The Smart NFC Door Lock System based on IOT

Group 5

P2213011 Ruizhe Zhou, Retro
P2212852 Yuan Duan, Hector
P2212871 Dashun Zheng, Dawson
P2212952 Di Kang, Vincent

澳門理工大學
Universidade Politécnica de Macau
Macao Polytechnic University

November 21, 2022

Contents

1 Project Description

1.1 Background

As the fast development and revolution in Internet, communication, texting and electron technology, the IC card is more and more applicated everywhere in people's daily lives, even become a necessity in daily traveling. The significant growth in the number of smart card issuance, thus the "Single function" development policies of different smart card manufacturers, the IC card caused a brand-new problem which brings fast and convenience at the same time: Individuals need to carry more and more smart cards to meet the various needs of daily travel.

1.2 Project Overview

With the significant growth in the number of smart card issuance, the smart cards have caused new problems while bringing convenience and speed to people's daily lives, thus, we design a smart card with NFC technology, which could store multiple cards' information, and it has the specific function of NFC card, which have a electronic ink screen to display some information.

Therefore, cards that people carry with them will become a problem that people often worry about while traveling around. And the loss of cards will cause a bunch of trouble, such as the loss of money, the loss of identity, and the loss of property. Therefore, we design a smart card with NFC technology, which could store multiple cards' information, and it has the specific function of NFC card, which have a electronic ink screen to display some information. The smart card is a combination of IC card and NFC card, which can be used as a IC card and NFC card, which can store multiple cards' information, and it has the specific function of NFC card, which have a electronic ink screen to display some information.

Simultaneously, we also design a door lock system, which can be used to open the door lock by sending AT commands to the module while the NFC card reader received the unlock signal from the Smart NFC card. The system can also be used as a relay to control the power of the door lock.

1.3 Project Architecture

For the Smart E-ink NFC card, we integrated the NFC card simulater and a E-ink screen to show some information on it. The information on the E-ink screen can be updated by chip ST25DV, which can communicate with the phone with a Android app under NFC protocol.

The NFC card simulation is processed by the STM32L051 chip and data is stored in different UID chips. The STM32L051 can also communicate with the phone in another Android application to overwrite the NFC card data into the chip.

For the door lock module, we used GD32 chip with W5500 Ethernet chip as a network relay to perform power-off and power-on operations by accepting AT commands from the back-end.

For the backend development, we used Java and Kotlin language, the main stream Spring Boot framework and MySQL database as the basis for the development and running on the

cloud platform. For security, we use the Shiro security rights management framework, the JWT single sign-on module to verify the user's identity. All the network requests and background function calls are stored in the Log4j2 database.

The IC card simulation is quite simple, which we integrate a few UID chip, and shared the same antenna, and we can switch cards by a dial wheel. At the good side, we can treat L-ink as a collection of multiple individual cards, copying and swiping are straightforward, but in another hand, as many cards are added, the number of buttons will increase.

2 Underlying Principle

2.1 NFC Technology

The Near Field Communication (NFC) technology is a short distance high frequency communication technology. NFC technology is developed from the integration of contactless radio frequency identification (RFID) and interconnection technology, which contactless readers, contactless cards and point-to-point functions are integrated into a single chip, allowing any two devices to be close together and communicate between devices without the need for plug-in cables.

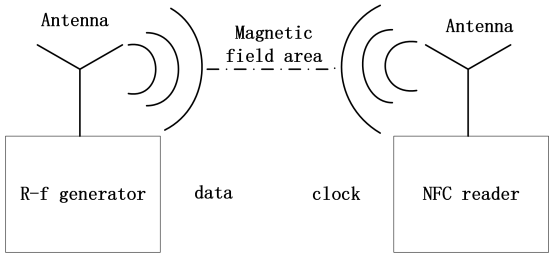

Fig. 1: NFC Working Principle

NFC technology transmits information through inductive coupling. The working principle of NFC is shown in Figure 1. After the NFC-enabled device boots, continuously generates radio frequencies (RF) with a center frequency of 13.56MHz signal. If there is an NFC tag in the signal magnetic field fluctuation range, the tag will initiate the tag RF signal generation circuit with a current generated by electromagnetic induction, which will generates a feedback signal after the frequency property is changed, what will make the reader detects the feedback signal of the tag to determine whether there is a tag around. The two NFC devices then establish a communication connection through magnetic field induced energy transfer and feedback signal acquisition and recognition, according to NFC protocol to enable identification and data exchange between close-range and NFC-compatible devices.

2.2 AT Command and Socket Protocol

AT Commands, developed by Dennis Hayes, are used to set data connections. The set of short string commands allows developers to set up calls with a modem, as well as perform far more complex tasks.

Socket is a software structure within a network node of a computer network that serves as an endpoint for sending and receiving data across the network.

In this project, the AT command is sent from the back-end to the relay using the Socket protocol, and the relay controls the door lock, as in Figure 2.

Fig. 2: Data Flow Diagram

3 System Architecture

To the design specification, we need to consider that the system involves the hardware part and the software part. Thus, we need to obey the design specification as following:

1. Provide a network interface, to make sure the system's scalability.
2. Ensure the security of the system and the rubustness of the system, to make sure the system's reliability that could operate under any harsh conditions.
3. Using more standard and open source components, to make sure the system's maintainability and the system functions' development.

3.1 Hardware Architecture

The selection of the hardware components is mainly based on the following considerations:

1. Provide a Internet controller chip, to send AT command by using the Socket protocol.
2. At lease exist a switch signal module, to control the open and close of the door lock.
3. Use an ARM based develop board as the network relay and have enough compute ability to handle the E-ink screen and massage handling.
4. The selected chip needs to support NFC-related protocols.

In conclution, we choose the GD32 chip as the network relay, and the W5500 chip as the Internet controller chip. At the same time, for the smart E-ink NFC card, we choose the ST25DV chip as the NFC communication chip and the STM32L051 as the master control chip.

3.1.1 Smart E-ink NFC Card

For the Smart NFC Card, we mainly used 2×IC chip, what are STM32L051 and ST25DV. The electronic ink screen is a 200 × 200 single color screen.

Fig. 3: Smart E-ink NFC Card

ST25DV communicate with STM32 chip through I2C bus as NFC's Physical Layer, which have 2 main functions, the energy harvesting and the NFC communication.

However, the ST25DV is only responsible for NFC communication with mobile phones to update those information on the E-ink screen, not for the read and write function for IC card. Thus, the ST25DV only supports ISO 15693's RFID protocol, but the IC card we commonly use is for ISO 14443 protocol, so we cannot directly use this chip to simulate IC card.

For the UID chips, we integrated two UIC chips into the Smart NFC Card module, what could store 2 cards' information. The UID chips share the same antenna with the ST25DV chip. The change between different cards is realized by a two-position dial button.

Besides, all the hardware mentioned above is powered by the internal integrated lithium battery, and the electronic ink screen will maintain the information on the screen when the battery is disconnected.

3.1.2 Smart Door Lock System

For the Smart Door Lock System, we integrated the NFC card reader, the magnetic door lock and a Internet controller to meet those needs.

The door lock is controlled through the Internet. By sending different AT commands, the NFC card reader could recognize the card's ID, which could transmit the cards' information to the software side, which could manage the access control and have a record of every NFC card recognition.

3.2 Software Architecture

The back-end using JAVA and Kotlin language as the basis for Spring Boot framework design and development of smart door lock system, through the single instance pattern to develop, using Spring Data persistence layer control MySQL database, and can be properly configured Web site, and can be well designed database and properly connected to the database. The overall implementation of remote unlocking, access control management, user management, door opening records and other functions.

The front-end page uses LayUI and zTree to implement the design of the page.

The sequence diagram of open door by card functions is shown in Figure 3.

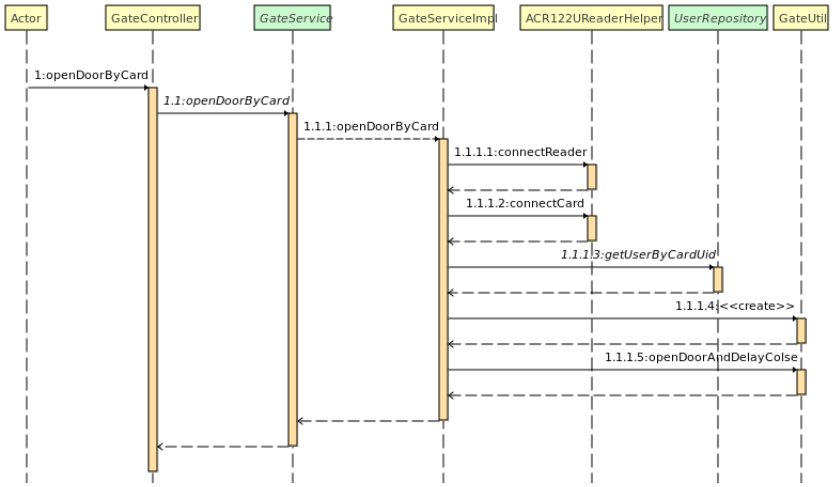

Fig. 4: System Running Sequence Diagram

4 Validation

4.1 Hardware Validation

For the hardware validation, we mainly use the simulation software, oscilloscope, DC source and the multimeter to test the hardware make sure there exist no unexpected bug in our device.

For the simulation software, we choose the Proteus, which is a professional circuit simulation software. The simulation software is used to simulate the hardware circuit, and it can simulate the hardware circuit and the software program.

For the oscilloscope, we use the Rigol DS1054Z, which is a 4-channel oscilloscope. The oscilloscope is used to test the signal of the hardware circuit, and it can display the signal of the hardware circuit.

For the DC source, we use the DS2482, which is a 16-bit ADC. The DC source is used to test the voltage of the hardware circuit, and it can display the voltage of the hardware circuit.

For the multimeter, we use the Rigol DM3058, which is a 5.5-digit multimeter. The multimeter is used to test the resistance of the hardware circuit, and it can display the resistance of the hardware circuit.

According multiple tests mentioned above, all the hardware validations showed that the hardware circuit works well.

4.2 Software Validation

Software validation environment we used JDK11, MySQL8.

Use Socket protocol to create TCP connection and send AT command to GD32 hardware.

For the back-end functional validation, we mainly use Postman to send post requests. The back-end will return the validation result.

After several verification, the software function works well.

4.3 Summary

According to the hardware validation and the black-box test, the system works well and no unexpected results or bugs have been found.

Use Case No	Use Case Description	Operation Process	Expected Result	Test Result
open_01	Door lock opened	User swipes the card normally for verification	Door opened successfully	Passed
open_02	Card swipe fails	Unknown user swipes the card for verification	Card is not bound	Passed
open_03	The user does not have the permission	The user who has been frozen by the administrator to swipe the card for verification	The door opening permission is frozen	Passed

5 Conclusion

We prepared this project mainly from two aspects (hardware and software). In terms of hardware, we designed a mini portable NFC smart card with screen. This smart card uses two IC chips, STM32L051 and ST25DV, and we added a 200*200 monochrome e-ink screen. We use the ST25DV for NFC communication with the cell phone. The STM32 is used to read and write to the IC card. In terms of software, we used a combination of JDK11, Spring Boot and MySQL infrastructure, which is a common combination in the market today. On this basis, we try some new technologies, such as Spring Data JPA, LayUI, etc. We also use a lot of excellent third-party libraries: JSON parsing, serialization and deserialization, database connection pools, etc. Both software and hardware aspects are integrated into this project.

The project has the following advantages: first, it can store multiple cards and the card contents can be erased. Secondly, it has NFC specific function, thirdly, it has an e-ink screen and can display the content through APP (there are many advantages of e-ink screen, such as displaying some information on the smart card, and if it is lost, it can be retrieved through the information on the card), and finally we designed a door lock system, when the NFC reader receives the unlock signal from the smart NFC card, it can open the door lock by sending AT command to open the door lock. The system can also be used as a relay to control the power of the door lock.

For the hardware of the Smart Card device, we had considered using the energy harvesting function of ST25DV to get the energy through the antenna while giving the transmission out for part of the MCU or other chips to use. Thus, most of the NFC reader's transmitting power are not the same. In some cell phones, to sense the power of about 30mw, while some cell phones are only 10mw.

Therefore, we considered the use of additional battery solution, adding a CR2032 coin cell battery into the Smart Card device. Because the total power consumption of this system is

extremely low, while the card is swiped is not power consumption, only when refreshing the electronic screen will consume a little power, and only in the case of insufficient power collection, the additional power consumption will be provided by the battery, if the electronic ink screen is refreshed 10 times a day, a button battery is enough to use for three years. Therefore this program is completely feasible.