International Journal of Engineering & Technology, 7 (3.34) (2018) 602-605

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Study of an Authentication Methods for IoT Services

Aeri Lee[1]

[1]*Departmentof Liberal Arts, Catholic Kwandong University, Gangneung, Korea*
[*]*Corresponding author E-mail: allee@cku.ac.kr*

Abstract

The Internet of Things refers to an intelligent technology and service in which information is mutually communicated between men and things and between things by connecting all things based on the Internet. Recently, as the connections accelerate among heterogeneous terminals, networks, and applications through the opening of IoT platforms, many technical and managerial security threats occur in the IoT environment. To deliver information accurately and securely in the IoT environment, it is getting very important to solve the problems of the safe authentication system. This study proposes an efficient authentication method for IoT services and analyzes its safety.

Keywords: *internet of things, Authentication, IoT device, Blockchain, IoT Services*

1. Introduction

The Internet of Things (IoT) is a technology in which all things are connected to the Internet, intelligent relationships are formed, e.g. mutually cooperative sensing and networking without human intervention and information is exchanged and processed in real time. IoT is applied to real life, such as Smart Grid, Smart Factory, and Smart Home. These IoT application technologies provide human with convenience while there may be various security risks in privacy or physical damage due to data manipulation without solving security problems[1].

Because of various environments and fields, not all IoT devices that have various performances do not provide safe security functions. Continuous security threats occur in the communication between heterogeneous devices, and various security vulnerabilities are found. In addition, even if they are equipped with security functions, low-performance IoT devices provide low-level security functions due to the limitation of hardware performance or are not equipped with security functions. Due to the absence of security functions like the lack of these authentication functions, IoT devices are infected, and attacks targeted at IoT devices increase, e.g. DDoS attacks occur. Especially, in the IoT environment, by the approach to unauthorized devices at the communication interval, various attacks exist as vulnerabilities of the IoT environment, such as Replay Attack, which leaks information and reuses information, Relay Attack, which replays the authorization value and Middle Attack, which intercepts and manipulates data[2,3].

Therefore, in the IoT environment, since the authentication process between things occurs frequently, the right authentication method is needed. It is necessary to introduce a lightweight and safe authentication system due to the characteristics of IoT. To provide a safe IoT service, devices must be authenticated.

This study proposes a technique for the authentication of devices using a blockchain-based ticket so that it can be applied to the network environment for IoT services. The proposed technique generates a ticket for authentication, using the characteristics of devices, stores it in a blockchain and uses it for the authentication of the devices. This method is safe from possible attacks in the IoT environment and provides mutual authentication between devices and the gateway, and between devices, and the user and the server share a session key for safe communication after the completion of authentication.

This study consists of the following. Chapter 2 describes related studies such as IoT service platform, device authentication and characteristics of the blockchain. Chapter 3 proposes a blockchain-based method for the authentication of devices for IoT services. Chapter 4 analyzes safety, and Chapter 5 states the conclusion and the direction of the future studies.

2. Related Studies

2.1. Internet of Things

The device platform constituting an IoT service can be classified into three layers, including device layer, gateway layer, and service layer[4]. The device layer consists of devices with various performances and functions, and each device communicates, using various network protocols with other devices or gateway, such as Wi-Fi, Bluetooth, Zigbee and wireless LAN. The gateway layer provides a service that connects the device layer with the service layer. The performance and function of the IoT gateway can vary depending on the use. There are various gateways, including simply, a low-power lightweight gateway that collects and bypasses information sensed in devices and a high-specification gateway that manages sensors and provides various security functions. The service layer is the layer that provides the functions necessary for the performance of various IoT applications, which mainly includes the functions of data processing and information storage.

Various sensors and devices used in the IoT environment are important elements in terms of function and security. There are various kinds of device, the subject that transmits data in the communication environment, and its topology may be changed frequently. Thus, since it is exposed to various security threats, it

is essential to get ready for them. It is very important to authenticate devices belonging to each IoT environment domain so that devices with limited performance can deliver accurate information[4].

There are many constraints and difficulties in the precise authentication and detection of the devices used in the IoT environment without the user's direct intervention and manipulation, and there are many limitations in satisfaction with security requirements, which differ depending on the circumstances[5]. Authentication is a mechanism that verifies the legitimacy of devices that connect to the server through a network and an essential security requirement to provide a safe service[6,7]. To detect and authenticate the right devices in the IoT environment, the following authentication technologies are used. In general, ID/PW-based authentication technology, MAC address-based authentication technology, and password-based authentication technology are often used, and considering environmental characteristics, challenge/response-based technology according to the network environment and temporary password-based authentication technology based on a mathematical algorithm are used, too[8,9].

2.2. Blockchain

A blockchain is a technology utilized in several crypto-currencies like Bitcoin, using security technologies such as digital signature, public key and a hash function, which allows the maintenance of security. The blockchain is a distributed ledger technology in which transactional information is not managed in the centralized server, but distributed and shared to all participants who participate in a blockchain network. As transactional information is distributed to a P2P network and managed by the participants, network participants can jointly record and manage it, and they can verify forgery and tampering of transactions through the block-chaining[10].

In the block header of each block, the hash value that can detect the previous block header connected to the relevant block is included, and the overall blockchain structure is constructed, referring to this hash value. The more the block that constitutes the chain structure, the more the security against the forgery and tampering of transaction information and data in the relevant block becomes, and the more the safety provided by the blockchain becomes[11]. For the ownership transfer, a verification step is made, which can prevent the forgery and tampering of transactions through the transaction process and hash value[12,13]. The chain structure of each block in the blockchain is like the [Figure1].

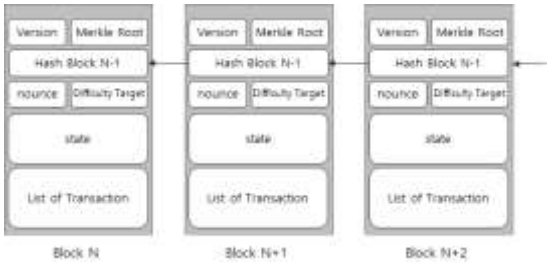

Figure 1: Blockchain structure

3. The Proposed Method

The proposed method controls various IoT devices and registers an authentication ticket, which consists of a gateway that can perform authentication, IoT devices that actually perform actions and a blockchain that can store transactions like an authentication ticket in the block. The overall system consists of the steps of key generation, device authentication ticket generation, ticket registration, and authentication. In this paper, we follow the notation of [Table 1].

Table 1: Notation

GW	Gateway
D1, D2	IoT Device
GI	Device Information of Gateway
DI_i	Device Information of IoT Device i
Kp_D_i	Private key of Device i
Ku_D_i	Public key of Device i
Kp_GW	Private key of Gateway
Ku_GW	Public key of Gateway
r	Random number
h()	Hash function

IoT devices authenticate each node through the authentication process. Also, the block once generated is shared by the devices, which is a merit of the blockchain, so utilizing the fact that it is difficult to manipulate the information, authentication information in each device is stored in a blockchain-based distributed database. Then, utilizing the information of the blockchain, reliable data communication is made possible between devices.

Step 1: key generation

①A device generates a pair of public key and private key. It extracts device information (device unique number, device attribute, device ID, etc.)

②The device hashes its public key and encrypts it with the private key to create the message. And sends the message and the public key to the gateway.

③The gateway verifies the message from the device and stores the device's public key. [Figure 2] shows the process of key generation step.

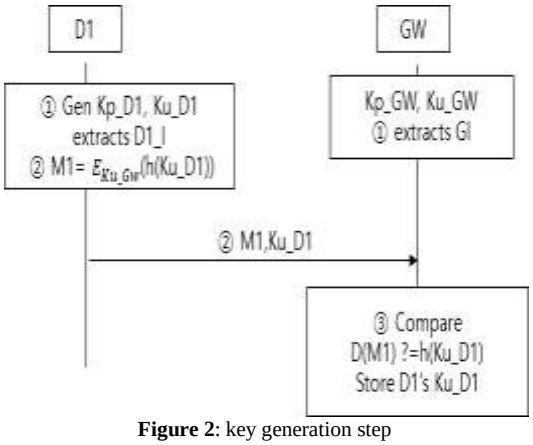

Figure 2: key generation step

Step 2: The step of authentication ticket generation

The step of authentication ticket generation is the procedure for generating a ticket that can authenticate whether an IoT device is a legitimate device. [Figure 3] shows the process of this step.

①The gateway generates a random number for authentication ticket generation. It hashes its public key. It generates a message by encrypting the random number and its public key hash value with the device's public key.

It sends the message and its public key to the device.

②The device verifies the message transmitted from the gateway, extracts the random number

③For the ticket generation, first, it hashes the device's authentication information and generates a digital signature, using its own private key.

④ A ticket for authentication is generated. The ticket includes a device ID, a gateway ID, an electronic signature, a hash value, and a time stamp.

⑤The device encrypts the ticket and the random number and transmits it to the gateway. The encryption of a ticket uses a random number as a symmetric key and encrypts it, and a random number is encrypted using a public key of a gateway.

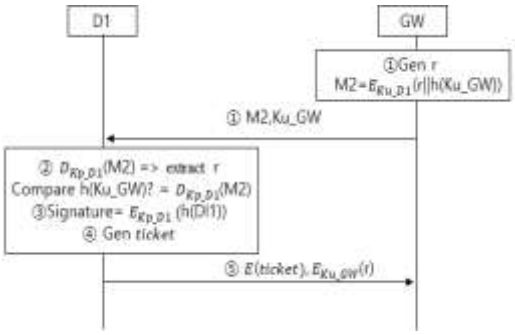

Figure 3: authentication ticket registration

Step 3: authentication ticket registration

The authentication ticket transmitted from the device is verified. [Figure 4] shows the process of ticket registration step.The generated transaction is shown in the [Figure5].

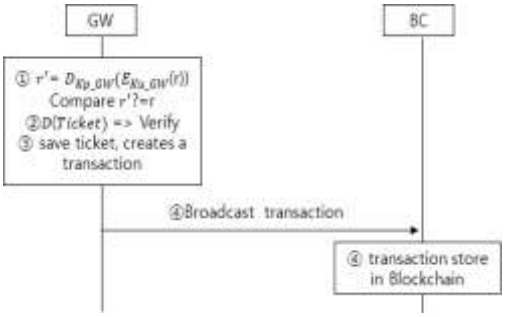

Figure 4: authentication ticket registration

①The gateway decrypts the message with its private key. and verifies whether the decrypted value is the same as its own random number.

②The encrypted ticket is decrypted with a verified random number, and verification is performed

③The gateway verifies the ticket, saves the ticket, and creates a transaction with the device's public key already stored.

④ Create a block chain and store the transaction in a block chain. When the authentication ticket registration is completed, the transaction is broadcast to the block-chain network.

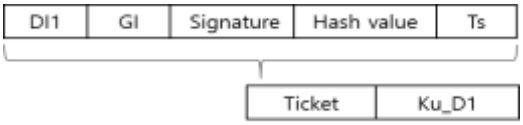

Figure 5: Transaction

Step 4: Authentication

The step of device authentication is the procedure for performing authentication between the gateway and IoT devices, or between devices.

When a device would approach another device through the gateway, the device transmits a ticket to the gateway. The gateway decodes the authentication ticket received from the device and extracts information such as Device ID, Gateway ID, digital signature and hash value. The extracted information and the value of the authentication ticket registered in the blockchain are extracted, and the device authentication is performed, by comparing the two values.

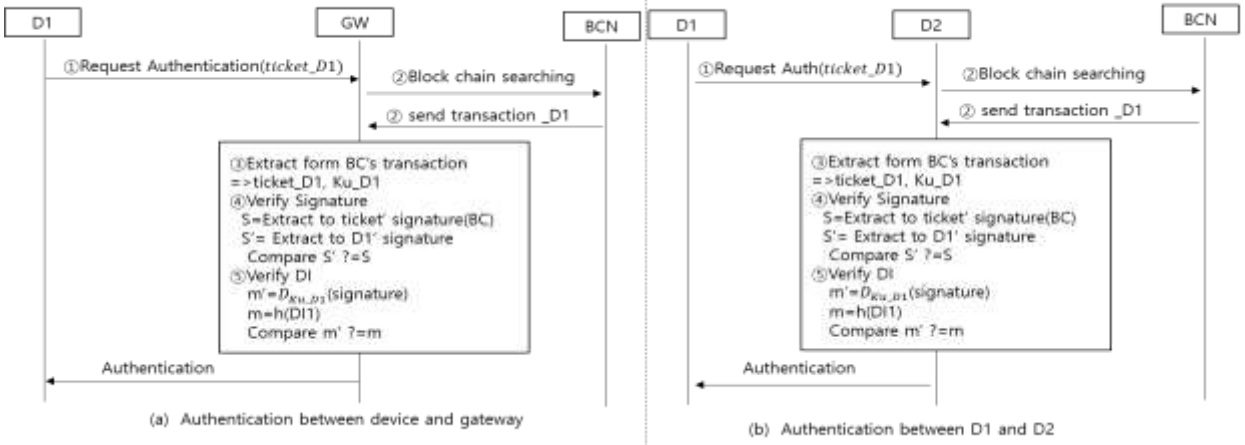

Figure 6: Step of Authentication

1) Authentication between device and gateway

The device performs the verification of the authentication ticket received from the gateway and authenticates the gateway through this. From the ticket received from the gateway, authentication information like the digital signature is extracted and compared with the information extracted from the ticket of the gateway registered in the blockchain to verify the gateway. [Figure 6](a) shows the method for the verification between the device and the gateway.

①The device transmits its own ticket to the gateway and requests authentication.

②The gateway retrieves the block-chain network and obtains a transaction of D1.

③The gateway extracts the ticket and public key of D1 from the transaction.

④The gateway verifies the S of the block chain ticket by comparing the S of the ticket received from the device.

⑤Compares the value obtained by decoding the Signature using the device's public key and the result of hashing the DI in the ticket received from the device.

In the same way as the previous task, the device can authenticate the gateway on the device by verifying the gateway authentication ticket using the block chain. As a result, the device and the gateway are mutually authenticated

2)Authentication between devices

All devices get the first authentication ticket verified through the gateway and have a blockchain distributed from the gateway. The authentication between devices without the gateway is performed as follows:

① D1 requests the D2 to authenticate with its own ticket

② D2 verifies the received authentication ticket of D1 using the

ticket of D1 stored in the block chain.
In Device 1, the authentication information is extracted from the ticket registered in the block chain, and the same value is also extracted from the ticket transmitted from the device, and the device is authenticated.
As a result, the two devices can make mutual authentication without a gateway. [Figure 6](b) shows the method for the verification between the device1 and device2.

4. Evaluation of the Safety of the Proposed Method

The authentication method for IoT services proposed in this study utilized the blockchain technology to meet security requirements for the authentication of IoT devices. In the proposed method, the authentication ticket generated in each device can generate a block according to the device's own characteristics. This chapter evaluates the safety of the proposed method.
First, IoT devices generate device authentication information through a hash value like their attribute information and make transactions with that to broadcast to the blockchain network. If IoT devices are exposed to malicious attacks by attackers, the device's own information such as device property information and kernel code is forged and tampered. In the proposed method, when IoT devices generated an authentication ticket, a hash value was added to the blockchain and ticket for the integrity verification. The information generated based on the information transmitted from the devices, infected by malicious attackers or forged or tampered is not the same as the integrity verification information stored in the blockchain transactions previously integrity, so the verification of the device integrity fails. Like this, the integrity of devices can be guaranteed through the hash value of their authentication ticket and blockchain transactions.
Second, in the authentication technique, Replay Attack is an attack in which the authentication request message transmitted for authentication from a normal device previously is collected and stored by an attacker, and then, the authentication request message collected in a session is transmitted, and it is authenticated as a normal device. Attackers can collect authentication request messages easily. Therefore, the authentication technique should be designed safe from Replay Attack so that an attacker would not be authenticated as a normal device. The proposed method registers a ticket generated from a device to the blockchain to perform authentication. In each authentication process, each time, a different random number is generated to generate a session key, so it is safe from Replay Attack.
Third, Man-in-the-Middle Attack is an attack of disguising as a device or authentication server, intercepting all messages between the device and the server in the middle of a device and an authentication server. Man-in-the-Middle Attack illegitimately modifies data, generates fabricated data and transmits the data, so it is an aggressive attack that can give a serious blow to a server or device. The proposed method can prevent Man-in-the-Middle Attack, using the blockchain technique and a new random number generated each time. Thus, the proposed technique is safe from Man-in-the-Middle Attack.
Fourth, this method was proposed for mutual authentication, and based on this, the mutual authentication can be made safely through the registration of a ticket using the blockchain technique. A device can directly receive identification from the terminal that they would access, based on the ticket. The terminal is identified through digital signature, and the relevant device can make identification legitimately when it makes a request for identification legitimately by checking the ownership of the private key corresponding to the public key in which the device belongs to the ticket. By this, mutual authentication is possible between the device and the gateway, and between devices.

5. Conclusion

Because of various environments and fields, not all IoT devices that have various performances do not provide safe security functions, and because of the communication between heterogeneous devices and environments, new security threats and security vulnerabilities occur in addition to the existing security threats.
This study proposed a method for the authentication of devices applying blockchain for safer IoT services. The proposed authentication protocol can prevent disguise as a malicious gateway or illegal devices by providing mutual authentication between the gateway and the device and can protect the secret key of the devices against the damaged gateway. The proposed authentication method generates, distributes and manages information for authentication as a block, so it has integrity, is safe from Replay Attack and Man-in-the-Middle Attack and can be effectively applied to the IoT environment, providing mutual authentication between devices. The more the IoT devices, the more the traffic to perform authentication with the IoT devices in the gateway becomes, which may lead to the problem of increasing overhead, as well. Thus, in the future, a study will be conducted on measures for the reduction of the traffic between IoT devices and the gateway.

References

[1] J. Granjal, E. Monteiro, J.S. Silva.(2015). Security for the internet of things: A Survey of existing protocols and open research issues. IEEE Commun. Surv. Tutor, 17(3), 1294-1312.
[2] Young-Seok Lee.(2015), Authentication Method for Safe Internet of Things Environments. The Journal of Korea Institute of Information, Electronics, and Communication Technolog, 8(1), 51-58.
[3] P. de Leusse, P. Periorellis, T. Dimitrakos, and S.K. Nair.(2009). Self managed security cell, a security model for the internet of things and services. In Advances in Future Internet, 2009 First International Conference on, 47-52.
[4] Chung Yong Sik, Cha jaesang. (2017). IoT device security check standard. The Journal of The Korean Institute of Communication Sciences, 34(2), 27-33. http://www.ndsl.kr/ndsl/commons/util/ndslOriginalView.do?cn=JAKO201713547379949&dbt=JAKO&koi=KISTI1.1003%2FJNL.JAKO201713547379949
[5] N. Mahalle, B. Anggorojati, N. R. Prasad and R. Prasad.(2013). Identity Authentication and Capability Based Access Control(IACAC) for the Internet of Things. Journal of Cyber Security and Mobility, 1(4),309-348.
[6] Mitchell, C.J., Chen, L.(2002), Comments on the S/key User Authentication Scheme. ACM Operating Systems Review. 30(4).
[7] L. Lamport.(1981), Password authentication with insecure communication, Communications of the ACM, 24(11), 770-772.
[8] PawaniPorambage, Corinna Schmitt, Pardeep Kumar, Andrei Gurtov and Mika Ylianttila.(2014). Two-phase Authentication Protocol for Wireless Sensor Networks in Distributed IoT Applications, IEEE Wireless Communications and Networking Conference(WCNC), 2728-2733.
[9] Yeh, T.C., Shen, H.Y., Hwang, j.j, "A Secure One-time Password Authentication Scheme Using Smart Cards," IEICE Trans. Commun. Vol. E85-B. No.11. Nov. 2002.
[10] Minhaj Ahmad Khan, Khaled Salah.(2018). IoT security: Review, blockchain solutions, and open challenges. Future Generation Computer Systems 82,395-411
[11] Satoshi Nakamoto.(2008). Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf
[12] Yu Zhang, Jiangtao We.(2016),The IoT electric business model: Using blockchain technology for the internet of things. Peer-to-peer networking and applications, 10(4), 983-994
[13] NirKshetri.(2017). Can Blockchain Strengthen the Internet of Things.Institute of Electrical and Electronics Engineers, 19(4), 68~72.