Advanced Science and Technology Letters
Vol.67 (Multimedia 2014), pp.25-28
http://dx.doi.org/10.14257/astl.2014.67.07

Design and Implementation of Access Authentication System Based on Cloud Messaging

Sungwook Yoon[1], Hyenki Kim[1*]

[1]Dept. of Multimedia Engineering, Andong National University,
388 Seongcheon-Dong, Andong-City, Gyeongsangbuk-Do, Republic of Korea
uvgotmail@nate.com, hkkim@andong.ac.kr
[1*]Corresponding author: Hyenki Kim, hkkim@anu.ac.kr

Abstract. This study designed and implemented a control authentication system through server with the conventional password and other recognition methods as a method for on-site authentication of smartphone users at a place requiring access control. This study implemented an interface to allow for real-time control in an economic ubiquitous environment by utilizing cloud messaging service while providing an authentication management mechanism through controlling the opening and closing for visitors with this system.

Keywords: Cloud Message, Authentication, Embedded, IoT(Internet of Things)

1 Introduction

Internet of Things(IoT) may create a super-connected environment in which all things such as people, things, spaces and data have a network connectivity and consequently information is generated, collected, shared and utilized. As a result, Internet of Things predicts a complex change in such areas as home automation and office environment automation. It is possible to configure a more converged Internet of Things for the aspect of access management based on USN(Ubiquitous Sensor Network).

In this thesis, a server control system was designed and implemented together with various types of password based authentication method in a case in which there was a need for controlling the opening and closing and access as well as the user authentication for visitors in a site when an IoT based opening and closing device was utilized in a physically secure space.

2 Related Studies

It is expected that Internet of Things will be leveraged in a variety of actual life areas to realize various economic values and increase the efficiency and convenience in regard to home and office environment and multi-composite facilities [1]. It becomes

ISSN: 2287-1233 ASTL

a terminal for collecting big data as it processes a large quantity of unstructured data in a process of connecting everything [2, 3].

However, information protection places importance on determining whether a given service request is valid when accessing the system. Thus, it corresponds to user authentication[4].

On the other hand, a service is IT resource service rented by users without owning it directly. It is a service paid by users directly depending on the usage [5].

3 Design of User Authentication Using Cloud Messaging

Fig. 1 is a schematic view of opening and closing authentication for users through a message server. When a visitor is verified at a server for smartphone location and user authentication at a sensor network, the controlling server proceeds to the authentication procedure through cloud messaging server. Then, it waits for input after transmitting password generated from a remote server in real time to user's smart devices. When a visitor inputs password, it receives the password in real time to determine whether the password is valid at the remote server. It allows visitors waiting to access by unlocking the access control device when visitors pass the password authentication.

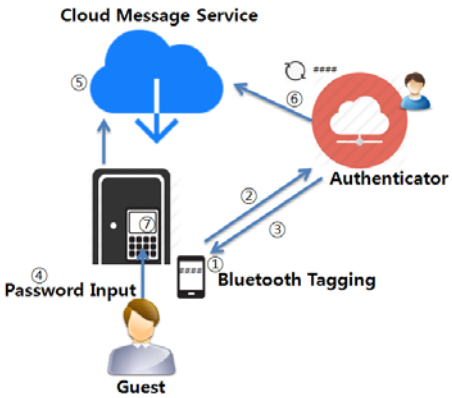

Fig. 1. User authentication using cloud messaging service

The access control system connected to a network is implemented based on the following design criteria for the access authentication of visitors. It allows for communication of real time security information by issuing temporary password for guest. It is used in processing security without leaving password at the access device. Thus, password will be immediately discarded or it approves reuse after being saved in a server for a certain period of time.

Fig. 2 shows the authentication process diagram for temporary issuance and management of user authentication password in real time.

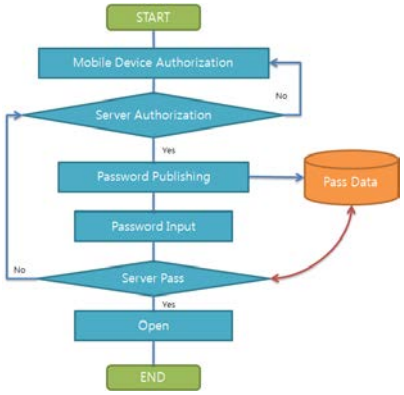

Fig. 2. Opening and closing authentication process for real-time password issuance

4 Implementation

The application prototype was implemented by utilizing the authentication mechanism method proposed in this thesis. As shown in Fig. 3, the existing door lock system was controlled with the implementation prototype based on Arduino Uno board using ATMel's ATMega328 micro-controller and Internet was connected through ethernet controller.

Fig. 3. Prototype of implemented access authentication system

To transmit cloud message, GCM (Google Cloud Message) Service was utilized and ID and authentication key value were secured and leveraged. In addition, the nodes were configured by applying the same authentication value in Arduino. The Arduino authentication key values of server and door lock were confirmed. Also, it became possible to transmit basic messages through messaging by Internet connection. It was

arranged to receive the key value as a variable when pressing the number of door lock, and it would be transmitted to the control server through GCM server.

Visitors tag mobile devices at the access control devices and wait for an approval for user access and transmit the relevant information of smart devices to the control server. Then, the control server generates character string of password for those corresponding visitors in real time and transmits the password to their smartphone. In this study, it was implemented by receiving numerical password. Visitors enter messages in the opening and closing device and those entered numbers will be transmitted to the control server in the form of cloud message. The control server confirms the issued number and validity and opens the opening and closing device through messaging.

5 Conclusion

Internet of Things provide a super-connected environment with the advent of ubiquitous environment. It is necessary to authenticate individuals for the network security in relation to the general access authentication method in order to improve the security against remote intrusion and extortion behind the convenience of connecting nodes between Internet and things.

This thesis implemented an interface allowing for real-time control while providing a better authentication management mechanism for the opening and closing related security in an actual site requiring access authentication for visitors. It becomes possible to authenticate visitors safely in a secure space by allowing a remote server to control. It is expected that this will be leveraged in accommodation facility control such as access control, personal safe, hotel, etc.

References

1. Byung Mun Lee ,Jinsong Ouyang, Intelligent Healthcare Service by using Collaborations between IoT Personal Health Devices, International Journal of Bio-Science and Bio-Technology, pp.155-164, Vol.6 No.1 (2014)
2. Kang-Yun Lee, Jung-Hun Lee, Changwoo Jung, Yeong-Ju Tak, IoT 3.0 and Internet of Things technology platform, Korea Information Processing Society Review, v.21, no.2, pp.3-13 (2014)
3. Sung-Chan Choi, Min-woo Choi, Nam Jin, Jae-Ho Kim, Internet of Things Platforms and Services Trends, Journal of The Korean Institute of Communication Sciences, Korea Institute Of Communication Sciences , Vol.31 No.4 , pp.20-27 (2014)
4. Seong-Whan Ju, Huiseok Seo, A study on User Authentication Technology of Numeric based Pattern Password, Journal of the Korea society of computer and information, Vol.17 No.9, pp.65~73 (2012)
5. Si-JungKim, Sang-Su Yeo, A Study on Secure Data Access Control in Mobile Cloud Environment, International Conference on Digital Policy & Management, Vol.11 No.2, pp.317-322 (2013)

