Design and Implementation of a Door Lock Control Based on a Near Field Communication of a Smartphone

Chi-Huang Hung *, Ying-Wen Bai, Je-Hong Ren
Department of Electrical Engineering, Fu Jen Catholic University, New Taipei City, Taiwan
Graduate Institute of Applied Science and Engineering *, Fu Jen Catholic University, Taiwan
Department of Information Technology *, Lee-Ming Institute of Technology, New Taipei City, Taiwan

Abstract--**In this paper we propose an integration design of both a near field communication (NFC) and a smartphone to achieve a door lock control system. This design consists of a built-in NFC capabilities of a smartphone combined with a dedicated application deemed to be a key to open the door by means of the logical link control protocol (LLCP) exchange together with a time stamp to match the user's own set of password information to verify who is a permissions user or not. When verified the specific door which is secured by this door lock control system immediately opens.**

I. INTRODUCTION

The NFC technology uses the radio frequency identification (RFID) technology to perform non-contact standard data exchange between two NFC devices. Previously, the RFID technology was very commonly used in contactless access control cards, electronic tags and ETC systems. And now, NFC communication applications of RFID technology have gradually been replaced. NFC technology has gradually become integrated in smartphones which can directly read NFC tags in a message, such as, for example: credit card numbers, travel card numbers and these transaction records are able to be stored in an NFC tag [1]. NFC communication results are convenient; moreover, this system can also be integrated into a door access security system [2].

This paper proposes a design that does not need to use a complex face identify system, but instead uses a certain safety lock system together with NFC technology. Figure 1 shows the diagrammatic sketch of the system which includes a magnetic lock, access control systems (ACS) and an NFC based smartphone. Only two steps are necessary for a user to be able to open a door, "sensing" and "Enter Password". In this system with a password application built in the smartphone, the security level will be higher than traditional in RFID door lock systems.

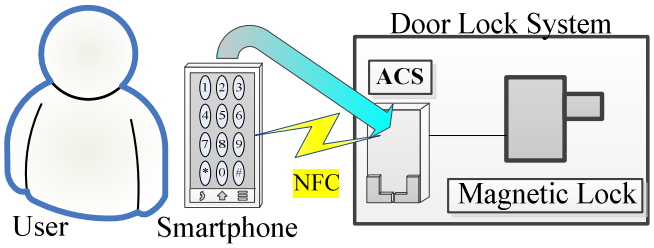

Fig. 1 Arrangements of the door lock system which includes a smartphone control mechanism.

II. HARDWARE ARCHITECTURE

Figure 2 shows a smartphone and a door lock system hardware architecture. The access control system can be divided into five parts: micro controllers (MCU), magnetic lock, real time clock module, status indication and the NFC reader module as shown in Figure 2, which is a low-power MCU chip. In addition to controlling the magnetic lock on/off, buzzer sounds inform and LED lights indicate what is taking place. There are two more functions. First, it reads the time by means of a real time clock, which will encode the card number, time and passwords, all which become a serial number. Second, it decodes those data which are obtained from a smartphone with an NFC card reader and compares the result with its own data area to determine if an individual is an authorized user or not.

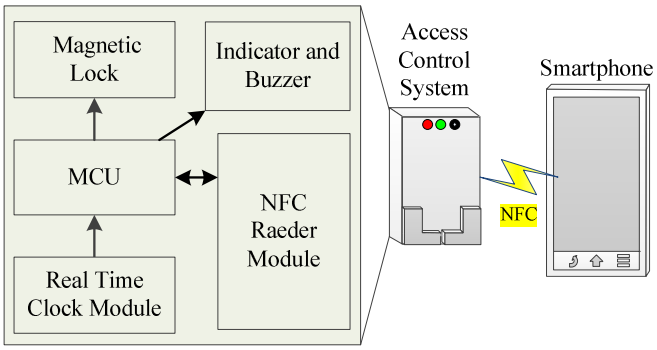

Fig. 2 Hardware architecture of the door lock system with a smartphone NFC.

Figure 3 shows that the door lock system with an internal MCU has become the main function module. The MCU uses a serial peripheral interface to connect with the NFC reader module. The NFC data exchange format (NDEF) message is designed by using an open source library supported by a smartphone. Therefore, MCU can easily to access the NFC tag information. The MCU uses an I^2C interface connected with a real time clock module to obtain the timestamp. When the smartphone accesses the system, the time will be recorded by the real time clock module. The system will combine it with the password into a sequence code to identify whether the door can be opened. Hence, this design will strengthen the security of the original password.

978-1-4799-8745-0/15/$31.00©2015 IEEE

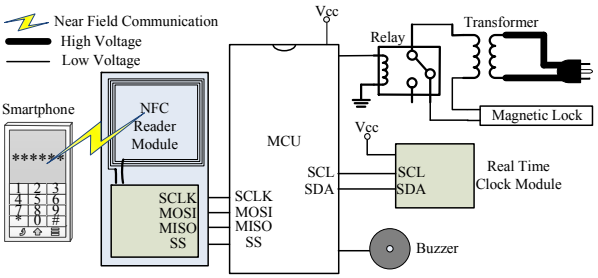

Fig. 3. Block diagram of the door lock system.

III. SOFTWARE DESIGN IMPLEMENTATION

The software design is divided into two modules: smartphone and DLS operation module. The smartphone should have an NFC system that can be compatible with our system. The DLS program is designed by using the embedded platform. The internal NDEF message part uses the open source library supported by the smartphone [4].

A. Smartphone Operation Module Flowchart

Figure 4 shows the initial interface and the keypad interface. The initial interface provides the "smartphone ID" which is input into the door lock system. When the system is set to the read mode, the user can enter the user password.

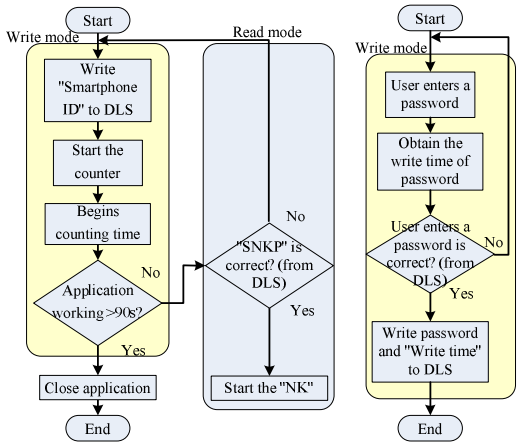

Fig. 4. Flowchart showing the smartphone initial interface and the numeric keypad.

B. Door Lock System Operation Module

When the DLS obtains permission, the smartphone provides the interface of the "start numeric keypad password (SNKP)" to the user. The door lock system reads the "numeric password" and obtains a timestamp via the real time clock module. If the identification of the door lock system "numeric password" is correct, then the door lock system opens the magnetic lock; if the "numeric password" is in error, then the door lock system triggers the buzzer to sound.

IV. EXPERIMENT RESULTS

Table I shows the actual measurement of the power consumption of each module. The NFC reader module of this design consumes only 158.4mW standby power. After comparing other designs, we note that our design consumes less standby power than that of other designs.

TABLE I
THE POWER CONSUMPTION OF EACH PART OF THIS DESIGN

Power Consumption	Standby Consumption	Operating Consumption
Active Buzzer	0.55mW	210mW
NFC Reader Module	158.4mW	528mW
MCU	70mW	73.5mW
Total	233.45mW	810mW

Table II compares our design with other door access system designs. Design A uses a smartphone with NFC reader communication, and obtains the pre-stored encoding pictures. The smartphone connects to a remote server, decodes the encoded pictures, and obtains a permission password. Design B uses a smartphone with a MCU Bluetooth connectivity. The MCU connects to the NFC reader, and its message is transmitted to the other end of NFC reader. Design A and B both use smartphones with an NFC function to verify and give permission to open the door. But in this design, we add a personal password that can provide more protection for the system.

TABLE II
A COMPARISON OUR DESIGN WITH OTHER SYSTEM DESIGNS

	Design A [2]	Design B [3]	Our Design
Passcode match	No	No	Yes
Time stamp	No	No	Yes
Convenience	Low	High	High
Security	High	High	High
Power consumption	High	High	Low

V. CONCLUSION

This paper is a design of a door lock system which can both identify a "smartphone ID", and avoid a malicious reading of a non-privileged device. The smartphone obtains the "start numeric keypad password" permission, which is converted into the numeric keyboard interface. When entering a password there is a limit of 3 times to prevent malicious people from breaking the lock code in order to break into a house. To prevent the leakage of any data message, the "numeric password" is combined with a timestamp. This design, which does not require the user to have an NFC tag, is both an improved and a more convenient door lock system.

VI. REFERENCES

[1]. Thomas Korak and Lukas Wilfinger, "Handling the NDEF Signature Record Type in a Secure Manner", *IEEE 2012 International Conference on RFID.- Technologies and Applications (RFID - TA)*, pp.107-112, Nov. 2012.

[2]. Peng-Loon Teh, Huo-Chong Ling, and Soon-Nyean Cheong, "NFC Smartphone Based Access Control System Using Information Hiding", *2013 IEEE Conference on Open System (ICOS)*, pp.13-17, Dec. 2-4. 2013.

[3]. Nurbek Saparkhojayev, Aigul Dauitbayeva, Aybek Nurtayev, and Gulnaz Baimenshina, "NFC-enabled Access Control and Management System", *2014 International Conference on Web and Open Access to Learning (ICWOAL)*, pp.1-4, Nov. 25-27 2014.

[4]. NFC Data Exchange Format (NDEF), NFC Forum Technical Specification, Rev. 1.0, Jul. 2006.