International Journal of Engineering & Technology, 7 (3.33) (2018) 301-304

International Journal of Engineering & Technology

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

Research paper

An Authentication Scheme Using Locations and OAuth in IoT Environments

Jeong-Woo Cho[1], Ki Young Lee[2]*

[1,2]Incheon National University, Incheon, Korea
**Corresponding author E-mail: kylee@inu.ac.kr*

Abstract

Recently, in the IoT environment, along with the emergence of many devices, the necessity of protected networks accessible only to certain users has been coming to the fore. Although network authentication systems can be more easily constructed by applying the OAuth protocol to IoT network environments for authentication, secondary authentication is recognized to be essential in the case of such systems because of the fact that such systems can be easily exposed to attacks when attackers have snatched the relevant token due to the characteristics of OAuth. Authentication through locations has the advantage that the user does not have to enter, remember, or carry any data. In addition, as the IOT advances, many APs are used leading to the improvement of the accuracy of WPS. Using the foregoing, this study is intended to enable user friendly authentication by taking the advantage of OAuth and using secondary authentication through location authentication, which is relatively convenient to users.

Keywords: *Authentication, IoT, Location, OAuth*

1. Introduction

The Internet of Things (IoT) has become to be no longer a future technology. Boilers or fluorescent lamps have already become remote-controllable, and services named IoT have begun to appear here and there. Although the state where numerous services and devices are connected on the IoT provides convenience to users, the damage that may be caused following the access of malicious users cannot but be much larger compared to other services. However, even in this situation, authentication methods with heavy loads cannot be used due to the constraints of IoT devices. In addition, the security of IoT is often achieved centering on services. It should be possible to limit those who can access depending on services. For instance, let us consider the doors at home. The front door should be accessible to all of our family members. However, the doors of individuals' rooms should not be accessible to others.
The most suitable method for this end is the OAuth method. Although studies on authentication using group keys have been conducted too [1], the relevant method has a disadvantage that the group keys should be continuously managed because they are changed frequently due to the nature of group keys. Unlike the foregoing, in the case of OAuth, only some of the database is changed even if the user withdraws from a group for a certain service, not so much overhead is incurred, no personal information leaks through membership registration because third parties are used and therefore, the cost incurred to protect the relevant personal information can be reduced from the viewpoint of the server. However, since OAuth, in which the user is enabled to receive access tokens after authentication through communication with a third party and the access tokens are used for authentication, has a disadvantage that the system will be easily attacked if the access token is snatched, many studies on secondary authentication are in progress [1,2,3].

2. Background of Related Techniques

2.1. OAuth

OAuth is a standard authentication method developed with Open API. This protocol is used to give the client the right to access the service provider's resource server where users' resources are stored instead of delivering user authentication information such as ID and password when a user accesses a resource server in order to use any service or data provided by service providers such as social networks such as Facebook and Twitter or a portal site at a client. The overall flow of the protocol is shown in Figure 1.

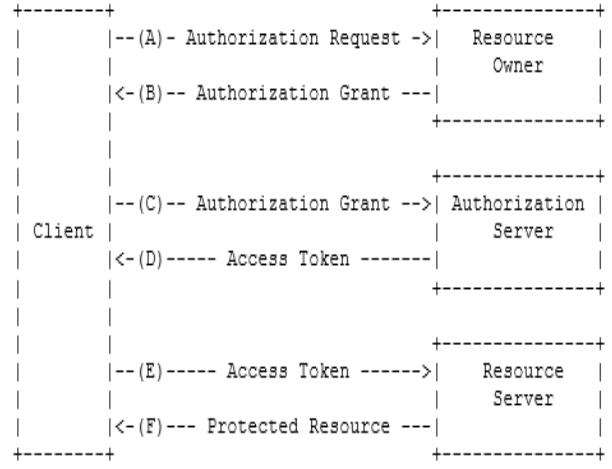

Fig. 1: Flow of OAuth2.0 [4]

Copyright © 2018 Authors. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

2.2. WPS

The Wi-Fi positioning system (WPS) is a method of estimating locations using the MAC addresses and received signal strength indications (RSSIs) of access points (hereinafter APs). The locations of the APs must be stored in the database. The RSSI is the value of the power received at the wireless receiver. Since this RSSI decreases as the distance increases in general, the distances to APs can be estimated using RSSIs and the distances to multiple APs estimated as such can be used to estimate the locations of the APs through the triangulation method. The WPS shows higher accuracy when the number of captured APs is larger and when the RSSIs of the APs are relatively stronger. Unlike GPS, the WPS does not provide altitudes [5]. Based on the experimental results, the average of differences in the values was the smallest when the values were filtered with RSSI values not smaller than -75 while being the largest when the values were filtered with RSSI values not smaller than -85.

3. Related Works

3.1. IoT-OAS: An OAuth-Based Authorization Service Architecture for Secure Services in IoT Scenarios [6]

The most important feature of the above paper [6] is that the service part and the authentication service part are separated to provide transparency to clients. That is, the service provider is not required to know how OAuth is implemented. This provides compatibility with other OAuth client programs. In addition, the authentication service has been separately set to separate authentication and the right. (Figure 2)

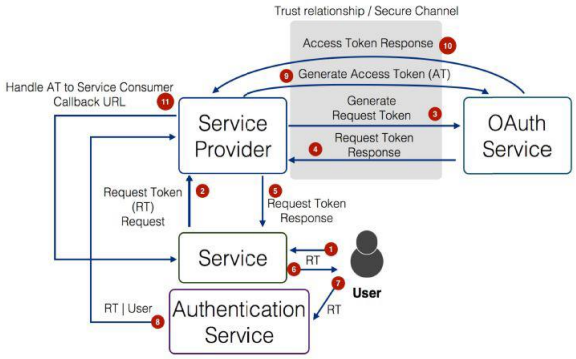

Fig. 2: Flow of IoT-OAS to acquire the right

The client (service consumer) requests the service provider for a certain service with the access token obtained through the above right acquisition flow. The service provider delivers the request to the OAuth service, checks whether the relevant user is accessible to the service, and gives a response to the user. It can be seen that this is service based authentication. (Figure 3)

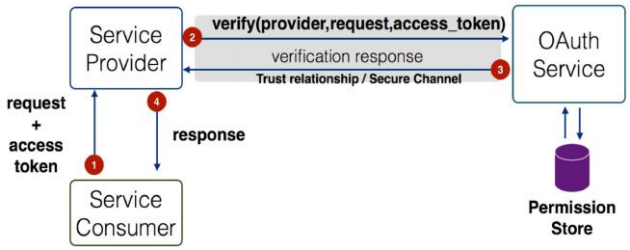

Fig. 3: Access flow of IoT-OAS

3.2. Location-Based Authentication: Grounding Cyberspace for Better Security [7]

This paper studied location-based authentication methods. Although authentication using locations is one of strong authentication methods, the fact that the attacker can deceive the system on locations cannot be overlooked. Therefore, this paper requires location signature sensors. They are sensors globally present and they communicate with GPS satellites to generate location signatures. Since the locations that can receive these location signatures are limited, the location signatures can be said to be a sort of OTP that can be used by the user to prove that his/her location is legitimate. This authentication method enables the user to access certain services remotely. A conceptual diagram of this paper is added in Figure 4.

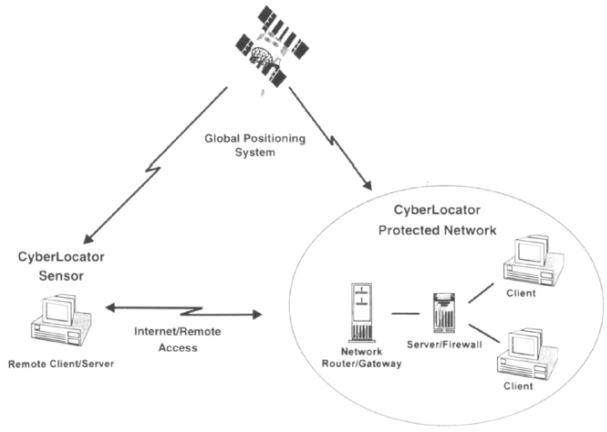

Fig. 4: Conceptual diagram of the paper

4. Proposed Method

Before proposing the method, the terms used are organized on following Table 1.

Table 1: Terms used

Notation	Description
EK	Encrypted using K as a key
HMACK	HMAC using K as a key
LOC sig.	Location Signature
LOC	Location information
AT	Access Token
Ts	Time Stamp
PU	Public key
PR	Private key
PRS	Server's private key
H(A)	Put A into the Hash Function.

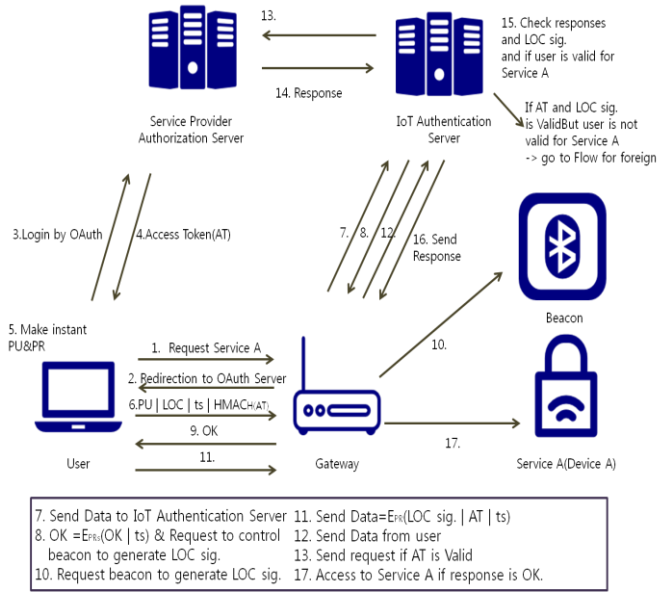

Fig. 5: Overall flow chart

Figure 5 shows the overall flow. The flow will be largely divided into three parts: OAuth login part, authentication part, and service provision and flow for foreigners.

4.1. OAuth login flow

The first flow is a part for login to the OAuth. The user who requested access to service A is redirected to the OAuth server. The user then obtains the access token through authentication with the OAuth server. Thereafter, temporary PU and PR are made. The public and private keys generated will be used in flow 2.

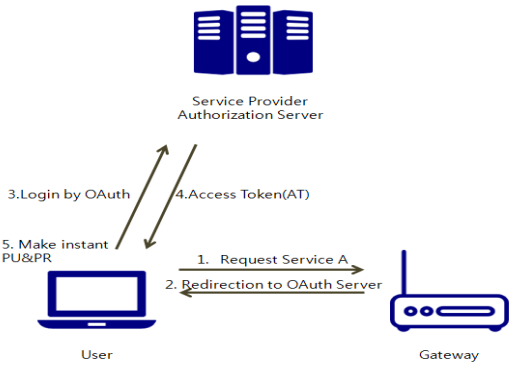

Fig. 6: Flow 1. OAuth login

4.2 Authentication flow

For authentication, location signatures will be used as with [8]. In [8], only the name location signature sensor is indicated without any mention. However, in this paper, location signature sensors will be used as beacons.

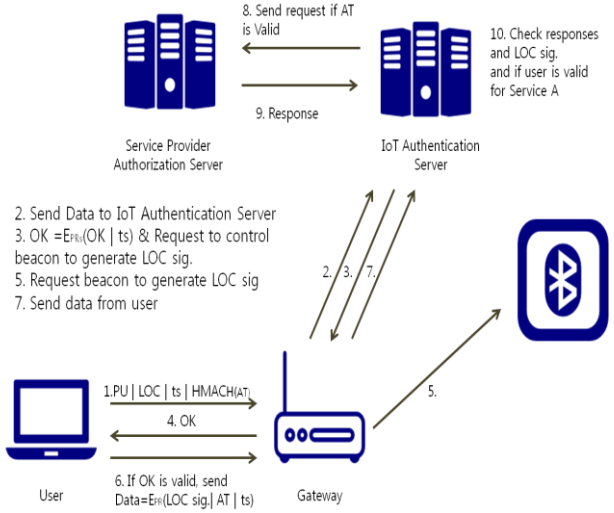

Fig. 7: Flow 2. Authentication part

This is a part where location signatures and the right of the relevant user are authenticated in the IoT Authentication Server for actual authentication.

4.3 Service provision and flow for foreigners

After undergoing the above two flows, the server allows the user to access the service. If both the AT and Location Signature are valid but the user does not have the right to access, the user will be sent to the flow for foreigners. Before explaining it, the database will be explained.

Table 2. Example of the database to be used in this study

Service	Valid user	ccess control
A	User A	
B	User B	

As shown in Table 2, in the proposed method, there are two types of access to the service: Valid user and Access control. In the case of the valid user, the OAuth ID of the user that enables access to the device is entered. In the case of the Access Control, F is entered if the valid user wants to give the right to access the relevant service to his/her friend registered with the OAuth ID (SNS account) and P is entered if the valid user wishes to use the service exclusively.

Figure 8 1. Shows the flow for foreigners.

1. In cases where F has been entered for Access Control, the friend list is requested to the OAuth server to allow those who are in the list to access the service.
2. In cases where P has been entered for Access Control, the user's permission is obtained before sending a message to the user of the right to the relevant service.

Through the foregoing, even users with no right can become accessible. The availability was enhanced by opening the accessibility to even users with no right in cases where the relevant users have undergone legitimate authentication.

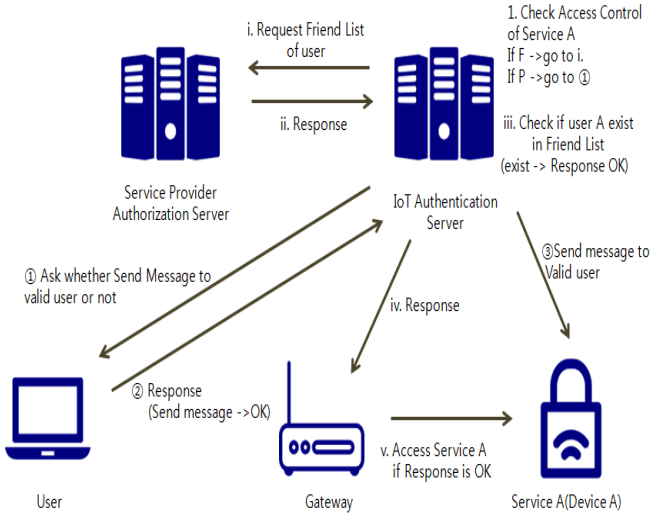

Fig. 8: Flow for foreigners

5. Security Analysis

Attacks occurring in OAuth are mainly made through the seizure of access tokens, and sham attacks, re-use attacks, and message modification attacks are mainly made [9,10].

5.1 Message modification attacks in flow 6

In cases where data have been snatched in 5 as shown in Figure 9, two types of attacks are possible.

i) In cases where PU was modified into PU`-> Decryption is impossible in flow 11.

ii) In cases where the location was modified -> HMAC is not correct in flow 11.

Both of the two types of attacks can be defended.

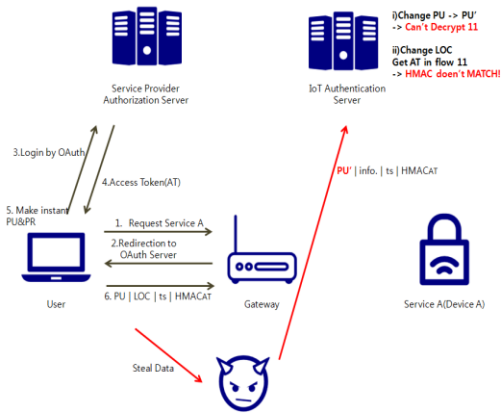

Fig. 9: Possibility of attacks 1

5.2 Message modification attacks in flow 10

In flow 10 of Figure 10, PR can be modified into PR` to make attacks. Even in such cases, the attacks can be detected because decryption is impossible since PU has already been transmitted in flow 6.

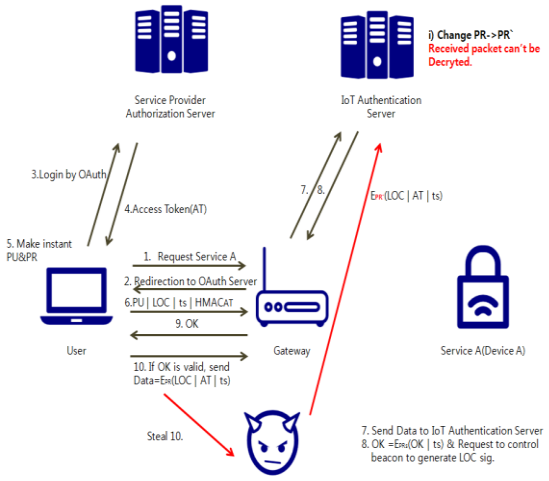

Fig. 10: Possibility of attacks 2

6. Experiment and Results

Since the beacon had to generate location signatures for the experiment, the information generated by the beacon information had to be controllable. Raspberry Pie 3 was used because both Bluetooth and Wi-Fi modules are embedded in Raspberry Pie 3. The functions of the beacon and beacon controller could be performed using only one body of Raspberry Pi 3 without the necessity to buy any additional modules.

To obtain the overhead, the amount of network packets and overall overhead were obtained after implementing authentication. Authentication was implemented using other methods and the resultant amounts of packets were compared and analyzed. Table 3 is summary of experimental results.

Table 3. Experimental results

Authentication method	Basic Auth authentication	Proposed method	Accredited certificate
Number of packets (piece)	24	24+12	69
Entire overhead (byte)	11350	11350+3463	20510

Although the experimental results may vary somewhat depending on the experimenter's ability to implement, of course, additional overhead of about 30% occurred compared to the basic OAuth method. Although the overhead increased because additional works such as encryption and messages were added, the overhead was shown to be about 29% smaller compared to the accredited certificate. Since the length of messages was shown to be shorter than thought although it was expected to be long, the results were satisfactory

7. Conclusion

With the growth of the IoT market, issues related to security, especially authentication related issues will continue to emerge. Although OAuth has many strengths as described above, it has not been used much because of its security weaknesses. To overcome these security weaknesses, this paper presented an authentication method using OAuth and physical locations. In addition, instead of preventing any other persons than users registered in advance from accessing the service, the proposed method enabled those users who want to access the specific service for a while to access the service after being approved by the authorized user and undergoing the legitimate authentication process.

The presentation of service-centered and user-friendly authentication methods as such is considered to be a way to satisfy users not only in terms of security but also in terms of IoT services. Given the success of applications with easy authentication such as TOSS, users seem to prefer to use less cumbersome authentication methods. In this regard, the physical locations may provide a fairly strong security without requiring the user to specifically enter or remember any certain data

Acknowledgement

This work was supported by the Incheon National University Research Grant in 2016.

References

[1] Heeman Lee, *A design of authentication protocol based on group key for efficient group communication in IoT environment*, Master's Thesis. Soongsil University, Korea, 2015.

[2] Young Kyu Choi, Seon Jeong Kim, and Kang Seok Kim, "An Authentication mechanism for IoT Network based on OAuth Protocol", Korea Computer Congress 2015, vol.2015, No.6, pp.1069-1071, June 2015.

[3] Young Kyu Choi, A user authentication mechanism for IoT network based on OAuth protocol, Master's Thesis. Ajou University, Korea, 2015.

[4] D. Hardt, The OAuth2.0 Authorization Framework, RFC6749, 2012.

[5] Overview of GPS, http://www.nmpnt.go.kr/html/kr/dgpsys/dgpsys_0203.html

[6] Simone Cirani, Marco Picone, Pietro Gonizzi, Luca Veltri and Gianluigi Ferrari, "IoT-OAS : An OAuth-Based Authorization Service Architecture for Secure Services in IoT Scenarios," IEEE Sensors Journal, vol.15, no.2, February 2015.

[7] Denning, D. E., & MacDoran, P. F., "Location-based authentication: Grounding cyberspace for better security," Computer Fraud & Security, Vol.1996, No.2, pp.12-16, Feb. 1996.

[8] A. Bose and C. H. Foh, "A Practical Path Loss Model for Indoor WiFi Positioning Enhancement," in IEEE 2007 6th International Conference on Information, Communications & Signal Processing, 2007.

[9] M. McGloin and P. Hunt, OAuth 2.0 Threat Model and Security Considerations, Internet Engineering Task Force (IETF) RFC 6819, 2013.

[10] Y. Feng, and M. Sathiamoorthy,"A security analysis of the OAuth protocol", IEEE Pacific Rim Conference on Communications, Computers and Signal Processing, pp.271-276, 2013.