Final Project

Group 5

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

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

November 17, 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 hardware side, we mainly used 2×IC chip, what are STM32L051 and ST25DV. The electronic ink screen is a 200×200 single color screen.

ST25DV communicate with STM32 chip through I2C bus as NFC's PHY, which have 2 main functions, energy harvesting and NFC communication. However, the ST25DV is only responsible for NFC communication with mobile phones, not for the read and write funtion 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. In 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 backend.

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 Working Principle

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.

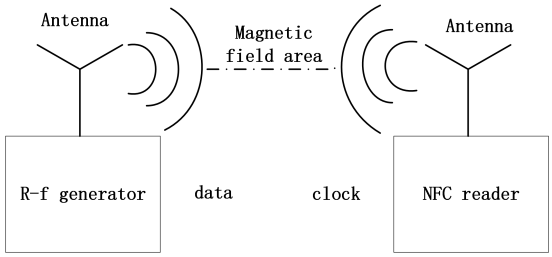

Fig. 1: NFC working principle

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

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. The set of short string commands allow 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.

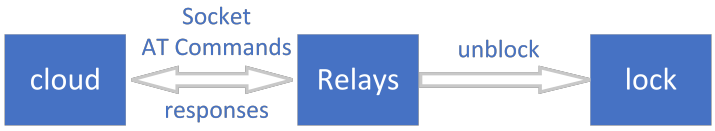

Fig. 2: data flow diagram

3 System Architecture

3.1 Hardware Architecture

3.1.1 Smart E-ink NFC Card

Hardware Architecture
Hardware Design
Hardware Implementation

3.1.2 Smart Dook Lock System

3.2 Software Architecture

4 validation

4.1 Hardware Validation

4.2 Software Validation

5 Conclutions

5.1 Future Works