only end-devices in the wired/wireless networks, but humans, vehicles, bridges, various electronic equipment, cultural assets, and physical things constituting the natural environment. By expanding the concept of machine to machine (M2M), through which intelligent communications can be conducted between person and machine and between machine and machine using mobile communications network, the concept has evolved into one that can interact with all information in the real and virtual worlds.

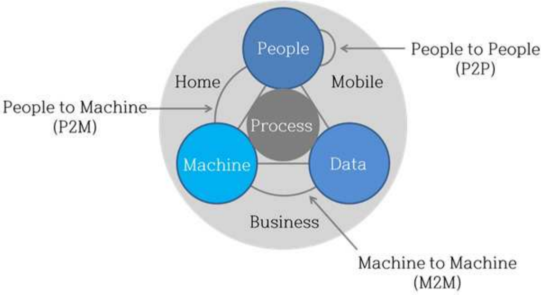

Figure 1: The concept of IoT

1.2 Security-Threatening Factors of IoT

Security threats by component of the IoT are as follows:

- Device layer: This refers to physical threats that include infrastructure paralysis and a threat to life by device suspension and malfunction, information falsification, leakage by the loss, theft, forgery, or falsification of devices, malicious code transition attack thereat between devices, and difficulties to apply IP security technology to lightweight/low power devices.
- Network layer: This refers to information falsification and leakage in the linkage communications process between heterogeneous things networks, damage diffusion due to network and gateway hacking and cross

network devices, and denial of service (DoS) of the IoT by large-scale thingbots.

- Platform service layer: This covers illegal access and attack to platforms by malicious devices/clients, platform collapse according to encryption key hacking after illegal capture, cloud, big data personal information leakage, and privacy infiltration. IoT constitutes specific services by combining various technological factors, such as device, network, and service/platform. Although security technologies to safely protect each technological factor exist, there can be security vulnerability without a method to integrate/link those technological factors.

1.3 Security Technology of IoT

Device security technology needs low power and low weight technologies. Most IoT devices are operated in a low power mode basically and they are low weight devices with low arithmetic operation or storage capacity. Therefore, low power and low weight encryption algorithms considering the performance and required security intensity of low power and low weight IoT devices are needed. Also, a function enduring no-suspension and malfunction, along with a physical threat prevention function, is necessary. Currently a variety of IoT security technologies are being developed worldwide. Low weight cryptographic techniques include PRESENT and KATAN overseas, and LEA and HIGHT domestically. However, the low weight cryptographic techniques developed so far are known to have vulnerability to hacking including auxiliary channel attack. In Korea, ETRI is developing a hardware security module for smartphones [2].

1.4 Network Security Technology

Currently included in the IoT are IEEE 802.15.4 low power communications technology ZigBee as a local area communications technology, IEEE 802.11 wireless LAN technology Wi-Fi whose usage has become universal as it has been used for smartphones, and radio frequency identification (RFID) which is an electronic tag technology adopted for the automatic recognition of things by replacing existing bar codes. As long distance communications technology, 3G or LTE, which are widely used wireless mobile communications modes, are included [3].

- ZigBee: ZigBee has two modes: standard security mode (SSM) for low level security and high security mode (HSM) for high level security. Because each ZigBee device is operated in the open trust mode, reliability of the device is assured. Thus, reliability can be secured if confidentiality and integrity are guaranteed in the communications process between ZigBee devices. However, preparation for a separate security measure is demanded since no encryption is made for all communications sections.Discussion, Implication, and Conclusion;
- Wi-Fi: Wi-Fi is a wireless LAN technology based on IEEE802.11 standard and where high performance wireless communications can be performed. Since communications are conducted in a wireless mode in Wi-Fi, it is especially vulnerable to security threats. If communications data encryption is not conducted in using Wi-Fi, attacks such as wiretapping, snipping, and non-authorized access can occur. As a method to safely protect data in the wireless section, there is a wired equivalent privacy (WEP) authentication protocol presented in the IEEE802.11 standard, and also Wi-Fi protected access (WAP) and WPA 2, which improved WEP's drawbacks, which were proposed in the IEEE802.11i. For security in the access process in addition to the communications process of wireless section, the use of encryption algorithms, such as temporal key integrity protocol (TKIP) and counter mode with CBC-MAC protocol (CCMP), is recommended.
- RFID: RFID is a technology using wireless frequency for the automatic recognition of things and it is based on ISO 18000-7 standard. RFID is a wireless network technology recognizing the tag information attached to things, regardless of physical and visual contacts. It can be the technology receiving most attention recently for the construction of ubiquitous sensor network (USN) environment. Since the passive tag mainly used in the RFID system has limited arithmetic operation capacity and also limitation in the power amount to be used, there is a demerit that high level security technology is difficult to be applied. Being based on wireless communications, RFID is also vulnerable to security threats such as information leakage. As the security requirements in USN, confidentiality and integrity on data communications are required, as well as a safe key control and distribution function. In addition, a safe platform design taking sensor network characteristics into account is needed. Recently, various techniques [8] have been studied for mutual authentication between nodes for data security transmitted in the RFID/USN environment.
- 3G/LTE: Although 3G mobile communications network was a closed structure mainly providing circuit switch, technology-based voice service in the early stage of its introduction, it has gradually evolved into a structure expanding data service in addition to voice, based on packet switching technology. Due to a recent increase in mobile malicious codes, malicious and abnormal traffic of infected terminals is flowing into 3G/4G network. Therefore, a variety of security threats occur. There are many cases in which application of the security equipment used in the existing Internet environment is difficult. Such security equipment has a limitation in that it is difficult to detect or cope with attacks aiming at the unique physical weaknesses of 3G/4G network.

As examined above, security technologies to block attacks, such as infiltration through network or DDoS, are required for IoT service. Studies on the IoT gateway, in order to block infiltration into the IoT network connected with different types of devices and thingbot attack prevention, are evaluated to be at their infant stage. Although Intel, Freescale, and Eurotech developed the IoT gateway, a security control function for the IoT devices and network including real time monitoring or infiltration blocking is not applied.

1.5 Platform/Service Security Technology

The IoT platform/service needs to have an opening structure that can add and develop new services in the mash up type of existing application layer, as well as external sensors or terminals. The relevant studies are actively carried out, centering on the IoT Architecture (IoT-A) project. Mutual authentication, communications encryption, and privacy protection functions between devices, clients, and services need to be provided [16].

As shown in Figure 2, automatic authentication and communications encryption are needed in the IoT without a person's intervention; specifically, a technology offering a new device's service participation registration and key distribution functions to be suitable for service types is necessary. When big data are analyzed by combining various types of sensing information collected in the IoT, a possibility of personal privacy being infiltrated occurs. Therefore, a technology to block automatic personal information collection and non-identification technology are needed in order to prevent personal identification/tracking risk by post-analysis of big data [13].

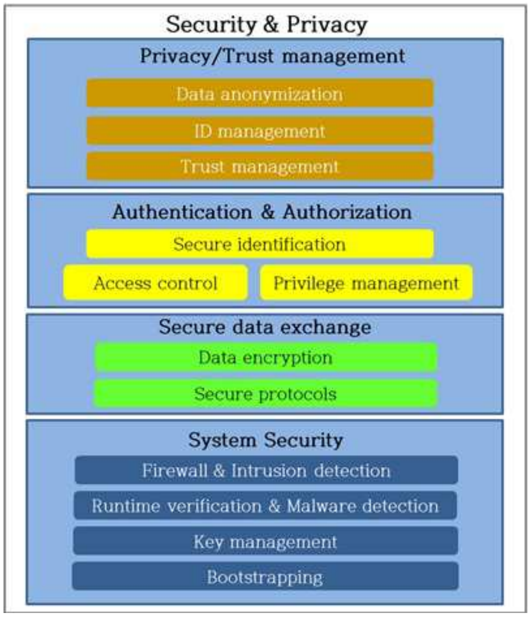

Figure 2: Security technology of IoT service

Although studies on service registration and key control are carried out for IoT equipment authentication, a technology used for user (client) authentication on the existing Internet including PKI is just applied. Even though high growth-applied service fields such as medical service, cars, and home network grow fast, the applied service security technology development is assessed as insufficient.

2 Recommended Encryption Algorithm of Each IoT Component

2.1 Device

A variety of processor platforms are used for the IoT service including 8- and 16-bit processors, which are lightweight devices and 32-bit processor with high performance in terms of IoT devices. Table 1 shows the characteristics of representative processors [6].

To meet confidentiality, integrity, and authentication/authorization, the security requirements in the seven major IoT services (smart home, medical service, traffic, environment/disasters, manufacturing, construction, and energy) should be met by operating symmetric key encryption and open key encryption, which are representative encryption techniques. Concerning symmetric encryption, HIGHT, SEED, ARIA, and LEA (domestic standards), as well as AES (international standard), need to be carried out. Because AES symmetric key encryption offering 128-bit security in the 8-bit processor, for which support is most scarce, requires 0.02ms on average per execution, it is expected to be able to adequately perform encryption/deciphering in the low specs devices.

2.2 Communications and Network

Various processors are used in the IoT devices, while a variety of communications protocols are used as communications stacks. IoT platforms offer various functions, including data control and user (client) and service authentications, so that data sensed from IoT devices can be used by the IoT service. They also have communications interface for communications like Ethernet. As for communications protocols, the IoT platforms support lightweight protocols such as CoAP used in the IoT devices and such protocols as HTTP used in application services. For connection between devices and IoT gateway, wireless communications are mainly used. ZigBee, Bluetooth, Z-Wave, IEEE802.15.4, LoRA, and Wi-Fi are included in the wireless protocols used for the IoT. For the connection between platforms and IoT gateway, REST communications including HTTP and message queuing protocols composed of publication/subscription such as MQTT are used. Between service and platform, protocols such as RPC and SOAP used by mainly API are used so that service can be created through mash-up by the IoT application service [7].

Table 1: Comparison of light and high performance IoT devices

Category	**Atmega128**	**MSP430**	**ARM-Coriex**
Data area	8 bits	16 bits	32 bits
Words	16 bits	16 bits	32 bits
Structure	Harvard	Von Neumann	32 Von Neumann
No. of registers	32	12/16	8/13/16
No. of commands	61	27	56
Core size	6140GE	4913GE	-
Application field	Arduino, Micaz	TelosB	Beagle, Odroid

Table 2 shows standard Encryption Algorithms for Communications/Network.

2.3 Platform

The IoT platform can be an important factor in the IoT environment for data control, client control, and service control and connection between virtual things and physical things. As such, security technology specialized for the platform environment in addition to confidentiality, integrity, and availability, which are the top three security factors in terms of cryptology, should be offered. AllJoyn is an IoT platform developed mainly by AllSeen alliance, centered on Qualcomm. AllJoyn framework consists of Apps and routers. Apps communicate with routers, and the communications between Apps can be conducted through only routers. AllJoyn platform currently supports Bluetooth, Wi-Fi, Ethernet, Serial, and PLC communications, and Zigbee and Z-Wave can be used through bridge software. To offer confidentiality, integrity, and availability (CIA) and authentication in the AllJoyn platform environment, TLS' Pin-code Logon and RSA-based certificate described in RFC5256 are used, and the three factors conduct initial stage communications using SASL. OneM2M recommends 128-bit AES-CBC and AES-CCM to guarantee confidentiality, and recommends the use of HMAC-SHA_256 to assure integrity [9].

3 IoT Authentication Protocol

3.1 ID/Password-based Authentication

This mode serves to store each user's (client's) ID and password in the server's DB, and authentication is carried out on the basis of the stored knowledge. This technology is mainly used in the server/client authentication environment. To prevent authentication disabling due to exposure to the password list stored on the server, there are many cases to adopt a mode storing values through a hash function. To assure higher stability, SSID is hidden, WEP key is used between AP and device, PAP authentication mode is adopted, or RFID mode is used. In the IoT environment, the ID/Password mode has some problems such as server control and load, in light of the IoT environment characteristics where many devices are used without human intervention. Additionally, there is a problem that human intervention should be preconditioned in the device correcting and adding process. The ID/Password mode is not suitable as an authentication technique in the IoT environment since it cannot offer a rejection prevention function [8].

3.2 MAC Address-based Authentication

This is a mode using media access control (MAC) address, which is the identification address allotted to network interface and is mainly used for network access control in the intranet environment. When a device requests access to network, a procedure to authenticate by comparing the MAC address registered in the server and the MAC transmitted with the message requested from the device is undergone. This mode is simpler and more convenient and faster than the ID/Password-based authentication mode. However, there is a need to define a new MAC address style due to the increase of various devices and the advent of IoT, and thus new standards such as EUI-48 and EUI-64 are defined. MAC address is vulnerable to attacks including spoofing due to the absence of separate security equipment as MAC address can be forged [10].

3.3 Code-based Authentication

As a protocol authenticating a thing based on open key codes and symmetric codes, this mode is mainly used for wireless Internet security protocol. This mode supports a variety of standards such as 802.1x/802.11i and WAP. The code protocol-based authentication mode can include such techniques as ID/Password-based authentication, MAC address-based authentication, and certificate-based authentication. By offering various authentication modes, clients can select a suitable authentication mode according to the use environment, and the rejection prevention function is also available according to the adopted code protocol. However, the authentication technique can be connected to vulnerability, if the weakness of code technique is found, because stability is dependent upon code technique [12].

Table 2: Standard encryption algorithms for communications/network

Communications/Network	**Support Codes**
ZigBee (IEEE 802.15.4)	AES-128
Bluetooth (IEEE 802.15.1)	SAFER-SK128, AES-128
6LoWPAN (IEEE 802.15.4, RFC 4919) hline Z-Wave (IEEE 802.11)	AES-128 RSA-1024, ECC-160 TDES, AES-128
LoRA	AES-128
CoAP (RFC 7252)	AES-128 AES-128 ECC-160
MQTT (OASIS MQTT Version 3.1.1)	AES-128, AES-256, TDES SHA-1, AHA-256, SHA-384
DDS (DDS Security V1.0)	AES-128, AES-256 SHA-1, SHA-256 RSA-2048

3.4 Certificate-based Authentication

Certificate-based Authentication is a mode to authenticate through electronic signature using an open key code. Authentication is carried out on the basis of containing the information for e-signature on the certificate. In Korea, through the E-Signature Act enacted in 1999, the certificate issue system and control regulations were devised. Under the top level certification agency, Root CA, the issue and authentication of certificates are conducted through five authentication (certification) agencies. In foreign countries, personal devices and cable model device authentication, WiMAX industrial certificates through Versign's device authentication service, are offered. In addition, certificate-based authentication technique is used in VoIP and network monitoring cameras, and the areas are gradually expanded.

The certificate-based authentication technique offers high stability through powerful authentication technique, and the reject prevention function is also provided. However, device certificate processing software and algorithms require a high level of arithmetic operation processing volume. Therefore, the technique is not suitable to be used in the low power and low performance IoT devices [13].

3.5 Authentication Using IBE

ID-based authentication is an open key code system using a user's (client's) ID, including email address, name, IP address as an open key, and signature, and where authentication is provided. Although there are such merits as pre-key distribution independence, small arithmetic operation volume, and relatively shorter key length, there is a demerit that ID-based authentication is vulnerable to ID sham attack. As a relatively new concept and technique, compared with other authentication techniques, there are various authentication schemes including Hess's Algorithm, Lunn's Algorithm, and Gentry and Silverberg's Algorithm [14].

3.6 Service-based IoT Authentication Techniques

The IoT environment-based smart home service system consists of home server, home gateway, and smart home devices. As for smart home devices that can be connected with the external Internet through mobile communications network like smartphones, they are limited in a type connected to the external Internet through home gateway [15].

3.7 Requirements of Smart Home Service Security

Table 3 classifies and defines the requirements of smart home service security according to the perspectives of confidentiality, integrity, and availability 3.

3.8 Smart Home Security Function

Smart home means a house or home to which the IoT system monitoring a variety of things and environments, controlling them remotely, or automatically controlling them is applied. The smart home service rapidly grows in the fields including smart home appliances control, cooling/heating control, energy use, HVAC control, crime prevention, and child/baby care. At the CES held in Las Vegas in 2015, smart home based on the IoT gained attraction. Table 4 defines the security function requirements to be applied to home server, home gateway, and home devices consisting of the smart home system. Here, smart home device user (client) authentication is addressed. Smart home devices offer useful information and services to clients through a connection between the service provider and devices within a home. In this process,

Table 3: Classifies and defines the requirements of smart home service

Category	**Requirements**
Confidentiality	Safe control is needed so that key information for encryption and deciphering used for a user's (client's) important data and encryption algorithms, transmitted and received between smart home devices, cannot be exposed externally. When the data created from a smart home device need to be transmitted externally, they should be transmitted by converting them into a cryptogram type, not in the form of plain text data. The identifier information, by which smart home devices can be identified, should be safely managed so that the information cannot be leaked externally, copied, or modified. Safe and powerful passwords should be set up for smart home devices, and a function to change the set up password cyclically should be provided. In setting up powerful and complex passwords to a home gateway that connects a smart home device with an external communications network, a security function needs to be consolidated.
Integrity	To maintain the reliability and safety of smart home devices, unauthorized devices or unauthorized user (client) access should not be allowed. Safe control is needed so that key information for encryption and deciphering used for a user's (client's) important data and encryption algorithms transmitted and received between smart home devices cannot be exposed externally. Data integrity should be provided when the data created from a smart home device needs to be transmitted externally. Reliable communications environment needs to be shaped through mutual authentication between the devices consisting of smart home service.
Availability	An external attack detection function that can cope with security threats such as cyber attack and hacking should be created. A security function needs to be offered so that smart home device software update can be safely carried out. A device security policy setup function considering various device characteristics and specifications consisting of smart home service should be provided. Smart home devices need to offer a device control system to cope with the theft, loss, addition, and disposition of smart home devices. Smart home device's status needs to be continuously managed and unnecessary remote access should be blocked. Upon detection of abnormal activity of a smart home device, a suitable action should be taken, and the details need to be recorded.

smart home devices can be protected by the security functions of home server and home gateway primarily; however, to cope with security attacks to smart home devices, security functions including compliance with the security grade of each device, hacking prevention, prevention of ID information duplication, and forgery/falsification prevention should be included [16]. A mutual authentication function between smart home devices also needs to be considered so that a data collection and exchange function can be safely conducted between devices in the IoT environment [17].

- Knowledge-based authentication: Knowledge-based authentication is based on what users know, and the passwords and personal identification numbers that users memorize are included. Knowledge-based authentication is based on the secret information shared by a user and the authentication system in advance, and separate devices are not required mostly. Therefore, the cost to build the system is very small, and it is convenient for clients to use, and thus the knowledge-based authentication utilized as a general authentication means a lot. However, there is a drawback in that authentication intensity is weak.

- Possession-based authentication: Possession-based authentication is a mode based on what a user possesses. The characteristic of the possession-based authentication is that users need to use the physical device that the user must possess in the medium used in authentication. Out-of-brand (OOB), OTP token, and open key token authentication are recently used a lot as the authentication means used for possession-based authentication.

- Bio-based authentication: Bio-based authentication is based on the user him/herself and what the user uses, namely, personal physical characteristics classified biologically according to users. Bio-based authentication includes fingerprint, glottis, retina pattern, iris pattern, face shape, palm type, and hand shape. The examples used by clients are signature, which is called behavioral biometrics, and key input pattern perception. Bio-based authentication technique's security is high, and its convenience is also high because it always possesses bio means, compared with possession-based authentication technique. However, system management and construction costs become high because of the high cost of perception devices to perceive body information. Due to such a reason, bio-based authentication is not widely used generally.

3.9 Authentication Techniques for Medical Service and Health Care

The convergence of medical service and ICT is the service including e-health and u-healthcare and has evolved to the mode by which medical service can be offered anywhere and anytime through ICT technology in terms of hospital and treatment environment. Smart healthcare rising recently means a more complex and intelligent level by adding welfare and safety to medical service. As an environment evolves, in which individuals can manage or control exercise amount, meal calories, and sports activity records, the service, provider, and user (client) scopes are expanded [12]. The smart healthcare industry includes hardware such as wearable healthcare devices, and software including healthcare apps, communications and data platforms for healthcare information delivery, and linked medical service.

3.10 IoT – Threats to the Security of Smart Healthcare

- Device hacking: Device hacking refers to the hacking control software that controls hardware, rather than hardware hacking. The control software controlling hardware is generally called firmware. The scope of firmware may mean the OS and also the boot loader uploading the OS to the software. Generally, device hacking means giving the control right of applications to a hacker by hacking OS from various firmware.

- Threats to network security: In the smart healthcare environment where electronic medical devices and wired/wireless network are combined, existing TCP/IP-based security threats and sensor security threats exist.

- Bio-based authentication: Bio-based authentication is based on the user him/herself and what the user uses, namely, personal physical characteristics classified biologically according to users. Bio-based authentication includes fingerprint, glottis, retina pattern, iris pattern, face shape, palm type, and hand shape. The examples used by clients are signature, which is called behavioral biometrics, and key input pattern perception. Bio-based authentication technique's security is high, and its convenience is also high because it always possesses bio means, compared with possession-based authentication technique. However, system management and construction costs become high because of the high cost of perception devices to perceive body information. Due to such a reason, bio-based authentication is not widely used generally.

- Threats to personal information infiltration from service perspective: Security measures for authentication have not been devised on sharing scope, reading/examination restriction, security auditing, and bio information exposure when a patient's personal information and medical information are shared for patient relocation or cooperative treatment. In Korea, incidents that not only leak medical information by hacking, but those that may harm life by capturing hospital information system, occurred (August 2013). A variety of medical information within domestic hospitals was collected by overseas servers, and hackers could manipulate prescriptions randomly by seizing PCs within the hospitals, in addition to medical information leakage.

Because the IoT is used as wearable devices a lot, it needs to be smaller in consideration of design, and there is a limitation that hardware performance becomes lower. Therefore, negligence can occur to security, while basic functions offering can be concentrated. In reality, damages occur gradually due to the IoT device hacking.

3.11 IoT – Information Protection Measures for Smart Healthcare

When communications are conducted with other devices in the IoT environment, the identification and authentication on whether the data are transmitted from the proper devices should be conducted. As for device authentication mode, ID/PW, certificate, and SIM are used. As for ID/PW mode, it is the most basic authentication mode, and separate application and protocol are required for ID/PW authentication between the administrator and device, and personal information needs to be shared in advance. Concerning certificate-based mode, a PKI-based device certificate is widely used. It is safe to use RSA (2,048 bits) and hash function SHA-2 (256 bits) or higher. SIM mode is an authentication mode using USIM or UICC mounted on the terminals, and studies on the mode are actively conducted as communications between devices have been made possible through mobile communications network recently. Since 2011, standardization has been carried out from ETSI and 3GPP starting the embedded SIM Project from GSMA. In Korea, various pilot projects are performed through the participation of mobile carriers such as KT and SKT.

In the IoT, measures to apply TLS, DTLS, IPsec, HIP, and PANA that were applied to the Internet environment to prevent security threats are considered. Specifically, the application of DTLS to a core protocol, CoAP, is set as a basic direction [6]. To apply existing IP-based security protocol, lightweight algorithms are needed in consideration of a device's calculation capacity and memory space. As the method to make DTLS protocol lightweight, there are methods like reducing the number of hand shake messages or simplifying authentication process on the certificate. The initial shaking process is delegated to the owners of resource-limited devices to reduce the hand shaking message packets. The device owners and each device share secret keys safely in advance and form a DTLS session with the server. The device owner encrypts the DTLS session information with pre-shared secret key to the device, transmits it, and closes the session. After that, the complex initial stage hand shaking process can be conducted on behalf of the device owner by resuming each session between the device and server. The proposed system, however, has a burden to upload DTLS protocol to the device for DTLS session resumption between the device and server, and thus compressed IPsec is used through various studies [1,4,11].

4 Conclusions

The service markets of the IoT are expanded through convergence and compound with various industries. Many studies on security technology in the seven major IoT industrial fields are carried out: Smart home, medical service, transportation, environment/disasters, manufacturing, construction, and energy. The authentication techniques addressed in this report have applied the cryptographic techniques supported in the fields concerned, and they are presumed to be used as baseline data in developing authentication techniques in each field.

Acknowledgments

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIP) (NRF-2017R1A2B1003394).

References

[1] D. Chatzopoulos and P. Hui, “Asynchronous reputation systems in device-to-device ecosystems,” in *2016 IEEE 17th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM’16)*, pp. 1–3, June 2016.

[2] F. Corso, Y. Camargo, and L. Ramirez, “Wireless sensor system according to the concept of iot -internet of things-,” in *2014 International Conference on Computational Science and Computational Intelligence*, vol. 1, pp. 52–58, Mar. 2014.

[3] D. M. Dobrea and M. C. Dobrea, “Concepts and developments of an wearable system - an iot approach,” in *2017 International Symposium on Signals, Circuits and Systems (ISSCS’17)*, pp. 1–4, July 2017.

[4] J. Furtak, Z. Zieliński, and J. Chudzikiewicz, “Security techniques for the wsn link layer within military iot,” in *2016 IEEE 3rd World Forum on Internet of Things (WF-IoT’16)*, pp. 233–238, Dec. 2016.

[5] R. Galambos and L. Sujbert, “Active noise control in the concept of iot,” in *Proceedings of the 2015 16th International Carpathian Control Conference (ICCC’15)*, pp. 133–137, May 2015.

[6] P. P. Lokulwar and H. R. Deshmukh, “Threat analysis and attacks modelling in routing towards iot,” in *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC’17)*, pp. 721–726, Feb. 2017.

[7] J. Marconot, F. Pebay-Peyroula, and D. Hély, “Iot components lifecycle based security analysis,” in *2017 Euromicro Conference on Digital System Design (DSD’17)*, pp. 295–298, Aug. 2017.

[8] S. A. Nauroze, J. G. Hester, B. K. Tehrani, W. Su, J. Bito, R. Bahr, J. Kimionis, and M. M. Tentzeris, “Additively manufactured rf components and modules: Toward empowering the birth of cost-efficient dense and ubiquitous iot implementations,” *Proceedings of the IEEE*, vol. 105, pp. 702–722, Apr. 2017.

[9] J. Ni, K. Zhang, X. Lin, and X. S. Shen, “Securing fog computing for internet of things applications: Challenges and solutions,” *IEEE Communications Surveys Tutorials*, vol. 20, pp. 601–628, 2018.

[10] S. M. A. Oteafy and H. S. Hassanein, “Resilient iot architectures over dynamic sensor networks with adaptive components,” *IEEE Internet of Things Journal*, vol. 4, pp. 474–483, Apr. 2017.

[11] A. Pfitzmann, B. Pfitzmann, M. Schunter, and M. Waidner, “Trusting mobile user devices and security modules,” *Computer*, vol. 30, pp. 61–68, Feb. 1997.

[12] K. Rostamzadeh, H. Nicanfar, N. Torabi, S. Gopalakrishnan, and V. C. M. Leung, “A context-aware trust-based information dissemination framework for vehicular networks,” *IEEE Internet of Things Journal*, vol. 2, pp. 121–132, Apr. 2015.

[13] H. Shuang and Y. Z. Author, “A study of autonomous method of iot component,” in *The 5th International Conference on New Trends in Information Science and Service Science*, vol. 2, pp. 294–298, Oct. 2011.

[14] S. N. Swamy, D. Jadhav, and N. Kulkarni, “Security threats in the application layer in iot applications,” in *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC’17)*, pp. 477–480, Feb. 2017.

[15] A. Syed and R. M. Lourde, “Hardware security threats to dsp applications in an iot network,” in *2016 IEEE International Symposium on Nanoelectronic and Information Systems (iNIS’16)*, pp. 62–66, Dec. 2016.

[16] P. Urien, “Introducing tls/dtls secure access modules for iot frameworks: Concepts and experiments,” in *2017 IEEE Symposium on Computers and Communications (ISCC’17)*, pp. 220–227, July 2017.

[17] T. Yu, X. Wang, and A. Shami, “Recursive principal component analysis-based data outlier detection and sensor data aggregation in iot systems,” *IEEE Internet of Things Journal*, vol. 4, pp. 2207–2216, Dec. 2017.

Biography

Sunghyuck Hong Currently, he is an associate professor in Division of Information and Communication at Baekseok University, and he is a member of editorial board in the Journal of Korean Society for Internet Information (KSII) Transactions on Internet and Information Systems. His current research interests include Blockchain, Secure Mobile Networks, Secure Wireless Sensor Networks, Key Management (Group Key Agreement Protocol), Networks Security (Authentication), Information Security, Embedded Networked Systems, Embedded Software, Wireless LAN, Distributed Systems, Computer Networks, Hybrid Wireless Network Architecture Design, and Mobility Design/Modeling/Simulation. To God, Gloria In Excelsis Deo.