International Journal of Security and Its Applications
Vol.9, No.8 (2015), pp.45-54
http://dx.doi.org/10.14257/ijsia.2015.9.8.05

Security and Usability Improvement on a Digital Door Lock System based on Internet of Things

Ilkyu Ha

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.

2. Related Works

Various studies [3–15] 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	O
[4] (2014)	Image transfer	Connection of mobile devices	O

ISSN: 1738-9976 IJSIA

[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	O
[7] (2011)	Diffusion of alarm using the door lock	Interconnection of door locks	O
[9] (2012)	Face Recognition	–	X
[10] (2015)	Face Recognition and automatic open	Sending SMS to Mobile phone	△
[11] (2015)	Door Lock for the home automation	–	X
[12] (2010)	Security application for door lock	–	X
[14] (2009)	Basic applications for remote control	Remote control	△
[15] (2013)			
This paper	Impact detection / notification Image transfer Recording access information Image recognition / remote control Recognition of user proximity and automatic open	Connection to a mobile device	O

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.

Hassan *et al*. [9] and Satti *et al.* [10] studied face recognition for the door lock open. In particular, the application of Satti et al. transfers the SMS about the legitimacy of the user to the mobile device. However, both of them cannot be a perfect IoT application because the door locks are not controlled by the mobile device remotely. Studies of Park *et al.* [11] and Verma *et al.* [12] are related to security applications for home automation. Studies of Khiyal *et al.* [14] and Ogri *et al.* [15], are initial studies [13] for remotely controlling a door lock, which cannot be classified also into application of the complete IoT.

The system proposed in this study strengthens the security functions. For example, if a physical impact is added to the intrusion attempt, the system notifies the user of the intrusion through the user's mobile device. Further, if someone inputs erroneous pass-codes more than a certain number of times, the system captures and transmits an image of the person [8].

To reduce the burden on the network, the proposed system transmits an image only when the input pass-code fails, unlike [4], which transmits a video of all accessing objects. In addition, it provides basic functions, such as remote control access and viewing all incoming and outgoing information that has been recorded on the system.

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.

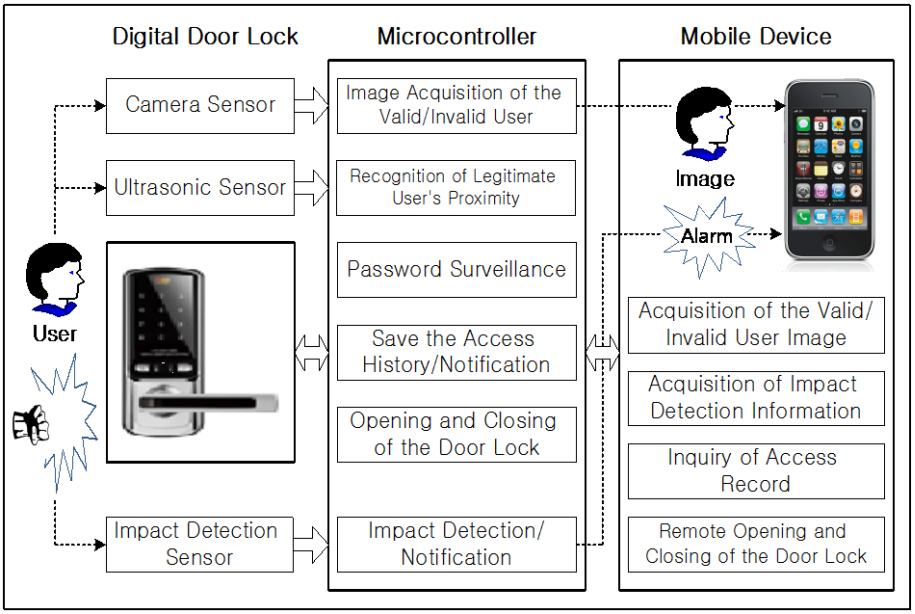

Figure 1. Structure of the Proposed Door Lock System

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. The pseudo code for the controller operation is shown in Figure 2. And the operation procedures for invalid and valid visitors are shown in Figure 3.

```
1.      foreach user
2.          input action
3.        switch action
4.          case "password":
5.              if password is request number then take and send image
6.              else if password is valid then open the door lock
7.            else if number of mismatch >=3 then take and send image
8.                          else go to step 2
9.           case "impact":
10.             impact sensor operation
11.             if impact value >= threshold value then camera sensor operation
12.         else go to step 2
13.       case "proximity":
14.         if distance >= threshold value then mobile device synchronization
15.           If valid user then send password, door open
16.           else go to step 2
17.         else go to step 2
18.     End
```

Figure 2. Pseudo Code for the Operation of the Door Lock Controller

4. Implementation

4.1. Hardware Components and Configuration of the Proposed System

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 of the system; the program to operate the controller is written in C; PHP and MySQL are used for the web programming and database management, respectively; and UHTTP is used for the web server instead of Apache.

Besides, various sensors for proximity and intrusion detection are connected to the system. A camera sensor for photographing an image of invalid users is installed, an impact sensor is attached for detecting a physical shock by an invalid user, and an ultrasonic sensor is attached to recognize the proximity of valid users. In addition, the G3 of LG is used as a mobile terminal for the experiment.

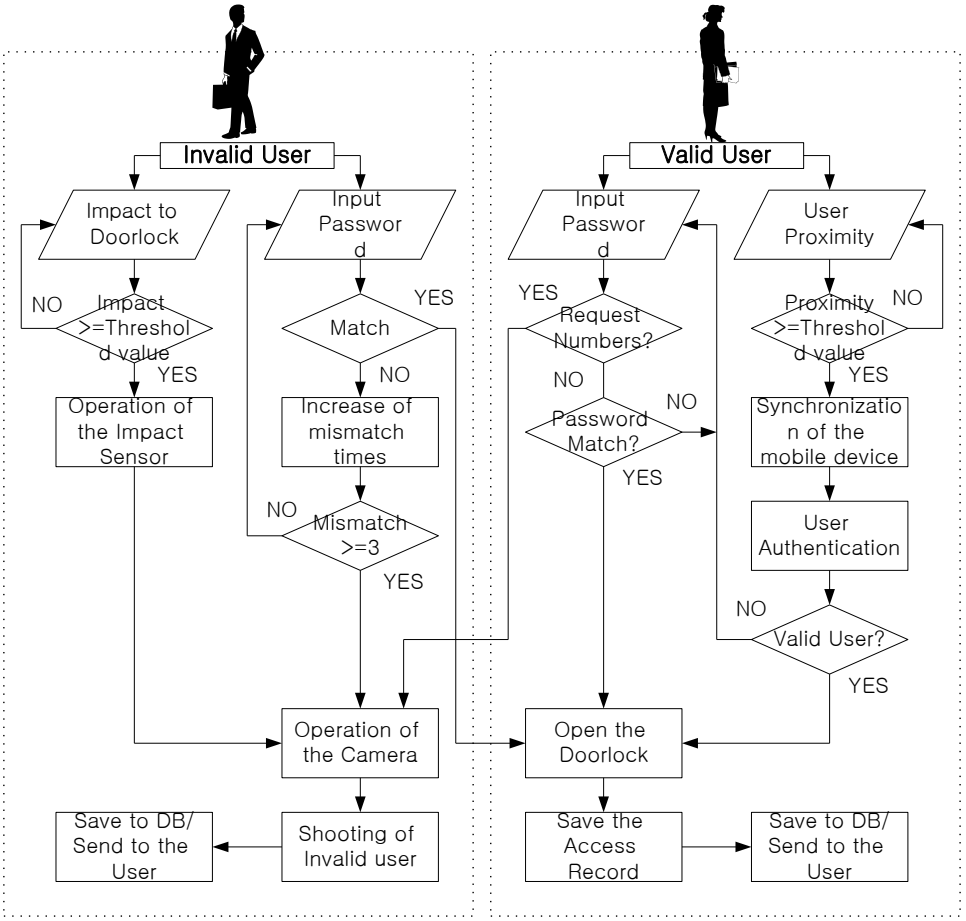

Figure 3. Digital Door Lock Procedures for Invalid and Valid Users

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

The components described above have been integrated, as shown in Figure 4. The ultrasonic sensor for sensing an impact, the camera sensor for taking a picture, and the vibration sensor are all connected to the micro-controller.

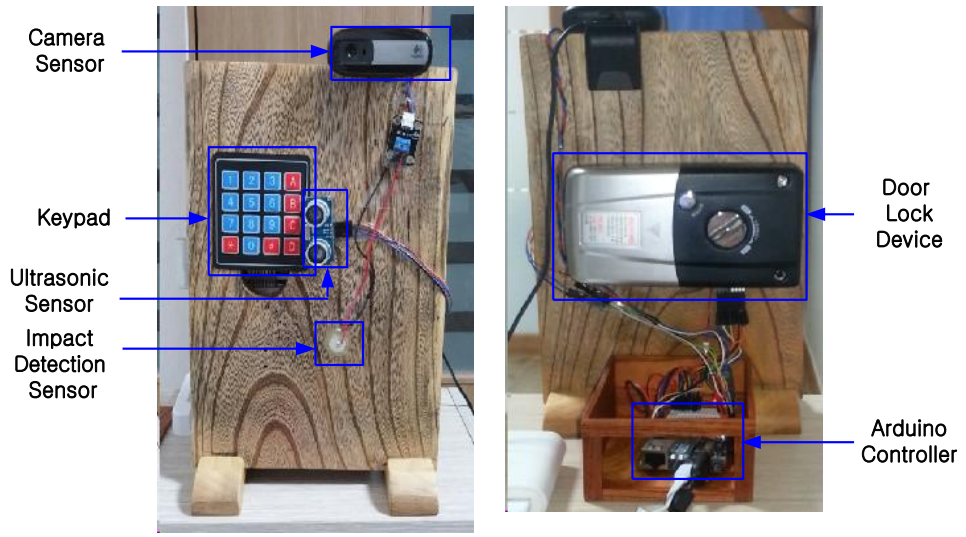

Figure 4. Hardware Configuration for the Proposed System

4.2. Apps for Remote Control

Figure 5 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 'Log (Access Record)' menu. The 'Capture Log (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 'Remote opening' menu allows for remote door operation. The 'Option' menu allows for password management and 'Bluetooth synchronization (Master mode)' menu is a setting menu for automatic opening when approaching the door lock. Figure 6 shows the application cases for remote controls. The left side of the top of the figure is the main menu of the App, the right of the top shows the Bluetooth setup button for proximity open and a keypad for the remote open. The left of the bottom of the figure shows a list of the image information that has been captured by physical shock and the input mistake of password. And the right of the bottom shows an image of the item in the list.

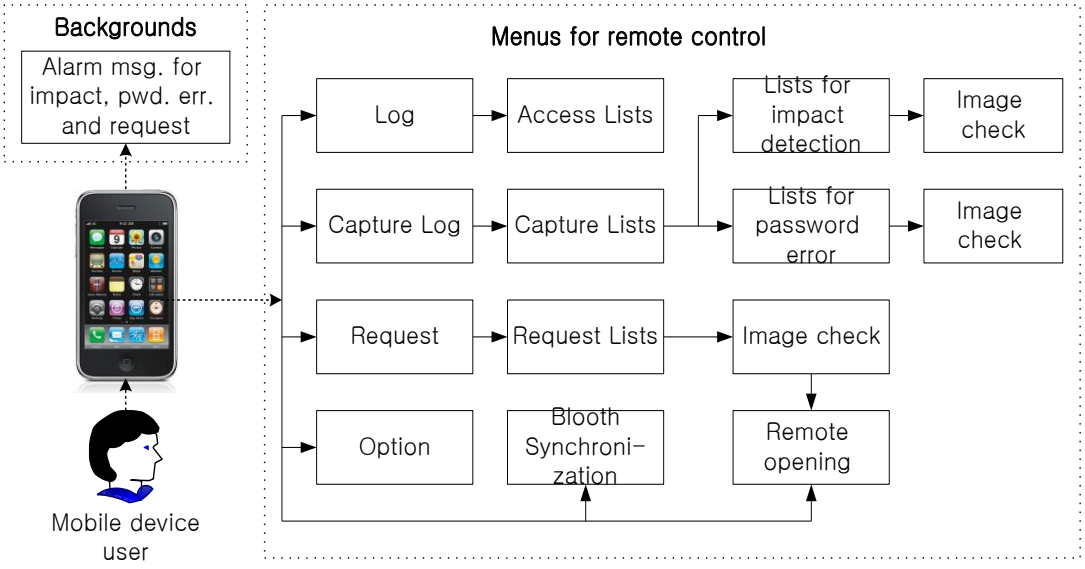

Figure 5. Mobile App Menu Structure for Digital Door Lock Operation

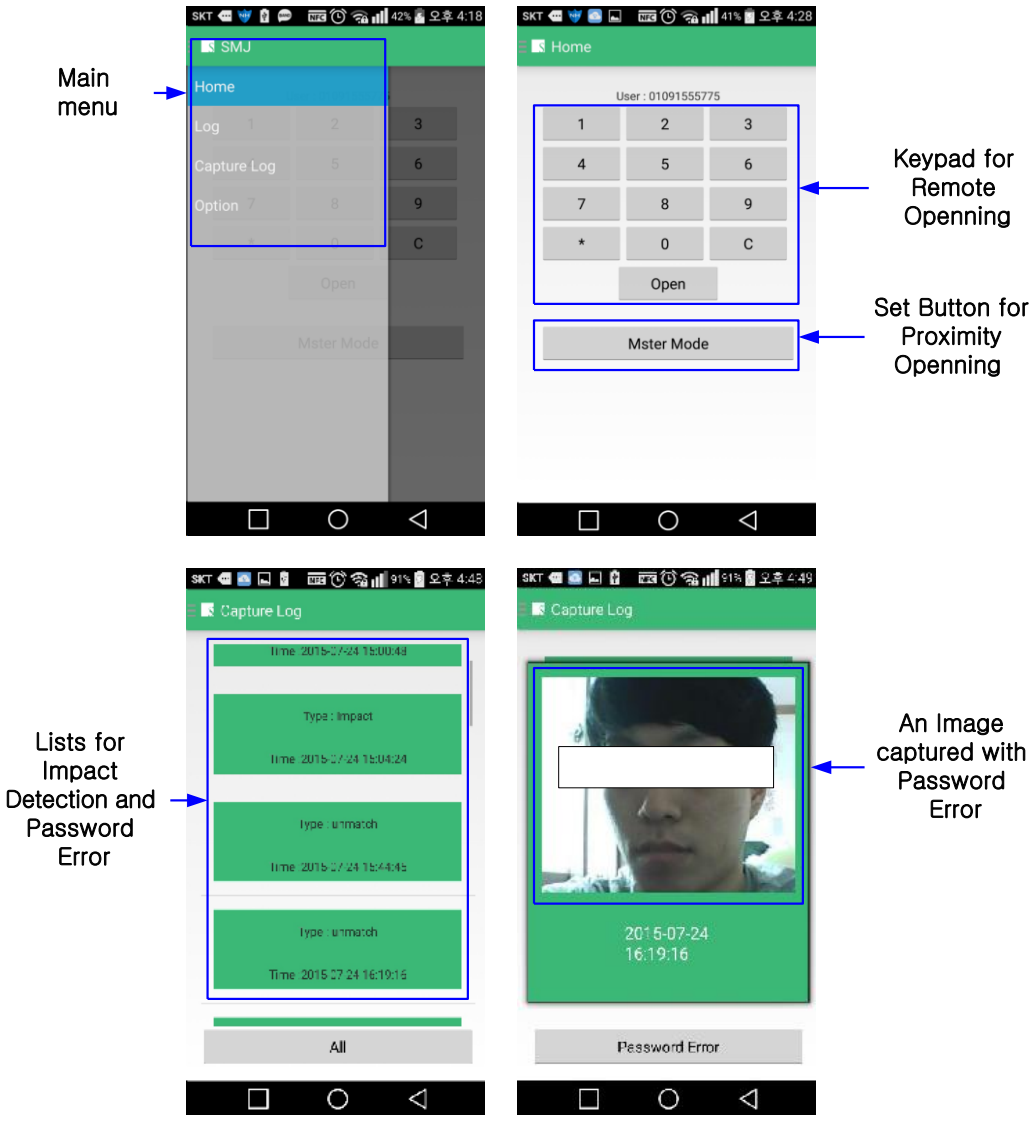

Figure 6. Apps for Remote Control

4.3. Experiments

Figure 7 shows the reaction time of each sensor. All of the sensors act to actions of the valid and invalid user in 2 seconds. For example, the ultrasonic sensor can take from 1.6 seconds to 1.8 seconds to check a valid user and open the door. One of the most important features of our proposed system is to check an invalid password of an invalid user. It takes 1.41 seconds on average to detect an invalid password, take a picture of the user and send the picture to a mobile device.

The proposed digital door lock system in this study has several implementation problems. The first problem concerns the image captured by the camera's sensor when an incorrect password is entered. If the invader intentionally covers the camera lens or deviates the focus from him, it will be impossible to collect an accurate image. Second, since the shock sensor senses a certain amount of impact whenever the door opens or closes, it is difficult to distinguish an abnormal impact. These problems will be resolved as future challenges.

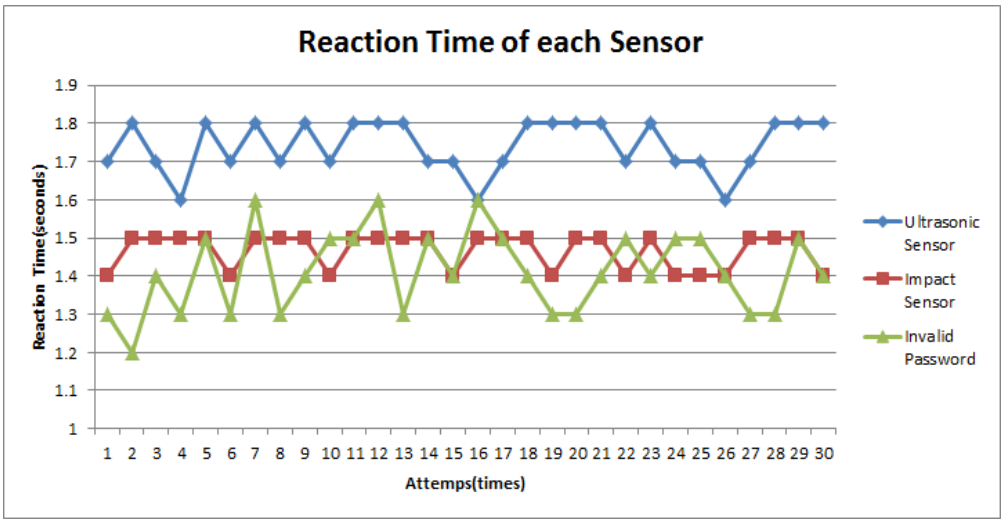

Figure 7. Reaction Time of Each Sensor

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.

Acknowledgements

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, (**2013**), pp. 8-17.
[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, (**2014**), pp. 27-47.
[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, (**2015**), pp. 215-222.
[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, (**2014**), pp. 237-242.
[5] T. Kwak and S. Moon, "A Digital Doorlock with Voice Recognition," in Proceedings of KIIT Spring Conference, vol. 2012, no. 5, (**2012**), pp. 345-348.
[6] J. Potts and S. Sukittanon, "Exploiting Bluetooth on Android Mobile Devices for Home Security Application," in Proceedings of IEEE Southeastcon Orlango, (**2012**), pp. 1-4.
[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, (**2011**), pp. 189-193.
[8] O. Hoh and I. Ha, "A Digital Door Lock System for the Internet of Things with Improved Security and Usability," Advanced Science and Technology Letters, vol. 109, (**2015**), pp. 33-38.
[9] H. Hassan, R. Bakar, and A. Mokhtar, "Face Recognition Based on Auto-Switching Magnetic Door Lock System Using", in Proceedings of 2012 International Conference on System Engineering and Technology, (**2012**), pp.1-6.
[10] R. Satti, S. Ejaz, and M. Arshad, "A Smart Visitors' Notification System with Automatic Secure Door Lock using Mobile Communication Technology," International Journal of Computer and Communication System Engineering, vol. 2, (**2015**), pp. 39-44.
[11] Y. Park, P. Sthapit, and J. Pyun, "Smart Digital Door Lock for the Home Automation", in Proceedings of TENCON 2009, (**2009**), pp. 1-5.
[12] G. Verma and P. Tripathi, "A Digital Security System with Door Lock System Using RFID Technology", International Journal of Computer Applications, vol. 5, no. 11, (**2012**), pp. 6-8.
[13] M. Roy, F. Hemmert, and R. Wettach, "Living Interfaces: The Intimate Door Lock," in Proceedings of the Third International Conference on Tangible and Embedded Interaction (TEI'09), (**2009**), pp. 45-46.
[14] M. Khiyal, A. Khan and E. Shehzadi, "SMS Based Wireless Home Appliance Control System (HACS) for Automating Appliances and Security", Issues in Informing Science and Information Technology, vol. 6, (**2009**), pp. 887-894.
[15] U. Ogri, D. Okwong, and A. Etim, "Design and Construction of Door Locking Security System using GSMY", International Journal Of Engineering And Computer Science, vol. 2,no. 7, (**2013**), pp. 2235-2257.

Author

Ilkyu Ha, He received the Ph.D. degree in computer engineering from Yeungnam University, Korea. He is currently an assistant professor in computer engineering department at Kyungil University. He was a software developer at Financial Supervisory Service (FSS) of Korea, a senior researcher at center for innovation of engineering education at Yeungnam University. His research interests include Sensor Networks, Body Area Network, Internet of Things and Research Trend Analysis.