

Case Study: Facility Management System Application Using Internet of Things

Jaeun Seo, Narae Jeong, Jaejoon Kim*

Daegu University, School of Computer and Communication, 201 Daegudae-ro, Gyeongsan, Gyeongbuk, 38453, South Korea.

*Corresponding author. Tel.: (+82)538506634; email: jkimsu@daegu.ac.kr

Manuscript submitted March 3, 2019; accepted May 5, 2019.

doi: 10.17706/jcp.14.5.366-372

Abstract: The purpose of this study is to solve problems of the modern society which are damaged or lost due to the immoral behavior of public facilities. By integrating Internet of Things (IoT) technology into the door lock system, the system can be implemented as a smart facility management system - complemented with the currently existing analogue facility management system. The implemented system consists of H/W and S/W part. For the H/W part, we used Wi-Fi module attached to an Arduino in order to connect digital door lock. The Web server and Wi-Fi module are composed of an Apache server and PHP. These parts can communicate with each other through the smartphone application (APP). By doing this, the user can reserve the facility by using the application. Since this system can manage members based on subscriptions and can control door lock only through application, it is more secure than other door lock control systems and thus minimizes loss and damage of public equipment.

Key words: Internet of things, facility management system, Arduino, port forwarding, security.

1. Introduction

Objects The Internet refers to all things in the world that can be networked and communicated with one another. At the Massachusetts Institute of Technology (MIT) in 1999, it is believed to have been the first to use RFID and other sensors as a means of building the Internet for objects that are used in everyday objects. As the technology of Internet of Things (IoT) [1] has developed, its statue has become increasingly more prominent in regards to security of related devices. In particular, as a result of hacking public utilities as well as various household appliances connected with IoT, the importance of security has been growing [2]. In addition, as the use of public and industrial facilities increases, many users are experiencing inconveniences because of the increasing number of cases hacking. Our system is aimed at enhancing the security of facilities by attaching locks to the facilities and reducing the damage for facilities by allowing the users to use the facilities by reservation through the smartphone application.

In this study, door lock was modified by connecting an Arduino and Wi-Fi module to door lock. For S/W usage, the smartphone App and the Web server are linked and the information in the App is transmitted to the Web server. The information delivered to the Web is then transmitted to the Arduino through the Wi-Fi module, and the facility with the door lock can be operated remotely using the App. Section 2 briefly discusses the related works for Wi-Fi and Arduino technology. Section 3 describes the proposed system including H/W and S/W implementation. Sections 4 and 5 conclude the paper by discussing experimental results, future works and other possible solutions.

2. Related Work

Currently, there are various security systems that are being developed [3]-[5]. It is a door lock control system using Near Field Communication (NFC), along with biometric recognition systems such as iris, facial and fingerprints. The door lock control system using smartphone application can enhance the security of public and industrial facilities. The usage of smartphone application that are not NFC, iris, facial, and fingerprint recognition, etc., is unspecified users of public and industrial facilities. Facial, fingerprints, and iris registration can be troublesome for individual registration. Many applications such as iris recognition, facial recognition, and fingerprint recognition have many user information to be stored in the database. Therefore, there is a concern that the amount of database is enormous and security and personal privacy may be violated [6]. The security system using the application can be candidate because it is easy and convenient to use.

This system uses a Wi-Fi module which is superior to Bluetooth or NFC even though Wi-Fi module is more expensive and more complicated than Bluetooth or NFC. The door lock system can be controlled by the flow of information in the database through communication of web, app, and Wi-Fi module for smooth operation of the system. Table 1 compares the overall specifications of NFC, Bluetooth and Wi-Fi [7]-[9]. Wi-Fi has a wide range of transmission and reception distances of 32-95 meters [m] compared to 5-30 meters [m] of Bluetooth and 10-20 centimeters [cm] of NFC. On comparing a transmission speed of 0.1 to 0.85 Mbps of NFC and 24 Mbps of Bluetooth, transmission rate of Wi-Fi shows higher value of 600 Mbps. In our study, the Wi-Fi module was utilized because it is superior to Bluetooth in terms of security, which is the most important aspect of our system.

Table 1. The Overall Comparison of NFC, Bluetooth and Wi-Fi Technology

	NFC	Bluetooth	Wi-Fi
Communication system	P2P		
Price	Low	Middle	High
Range	10 cm	10 m	100 m
Speed	0.1-0.85Mbps	24Mbps	600Mbps

3. Proposed System

As shown in Fig. 1, the security of the modified door lock was strengthened by linking the web that can identify the user's identity and the application that restricts the use of the user.

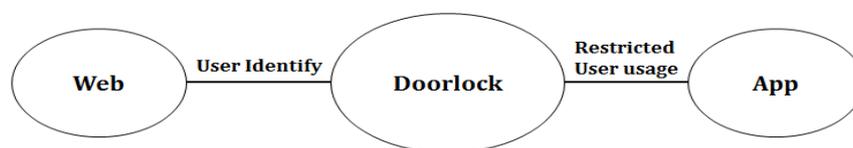


Fig. 1. The fundamental security framework for Doorlock, web, and application.

3.1. H/W Configuration

The existing door lock is composed of a keypad and a locking device. Since the door lock used in the public equipment security system does not require a keypad, it is necessary to modify door lock and supporting H/W components. In our system, the door lock opening/closing function can be controlled by a smartphone application and the switch line of the door lock device is connected to the Arduino. In addition,

the smart phone application and the web server communicate with each other through the Wi-Fi and the door lock can be opened and closed by transmitting the signal to attached Arduino to the door lock.

The Arduino product we used in our study is Arduino pro mini, which is small enough to fit inside the door lock and is easy to mount on the finished product. The Wi-Fi module uses a typical Wi-Fi esp8266 [10]. Table 2 shows the type and specification of the Wi-Fi module. In order to use the two modules programs developed by Arduino, we must upload specific software. However, the Arduino pro mini does not include a USB upload function, so a serial communication device is required for uploading the software. this study, we uploaded the pc program to Arduino pro mini using FTDI (FT232RL), which made it possible to operate only the Arduino pro min with the modified digital door lock. We experimented with tablet PCs to check communication between the APP and web. The used tablet PC is the SM-T280 as a specific small-output wireless device.

The Door Lock, APP, and WEB modules described in Fig. 2 can communicate only with each other by using the same IP address. In our study, we used port forwarding technique to set an external IP address, rather than an internal IP address, to enable communication of each module.

Table 2. The Wi-Fi Module Comparison

Name Spec	Official Wi-Fi Shield	CC3000 Wi-Fi Shield & Module	ESP8266 Wi-Fi Module
Voltage	5V	5V	3.3V
Processor speed	2.4-2.497GHz	11Mbps+18dBm	80-160MHz
Size	55X53X11mm	60X53X12mm	30X10X11mm
Cost(\$)	\$110	\$70	\$6

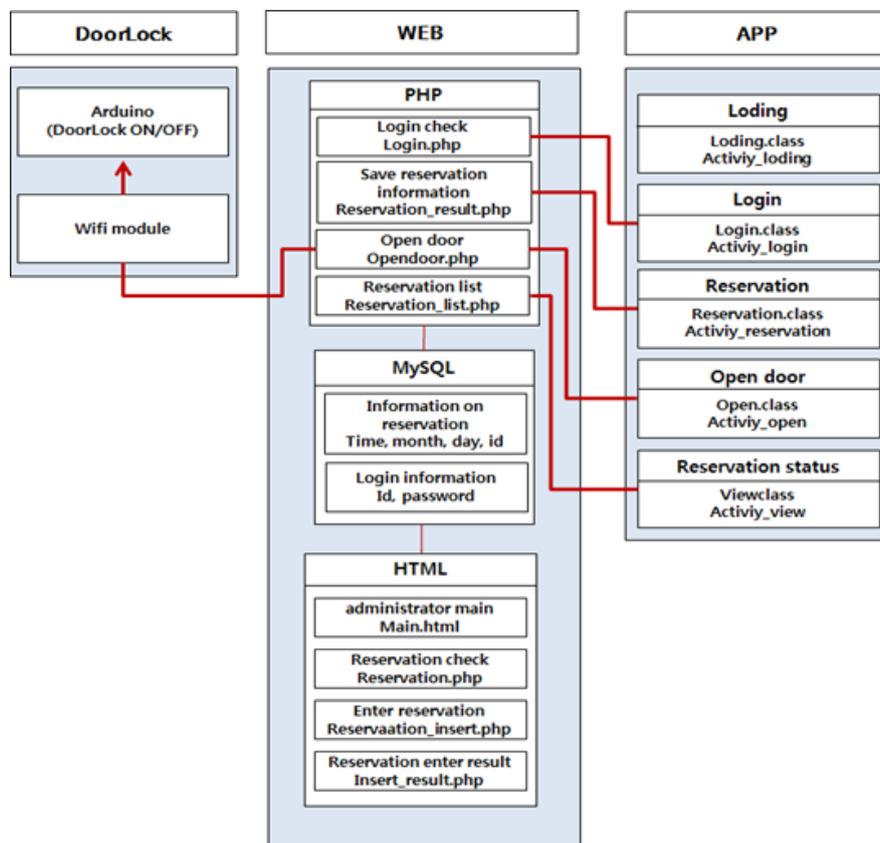


Fig. 2. The application flow diagram for DoorLock, WEB and APP component.

3.2. S/W Configuration

In order to implement the proposed system, the S/W configuration consists of PHP [11] for the S/W web language, MySQL [12] for the database, Apache for the web server, and Android studio [13] for the mobile platform. The reason for selecting them is because they are very popular and very easy to integrate with other programs and constantly updated. Continuous updates were especially a big factor in our choice since this means we can constantly improve our security performance. The most important function in our system is the database. In the database, user information and reservation information are stored. It is also where reservation management and visiting history management are performed. The table of the database is composed of two tables, one each for user and reservation. In the user table storing user information consists of user ID, password, name and gender. The reservation table in which the reservation information is stored consists of ID of the reserved user, reservation time and period. The format of the data field of the user table is all specified as VARCHAR, and the data field of the reservation table is specified as INTEGER except for id. Therefore, in order to utilize the key functions of our system such as door lock opening, user information, authority, reservation the software and hardware must communicate with each other by exchanging information of database through PHP. We used PHP's POST method to exchange information with the Android studio and database, and we used SQL statement to exchange information between database and PHP. The reason for using the database through PHP is to improve security by preventing direct access to the database through PHP because our system is important for security of user information and reservation information. The user can use the system after logging in through the smartphone application. The login information can be logged in PHP after checking that it matches the information in the database, and the reservation information is also stored in the database via PHP. When the user presses the door open button of the application, PHP confirms the reservation information stored in the database. And when it is matched, it is given permission to open the door.

Furthermore, the administrator can manage the reservation information, the user information, and the visiting history. When administrator inquiries about reservation information, user information, visit history, etc. via HTML, PHP processes it using database information and displays it on the administrator page.

4. Result and Discussion

4.1. Doorlock Function

For experimental implementation, we connected the serial communication device called FTDI to the Arduino pro mini attached to the door lock and uploaded the program of the PC [14]. When the application logs in and makes a reservation, the information is transferred to the Web and stored. Comparing the information (name, reservation date, and reservation time) stored on the web with the current time, the door lock is opened when the button opens the door to the app according to the reserved time. After comparing the information such as name, reservation date, and reservation time stored on the Web with the current time, the door lock is opened. AT+ CIFS command is given to identify the assigned IP address first and AT+CWLAP command to find the Wi-Fi network in order to check the list. If AT+CWJAP = "Wi-Fi name", "Wi-Fi password" is input, the Wi-Fi module will connect to the Wi-Fi what we entered. If Wi-Fi IP address set in Wi-Fi module is set to same in web server and app, each module can communicate.

The Wi-Fi module should open the serial port in the Arduino software and work on it. Once H/W component works well, we should check the assigned IP address, find the Wi-Fi network, check the connected network list, and then enter the Wi-Fi name and password. If Wi-Fi IP address set in Wi-Fi module is assigned to web and App, each module can communicate.

4.2. Smartphone Application

On Android studio application, we can run it on our Android smartphone or tablet PC. In our study, we used the Galaxy Tab A6 to run the application. The application generally consists of a loading screen, a login screen, a reservation screen, and a door open screen. The loading screen is not the actual loading but the startup screen that informs the application. When the loading screen finishes for 2 seconds, it goes to the login screen. The user can go to the reservation screen and select the date and time by clicking the reservation button on the login screen. The selected date and time are then stored in the reservation information table of the database through PHP. When using the facility, the user can open and close the door lock with the door open button on the door open screen by selecting the door open screen on the main screen. The administrator can manage the reservation by checking the reservation information and login information on the reservation management page. Once we click on the inquiry on the main screen of the administrator's reservation management page, we can go to the inquiry screen and make a reservation inquiry. After we click register on the main screen, we can register the reservation after being moved to the registration screen. The registration on the registration screen allows the administrator to register the reservation without needing to check the App for possible failures.

Fig. 3 shows the H/W configuration and S/W application for proposed system. Fig. 3-(a) shows the wired module attached to the back of the door lock after attaching Arduino module. Fig. 3-(b) shows registration display on smartphone application. When the user presses the door open button in the application, the Android studio passes the user information entered in the application to PHP. When the time and the information of the user are matched, the door open button is activated and the door lock is opened as shown in Fig. 3- (b).

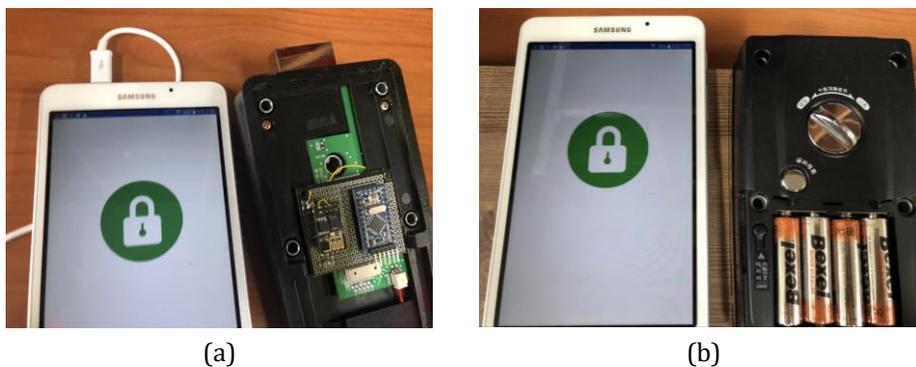


Fig. 3. The operation of the proposed system: (a) The integrated component configuration with door lock, Arduino and Tablet PC, (b) opening/closing function with smartphone application.

5. Conclusion

As IoT evolves, security problems will always exist. There for we must continue to utilize and improve IoT applications in order to ensure a secure environment [15]. In this study, IoT system was applied to the door lock to develop the security system of the equipment of the public facilities. Our system is not simply a door lock control system using a reservation system, but a certain user can control only at a specific time, and prevented access to other users or other times. In addition, web pages are integrated with door locks and applications so that administrators can easily manage the system anytime and anywhere.

Since the information of the user who reserved and opened the doorlock is recorded on the Web, it is expected that the manager will be able to manage the equipment of public facilities more efficiently and reduce the leakage of information of users. In addition to this, when the equipment of the public facility is damaged or lost, the manager can find the user directly and warn or ban the use of the equipment so that

damage or loss can be minimized.

In future work, we should apply various advanced technologies to the public security systems by adding more biometric information. In addition, when an Arduino is embedded in a conventional door lock, it can be developed into a built-in door lock system that can utilize the Internet.

References

- [1] Madakam, S., Ramaswamy, R., & Tripathi, S. (2015). Internet of Things (IoT): A literature review. *Journal of Computer and Communications*, 3(3), 164-173.
- [2] Chahid, Y., Benabdellah, M., & Azizi, A. (2017). Internet of things security. *Proceedings of International Conference on Wireless Technologies, Embedded and Intelligent Systems* (pp. 1-6).
- [3] Hung, C. H., Bai, Y. W., & Ren, J. H. (2015). Design and implementation of a door lock control based on a near field communication of a smartphone. *Proceedings of International Conference on Consumer Electronics-Taiwan* (pp. 45-46).
- [4] Pandurang, B., Pedde, J., & Rahul, G. (2016). Smart lock: A locking system using bluetooth technology & camera verification. *International Journal of Technical Research and Applications*, 4(1), 136-139.
- [5] Verma, G. K., & Tripathi, P. (2010). A digital security system with door lock system using RFID technology. *International Journal of Computer Applications*, 5(11), 6-8.
- [6] Prabhakar, S., Pankanti, S., & Jain, A. K. (2003). Biometric recognition: Security and privacy concerns. *IEEE Security Privacy Mag*, 1(2), 33-42.
- [7] Townsend, K., Cufi, C., Davidson, A., & Davidson, R. (2014). *Getting Started with Bluetooth Low Energy: Tools and Techniques for Low-Power Networking*. Sebastopol: O'Reilly Media, Inc.
- [8] Enhancing bluetooth location services with direction finding. Retrieved from <https://www.bluetooth.com/>
- [9] Wi-Fi. <https://en.wikipedia.org/wiki/Wi-Fi>
- [10] Schwartz, M. (2016). *Internet of Things with ESP8266*. Birmingham: Packt Publishing Ltd.
- [11] Royappa, A. V. (2000). The PHP web application server. *Journal of Computing Sciences in Colleges*, 15(3), 201-211.
- [12] Welling, L., & Thomson, L. (2003). *PHP and MySQL Web Development*. Indianapolis: Sams Publishing Ltd.
- [13] Zapata, B. C. (2013). *Android Studio Application Development*. Birmingham: Packt Publishing Ltd.
- [14] What is arduino. Retrieved from <https://www.arduino.cc/>
- [15] Hossain, M., Fotouhi, M., & Hasan, R. (2015). Towards an analysis of security issues, challenges and open problems in the internet of things. *Proceedings of IEEE World Congress on Services* (pp. 21-28).



Jaeun Seo is currently undergraduate students of School of Computer and Communication, Daegu University, Republic of Korea.



Narae Jeong is currently undergraduate students of School of Computer and Communication, Daegu University, Republic of Korea.



Jaejoon Kim received the MS and Ph.D degree from the Department of Electrical Engineering, Iowa State University, USA. He received bachelors from Department Electronics Engineering and Mathematics, Hanyang University, Korea. From 2001 to 2002, he was a senior researcher at ETRI (Electronics and Telecommunication Research Institute). He is currently a professor at Daegu University, Republic of Korea. His research interests include image processing, neural networks and non-destructive evaluation.