A Comparative Study on Biometric based Authentication Method for IOT Service

Aeri Lee

Abstract: ***Along with the development of high-tech information and communication technologies, the Internet of Things (IoT) is drawing attention as a core technology of the Fourth Industrial Revolution because the IoT is linked to all industrial sectors. All things are connected to the Internet and automated without the intervention of humans. Furthermore, they provide intelligent services to change the overall lives of people. The development of IoT technology has improved the convenience of everyday life. However, on the other hand, it has raised issues in the aspect of security such as personal information leakage, data forgery, and personal information infringement. The IoT has suffered from privacy issues because it collects and generates data. It reflects that authentication is a very important element in the IoT. This study proposed a safe authentication method that can mutually authenticate with various objects by using the biometric information of a user and the information of a device in the IoT environment. The performance analysis has also proven that it is a safe and efficient technique.***

Keywords: internet of things, Authentication, IoT device, Bio information, IoT Services

I. INTRODUCTION

The Internet of Things (IoT) refers to the provision of services in new forms between things. It is possible because the IoT connects tangible and intangible things. In the past, home appliances such as refrigerators, televisions, washing machines, and medical devices in various forms were not connected to the internet. However, they are now connected to the internet for exchanging information with each other. They can analyze the information and various devices are connected with each other through the information. It is the IoT. In other words, it means to apply the communication and information, which were only needed between people, to a range of devices. It is a concept extended to things. As services are changing and infiltrating into the life of people in the IoT environment, many experts are expecting that the IoT technologies will penetrate into our daily life deeply. The IoT has been applied in the actual life: smart grid, an intelligent transportation system, smart home, and telemedicine are good examples. Although these IoT application technologies can provide convenience to people, they can risk personal-level and national-level securities and cause physical damages such as privacy and data fragmentation unless the security issues are fully resolved. Therefore, the range of application can be limited.Therefore, it is necessary to study the security system considering the efficiency and security of the IoT. The IoT can be divided into a large number of object devices that structurally acquire information, a gateway that collects them, an application-based database, and a user. A secure authentication method is required for users to share necessary information securely. [1-3]

This study proposes an authentication method that can mutually authenticate diverse nodes and objects through biometrics and device information in the IoT environment. This study proposes the authentication between the gateway and a user, the authentication between the IoT node and the gateway, the registration method for communication, and a safe and efficient mutual authentication method between a user and a node based on the registered gateway.

This article is composed of as follows: Chapter 2 will explain the IoT service platform, conventional authentication methods, Chapter 3 biometric-based authentication for the IoT services; and Chapter 4 analyzes safety; and Chapter 5 describes the results and future study directions

II. RELATED STUDIES

2.1. *Internet of Things*

The IoT means a complex network and computing environment that collects, stores, and processes information by connecting devices, people, physical space, and data through the internet. The concept of the IoT is defined differently according to each organization. However, these definitions are similar. The existing definition of the IoT is "to exchange information with other objects on its own without the direct intervention of a person when a thing exchanges information with a thing or computer systems including a server or with people." The key of the IoT architecture is to define and design the relationship between each component, starting from the interface design, which is the connection relationship where the IoT components interact, from the perspective of the entire IoT service. Based on the entire IoT architecture, the functions necessary for the interactions between components adjacent to IoT devices are designed[4-5]. [Figure 1] shows the architecture of the IoT.

Revised Manuscript Received on May 22, 2019.

Aeri Lee, Department of Computer Education, Catholic Kwandong University,25601, Korea
allee@cku.ac.kr

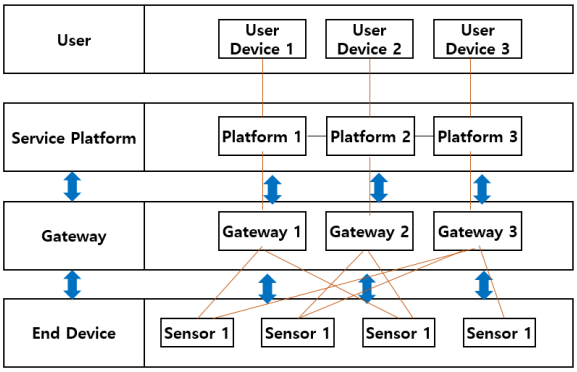

Figure 1.IotArchitecture

The IoT means a complex network and computing environment where regular devices, data, people, and space are connected to the internet network environment to process, create, and store information. Although various advantages and conveniences are provided beyond the convenience and applications of the existing computing environment, diverse security threats, which did not exist, are generated as well. The user authentication is very important in the IoT network. Consequently, only legitimate users can access the IoT node during the service. Since the node or sensor of the IoT network has limited resources in terms of processing power and memory requirements, the node or sensor can provide and manage data or information quickly by adding a gateway node, which has rich resources for supporting a limited node or sensor[6].

2.2.User Authentication

One of the important considerations in terms of the security of the IoT environment is user authentication technology that can authenticate the user's correct credentials. It is one of the most important security technologies because a lot of damages have been reported due to the illegal access of unauthorized users. There are mainly three types of technologies that can check and authenticate the user's identity in general. Depending on the applied technologies, they are classified into knowledge-based technologies, ownership-based technologies, and Biometric-based technologies. Each authentication method has different characteristics in terms of convenience and security[7].

2.1.1. Knowledge-based Authentication

Knowledge-based authentication has the best utilization and is the most widely used authentication mechanism. The password authentication method is a good example of it. The knowledge-based authentication method is based on what a user knows and specific information that a user memorizes is used as a medium having the authentication effect. A password, a personal identification number (PIN), and a passphrase are representative examples of the medium. Knowledge-based authentication is based on confidential information that is shared between a user and an authentication system in advance. In most cases, it does not require a separate device. Therefore, it does not cost much money to construct it and it is convenient for a user to use. Consequently, it is frequently used as an authentication method. However, the authentication strength is weak, which is a shortfall of this method[7].

2.2.2 Ownership-based Authentication

Ownership-based authentication is a method to authenticate a user's identity using a tool that the user owns. A user must have the medium used for the ownership-based authentication at the moment of authentication. The medium includes a smart card, an authentication token memory card, and a USB drive. Ownership-based authentication is a technology to authenticate a user based on whether the information on the medium owned by the user is the same or not. When the information is identical, it confirms the identity of the owner (user) of the information and authenticates the user. Although the ownership-based authentication has higher security than the knowledge-based authentication, the cost of implementing the system is relatively high, which is a shortfall of this method. Out-of-band (OOB) authentication, OTP token authentication, and public key token authentication are the most commonly used techniques as the ownership-based authentication[8-9].

2.2.3 Biometric-based Authentication

Biometric-based authentication is a method of using the biometric information of a user who asks for authentication, unlike knowledge-based and ownership-based methods. It checks the identity of a user by classifying the biological characteristics possessed by the person. The Biometric-based authentication can use fingerprints, voiceprints, retina patterns, iris patterns, facial shapes, and hand shapes. Signatures and keystroke patterns, which are behavioral elements of a user, can also be used.

The Biometric-based authentication technology provides higher security than the knowledge-based and ownership-based technologies. Moreover, it is very convenient because it can immediately use the biometric information of a user without using any separate memory and ownership. However, the cost of establishing separate recognition equipment and system management is high because it requires recognizing biometric information without an error. It is used in limited and less common fields, compared to the knowledge-based and ownership-based methods[10].

III. A PROPOSED METHOD

This chapter will propose a secure authentication method that can use various nodes by utilizing biometric information of a user and the information of a device in the IoT internet environment. This study proposes a safe and efficient technique that mutually authenticates between a user and a node by authenticating between a gateway and a user and between an IoT node and a gateway based on the registration method for communication and the registered gateway. The proposed multi-component biometric user authentication method consists of Two steps. Registration Step and Authentication Step. we

follow the notation of [Table 1].

Table 1: Notation

GW	Gateway
IDUi	Identifier of User i
IDNj	Identifier of IOT Node
IDG	Identifier of Gateway
OID	Object identifier
Sg	Secret parameter of Gateway
Sgn	Secret parameter between GW and node
Sgu	Secret parameter between GW and User
BI	User biometric information
TS	Timestamp
ri,	Random number
h()	Hash function
SK	Session key between user and node

3.1 Registration Step

3.1.1. Registration between User and Gateway Node

In this stage, a user attempting to access the IoT service through a device must register with the gateway.

When the registration is successfully completed, the user can mutually authenticate with the IoT network nodes. This step is illustrated in [Figure2].

①User generates information. (Random value, user biometric information, user OID, etc.).

②Users calculate M1 = h (pw || ri || ts), M2 = h (IDUi || ri|| ts) and M2 = h (BI|| ri|| ts) and transmits it to the gateway.

③Gateway computes Mu1 = h (M1 || Sg) and Mu2 = h (M2 || Sgu). Mu3 = Mu1⊕Mu2 and transmits it to the user.

④The user saves this message.

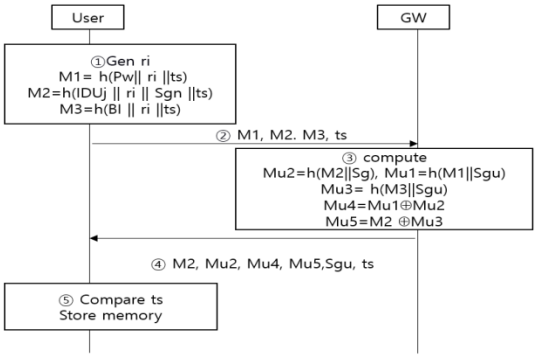

Figure 2. Registration between User and Gateway

3.1.2 Registration between Gateway and IoT Node

This step executes the registration between the gateway GW and the IoT node. Since the IoT network can be dynamically incremented due to the added IoT device at any time, it is needed to add a node to a network dynamically. This process is described by [Figure3]. The next step is performed while registering the IoT node Nj with the gateway GW.

①IoT node generates random number. The node computes M4=h(IDNj || rj || Sgn ||ts), M5=rj⊕Sgn, M6=M3⊕ M4

②node sends M4, M5, M6 and timestamp to gateway

③Gateway checks timestamp.

④The gateway verifies the value received from the node.

⑤M4= M6⊕M4 , M5'=Sgn⊕M4, M4'= h(M5' || IDNj||sgn) If the M3 received from the node is the same as the M3' calculated by the gateway, the node is regarded as legitimate, and if not, a registration reject message is sent to the node.

⑥The gateway calculates Mj1=H(IDNj || Sg), Mj2=H(M4 || Sgn), Mj3=Mj1⊕Mj2

⑦The gateway transmits Mj1, Mj2, Mj3 and ts to the node.

⑧After receiving the message from the gateway, the node compares the time stamp with the time stamp sent by the node and stores it in its memory if it arrives within the legitimate time.

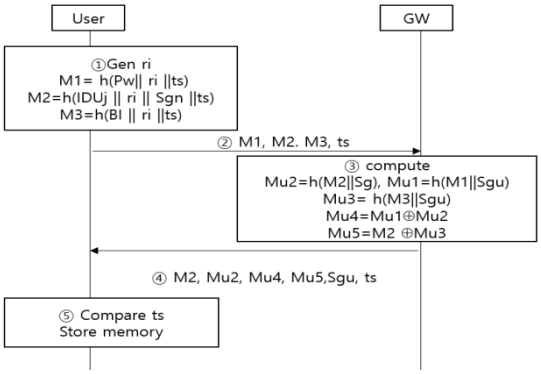

Figure 3. Registration between Gateway Node and IoT Node

3.2. Authentication Step

The next step is regarding the mutual authentication technique when receiving the service. In this authentication technique, a user approaches a node to authenticate it for using an IoT service. In the above registration step, a user approaches a node registered with a gateway through the registered gateway. In this step, the user and a node generate a disposable shared password session key. Once agreed, it is possible to communicate securely using the session key.

3.2.1. Authentication request

[Figure 4] shows the authentication Request steps of the proposed system.

①The user runs the IoT application and inputs the IDUi ', PW', bio identification BI '. The user's device then computes the input M2' = h (BI' || ri) , M1' = H (PW * || ri)

②User's smart device computes Mu2 '= H (M2' || Sgu).

③Compute Mu1 = Mu2⊕MU4, Mu3 = Mu2⊕M5

④Verify whether the Mu1 and Mu3 values are the same as the calculated Mu1 'and Mu3'.

⑤When verification is performed, MKU = H (Mu1 || Mu3 || Sgu || TS1) is calculated and nonce n is generated. MKN = n x i is calculated. The user Ui selects the IoT node Nj that provides each service and sends the message to the IoT nodes M2, Mu4, Mu5, MKU, MKN, TS1 through the non-secure channel.

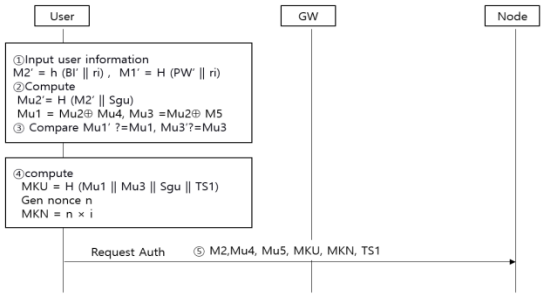

Figure 4. Authentication request

3.2.2 Authentication of Node

The authentication step is as follows. [Figure 5] shows the authentication of node steps of the proposed authentication system.

①User generates a random value and sends M2, Mu4, Mu5, MKU, MKN, and TS1 to the authentication message node to the node.

②The node computes Mj2=Mj3⊕ Mj1 using Mj3, Mj1.

③The node computes AG. The AG is used to mutually authenticate the node Nj and the gateway GW. The node then sends M2, Mu4, Mu5, MKU, IDNj, Mj3, AG, TS2, and TS1 messages to the gateway

④Gateway uses the received Values to authenticate the user and send the user's status to the node.

⑤The gateway checks the validity of the timestamp. If the timestamp is not valid, the gateway GW terminates the next operation, sends a reject message to the IoT node. If valid, the gateway will calculate Mj1'= H (IDNj || Sg).

⑥The gateway next computes Mj2' = Mj3⊕ Mj1'. In addition, the gateway computes its own Mj2 = AG ⊕ H (Sgn || ts1 || ts2)

⑦The gateway will check if Mj2 and Mj2 'are the same and authenticate the iot node as an effectively registered node from the IoT network if they are identical.

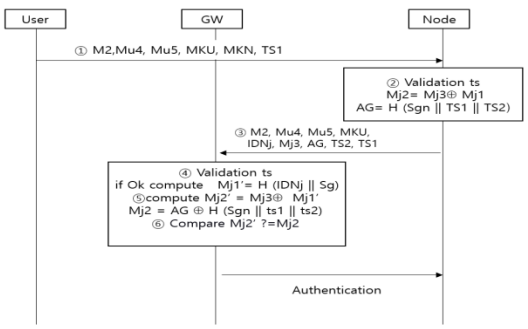

Figure 5. Authentication of Node

3.2.3. Authentication of user

The authentication step is as follows. [Figure 6] shows the authentication of node steps of the proposed authentication system.

①If the node successfully authenticates the node, Mu2 '= H (M2 || Sgn). Then, Mu1 '= Mu4⊕ Mu2', Mu3 '= Mu5⊕Mu2' are calculated. The gateway computes AU = H (Mu1 '|| Sgu || TS1 || Mu3') using Mu2 'Mu1'.

②The gateway verifies whether the received MKU is the same as the calculated AG. If they are the same, the gateway successfully authenticates the user.

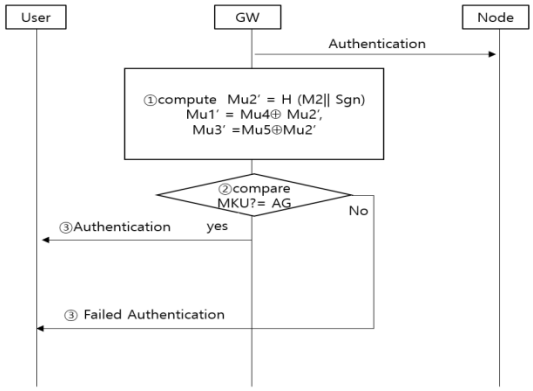

Figure 6. Authentication of user

IV. SAFETY EVALUATION OF THE PROPOSED METHOD

This section presents a security analysis for understanding the safety of the proposed method. The proposed method sets a security key, provides mutual authentication, guarantees password protection, and is resistant to various attacks.

First, the method proposed in this study guarantees the integrity of the message because it uses a secret value only known to the gateway and the IoT node in the communication between them, a third party cannot obtain a meaningful value even the party captures a message owing to the hash calculation and xor calculation, the third party consequently cannot produce a message, and the forgery and alteration of the message are continuously checked through a trial-response method.

Second, the proposed method authenticates a user and a node mutually through a gateway, a third party, between them. The gateway is granted an authentication agency role because it mutually authenticates a user and a node using the secret value and key in the registration process and it can deliver information safely by establishing a safe channel. Moreover, it helps the authentication process between a user and node and it delivers parameter values required for the symmetric key agreement. After that, the user and the node generate a symmetric key and send it with a hashed random value in order to confirm and conclude the mutual authentication.

Third, the man in the middle attack means an attack that disguises it as a device or a server in the

middle of a device and an authentication server by stealing all messages between a device and a server. The man in the middle attack is an aggressive attack that can seriously damage a server or device by modifying the datail legally, generating false data, and transferring the data. Since the proposed method uses a newly created random number every time in the authentication step, it can prevent the man in the middle attack. Even if the attacker collects all messages between a user and a gateway, the attacker cannot create a session key required for transferring messages safely because they do not know each random number. As a result, an attacker cannot modify messages sent in the login and authentication steps. Consequently, the proposed technique is safe from the man in the middle attack.

Fourth, the communication between an IoT node and a gateway of the proposed technique can guarantee the confidentialness because it hides important information using a hash function and a xor calculation with considering the limited computation capability of the node and it is designed not to produce meaningful values even if all messages in the communication process are combined. Since the symmetric key is renewed whenever a new session is established, it is impossible for an attacker to find the key within a meaningful period.

V. CONCLUSION

Recent developments of the ICT technology have improved technologies that make our lives more convenient using the communication technologies between sensors, represented by the IoT. However, although this advancement improved the convenience of our life greatly, it has made us more vulnerable to various threats abusing the characteristics of the IoT such as personal information leakage, data forgery, and privacy infringement. The increase of these threats is due to the gap between the development of the applied technology and the applicable security technology. In other words, due to the characteristics of the IoT terminal, there is a limit to apply the currently used encryption and authentication technology without a modification. As a result of the research, the IoT pursues low-capacity and lightweight. However, the security technology used in the current computer environment cannot be applied as is because it requires high performance. Due to this reason, it may be possible to steal personal information or penetrate into the internal network by illegally penetrating the relatively weak IoT's security technology, especially bypassing the authentication technology. In order to overcome these shortfalls, this study evaluated and proposed a biometric-based multi-factor authentication method that can be easily applied to various IoT environments.

The proposed method may be very suitable for the resource constraint device of the IoT because the protocol of it is light. The protocol is light because it only utilizes a one-way hash function and an XOR calculation, which takes low operation cost. The safety analysis proved that the proposed technique provided security that can prevent security threats and satisfy security requirements in the IoT environment. The efficiency analysis also proved that the proposed protocol has better computation efficiency than previous studies. In the future, we will extend this study and evaluate ways to apply it to various IoT terminals. We also plan to systematically expand the study by establishing a model for verifying the effectiveness and validity of the proposed authentication method against various attacks.

REFERENCES

1. Lee, Woo-Kwon, A Study on Issues and Alternatives of Privacy Protection in IoT, Korean Journal of Local Government & Administration Studies, 2015 Dec; 29(4), 215–234. https://www.kci.go.kr/kciportal/ci/sereArticleSearch/ciSereArtiView.kci?sereArticleSearchBean.artiId=ART002065391
2. Chung Yong Sik, Cha jaesang. IoT device security check standard. The Journal of The Korean Institute of Communication Sciences, 2017; 34(2), 27-33. http://www.ndsl.kr/ndsl/commons/util/ndslOriginalView.do?cn=JAKO201713547379949&dbt=JAKO&koi=KISTI1.1003%2FJNL.JAKO201713547379949
3. Aeri Lee. Study of an Authentication Methods for IoT Services. International Journal of Engineering & Technology. 2018 Sept; 7(3.34), 602-605.
4. S. Sicari, A. Rizzardi, L.A. Grieco, and A.Coen-Porisini, Security, Privacy and Trust in Internet of Things: The Road Ahead. Computer Networks. 2015; 76(15), 146-164.
5. Yan Z, Zhang P, Vasilakos AV. A survey on trust management for internet of things. Journal of Network and Computer Applications. 2014 June: 42, 120-134
6. Q. Jing, A.V. Vasilakos, J. Wan, J. Lu, and D.Qui, Security of the Internet of Things: Perspectives and Challenges. Wireless Networks. 2014; 20(8), 2481-2501.
7. Canmingjiang, Bao Li and Haixia Xu,. An efficient Scheme for User Authentication in Wireless Sensor Networks. 21st International Conference on Advanced Information Networking and Applications Workshops, 2007May; pp. 438-442,
8. Guanglei Zhao, Xianping Si, Jingcheng Wang, Xiao Long and Ting Hu,. A novel mutual authentication scheme for Internet of Things. 2011 International Conference on Modeling Identification and Control, pp. 563-566, 2011.
9. PawaniPorambage, Corinna Schmitt, Pardeep Kumar, Andrei Gurtov and Mika Ylianttila. Two-phase Authentication Protocol for Wireless Sensor Networks in Distributed IoT Applications, IEEE Wireless Communications and Networking Conference(WCNC), 2014; 2728-2733
10. Kuo WC, Wei HJ, Chen YH, Cheng JC. An enhanced secure anonymous authentication scheme based on smart cards and biometrics for multi-server environments. Information security (AsiaJCIS), 2015 10th Asia joint conference on, May. IEEE. 2015 May; 1–5