Advanced Science and Technology Letters
Vol.109 (Security, Reliability and Safety 2015), pp.33-38
http://dx.doi.org/10.14257/astl.2015.109.08

A Digital Door Lock System for the Internet of Things with Improved Security and Usability

Ohsung Doh[1], Ilkyu Ha[1]

[1] Kyungil University, Gyeongsan, Gamasil-gil 50, 712-701, Republic of Korea
ikha@kiu.kr

Abstract. Recently, digital door locks have been widely used as part of the IoT (Internet of Things). However, the media has reported digital door locks being opened by invalid users to invade homes and offices. In this study, a digital door lock system that can work with the IoT environment is proposed. It is designed and implemented to enhance security and convenience.
The proposed system provides strengthened security functions that can transfer recorded images to a user's mobile device when an invalid user attempts an illegal operation; it can also deliver alarm information to the mobile device when the door lock is physically damaged. The proposed system enables a user to check the access information and remotely operate the door lock to enhance convenience.

Keywords: Internet of Things, door lock system, digital door lock

1 Introduction

The Internet of Things (IoT) can be defined as a global infrastructure which combines intelligent services with situational awareness, and allows mutual communication between one thing and another, and between people and intelligent things over a network [1]. Machine to Machine (M2M) communication is different from IoT because a person does not directly control the equipment or intelligent instruments; they are responsible for communicating on behalf of people [2].

More recently, a variety of communication technologies have been fused to receive and provide information about things. Especially, IoT technologies have been enabled to communicate by the fusion of home appliances and mobile devices.

Recently, digital door locks have been widely used in households and offices. However, in many cases, an intruder has tried to penetrate a private area by circumventing the lock. In this study, we design and implement an IoT-based digital door lock to reduce the damage of digital door lock tampering and to enhance the various security and monitoring functions using IoT technologies.

ISSN: 2287-1233 ASTL

2 Related Work

Various studies [3–7] for enhancing the security and convenience of digital door locks have been proposed. Their summarized features are shown in Table 1.

Table 1. Features of previous digital door lock systems

Study (Year)	Main Function	Networking	IoT
[3] (2015)	Connecting to mobile devices Key sharing Access notification	Connection to a mobile device via Bluetooth	–
[4] (2014)	Image transfer	Connection of mobile devices	–
[5] (2012)	Door opening and closing by speech recognition	–	X
[6] (2012)	Controlling door lock in a short range with a mobile application	Communication via Bluetooth	–
[7] (2011)	Diffusion of alarm using the door lock	Interconnection of door locks	–
This paper	Impact detection / notification Image transfer Recording access information Image recognition / remote control Recognition of user proximity and automatic opening	Connection to a mobile device	X

Seo et al. [3] studied convenient digital door lock functions, such as remote control via the integration of mobile devices and key sharing. Lee et al. [4] proposed a method for detecting an accessing object and transmitting the object image. Kwak et al. [5] studied a method for opening and closing the door lock using voice recognition, without using a network. Potts et al. [6] proposed a security system that interfaces with an Android mobile device. The mobile and security system communicate via Bluetooth in a short range. Choi et al. [7] developed an application for communication between devices for transferring the state of the alarms generated in a home through a door lock in the neighborhood.

3 Design of the Proposed Digital Door Lock System

3.1 Main features of the proposed system

The main features of the proposed system are as follows. First, it has impact detection and alarm functions. This is to detect an intruder who tries to invade by applying physical force to the lock. Second, it has an image transfer function. Generally, an attacker who does not know the password will make a variety of attempts. Therefore,

if an attacker mistypes the password more than a given number of times, the system obtains images of the intruder and transfers them to the mobile device.
Third, the user can query the records of typed passwords and all incoming and outgoing records that are stored in the database. Fourth, the system can open the door lock in real-time after recognizing a visitor's image. If a visitor forgets the password, he can type a code into the door lock; then, the door lock system transmits his image to the mobile device user. The user can remotely control the door lock after reviewing the image. Fifth, the controller can detect a valid user approaching the digital door lock, if he is carrying the mobile device, and will open or close the door lock automatically.

3.2 Overall structure of the proposed system

The overall structure of the proposed system is shown in Figure 1. The proposed system consists of a digital door lock, a Raspberry Pi control board that is mounted in the lock, and the end-user's mobile device.

The controller detects physical impacts applied by a visitor, and notifies the user's mobile device. The controller detects if a password error occurs more than a certain number of times, and uses the camera to capture an image of the visitor. It then transfers the image to the user's mobile device. All of the access records are stored in the controller's database, which can be queried via the user's mobile device.

If a visitor has lost his key, his image is captured and transferred to the user's mobile device by pressing a specific key; the user can then control the door lock remotely after verifying whether the visitor is valid. Another important function of the controller is automatically opening or closing the door when a valid user comes near. When a valid user accesses the gate holding an object, because it is difficult to operate the door lock, the controller communicates with the user's mobile device via Bluetooth and opens the door lock automatically.

The mobile device acquires the impact detection information and the invalid visitor image information from the controller, and then the user can take appropriate action. Further, if the user acquires image information for a valid visitor, it is possible to open or close the door lock remotely. It is also possible to query the incoming and outgoing records.

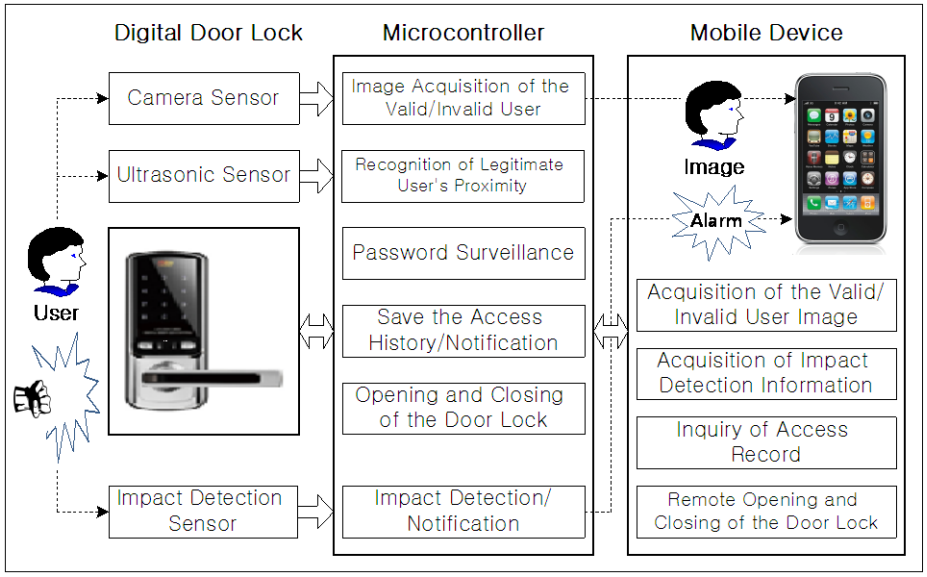

Fig. 1. Structure of the proposed door lock system

4 Implementation

The components of the proposed digital door lock system and their functions are shown in Table 2. A microcontroller is required to control the door lock and a Bluetooth module is used for communicating with the mobile device. An ultrasonic sensor is required to recognize a nearby user; an impact vibration sensor is also required. OpenWrt is used as the operating system; the program to operate the controller is written in C; and PHP and MySQL are used for the web server and database management, respectively.

Table 2. Components and features used to implement the door lock system

Component	Specifications	Function
Microcontroller	Arduino	Controller
Operating System	OpenWrt	Operating System
Web Server	UHTTP	Mobile App. Service
Database	MySQL	Data Storage
Language	PHP, C, Java	DB access, Shell, App
Camera	Logitech Webcam C170	Photograph shooting
Bread Board	Mini bread board	Sensor Accumulation
Ultrasonic Sensor	Grove-Ultrasonic Ranger	User Detection
Vibration Sensor	Analog Piezzo Vibration Disk	Impact Perception

Bluetooth Mobile Device	HC-06 Wireless Serial 4 Pin Bluetooth LG elec. G3	Communication Controller & Mobile Device Mobile Device

The mobile device and the microcontroller use Bluetooth for close range communication and WiFi communication for long distance. The digital door lock and the microcontroller are adjacent and connected by wire. The Arduino microcontroller and the mobile client use WiFi or Bluetooth, depending on the distance. A web server built into the microcontroller communicates with the mobile client via the HTTP protocol.

Figure 2 shows the menu structure of the mobile app for the digital door lock operation. The user can query all records of comings and goings from the 'Inquiry (Access Record) menu'. The 'Inquiry (Intrusion Record) menu' is for querying intrusion information, such as an invader's image taken by the controller when a password input error occurs. When an access request is generated by a valid visitor who does not possess the key, the 'Request menu' allows the user to check the image of the requester and open the door. The 'Open menu' allows for remote door operation. The 'Setup menu' allows for password management, etc.

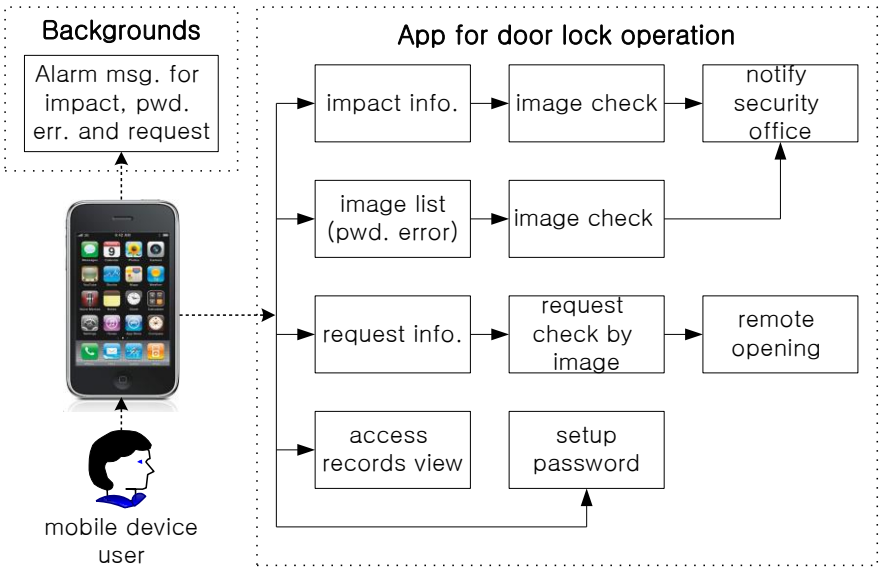

Fig. 2. Mobile app menu structure for digital door lock operation

5 Conclusion

In this paper, a digital door lock with enhanced security functions was designed to work with the Internet of Things. The designed digital door lock senses the physical impact of an invalid visitor and notifies the user's mobile device. If an incorrect pass-code is repeated more than a certain number of times, the lock captures an image of the invalid user and transfers it to the mobile device, thus, strengthening the security function.

The lock was designed to improve user convenience by allowing him to check the image of a valid visitor and open or close the door lock remotely. Another efficient system function is that when a valid user approaches the door, the door lock system opens or closes the door without additional operations. We expect that if the problems mentioned previously are resolved, the proposed system can be commercialized into a useful product, such as a secure security system with enhanced convenience, especially when compared to existing digital door lock systems.

Acknowledgment. This work was supported by the Korea Foundation for the Advancement of Science & Creativity (KOFAC), and funded by the Korean Government(MOE).

References

1. C. Pyo, H. Gang, N. Kim and H. Bang, "technology trends and prospects of development of IoT (M2M)," OSIA Standards & Technology Review, Vol.26, No.2, pp. 8-17, 2013.
2. Y. Ko, "Study of Policies of Major Countries on Internet of Things and Market Forecast," International Commerce and Information Review, Vol.16, No.5, pp. 27-47, 2014.
3. D. Seo, H. Ko and Y. Noh, "Design and Implementation of Digital Door Lock by IoT," KIISE Transactions on Computing Practices (KTCP), Vol.21, No.3, pp.215-222, 2015.
4. S. Lee, J. Park, B. Woo and H. Choi, "Video Digital Doorlock System for Recognition and Transmission of Approaching Objects," KIPS Transaction: Software and Data Engineering, Vol.3, No.6, pp.237-242, 2014.
5. T. Kwak and S. Moon, "A Digital Doorlock with Voice Recognition," in Proceedings of KIIT Spring Conference, Vol.2012, No.5, pp.345-348, 2012.
6. J. Potts and S. Sukittanon, "Exploiting Bluetooth on Android Mobile Devices for Home Security Application," in Proceedings of IEEE Southeastcon Orlango, pp.1-4, 2012.
7. Y. Choi, Y. Park, W. Back, D. Lee and J. Byun, "Development of Home Automation System using Digital Doorlock based on Wireless Sensor Network," in Proceedings of KIIT Summer Conference, Vol.2011, No.5, pp.189-193, 2011.

