Development and application of an internet of things door lock Network Bridge for classroom access control management

Cheng Hsiu Li, Chi Yu Chen, Xuan Rui Huang, Ting Fu Tsai and Bo Yang Liu
Department of Information Management, National Taitung Junior College, Taitung, Taiwan

E-mail: lcs@ntc.edu.tw

Abstract. School classroom doors are usually managed using conventional machine locks. This can cause inconvenience for the borrowing and returning of keys. In addition, issues on the copying and embezzlement of keys are persistent. To avoid these problems, schools have replaced conventional locks with card readers and magnetic locks to manage classroom access; users need only a RFID card to enter and exit classrooms. However, the hardware and software equipment required for such control schemes is expensive and entails cumbersome installation processes. This study developed an innovative Internet of Things (IoT) door lock network bridge, which can be installed on conventional electronic locks to transform it into IoT locks. The developed bridge can be integrated with a customized web-based classroom access information system and QR code scanning to establish a low-cost classroom access control system. The system can be provided to schools to perform user management, lock management, and lock matching. Each door in the school is assigned with a unique QR code for unlocking. Users only need to use the QR code scanner on their smart phone to send relevant information required for unlocking a door to the web-based classroom access information system, which then performs user and lock matching verification. Verified users can then unlock the door and enter the venue. The proposed classroom access control system does not require card readers or RFID cards. The cable installation of the system is simplified through by using wireless connections, thereby greatly reducing the time, cost, and human resource required for installation. In addition, users and locks can be matched directly using the proposed system. This greatly improves the convenience of classroom management in schools.

1. Introduction
Access to school classrooms is generally controlled with traditional mechanical locks. Apart from the inconvenience of borrowing and returning keys, traditional mechanical locks all provide poor security due to a notable disadvantage: keys are easily copied [1-2]. Electronic locks are common door management devices. Some common electronic locks are electric bolt locks, magnetic locks, electric control locks, silent locks, and electric motor locks. Electric bolt locks are divided into 2-line electric bolt locks, 5-line electric bolt locks, and 8-line electric bolt locks according to the number of wires. The common parts are the red and black wires. The red wire connects to the direct current (+12 V), and the black wire is the ground wire (GND). When the power is cut, the lock retracts, and the door opens. Magnetic locks are also called electromagnetic locks. They are locks that rely on the attraction force generated between electromagnets and iron blocks. They are also electric locks that open when
power is cut. Electric control locks have large impact currents; they make an audible “snap” sound when the door opens. The noise is louder, and the installation is less convenient. During installation, installers must be noted that the time delay of opening the door must not be too long, and it is generally set within one second. Due to the loud-noise disadvantage of the electric control lock, the silent lock was designed. Another quiet electric lock is the electric motor lock. It drives a small motor to move the bolt. Electric control locks, silent locks, and electric motor locks can also be opened with a lock knob inside the door or a key. They are mainly used in household doors of communities and combined two-door emplacements in banks. For the type of electric lock required when installing access control, the door type is the crucial point for consideration [3].

Radio Frequency Identification (RFID) is a wireless communication technique that identifies specific targets through radio signals and reads related data. The system does not require mechanical or optical contact between the identification system and the specific targets. The radio signals transmit data from the tags attached to the object by tuning the electromagnetic fields of radio frequencies to automatically identify and track the objects. For a typical identification event, some tags can obtain energy from the electromagnetic field emitted by the identifier and does not require a battery. Some tags have power themselves and can actively emit radio waves (that are tuned to the electromagnetic fields of the radio frequencies). The tags contain digitally stored information that can be identified within several meters. Unlike barcodes, radio frequency tags are not required to be within the scanning vision of the identifier, and they can also be embedded into tracked objects. The RFID technique is used in various industries. In automobile manufacturing, tags are attached to a car that is in production, and the factory can easily track the progress of this car in the production line. In pharmaceutical logistics, locations of medication can be tracked in warehouses. RFID tags can be attached to livestock and pets for identification. RFID cards can allow employees to enter locked doors in buildings with gate control. The radio frequency transponders on cars can also be used to collect the fees for toll roads and parking lots [4-5]. RFID technology offers identification without contact, so card readers and electromagnetic doors are gradually being used in current classrooms to assist management. Each user only requires an RFID card to enter or leave the classroom. However, relative to the costs of other software, hardware, and installation projects, RFID costs are high, and installation is time- and labor-consuming [2].

In 1995, Bill Gates developed his smart home fantasy in his book The Road Ahead, which proposed ubiquitous Internet-connected devices. In 1998, Kevin Ashton, the Auto-ID center director at the Massachusetts Institute of Technology proposed the term Internet of Things (IoT). Globalized Internet infrastructure connects physical objects and virtual data through data extraction and communication for different types of control, detection, identification, and service. Since then, the term has been circulating extensively. Since the introduction of IoT, objects such as cell phones, refrigerators, tables, coffee machines, and weight scales have become smart devices. Consider, for example, a smart refrigerator: when it is out of order, it automatically sends maintenance information. Refrigerators also connect with gas company databases and remind people if the gas has run out. IoT not only makes peoples’ lives more convenient but also brings greater safety [6].

Gao He-xuan, the chairman of D-Link Corporation, stated that the most important factor of the rise of IoT is smart phones. Cell phones are the control centers of IoT devices [6]. Barcodes can be seen everywhere in peoples’ lives, from the backs of merchandise packages in convenience stores to the tags of registered-mail items. The use of barcodes makes it easier to manage merchandise items. The information can be obtained with barcode scanners. Due to technological advancement, every cell phone has high-pixel camera lenses. Barcodes can be shot and decoded with programs. Thus, cell phones can become barcode scanners that can easily read the information in barcodes.

Consequently, this study aims to develop a brand-new IoT door lock network bridge. After this network bridge has been installed on a traditional electric lock, it can become an IoT door lock that connects the electric lock to the Internet. Thus, the lock can be controlled through cell phones. Then, the device is combined with a customized Web-based classroom access information system and Quick Response Codes (QR codes) to establish a low-cost classroom access system. This system provides the
access management functions of user management, door lock management, and door control for schools. This system can replace old classroom access management systems that feature RFID card readers and electromagnetic doors.

2. Literature review
In this study, related RFID literature was examined, and the aspects of hardware design, certification mechanism, virtual key, and establishment cost were discussed as the academic foundation of this study.

Regarding hardware design, Qiu (2018) used Raspberry Pi, RFID, and camera lens modules to develop a card-sensing classroom access system. The system offered the functions of clock punching, photography, and recording, and the records were stored for inquiry [7]. Liao (2010) used the characteristic of super-high-frequency near-field and far-field RFID to read electronic tags; this achieved the goal of access control for people and cars with only one card. When people and cars enter or leave a restricted area controlled by Liao’s system, only one access control card is required. The system offers indoor and outdoor access with only one card. It not only avoids extra cost of card manufacture for cars but also integrates access control card management for cars and people [2]. Currently, most access control systems use RFID card access control.

For an access control certification mechanism, Hong, Tsai, and Hong (2005) proposed a RFID smart card. The four techniques of Hash, AES, Random values, and XOR were combined with third-party certification to solve the safety problems of eavesdropping, tracking, and forgery of RFID smart cards. In addition, an active protective system was also added in the structure to further reinforce the safety system. Thus, the risk of attackers using replay attack or DoS attack to overload the safety system was avoided [5]. Chen (2018) proposed a RFID safety certification protocol in the tags with low calculation cost; this protocol was founded on SCR. This smart reader can run the calculations of XOR functions, hash functions, and random number generators while having memory to store the results. The safe qualities of forgery prevention, two-way certification, privacy protection, replay attack protection, and forward safety can be achieved. The proposed certification protocol is more suitable for the application in the IoT operating environment [8]. Liu (2010) used access control keys with RSA and DES encryption algorithms to improve the safety of the data transmission process of access control keys. In addition, the keys are transmitted to cell phones through the PDA wireless Internet function. Then, they are transformed into visualized access control keys of QR codes for the classroom access safety management. The purpose is to allow users to verify their identities and obtain QR code access control keys through mobile devices. For users, the manufacturing cost for lost access control cards is reduced, and the administrative procedure of reissue and cancellation is simplified [9].

For the establishment cost, the cost of the RFID access control used by Yang (2014) is substantially lower than that of manual management. The cost is only 4.78% of the full manual cost, and superior management effects can be achieved. The system records were analyzed, and the average normal door opening probability was higher than 98%. The average incidence rate was lower than 2% [10].

3. System structure and operation model
The classroom access control system (abbreviated as “this system”) is composed of three major components. They are the web-based classroom access information system, QR codes, and IoT door locks. The IoT door locks consist of IoT network bridges and electronic locks. The system structure is illustrated in Figure 1. The web-based classroom access information system mainly manages member data, door lock data, access control matches, and QR code decoding. The QR codes transmit the decoding information of lock opening locations. The IoT door locks receive the lock opening information and open the locks.

The system operation model is depicted in Figure 2. Students can open the locks through smartphones and the QR codes on the door locks of every classroom on campus. Assume that a campus has m students (m > 0) and n classrooms (n > 0). Then, that campus has n QR codes and IoT door locks. Only one IoT server is required to be operational for lock opening verification. If a student wants to
open a classroom door lock (door lock #2), the student will scan the QR code on the door lock (QR #2) with a smart phone. The system first guides the student to an account and password login screen for identity verification. After the verification is successful, the location code on the QR code will be checked for location verification. Then, the door lock matching verification of the user, door lock, and usage period is conducted. If the user is in the authorized usage period, the door lock opens and allows the user to enter.

![Diagram of system structure](image1)

**Figure 1. System structure**

![Diagram of system operation model](image2)

**Figure 2. System operation model**

4. **System design and implementation**

4.1. *IoT door lock network bridge design and IoT door lock implementation*

In this study, IoT technology was used for the design and implementation of the proposed IoT door lock network bridge. This network bridge can connect the electronic lock on the door to the Internet; that connection defines the door lock as an IoT door lock. This door lock can then be controlled through the Internet. Its design concept is schematized in Figure 3. The input end is connected to electrical power, and the output end provides the trigger message to the electronic lock.

Figure 4 presents the hardware structure of the IoT door lock network bridge. It is mainly composed of a Webduino development board and a relay. The Webduino development board consists of an Arduino pro mini development board and a Wi-fi chip. The input end (VCC) is connected to 5V of DC power, and the output end transmits the signals of VCC, GND, and trigger (IN) to the relay. The input end of the relay receives the signals of VCC, GND, and trigger (IN) from the Webduino,
and the normally-open switch of the output end (NO and COM) is connected to the electronic lock. After the input end of the relay receives the trigger signal, the normally-open switch must close, which triggers the electronic lock to connect the circuit and open the door. A photograph of the actual completed system is given in Figure 5.

Figure 3. Design concept of the IoT door lock network bridge

Figure 4. Hardware structure of the IoT door lock network bridge

Figure 5. Implementation of the IoT door lock
4.2. Lock opening mechanism
A triple verification mechanism is adopted. The location match, password match, and door lock match are verified. First, a QR code is scanned by a cell phone to transmit the location decoding information through the Internet for location verification. Then, the web-based classroom access control information system decodes the location and verifies the password. After the location and password verifications are passed, the information system must conduct the door lock match verification. If the user is authorized to use that door lock, and the time is within the authorized usage time, the information system connects over the Internet through the wireless access point to the IoT door lock. The lock opening signal is then transmitted to the IoT door lock to open it.

The web-based classroom access control information system provides the functions of user management, door lock management, and door control matching. Each user must apply for an account and use the related services after logging into the system through a personal account and a password. The services include checking the authorized classroom door locks, door lock usage records, and checking or changing personal information. Managers can manage user information, door locks (creating doors), door control match (designating doors), and viewing all lock opening records. When a door is created in door lock management, the IoT door lock network bridge number (Webduino device ID) and the name of the classroom are set (through the interface presented in Figure 6). After users and doors have been recorded in the database, the door control matching of users and doors can be conducted. The authorized usage periods of door locks must be set (as presented in Figure 7); these periods specify which users are allowed to enter which classrooms during which periods.

The verification of location mainly verifies if the user is at the door to avoid opening locks by mistake. The system has multiple methods to verify the location. Passive infrared sensors or image identifiers can be used to sense whether the user is at the door. However, such sensors increase the costs of hardware, wiring, and development. In this study, the location verification was conducted with software. The Internet was the medium between QR codes and IoT servers. To avoid counterfeiting in the transmission process and verify that the user is indeed at the location of the lock, a random code was added referencing the randomized access control method in this study. The website address of the server (such as http://IoTwebsize) is embedded into the lock opening key (key=randomcode) into a QR code. The QR code transmits a coded website address (such as http://IoTwebsize/index.php?key=20200410081112) to the information system for decoding. After the lock opening key has been verified to be the correct random code, the lock opening screen is opened so that the user can open the lock. Because the lock opening key in the QR code of every classroom is randomly generated, users cannot know it in advance or enter the information system through a remote connection. They must scan the QR code at the classroom door to transmit the lock opening key. Thus, the location is verified. In addition, using software for verification not only substantially reduces the cost of hardware purchase and installation but also simplifies the construction. The process of QR door lock coding and decoding is presented in Figure 8.

![Figure 6. Door lock management](image)

![Figure 7. Door control match](image)
5. System test and efficacy evaluation

5.1. System test

1. Test environment and subjects

Almost every student on campus has a cell phone, so the campus has a sufficient number of mobile devices. Classrooms are one of the best locations for the establishment of this access control system.

In this study, the management department classroom in National Taitung Junior College was selected as the test environment, and 10 students of the management department were randomly selected as the test subjects.

2. System test

In this study, 10 test subjects were randomly selected for the system test. The test is presented in Figure 9.

According to the test results listed in Table 1, the average lock opening time was 9.2 seconds, and the lock was successfully opened at a 100% rate.

| Test subject number | Opening time (second) | Successful opening or not |
|---------------------|-----------------------|---------------------------|
| Student #1          | 10                    | Yes                       |
| Student #2          | 9                     | Yes                       |
| Student #3          | 11                    | Yes                       |

Figure 8. Coding and decoding process of a QR door lock

Figure 9. IoT door lock test
5.2. Establishment cost analysis
An investigation indicated that the price of general smart electronic locks (including cloud functions) (reference https://my-best.tw/21229) on the market was between 9,690 NTD and 20,760 NTD (at the time of writing). The price of the IoT door lock developed in this study was 2,000 NTD; the IoT door lock cost analysis is listed in Table 2. If the original environment already has an electronic lock, only a 1,000 NTD IoT door lock network bridge is required. Consequently, the equipment cost can be substantially reduced by a factor ranging from 4.8 to 10.3 (with the price of 2,000 NTD for comparison). The installation cost can be substantially reduced.

| Number | Item name                  | Cost | Note               |
|--------|----------------------------|------|--------------------|
| 1      | Webduino development board| 840  |                    |
| 2      | Relay                      | 35   |                    |
| 3      | Electronic lock            | 1,000| (optional)         |
| 4      | Miscellaneous              | 125  | Wire and 3D printing materials |
| Total  |                           | 2,000|                    |

6. Conclusions
In this study, a new IoT door lock network bridge was successfully developed. Combining the network bridge with an electronic lock can produce an IoT door lock. A low-cost classroom access control system can be established by combining an IoT door lock with a customized web-based classroom access control information system and QR codes. According to the system test results, the average lock opening time was 9.2 seconds, and 100% of users successfully opened the lock.

This classroom access control system does not require card readers and RFID cards. The wireless connection also simplified the installation. According to the analysis, typical equipment costs 4.8 times to 10.3 times as much as the proposed hardware. In addition, if the original campus already has electronic locks, only the IoT door lock network bridges are required. The proposed system can substantially reduce the cost, time, and manpower required for lock deployment and management. The classroom management can be done with door control that matches directly through the system. The convenience of classroom management can be substantially improved.

References
[1] What is the Difference between the Door Lock and the Electronic Lock? Safety Comparison of 4 Door Lock Types 2016 https://decomyplace.com/newspost.php?id=4580&ref=sg
[2] Liao D Y 2010 Application of UHF RFID Technology in Security Access Control https://www.digitimes.com.tw/iot/article.asp?cat=130&id=0000179326_ed94ito01nf3be7h3nxc
[3] Graphic Classification and Installation of Access Control Electric Lock 2018 https://kknews.cc/zh-tw/news/q5pjary.html
[4] Weis S A 2007 RFID (Radio Frequency Identification): Principles and Applications (MIT CSAIL)
[5] Hung Y C, Tsai C W and Hong C H 2005 Discussion on Security Framework of RFID Access Control Identity Authentication System RFID In Proceedings of 2005 Taiwan Academic
Network Conference (TANET 2005)

[6] Wong S T 2015 30 Keywords! Let You Understand the Internet of Things (IoT) https://www.bnext.com.tw/article/34549/bn-article-34549

[7] Chiu S W 2018 College of Science, National Chiao Tung University (Unpublished Master Thesis)

[8] Chen Y C 2018 Department of Computer Science and Information Engineering, Chung Hua University (Unpublished Master Thesis)

[9] Liu C Y 2010 Institute of Information Technology and Application, College of Informatics, Kao Yuan University (Unpublished Master Thesis)

[10] Yang M H 2014 Department of Industrial Engineering and Management, National Chiao Tung University (Unpublished Master Thesis)