Authentication and Access Control Methods for Secured Smart Home IoT Service Environment

Sei-Youen Oh, Aeri Lee

Abstract: ***The development of the Internet of Things has increased the interconnections between things, and the IoT has been applied not only to our everyday life but also to various industrial fields. A variety of services are being developed for many people to use for the IoT environment. More focus is also being put on the smart home service market which applies the IoT to the residential space - an area close to an area close to their everyday life among the IoT services. Though the smart home service market is growing and being used in a variety of fields, security threats exist - such as data fabrication and falsification, illegal authentication and privacy violation. When the device data of the smart home becomes exposed to the security threats, there is also a risk of a secondary damage due to the nature of the smart home environment. Therefore, this paper proposes figuring out related security threats and requirements for a safe access to the smart home system in the IoT environment, as well as safe authentication and access control methods. It is expected that the analysis of the stability and efficiency of the proposed methods will be used as the base research on the security in the rapidly-growing smart home service environment.***

Keywords: Authentication, IoT device, IoT Services, Internet of things

I. INTRODUCTION

The IoT (Internet of Things) refers to a technology or environment in which products with IT-based technology such as sensors or actuators are combined with things to get connected to things, people and space through wireless communications. Thanks to the development of network technology, smart sensors and devices, the IoT has continued to get a lot of attention and showed development over recent years, we are getting near the hyper-connected society which various things and people are connected to the internet. The IoT is being used in our daily lives as well as various industrial fields. Korea, major countries in the world and global companies are also jumping into aggressive investments in and development of the IoT. This move is bringing the development of a variety of services using the IoT. And it is the smart home service among all those services that can be most accessible to our everyday life. With the application of the IoT technology at home - residential space- the smart home provides services allowing the user to control the power to in-home appliances remotely or to adjust its temperature to the desired level while staying outside home, helping make life more convenient. In spite of the recent smart home market continually growing in size, the smart home has smart devices connected based on network communications, which allows the presence of security threats - such as the third party can gain access by being disguised as the user or device with a malicious intention, or can be involved in fabrication or falsification by intercepting the protocols being transferred on the network. If a malicious attacker gains access to the smart home network, makes sure nobody is home using the home cam and opens the door lock, it could incur an financial loss from the break-in and work even as threats leading to a critical accident by controlling the gas valve.

To prevent such security threats from happening, security solutions must be applied to the smart home. In particular, a user authentication must be provided for an attacker not to be able to be disguised as the user or device. In order to solve a vulnerability where an attacker can get the authenticated session by fabricating himself/herself as a legitimate user through a replay attack, it is necessary to have security technology that prevents the replay attack and provides the user authentication, as well as control technology for the prevention of an abnormal approach to the device. This paper proposes authentication methods to improve safety and efficiency between the user and the device as well as control techniques to allow an only authorized access while considering security requirements smart home services in the IoT environment. It conducted an analysis of the safety about proposed methods. This paper consists of the following. Chapter 2 deals with studies with regard to the smart home and smart home security threats and Chapter3 describes methods proposed in this paper. Chapter 4 conducts an analysis of the safety regarding the proposed methods and Chapter 5 reaches a conclusion.

II. RELEVANT STUDIES

A. Overview of Smart Home Services

Smart home is a term that refers to a concept that including IoT-based smart home - such as appliances, energy management, network, security, heating, cooling and ventilation, home entertainment, as well as solutions and related services used for interlocking and controlling a variety of smart devices. The IoT here refers to computer communication networks that share information created by several objects, among these, the smart home can be referred to as interlocking with appliances, lighting energy, security devices as well as smart cars, smart cities and smart education. In one word, the smart home is the very human-centered living space that makes their

Revised Manuscript Received on July 22, 2019.

Sei-Youen Oh, Department of Police Administration,Semyung University, Jecheon, Republic of Koreay. Email: s092724@naverl.com

Aeri Lee *, Department of Computer Education, Catholic Kwandong University, Gangneung, Republic of Korea. Email: allee@cku.ac.kr

quality of life far better by providing a wide range of various information and services. This then enables economic convenience, health and welfare improvement and safe living through converging information and communication technology with our living environment, without being restricted to space and devices[1-3].

The smart home is connected to the outside internet through wired or wireless network infrastructure and in-home wireless internet becomes active. The use of this network can enable a variety of smart devices such as in-home lighting devices and energy consuming devices to communicate. The communications on a smart device comply with communication standards between IoT terminals. Control devices such as smartphone or tablet PC can enable the users to access and control the smart home. The applications installed on the control device allow the users ultimately to be able to receive a variety of contents based on in-home smart devices[4-6].

B. Smart Home Service Security Threat

Smart home environment controlled by the user consists of three types of object - the legitimate user capable of controlling in-home devices, the home gateway inside smart home and the smart device. A variety of security threats may arise because the use of smart home service is based on the environment where the user should be connected to the smart home network through a control device such as smartphone or tablet PC. Its leading examples involve intercepting the data over the network to fabricate or falsifies the data, DDoS attacks, system hacking and leaks of personal information due to the loss of a terminal [7-9].

1) Data Leakage

Smart home environment is where the user can share data by accessing the smart home through the wireless network from the outside and can download as needed. Thereby, an attacker can access the smart home through an unauthenticated device and cause a data leakage. When an attacker collects information and leaks smart home data, it may cause a matter of privacy and lead to a secondary damage. This cannot guarantee confidentiality of the critical data saved in the smart home.

2) Data Fabrication and Falsification

Smart home data reaches the use through wireless network. As an access to smart home through wireless network becomes possible, the attacker may fabricate or falsify data along the way. The attacker can intercept data and cause a malfunction through data fabrication and falsification or can intercept user's message in the middle of communications to manipulate the message, which enables the manipulation of the smart home system. This means there is no guarantee on the integrity of the critical data saved in the smart home or of the device.

3) Unauthenticated Access

When sending or transmitting data through wireless network in smart home environment, an attacker can access the smart home with an unauthenticated device to insert a malicious code in the data device. The smart device with the malicious code inserted sends malicious emails and can turn into a zombie smart device which can provoke DDoS attacks. Furthermore, a malicious code can be inserted into the smart home device installed on the camera to generate a privacy violation. These types of cyber attack is continually on the rise and poses a critical security threat to smart home users.

C. C. Analysis of Smart Home Security Requirements

In smart home environment, there are the presence of security threats, such as data fabrication and falsification, illegal authentication and a privacy violation. Therefore, security techniques to counteract the threats are needed to be studied. The following shows an analysis of security requirements for secure communication in smart home environment :

1) Data Confidentiality

In the smart home communication environment, sensitive information which can violate privacy such as personal information control messages is transmitted through the network. When data is disclosed, it may cause a variety of security issues, such as a privacy violation and potential secondary damage. Therefore, it is required to encrypt data before send or receive it during communication so an unauthenticated person may not know the content of data.

2) Data Integrity

In the smart home communication environment, the access of a malicious device through wireless network allows messages and data of smart home devices to be fabricated and falsified. Message fabrication and falsification may lead to a device malfunction, confusing the user. Therefore, messages and data transmitted in the smart home environment should be secured so they cannot be fabricated or falsified by the access of an illegal advice.

3) Access Control

The smart home communication environment does not allow an unauthenticated user to gain an indiscriminate access. An unauthenticated access brings a variety of security threats such as data fabrication and falsification, data leakage and a privacy violation. Thereby, it is required to distinguish all access authorities such as read or modify using data access control. Besides, in smart home environment where sensitive information is included, a data authority should be distinguished to control an access from an unauthenticated user.

4) Device Integrity

A smart home device can be accessed both through the network and physically, therefore, it is necessary to have a device prepared to protect it. In addition, an attacker can insert malicious software and modify its usage through a malicious code. If the integrity of the device is not guaranteed, it may result in its turning into a malicious device. What's worse, the smart home system itself may be infected by the malicious code and consequently the availability of the smart home system may be damaged. Therefore, it is necessary to secure the integrity of the smart home device.

5) Device Authentication

In the case of smart home devices, many of the devices are used without considering security and this enables unauthorized smart devices to gain access through wireless network. When a destroyed and duplicated smart home device accesses, it is likely that it may be used with a malicious intentions - such as inserting a malicious code or polluting smart home communication environment. On top of this, when an attacker is disguised as a normal device, the user may not use the device in normal condition. Therefore, an authentication on the smart home device should be provided[10-11].

III. PROPOSED METHODS

Here are proposed methods : A secured smart home gateway provides an access control over all smart devices registered in the smart home. The smart home gateway performs secured communications through the device-based group key and provides a permission to the authorized access to offer secured and convenient services.

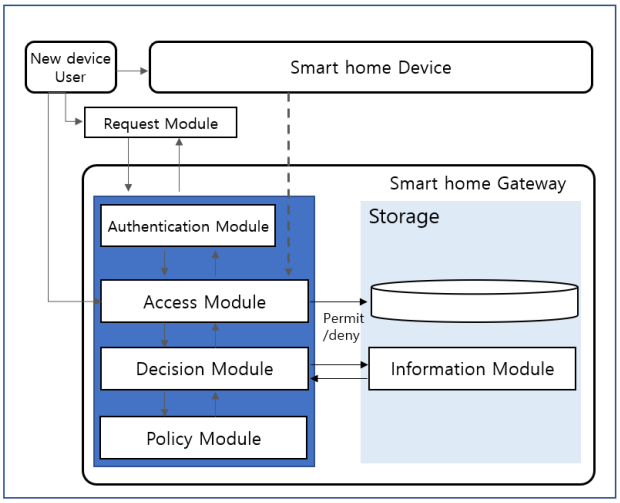

Fig 1. Proposed Methods

Fig. 1 as shown below demonstrates authentication and access control methods for secured smart home IoT service environment proposed in this paper.

Ways to propose include RM (Request Module) for a user authentication and an authority request and authentication modules, access modules, decision modules, policy modules and data storage. RM exists either in USER or smart home devices, while authentication modules, access modules, decision modules, policy modules and data storage exist in the smart home gateway.

- User's Smart Device: Refers to a person in use of the service by access the smart home from the outside, performing an authentication request for a user device to the smart home gateway through the smart device.
- Smart Home Devices: Refers to a device which creates and collects data in smart home environment. A smart home device includes not only in-home TV, a refrigerator and Wi-Fi, but also smartphones and tablets enabling the user to access the smart home from outside home. The smart home device plays a role in transmitting the data created and collected to the smart home gateway. In addition, the device works as sending the user's message and receiving data for the requested message.
- Smart Home Gateway: The smart home gateway is a system the whole system in smart home environment, such as authentication, data processing and access control. The smart home gateway consists of authentication modules, access modules, decision modules, policy modules and data storage.

A. Authentication Module in Smart Home Environment

An authentication module proposed consists of three phases - the initialization phase of a new smart home device based on the group key, the registration phase where a group key is created by listing the smart home device in the smart home gateway, and the connecting phase where the user is authenticated and communicates with the smart home device.

1) Notation

Parameters used in the proposed methods are shown in Table 1 below.

Table- I: Notation

GW	Smart home Gateway
D1, D2	Smart home Device
ID_D_i	Identifier of Smart home Device
ID_GW	Identifier of Smart home Gateway
DI_i	Device Information of Smart home Device i
pw_GW	password of Smart home Gateway
pw_D_i	password of Smart home Device i
h( )	Hash function
GK	Group Key of Smart home

2) Initialization Process

The process of generating the key involves first registering the smart home device in the smart home gateway to generate a secret key for one smart device and smart home gateway.

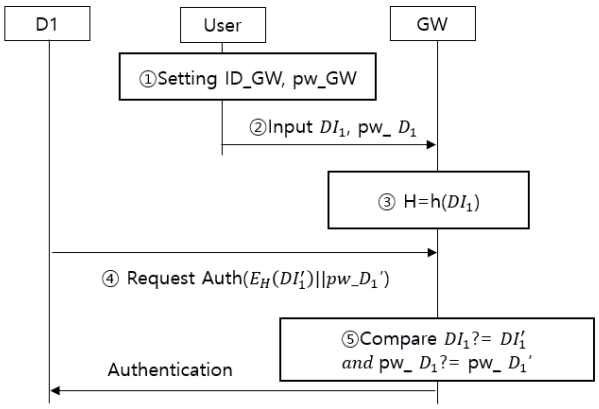

Fig 2. Initialization Process

① The user sets a username of and password to the smart home gateway.

② The user makes an direct access to the smart home gateway with the username and password set in the previous phase and enters information about a new smart home device (Unique serial number and device information) and the password.

③ When a single smart device exists in smart home, the smart home gateway hashes smart home device information to generate a value for the secret key

and store it.

④ A new smart home device transmits the encrypted value and password of the device information using hash values for device information to request an authentication to the smart home gateway.

⑤ The smart home gateway compares between the information and password stored on the smart device and the information and password on the hashed device requested for an authentication, before authenticating the device.

3) Registration Process

The process of registering the smart home device involves listing a new smart home device on the smart home gateway and generating a group key.

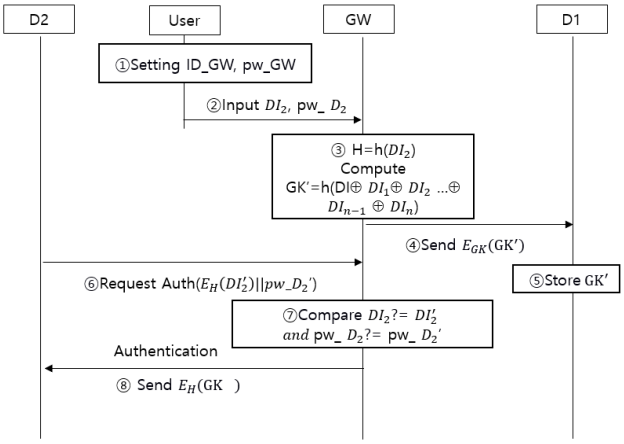

Fig 3. Registration Process

① The user makes an direct access to the smart home gateway with the username and password set in the previous phase and enters information about a new smart home device (Unique serial number and device information) and the password.

② The smart home gateway hashes smart home device information, generate and store it.

③ The smart home gateway puts information about a new device and even information about the existing device in XOR operation to generate a new smart home group key.

④ The smart home gateway sends a new smart home group key encrypted with the existing smart home group key to the existing smart home devices.

⑤ The existing smart home device stores a new smart home group key.

⑥ A new smart home device transmits the encrypted value and password of the device information using hash values for device information to request an authentication to the smart home gateway.

⑦ The smart home gateway authenticates the device through comparing the information and password stored on the smart device and the information and password of the device requested for an authentication.

⑧ A new smart home device stores a new group key and ends the communication.

3) Connecting Process

Refers to a process of connecting sessions for the user to be able to send messages or receive data after accessing the smart home.

① In order to access the smart home gateway and smart home device using the mobile device registered from the outside, the user uses a smart home group key to encrypt the time stamp value and a random numerical value to prevent mobile device information and user's request messages and their retransfer from occurring, then transfers it in connection with an authorized password.

② The smart home gateway, in order to check out the validity of a time stamp, compares the difference between the time when receiving the time stamp and the threshold value of transfer delay time.

③ The smart home gateway authenticates the device through comparing the information and password stored on the smart home gateway and the information and password of the device requested for an authentication.

④ When the time threshold and the password to mobile device information are not consistent and fail to be authenticated, disconnect the communication, whereas when successfully authenticated, an encrypted message and random numeric value with a group key is sent to the smart home device.

⑤ The smart home device is decoded to identify the user message.

⑥ The smart home device transmits a random numeric value to the mobile device to get confirmation of its legitimacy.

⑦ The smart home device connects its session with the mobile device and communicates with the user using verified SSL protocols.

B. Access Control Module in Smart Home Environment

①The unauthenticated device should perform its authentication through the authentication module process.

②Anaccess requestor sends an access request to the access module.

③The access module creates an access control decision request according to details about the access request from the access requestor and sends it to the decision module.

④The decision module sends the access policy request based on the access decision request to the policy module.

⑤The policy module finds out all applicable access control policies as to details about the access request and sends the policies to decision module.

⑥The decision module sends the attribute request to the information module, if attribute information is needed, in judging access control policies.

⑦The information module searches for requested attribute information to the decision module.

⑧The decision module determines whether to allow access using access control policies and attribute information.When there are several applicable policies, the decision module calculates final access control decisions using policy combining algorithm.

⑨The decision module sends final access control decisions to the access module.

⑩The access module runs access control decisions.

IV. ASSESSING SAFETY OF PROPOSED METHODS

Smart home retains sensitive information capable of privacy violations such as personal information control messages, therefore its confidentiality should be guaranteed. The smart home architecture proposed in this paper allows a group key to be distributed through hash values for device information. Therefore, a device not registered on the smart home server is incapable of decoding a group key. Also, now that the disclosure of one smart home device leads to failing to know the information value of another device, there is no way to decode the smart home group key. The group key is used to have data encrypted for data transmission and reception, therefore, it provides data confidentiality. In this respect, the proposed method offers confidentiality.

In smart home communication environment, sensitive personal information exists, thus any attempts for access to an unauthorized device should be intercepted. The smart home security architecture proposed in this paper enables only an authorized smart device to gain access. This is why data should not be disclosed and a primary authentication becomes possible through the device user authentication. Furthermore, an unauthorized access can be intercepted through the smart home access control module. As shown above, the smart home security architecture proposed in this paper helps acquire data in secure manner.

A smart home device allows an attacker to insert malicious software or modify its usage with a malicious code and infect the communication network. The methods proposed in this paper deal with storing the hash values by hashing smart home device information to provide the integrity for device information added or modified to smart home. In addition, any smart device not registered on smart home cannot gain access and there is no way to know a group key because hash values of all smart devices keep secured even though they acquire information about one smart device.

On the rise are zombie smart devices that generate zombie smart device DDoS attacks which insert a malicious code through an access to an unauthorized smart device and then send malicious emails. The system proposed in this paper is capable of blocking the access of au unauthorized smart device by each device in the first registration process sharing a smart home group key on the server and storing it. It also provide an authentication on the device.

V. CONCLUSION

At present, IoT technology both at home and abroad is rapidly expanding into industrial fields. However, security threats that occur due to applying this new technology to conventional industrial fields without the consideration of security are reaching a critical level. The IoT technology is rapidly applying to smart home environment in recent years, but it raises growing concerns about privacy violations of individuals and families. Therefore, it is needed to strengthen security for smart home IoT environment. In particular, when an access between IoT devices is not controlled in home IoT environment, it may lead to privacy violations and an obstacle to the development and expansion of IoT business. While security threats in IoT environment are increasingly growing and evolving, it is very urgent to set up countermeasures for an authentication in IoT environment and access control. However, technologies to control the device access in the current smart home environment stay at a beginner level where a device is authenticated with access control after registering a device ID. More should still be done to control mutual access to IoT devices while considering user environment, prevent security-related accidents from occurring and to protect privacy.

This paper deals with an analysis of security requirements in smart home environment and proposes authentication and access control methods for safe smart home IoT service environment. Proposed methods include group-key based communication techniques and data management methods. Proposed techniques involves operating information about each device, hashing it and authenticating the device based on the generated group key and controlling the access from a malicious smart device to provide safe smart home environment. On top of this, proposed methods are also expected to be applied to a variety of environments because they are also applicable to lightweight system based on low power by using the group key.

At present, studies related to smart home are actively underway not only in Korea but also in foreign countries. As smart home retains sensitive information, secured communication is very important. Thus, it is expected that authentication and access control methods in favor of safe smart home IoT service environment proposed in this paper will be of help with development and research with respect to safe smart home environment.

REFERENCES

1. K.Nikos, P.Eleni, P. Andreas. “Survey in smart grid and smart home security Issues, challenges and countermeasures”, IEEE Communications Surveys & Tutorials, Vol.16, No.4,2014,pp.1933-1954
DOI: https://doi.org/10.1109/comst.2014.2320093
2. Dae-Hwi Lee and Im-Yeong Lee. “A Study on Enhanced 3PAKE Scheme against Password Guessing Attack in Smart Home Environment”, Journal of the Korea Institute of Information Security & Cryptology,Vol.26,No.6, 2016, pp.471-481.
http://www.ndsl.kr/ndsl/commons/util/ndslOriginalView.do?cn=JAKO201606557486772&dbt=JAKO&koi=KISTI1.1003%2FJNL.JAKO201606557486772
3. Ho-seok Ryu and Jin Kwak, “Group Key Management Method for Secure Device in Smart Home Environment”, Journal of the Korea Institute of Information Security & Cryptology, 25(2), 2015, pp.479-487.
http://www.ndsl.kr/ndsl/commons/util/ndslOriginalView.do?cn=JAKO201514751644742&dbt=JAKO&koi=KISTI1.1003%2FJNL.JAKO201514751644742
4. D.Hussein, E. Bertin, V. Frey. “A Community-Driven Access Control Approach in Distributed IoT Environments”, IEEE Communications Magazine, Vol.55,No.3, 2017, pp.146-153.
DOI: 10.1109/MCOM.2017.1600611CM
5. J.Nin, J. Herranz,” Privacy-Aware Access Control in Social Networks: Issues and Solutions. Privacy and Anonymity in Information Management Systems”, Springer London, 2010, pp.181-195. DOI:10.1007/978-1-84996-238-4_9
6. S. Gusmeroli, S. Piccione, D. Rotondi, “A capability-based security approach to manage access control in the Internet of Things. Mathematical and Computer Modelling”,Vol.58,No.5-6, 2013,pp.1189-1205
DOI : 10.1016/j.mcm.2013.02.006

7. Yoon, Seokung; Park, Haeryong; Yoo, Hyeong Seon, "Security issues on smarthome in IoT environment. Computer science and its applications", Springer, Berlin, Heidelberg, 2015,pp.691-696. DOI: https://doi.org/10.1007/978-3-662-45402-2_97
8. Sivaraman, Vijay, Et Al, "Network-level security and privacy control for smart-home IoT devices", In: Wireless and Mobile Computing, Networking and Communications (WiMob), 2015 IEEE 11th International Conference on. IEEE, 2015, pp.163-167. DOI: https://doi.org/10.1109/wimob.2015.7347956
9. Ting Jiang, Ming Yang, Yi Zhang, "Research and implementation of M2M smart home and security system", Security And Communication Networks., 8(16), 2015, pp.2704-2711. DOI 10.1002/sec.569
10. Shen Jian, Wang Chen, Li Tong, Chen Xiaofeng, Huang Xinyi, Zhan Zhi-Hui, "Secure data uploading scheme for a smart home system", Information Sciences, 453, 2018,pp.186-197. DOI ; 10.1016/j.ins.2018.04.048

AUTHORS PROFILE

Sei-Youen OhShe received the Ph.D. degree in Police Administration from Dongguk University. Korea in 2009. She is now a professor in Department of Police Administration, Semyung University, Korea. Her research interests include criminology, IT Conversions

Aeri Lee*She received the Ph.D. degree in Computer Engineering from MyongJi University.Korea, in 2007. She is now a professor in Department of Computer education, Catholic Kwandong University, Korea. Her research interests include networks and security, IT Conversions, coding education