International Journal of Control and Automation
Vol.8, No.11 (2015), pp.63-68
http://dx.doi.org/10.14257/ijca.2015.8.11.07

A Study on Automatic Doorway Access Control System Including Server Based On Bluetooth Local Communication

Am-Suk Oh

Dept. of Media Engineering, Tongmyong University, Busan, Korea
asoh@tu.ac.kr

Abstract

Most of existing doorway systems are directly controlled by a central system. Most of central control systems have the function of fingerprint recognition, biometrics (face, iris), encryption key and so on. However, it costs a lot of money and may be vulnerable to security, and inspection history management is inconvenient because most of I/O devices like readers are connected with external networks. We will study automatic doorway control systems based on authorized encryption key from servers under Bluetooth local networks linked with smart phones. We aimed to construct a doorway Access control system by using smart phones. In addition to this, the server we studied can control automatic doorway systems and access authorization of visitors including inspection history management of engineers. It also provides real time monitoring function by transmitting the status information to smart phones.

Keywords: *Access Control System, Bluetooth, Smart Phone*

1. Introduction

The trend of worldwide security industry is changing rapidly from protection of communication information to social safety. Conception of information security is extending to social security from computer network security. As the security industry area is extending to physical security, convergence security from simple information security, knowledge based on the information security industry has emerged rapidly. Security control service is one of the most active fields among convergence security areas. The technical trend of this area is going toward integration of CCTV, doorway control system with private security services like PC usage information, IP, network information, printed documents information and so on. Currently, Networks are constructed among central system and automatic doorway controller in most doorway control systems and operate via verification systems such as RFID fingerprint recognizer. Most of them receive authentication from a central system that is connected to the doorway access control system via RFID/NFC tag of visitor. Automatic doorway access control systems make use of wired communication lines and most of the access roasters belong to fixed residents. However, network construction costs much money in addition to the security weakness problem and efficiency issue of maintenance.

Thus we suggest a smart doorway access control system including servers using smart phone authentication key for efficient access management.

ISSN: 2005-4297 IJCA

2. Automatic Doorway Access Control System

2.1. Smart Access Control System

Figure 1 shows the configuration of the Smart Access Control System suggested here.

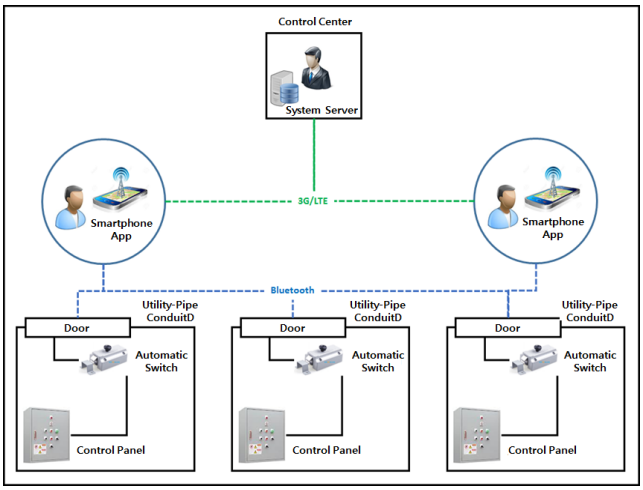

Figure 1. Smart Access Control System

The Smart Access Control System we suggested has no need to construct extra networks, readers or other extra facilities because it operates under Bluetooth communication environment. Authentication method is accomplished by smart phone applications and it provides flexible inspection & release right depending upon inspection time.

2.2. Automatic Access Control Device

The Smart Access Control System we suggested is composed of an Automatic Access Control Device and Control Panel as shown in Figure 2. The Control Panel is composed of a controller board that includes Bluetooth communication and controls the Automatic Access Control Device that is connected by a wired line thru a smart phone application.

Automatic Access Control Device is one of general doorway open/close devices that can switch on/off automatically by electrical signal.

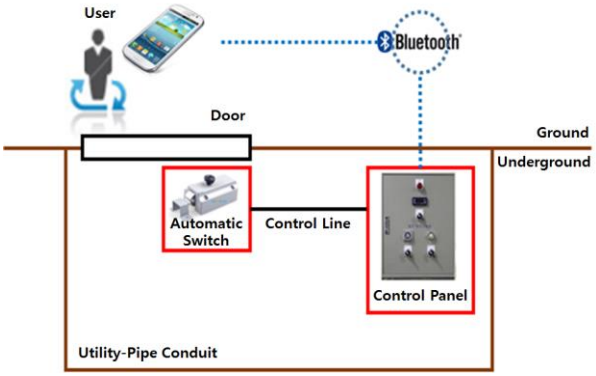

Figure 2. Automatic Access Control Device and Control Panel Configuration

Detail contents of development are as follows.

- Bluetooth Communication: connect smart phone app with network thru Bluetooth communication board in Control Panel.
- Connection with smart phone Authentication key: Control Access Control Device via Control Panel when connected to smart phone with Bluetooth.
- Status monitoring: Transmit status information of Control Panel (power, control part) to smart phone.

Control panel board of Automatic Access Control Device is shown in Figure 3.

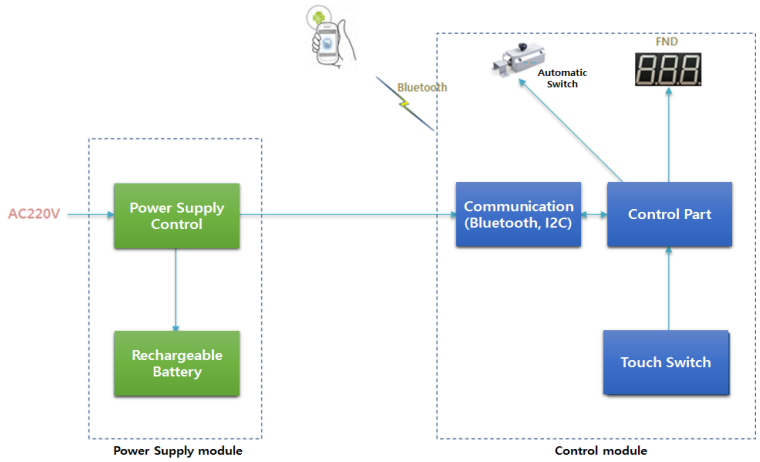

Figure 3. Automatic Access Control Device and Control Panel Configuration

3. System Server for Access Control

3.1. System Architecture

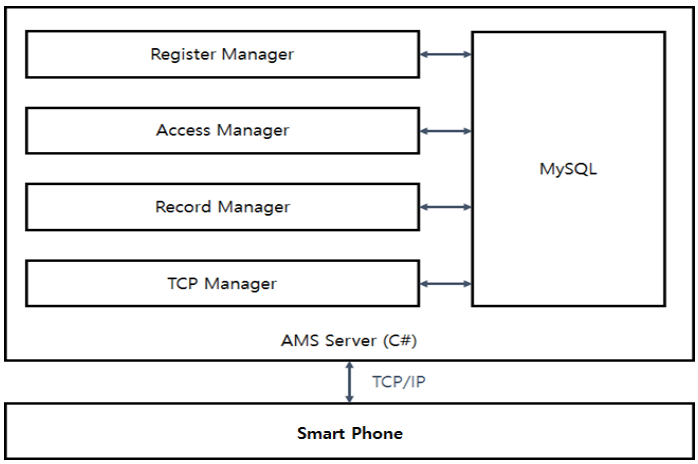

Figure 4. System Server Architecture

The architecture of system servers for access control is shown in Figure 4.
It is composed of Register Manager, Access Manager, Record Manager, TCP Manager.

3.2. Automatic Access Control Device

Register Manager manages the information of visitors and Access Control Device. This information is stored in a database. Figure 5 shows the screen of Register Manager.

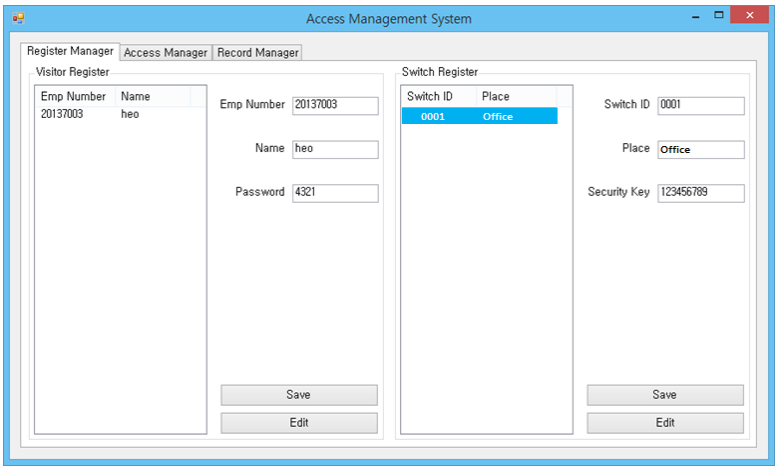

Figure 5. Register Manager

3.3. Access Manager

Access Manager manages visitors' access right. It verifies the visitor's record and Access Control Device, and then gives the right to the visitor for accessing the door at that time. Figure 6 shows the screen of Access Manager.

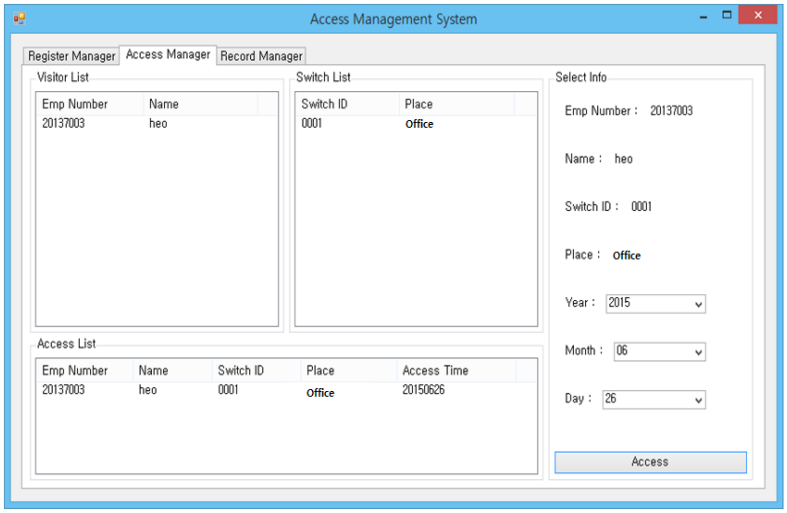

Figure 6. Access Manager

3.4. Record Manager

Record Manager inquires the history of access. Whenever visitors are going in and out of the Access control Device, the Record Manager can monitor the events and also store the record into database.

Figure 7 shows the screen of Record Manager.

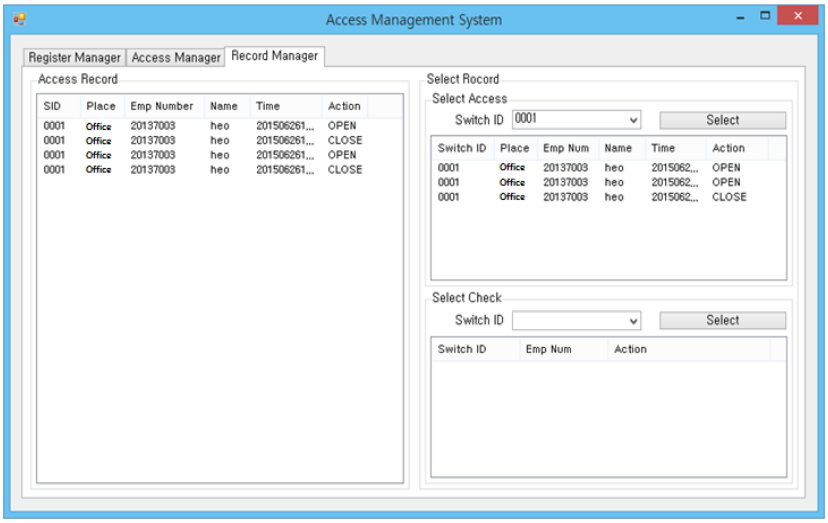

Figure 7. Record Manager

3.5. Tcp Manager

TCP Manager manages TCP communication with smart phones. It sends the response message after inquiring the required information. Whenever a visitor requests login, it compares the identification number of the visitor information table with the visitor's input data, and then it transmits the signal of "accept" or "reject". It also transmits an encryption key after receiving requests from the visitor and confirms the access right. It transmits the visitor's record such as coming-in time and going-out time to server. The server stores this information into the database after receiving.

4. Conclusion

We suggested an Automatic Access Control Device and Control Panel under the smart phone authentication key environment. Automatic Access Control Device and Control Panel can be operated by the server after connecting with a smart phone and given an authentication key from the server. There's no need to construct extra networks in this system, and it can control a visitor's access to the doorway efficiently using the Bluetooth of smart phones including other convenient services. Nowadays, the worldwide IT security industry has been extending from simple information security to the physical convergence area, thus, security control fields like doorway control systems have trends of integration with private security services. We also suggested a server system using a smart phone authentication key for efficient access management. We expect this system would be a cost effective system in comparison with other existing systems.

Acknowledgements

This work (Grants No. C0276645) was supported by Business for Cooperative R&D between Industry, Academy, and Research Institute funded Korea Small and Medium Business Administration in 2015.

References

[1] K. S. Lee, H. Sim and J. C. Oh, "The Design and Implementation of Intruder Access Control System by based of Ubiquitous Sensor Network", The Journal of The Korea Institute of Electronic Communication Sciences, vol.7, no. 5, **(2012),** pp. 1165-1171**.**
[2] Common Access Card Pre-Issuance Technical Requirements, vol. 4.1.2, **(2005)**.
[3] K. H. Choi, J. M. Kim and D. H. Lee , "Network 2-Factor Access Control system based on RFID security control system", Journal of information and security, vol. 12, no. 3, **(2012),** pp. 53-58**.**
[4] K. H. Nam, "Convergence security trend", Institute for Information & Communications Technology Promotion Week Technology Trends **(2014).**
[5] Korea Internet & Security Agency, World Knowledge Information Security Industry Comparison **(2012).**
[6] J. I. Choi, Y. J. Chang, Ye-Jin and O. D. Lee, "Status and prospects of Knowledge Information Security Industry" ,Korea Security Science Association, vol. 39, **(2014),** pp. 269-294**.**
[7] Lawrence Orans and Mark Nicolett, "Gartner's Network Access Control Model", Gartner IT Security Summit 2005, June **(2012).**
[8] S. M. Cho, "An RFID Multi-Reader System Development for TCP/IP Based Security Control", Journal of the Korea Institute of Information and Communication Engineering, vol. 13, no. 8, **(2009),** pp. 1587-1592**.**
[9] K. H. Kwon and H. B. Lee, "Gate Management System by Face Recognition using Smart Phone", Journal of the Korea society of computer and information, vol. 16, no. 11, **(2011),** pp. 9-15**.**
[10] B. S. Song and J. H. Kim, "Implementation of Secure Access Control Service Module based on RFID/ USN", Journal of Security Engineering, vol. 7, no. 4, **(2010),** pp. 351-361**.**
[11] J. P. Kim, "international trends and forecasts of NFC-based application services", Telecommunications Technology Association **(2011).**
[12] U. Karthaus and M. Fisher, "Fully inte grated Passive UHF RFID TransponderIC with 16.7-uW Minimum RF Input Power", IEEE Journal of Solid-State Circuits, vol. 38, no. 10, **(2003)** October**,** pp. 1602-1608**.**

Author

Am-Suk Oh, He received his B.S. and M.S. degrees in Computer Science from Busan National University and Chung-ang University, respectively. He received his Ph.D. degree in Computer Engineering at Busan National University. He is currently with the Department of Media Engineering, Tongmyong University as a Professor. His research interests are database, healthcare system and medical information system.

