Security of NFC payment on mobile payment application

By

WONG WEN TENG

A REPORT

SUBMITTED TO

Universiti Tunku Abdul Rahman

in partial fulfillment of the requirements

for the degree of

BACHELOR OF COMPUTER SCIENCE (HONS)

COMPUTER SCIENCE

Faculty of Information and Communication Technology

(Perak Campus)

MAY 2018

UNIVERSITI TUNKU ABDUL RAHMAN

REPORT STATUS DECLARATION FORM

Title: SECUTIRY OF NFC PAYMENT ON MOBILE PAYMENT APPLICATION

Academic Session: MAY 2018

I WONG WEN TENG

declare that I allow this Final Year Project Report to be kept in

Universiti Tunku Abdul Rahman Library subject to the regulations as follows:

1. The dissertation is a property of the Library.
2. The Library is allowed to make copies of this dissertation for academic purposes.

Verified by,

_____ _____

(Author's signature) (Supervisor's signature)

Address:

120 Kg Baru Jeram 31850 Perak

_____ _____

_____ Supervisor's name

Date: 21 August 2018 **Date**: _____

Security of NFC payment on mobile payment application

By

WONG WEN TENG

A REPORT

SUBMITTED TO

Universiti Tunku Abdul Rahman

in partial fulfillment of the requirements

for the degree of

BACHELOR OF COMPUTER SCIENCE (HONS)

COMPUTER SCIENCE

Faculty of Information and Communication Technology

(Perak Campus)

MAY 2018

DECLARATION OF ORIGINALITY

I declare that this report entitled "**Security of NFC payment on mobile payment application**" is my own work except as cited in the references. The report has not been accepted for any degree and is not being submitted concurrently in candidature for any degree or other award.

Signature : _____

Name : _____

Date : _____

ACKNOWLEDGEMENTS

I would like to express my sincere thanks and appreciation to my supervisor Mr. Ku Chin Soon who advises me on my Final Year Project – Security of NFC Payment on Mobile Payment Application. Without Mr. Ku I would be able to create such a mobile app. Thank you very much, Mr. Ku.

Besides, I also would like to thank my family that giving me mental support during the period I am doing this FYP.

ABSTRACT

In this booming technology world, the payment is no longer just use cash or cards. There is a more advanced way to pay the bill now – the online payment. It is very convenient, just a tap then the payment is done. However when it comes to payment, users are very aware of the security. People are very cautious on their privacy including their data. This project is to design a security protocol in NFC payment application system. The use NFC payment system is getting popular. Since it is famous nowadays, the attacker will try to exploit its weaknesses. This information during transaction is very important as it contains the private data of the user wallet details. After that the attackers may crack the transaction details and make the victims to lose money. Thus, it is important to make the NFC transaction safe. Since NFC itself does not provide a secure encryption. The job is depends on the programmer to design a safe protocol. In order to make the transaction not easy to crack. This project aims to solve the problem of eavesdropping during the transaction.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

NFC	Near Field Communication
SE	Secure Element
APDU	Application Protocol Data Unit
TSM	Trusted Service Manager
PIN	Personal Identification Number
DES	Data Encryption Standard
RSA	Rivest–Shamir–Adleman
PIN	Personal Identification Number
DAN	Device Account Number
TSP	Token Service Provider

Chapter 1 Introduction

1.1 Project Inspiration

In this era of technology, people are starting to use the cashless payment. It is very common nowadays because it is very convenient. Some of the examples are credit card, debit card, Near Field Communication (NFC) payment, paypal, touch and go, wechat pay, cryptocurrency and so on. According to Indiatoday In website, there are some countries that have almost gone cashless. For examples, Sweden, Norway, Denmark, Belgium, France, United Kingdom and many more. There is an interesting fact in Sweden: you can see even the homeless magazine vendors are accepting cards and mobile payments.

However, in Malaysia we are still using the old way of making payment. Thus, the aim of project is to introduce a new way for people to pay the bill with a more secure way. Cashless payment make life much easier since you just need to bring your phone instead of the heavy wallet. In fact you can prevent your wallet to get stolen by the thief as there is no reason to bring the wallet. Although they can steal your phone but all this phone have the authentication. Without this, the thief cannot transfer that money.

There are several payment apps started to get famous in Malaysia. For example, FavePay. However FavePay make the payment by scanning QR code, it is same as the wechat pay. In this project, NFC is chosen to make the payment because this useful technology is so less familiar with the crowd. Thus, the potential of the NFC technology is hoped to fully utilize in the app.

1.2 Project Background

In this project, a secure NFC payment protocol is design. First of all, what is NFC? NFC technology enable the devices to communication by using a short-range wireless connectivity standard that uses magnetic field induction. However, this communication can be established only when the devices are within a small range for about 10 cm (Rouse, 2007). Therefore, NFC technology can use to perform many functions such as contactless payment, information sharing and smart poster.

There are many advantage of using NFC. First of all, NFC is very convenient. User just need to use their phone and then move the mobile near the NFC tag then the payment is done. This payment is instant. The process of NFC payment is easy and simple to use even the elder can use it. Next, versatility is another advantage of using NFC. The reason is we can use NFC everywhere. It covers a lot of industries and services. We can use NFC payment in shopping center, buying ticket in cinema, purchase train ticket and many more.

However, nothing is prefect. Indeed there are some security problems in NFC technology. In section 1.2, we will discuss all the problems in NFC technology. With these vulnerabilities of NFC, a strong and secure NFC transfer protocol is needed to make the transaction safer. It is very important because the NFC is getting popular and more people are using it. Furthermore, during the transaction the NFC will transfer some sensitive and private data and we do not want the attacker to gain unauthorized access to these data. Thus we need to ensure that these data is well-protected.

1.3 Problem statements

Below are some problems in NFC technology (Nelson et al., 2013):

- **Eavesdropping**

Eavesdropping is a process that describe the attacker to sniff the sensitive information during the communication. NFC technology does not offered protection against eavesdropping. Attacker can easily get the private data if the application do not encrypt the information. Thus, it is a must for the developer to implement the encryption method as NFC lacks of the default encryption.

- **Man in the Middle**

In man in the middle, the attacker will intercept or if possible will modify the information between two parties. But it is difficult because the information is encrypted by the application. Another problem is the communication can only occurred when both devices are close to each other less than 10 cm.

- **Relay Attacks**

This attack happens when the attacker relays a message from the victim to the reader of the message. In order make this attack happen, the attacker much get close to the victim. To start the attack, the attacker needs a NFC system sent the message with the victim. This NFC system need to connect to another NFC system via Bluetooth, wireless LAN or internet. The second NFC system is used to get the message from the victim.

- **Data Corruption**

It happens when the attacker jams the NFC transmitter with radio pulses at 13.56 Mhz and with a correct timing. However, this will cause the data to destroy and this is not the attackers want. They want to get the data not destroy it. So, this situation is rarely happened.

- **Data Modification and Insertion**

The attacker captures the exchange data. Then, these captured data will be modified by attacker. This attack is hard to implement as the attacker and the valid source must transmit the waveform

simultaneously to the NFC device. Same as data corruption, a correct timing is needed in order to make this attack successful.

1.4 Project Objectives

To allow the sure to make payment by using NFC

This is the main focus of this app. The main objective of this app is that user can make payment by using NFC in this app. This can be achieved easily by learning the NFC structure and how it is use to transfer message.

To enhance the security of the system

- **To encrypt the data before transaction**

  Since this is a payment app, thus the security of the payment is really important, especially the transaction message during the transaction. It is because the attacker might get the message and use it to create the fake transaction to trick the victim.

- **To prompt user to enter PIN when making payment**

  This step is very important to ensure that the user is authentic and real user to make the payment. This is also one of the common feature that many system use.

- **To show the payee information to the payer before the transaction starts**

  The feature is also very important to prevent the attacker to make a false transaction to fool the victim. Since all the payee information is show on the payer side, thus the payer can manually identify the real payee. As a result, it can prevent the man-in-the-middle attack.

To allow the user to check back the previous transaction history

This is very important as user might want to check back the previous transaction record sometime. Thus, it is necessary to have a history page.

1.5 Project Scope

At the end of the project I would like to develop a secured NFC phone-based payment application. This app can be only use in face to face transaction. For example, buying the groceries in supermarket. This happen because the limitation of NFC. NFC can only works when two NFC devices are in very close range. This system can be used in UTAR cafeteria as it is convenient. With this cashless payment system, students are not required to bring their real money to university. Besides that the payment process is faster as the change process is excluded.

Below are some functionality in my system:

- **User can choose the encryption type during transaction.**

A list of encryption type is displayed to let the user to choose which encryption type they preferred.

- **Create account**

User can register an account and login to use the system.

- **User can manage their account**

User can check the balance in the mobile app. User can also send the balance to his or her family and friend.

- **Check transaction record.**

User can check the details of previous transaction record.

- **A transaction PIN is needed before the transaction.**

User is requested to key in the transaction PIN before transactions. It is a safety measure. This is to ensure that the owner is using the app.

In my project, in hardware aspect, two NFC phones are needed. One act as the sender and another one act as the receiver. On the other hand in software aspect, Android studio is chosen as

the system is in android platform. Next, firebase is selected as the database of the mobile application.

1.6 Project Impact and Contribution

With this system, user is able to use the cashless payment which mean he or she does not need to bring the money when going out. It is convenient and this system enhance the payment experience. It is because the payment process is faster and the change process is eliminated. Besides that, the payment is easy and simple to use. Just use the phone and tap the NFC tag, the transaction is complete. Furthermore, the app itself provide different encryption type to encode the transaction information. This make the transaction process safer.

1.7 Chapter summary

Cashless payment seems to be the new trend to pay the bill in the near future. Thus, I hope that this app can help people to make payment safely. This app have several features that can help user. The selectable secure protocol to ensure the transaction is safe. Transaction history to let user recall on what is the spending and many more useful functions.

Chapter 2 Literature Reviews

Below are some papers about different type of NFC payment system:

In the research paper "Offline NFC Payments with Electronic Vouchers", the authors had introduced a way to use offline NFC by using electronic vouchers. Figure 1 shows the steps in NFC transaction:

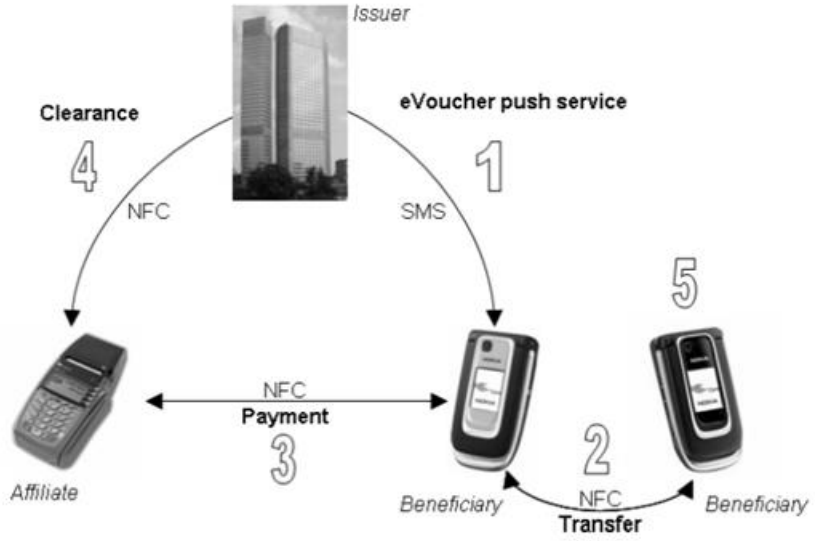

Figure 2.1 The eVoucher system

1) Issuer sends eVoucher by using SMS.
2) eVouchers can be transferred by using NFC.
3) Use NFC to make payment.
4) Clearance of eVoucher between issuer and affiliate.
5) Usesr can check their eVouchers details.

Here is how the system work in order to get eVouchers though SMS: First of all the NFC voucher software is installed in the beneficiary side. This software contains MIDlet2 and JavaCard Applet. MIDlet2 will run on the phone OS while JavaCard will run on a hardware called Secure

Element (SE). All the data will be stored in SE as SE has limited access for unauthentic user. Thus, the sensitive data is secured in SE. After successfully installed, a protocol is run with Issuer. Next, the ID and public key of the beneficiary are registered by the issuer. Then, issuer can generate eVoucher by creating signatures and send the eVoucher by using SMS. The encrypted eVoucher is decrypted in MIDlet. This eVoucher contains many information such as serial number, expiration data, money amount, status byte and RSA signature.

Figure 2 shows the phone-to- phone protocol:

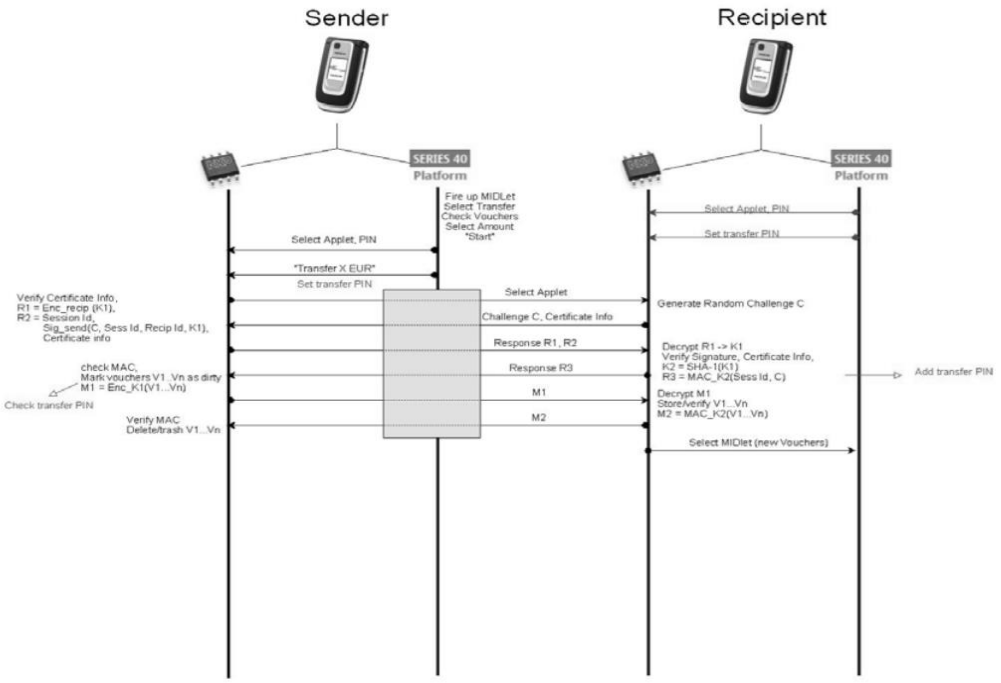

Figure 2.1: phone-to- phone protocol

1) MIDlet is fired up to select the transfer voucher. The amount is selected.
2) MIDlet calls the transfer applet to transfer the money.
3) The selected applet in SE communicate with the receiver's SE to select the transfer applet.
4) The receiver's SE generates a random challenge C and send back to sender.

5) In sender side, it verify certificate info and generate R1 and R2 by the formula in diagram above. R1 and R2 is sent to receiver's SE.
6) In receiver side, R1 is decrypted into K1. K2 and R3 is generated based on the formula in diagram above. R3 is sent to sender's SE.
7) MAC is checked. Next, the vouchers is marked as dirty. M1 is generated based on the formula in diagram above and sent to receiver's SE.
8) M1 is decrypted and the eVoucher is stored and verified. M2 M1 is generated based on the formula in diagram above and sent to sender's SE.
9) MAC is checked and the eVouchers is deleted.
10) On recipient SE, the MIDlet is selected when there is the new voucher.

The first strength of this system is this is an offline system. It allows user to offline transfer money. Since the system is offline, these eVouchers are transferred by using SMS. However this may cause some problems. It is because there is no main server to control all the transaction that happened. Thus, the system is vulnerable as the attacker may makes the fake eVouchers and cheats the system. Therefore, the eVouchers issuer should make the eVouchers hard to imitate. The same thing goes to the digital value too. At the same time, the digital value may be lost during the transaction. This system can prevent this two problems from happening.

In this research, the authors discuss some limitation on this system. First of all, SE cannot store many eVouchers without control. 20 eVouchers store in the system use up 30KB of memory. The size of 1 eVoucher is 148 bytes. Based on the experiment phone, it can only store up to 262 eVoucher. Next limitation is about the application protocol data unit size (APDU). The maximum APDU size is 256 bytes, any transaction message more than the maximum APDU size will be segmented and the status will change to pending. It will slow down the transaction.

The limitation is no longer a problem for this system. It is because this research is conducted in 2009 and the phone nowadays is more advance, the memory is much larger compare to the experiment phone in 2009.

In the paper "An Unlinkable Anonymous Payment Scheme Base OnNear Field Communication", the authors proposed a system that consist of 4 phases:

1) Registration phase: The system will generate all the necessary parameters like the public key of the user and bank's share key.
2) Anonymous virtual bank account generation phase: A user uses an anonymous account to make the payment from his bank.
3) Anonymous transaction account generation phase: The virtual bank account ID is took by the user to the Trusted Service Manager (TSM) to generate a transaction account.
4) Virtual credit card generation phase: A temporary virtual credit card is given to user from TSM and it is stored in SE.

First strength of this system is confidentiality of the data. All the transaction message is encrypted with asymmetric keys. Therefore, the attacker is unable to access the encrypted information. Second strength is the data anonymity. By using this system, only the bank knows the user's real identity while the merchants don't.

According to Lee et al., this system is vulnerable to DoS attack. Dos attack is an attack to make the server unavailable to user. At anonymous transaction account generation phase, TSM is vulnerable to be attacked. It is because the TSM will always accept the incoming message without checking the User-issued ID. Next weakness is the symmetric key may leak to user. This problem caused by the user stores some sensitive data. After that, this system also does some duplicate work by generating unnecessary anonymous transaction account. This make the transaction process inconvenient and inefficient.

However, these limitations and weaknesses are resolved by Lee at al. in the research paper named "An Enhanced Unlinkable Anonymous Payment Scheme Based on Near Field Commnication". The DoS attack is solved by adding a verification function in the virtual credit card generation phase. For the leakage problem, some of the procedures in the scheme are eliminated.

Based on the research paper "Near-Field Communication-Based Secure Mobile Payment Service", the authors suggested a NFC-enable mobile payment system. Figure 2.3.1 below shows the overall idea of the payment system.

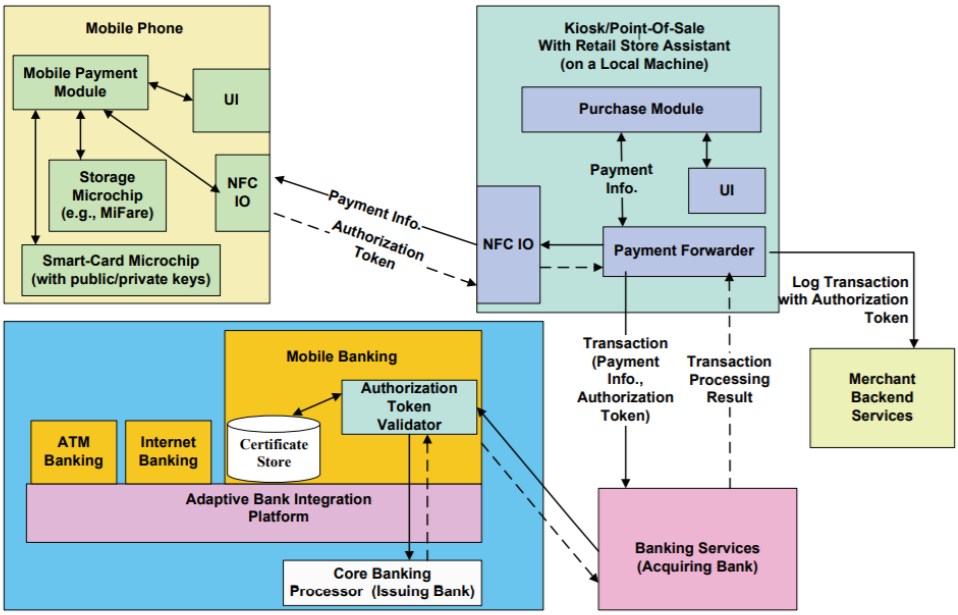

Figure 2.3: The overall NFC-enable mobile payment system

In this system, there is 3 important secure transaction protocols that make the transaction safe.

1) Payment Authorization Token. The phone will generate an authorization token to start the transaction.
2) Detail Communication Protocol. The token has been processed by several procedures.
3) Key Management. The function is to manage the public key and private key.

One of the advantage of this system has a more flexible payment. It is due to the phone only issued authorization token. Thus the merchant do not need to store the secret key pre-distributed to communicate to the NFC chips. Moreover this system supports remote transaction. It can use by those who use online shopping but want to make the payment by NFC phone.

Type of NFC payment	Strength	Weakness
Offline NFC Payments with Electronic Vouchers	• Offline payment system. • eVoucher cannot be mimic.	• The phone cannot store the eVoucher without control. • The maximum size of APDU size is 256 bytes.
An Unlinkable Anonymous Payment Scheme based on near field communication	• The data is confidential. • The data is anonymised.	• Vulnerable to DoS attack. • Symmetic key leakage problem.
Near-Field Communication-Based Secure Mobile Payment Service	• Flexible payment. • Support remote transaction.	Cannot be identified

Table 2.1: Comparison table between different types of NFC payment

Below are some study on the existing system:

In the paper "A Comprehensive Study of Google Wallet as an NFC Application", the authors had discussed about the Google Wallet. According to the authors, they claimed that the Google Wallet application is based on card emulation NFC mode which mean the NFC phone becomes a contactless card to a payment terminal or reader. The debit cards, credit card, gift cards and loyalty point is stored in the phone. This make it become a virtual wallet. The launch of cloud-based version also provide extended support from credit card and debit card companies. This system also be accessed from any electronic devices as long as it is compatible.

The payment process by using Google Wallet is simple. First, user need to open the app. If the user did not enter the Personal Identification Number (PIN) recently, he or she is requested to do so. After that, user need to place the phone near the NFC reader. At this moment, the payment credentials will be transfer to the merchant side. Merchant will get a confirmation and a receipt will be printed. On the other hand, user will also get a confirmation on his or her phone.

There are several security measures that Google Wallet use. First, the transmitter chip not on when this phone screen is off. This is use to avoid the scanning of bypass attacker. Next, user need to enter a 4-digit Personal Identification Number to view and use the card. Besides that, User can disable their account when their phone is lost. By doing so, your Google Wallet account will be cancel and prevent the unauthorized spending. The linking debit card or credit card will be masked for security purpose.

There are some weakness on this Google Wallet. One of them is Google Wallet is vulnerable to an attack named 'fuzzing'. This attack will cause the application to damage the data and find the vulnerability. After that, the attacker can inject a crafted NFC tags and monitor the result. For the user who root their phone, the attacker can get the hashed PIN and crack it using brute force. This happen because the PIN is stored in the mobile device itself not in the Secure Element. Furthermore, in NFC payment application perspective, the application is vulnerable to eavesdropping, data modification and data insertion.

The second existing example is Apple Pay. Chen (2016) the author of "Information Security of Apple Pay" had discussed about Apple Pay.

Apple Pay is used in any IOS devices including apple watch and it enables the user to make payment using NFC. The idea of create Apple Pay is to change the way of people shopping. Apple uses two techniques in Apple Pay. One is NFC and another one is Touch ID. Touch ID is actually a new biometric fingerprint authentication technology as everyone has a different fingerprint. New Apple Pay user needs to add their credit or debit card first. European Union Agency for Network and Information Security (December 2016) had demonstrated how this process works in the paper called "Security of Mobile Payments and Digital Wallets".

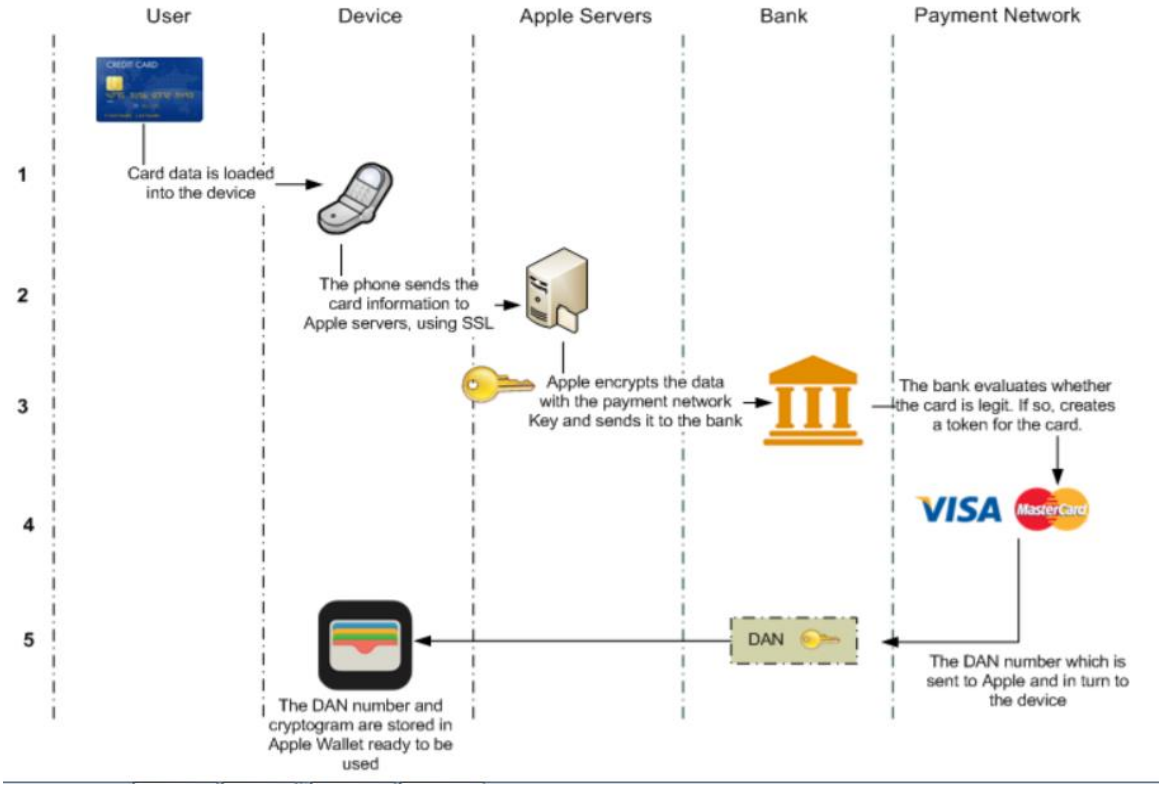

Figure 2.4: Apple Pay Card Enrolment Process

Figure above show Apple Pay Card Enrolment Process. First user need to key in or take a picture of the card. Then the information will send to the Apple server, using SSL. Next, the bank will receive the information from Apple server and start to evaluate the information. If the card is accepted, a token will be created by Token Service Provider. A Device Account Number (DAN) will be send to Apple server and then to the device.

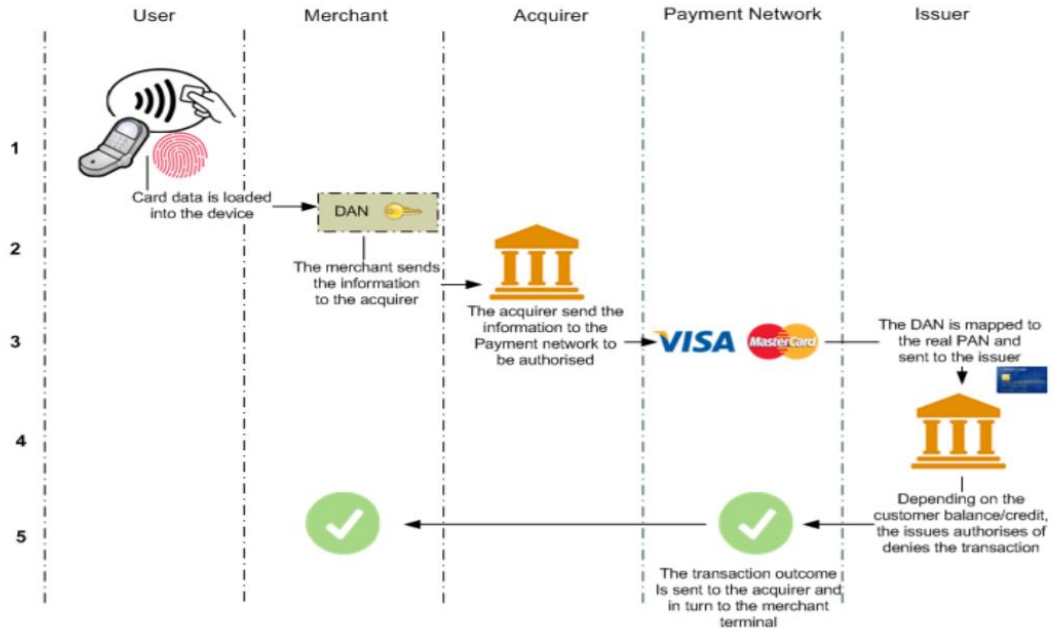

Figure 2.5: Apple Pay Payment Process

Figure above shows Apple Pay Payment Process. In order to start the transaction, user need to place the phone close to the NFC terminal. A PIN or Touch ID verification is required. Next, the acquirer will get the information from merchant. Acquirer receives the DAN number. Furthermore, the payment network will identify the DAN and send it to Token Service Provider. Finally the issuer will accept or cancel the transaction and send the notification to acquirer and then to merchant.

Apple pay uses several measures in data protection. First and foremost, Apple Pay use tokenization. This means that the real primary account number and the card verification are never used. This step is to reduce the exposure of the real private data. Besides that, Apple Pay also leverage the Secure Element. Secure Element is a chip embedded inside the Apple device. It is secure because it is temper-resistant.

The first advantage if using Apple pay is the sensitive data is stored in the database in a secure cloud. It also uses tokenization to reduce the exposure of sensitive data. Next, Apple Pay implements Apple ID to ensure that it is a authorized transaction. Furthermore, Apple Pay limits the use of security key.

Next, Samsung Pay. In the paper "Security of Mobile Payments and Digital Wallets" by European Union Agency for Network and Information Security (December 2016) had discussed about Samsung Pay.

Samsung Pay is developed by Samsung. Samsung Pay uses NFC technology to make payment. Besides that Samsung Pay also implement the Magnetic Secure Transmission to make the transaction. By doing so, Samsung Pay will emulates a magnetic card stripe reader. This technology provides the user another choice to make payment not only to use the new technology – NFC but the old fashion way – traditional magnetic stripe terminal.

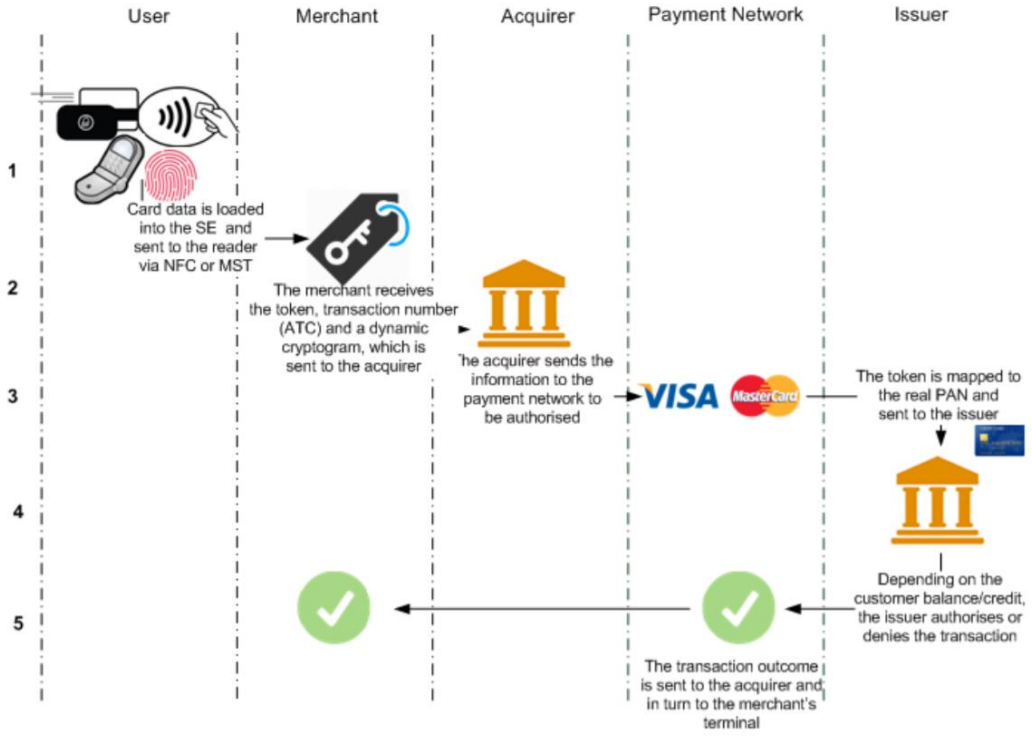

Figure 2.6: Samsung Payment Process

Figure above shows the Samsung Payment Process. As usual, user need to place their phone close to the NFC reader or magnetic stripe POS. After that Samsung Pay will start the payment process. 3 pieces of information will be generated, a token, a transaction counter and a cryptogram. After that, merchant side will receive the information and forward the message to acquirer. Acquirer will check the appropriate payment network and send the information to it. The

token will be identified by TSP and retrieve the real primary account number. The issuer will decide whether the transaction is successful or not.

There are some strength in Samsung Pay. First one is the tokenization is used. It is mentioned before the user details will be protected because the real information does not leak. Second, it can be used in the store that does not support NFC payment. Because Samsung Pay also uses Magnetic Secure Transmission.

Salvador (2016) in his paper "Samsung Pay: Tokenized Numbers, Flaws and Issues" suggested that one threat faced by Samsung Pay user. The credit or debit card in the database is encrypted. However, it is easy to decrypt it with the static passwords in code. Next, although the tokens cannot be reuse but the attackers can guess the last 3 digits of next token. This can be done by analyze the tokens and use the brute force attack or tokens' dictionary attack.

Type of NFC payment application	Strength	Weakness
Google Wallet	• Transmitter chip will not turn on when this phone screen is off. • PIN is needed to view and use the card. • User can disable their account when their phone is lost. • The linking debit card or credit card will be masked.	• Vulnerable to 'fuzzing' attack. • Hashed PIN can be cracked using brute force. • Vulnerable to eavesdropping, data modification and data insertion.
Apple Pay	• Sensitive data is stored in the database in a secure cloud. • Use tokenization. • Limit the use of security key.	Cannot be identified
Samsung Pay	• Tokenization is used. • Can be used in the store that does not support NFC payment	• Easy to decrypt it with the static passwords in code. • Vulnerable to brute force attack or tokens' dictionary attack.

Table 2.2: Comparison table between different types of NFC payment

Chapter 3 System Methodology

3.1 Chapter Overview

In this chapter, the methodology and technology for this project will be covered and discussed. Each and every steps of the system methodology will be clearly explained. Next, a planned Gantt chart is created to make sure that the project will be finished on time. Last but not least, some system analysis and UML diagram will be also covered in this chapter.

3.2 Software Methodology

The software development life cycle (SDLC) is a conceptual model, used in project management, to describe the stages and tasks involve in each step of a project to write and deploy software. (Margaret Rouse, 2015). In general, SDLC consists of 6 stages that is planning, analysis, design, implementation, testing and deployment. There are many SDLC models that can be choose when develop the software. Rapid Application Development (RAD) model is chosen in this project. It is because this model is designed to suit the system to be produced in a short span of time.

Diagram below shows the RAD diagram for NFC Pay:

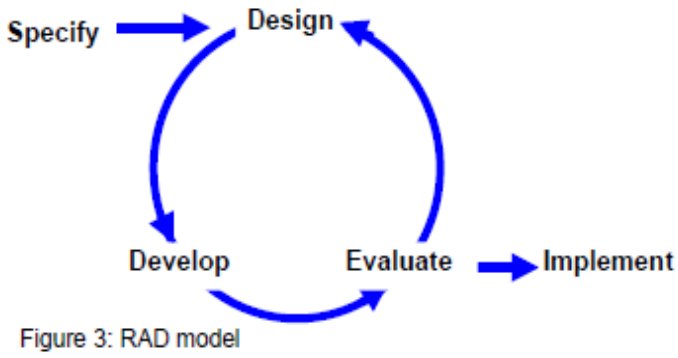

Figure 3.1 RAD diagram for NFC Pay

Specify

In this phase, a research is conducted at first. The problem of the current payment system is examined by reading the research papers and interviewing the people. It is because a strong understanding is needed in order to create a solution for the problem.

At the same time, a study to evaluate the existing system in the market is needed. This is to give an insight of what really happening in the existing world. Next, the result of the research needed to be analyzed and a better solution need to be proposed to solve the problem. The system requirement shall be listed down. Besides that, in order to build a successful application, the existing technologies and skills to develop the system needed to be study.

Design

In this design phase, it turns the software specification into a design plan. The layout of the app is designed. This is very important to have a user friendly interface. Next, the system architecture is also decided. The programming language and the database are selected. Last but not least, the flow of the system needs to be clearly designed.

Develop

During this develop phase, all the requirements will turns into the code. Furthermore, the system will connect to database. Each module that produced will be reviewed by advisor. This is very important to ensure that the module that develop is correct and the development process is on right track.

Evaluate

After a module is developed, then this module will be tested and evaluated. This is to make sure that the module has no error or bug. Then, it will proceed to develop the next module and evaluate again. This cycle will stop until all the modules is completed. Next, an overall test will be conducted to ensure the system can work as a whole without any bugs or errors.

Implement

Implement is the last phase of this model. In this phase, the whole system is implemented. A documentation or manual of the system is created. Besides, the maintenance and version upgrade show be carried out in the future in order the keep the user active.

3.3 Project Timeline

In this phase, the project timeline is planned. Below is the timeline for this project.

NFC Pay Timeline			DURATION (days)
DESCRIPTION	START DATE	END DATE	
Section1 - Planning	16/10/17	29/10/17	13
Select Title	16/10/17	20/10/17	4
Define Objective & Scope	21/10/17	24/10/17	3
Schedule & Budget Planning	25/10/17	29/10/17	4
Section 2 - Analysis	30/10/17	25/12/17	55
Research for Existing System	30/10/17	15/11/17	15
Fact Finding	15/11/17	30/11/17	15
Summary	30/11/17	03/12/17	3
Preparation &Submision of Proposal Report	03/12/17	25/12/17	22
Section 3 - Design	15/05/18	30/06/18	45
Conceptual Design	15/05/18	20/05/18	5
Logical Design	21/05/18	25/05/18	4
General Work Proceudre Design	26/05/18	31/05/18	5
Database Design	01/06/18	05/06/18	4
Interface Design	06/06/18	10/06/18	4
Flow Chart	11/06/18	30/06/18	19
Section 4 - Implementation	01/07/18	10/08/18	39
Develop Prototype	01/07/18	25/07/18	24
Testing	26/07/18	03/08/18	7
Debug and Evaluation	04/08/18	07/08/18	3
Refinement	07/08/18	10/08/18	3

Figure 3.2 Project Timeline for NFC Pay

Figure 3.3 Gantt chart for NFC Pay

This project consists of two part that is FYP1 and FYP2. It takes 2 semester to finish it. The duration time has a gap is because this two subject did not took in consecutive semester. From 16/10/2017 to 25/12/2017 is mainly the planning and analysis phase. Afterwards start from 15/05/2018, the project is started to code, implement and test.

3.4 System analysis

Functional Requirements

User Registration Module

- The system shall only accept the email registration from user.
- The system shall only accept the password with at least 6 digits length.
- The system shall allow unique email registration.
- The system shall allow the user to input the unique username.
- The system shall allow the user to choose the encryption method to use.
- The system shall allow the user to set the PIN during the transaction.
- The system shall ensure that two same PIN is entered.
- The system shall store the user information into the database after the successful registration.

Login Module

- The system shall allow the user to key in the email and password.
- The system shall validate the username and password.
- The system shall redirect user to main menu after the successful login.

Forget Password Module

- The system shall let user to retrieve the password.
- The system shall validate whether the email entered is in database.
- The system shall send an email to allow user to reset password.

Pay Module

- The system shall allow user to pay money.
- The system shall check whether the device is turned on NFC.

- The system shall authenticate the user by key in the PIN.
- The system shall able to display an alert box to show the transaction details after the device receive the information form another device.
- The system shall allow the user to accept or reject the transaction.
- The system shall notify the user when the balance is lower than the amount to be paid.
- The system shall notify the user when the transaction is completed.

Receive Module

- The system shall let user to receive money.
- The system shall allow the user to key in the payer details, like payer username, amount and comment.
- The system shall allow the user to choose the username from the favourite list.
- The system shall notify the user when the transaction is completed.

Change PIN Module

- The system shall allow user to change pin.
- The system shall authenticate the user by key in the PIN.
- The system shall let user to key in the new PIN twice.
- The system shall check the two PIN whether these two match or not.
- The system shall update the new PIN to database when two pin is matched.

Change Encryption Module

- The system shall allow user to change encryption method.
- The system shall authenticate the user by key in the PIN.
- The system shall let user to choose the encryption method to use in a list.
- The system shall update the new encryption method to the database.

Manage Favourite List Module

- The system shall allow user to manage the favourite list.
- The system shall allow the user to add the favourite username into the list.
- The system shall allow the user to delete the favourite username into the list.
- The system shall update the new list to the database.

History Module

- The system shall let user to check the previous transaction record.
- The system shall let user to have a detail receipt when tap on a specific transaction record.
- The system shall let user to search the transaction record within certain time range.
- The system shall let user to see a pie chart to show the overall money receive and spend within a certain time range.

Non Functional Requirements

Interface

- The user interface shall be user friendly.
- The system shall allow user to navigate easily throughout the system.
- The Graphic User Interface shall be attractive to user.
- The font size shall be big enough to let user see easily.

Performance

- The transaction speed shall be as less than 3 seconds.
- The system shall be able be available 24/7 for every day.

Operational

- The system shall operate in android phones.

Security

- The system shall authentic authorized user to login.
- The system shall prompt the user PIN when user want to make transaction.
- The system shall encrypt all the transaction message.

Usability

- The system shall easy to use.

Reliability

- The system shall provide real data without any error.
- The system shall correctly calculate the transaction amount and balance during transaction.

3.5 Hardware and Software Requirement

Hardware:

Below is the laptop specifications to develop the system:

Model	Lenovo Y50
Operating System	Windows 7 Professional
Memory(RAM)	8.00GB
Processor	Intel® Core™ i7-4710HQ CPU @ 2.50GHz 2.50GHz

Below is the phone specifications to test the system:

Model	Lenovo A7010a48
Operating System	Android 5.1
Memory(RAM)	3.00GB
Processor	MediaTek MT6753 (8 core 1.3Ghz)

Software:

- Android Studio

  It serves as the main IDE for me to develop my system. It is a well-known software that provide a lot of features for me to develop my software.

- Firebase

  It serves as the database of this project. It is very useful as it do not need to set up a virtual server in the computer.

3.6 Use Case Diagram

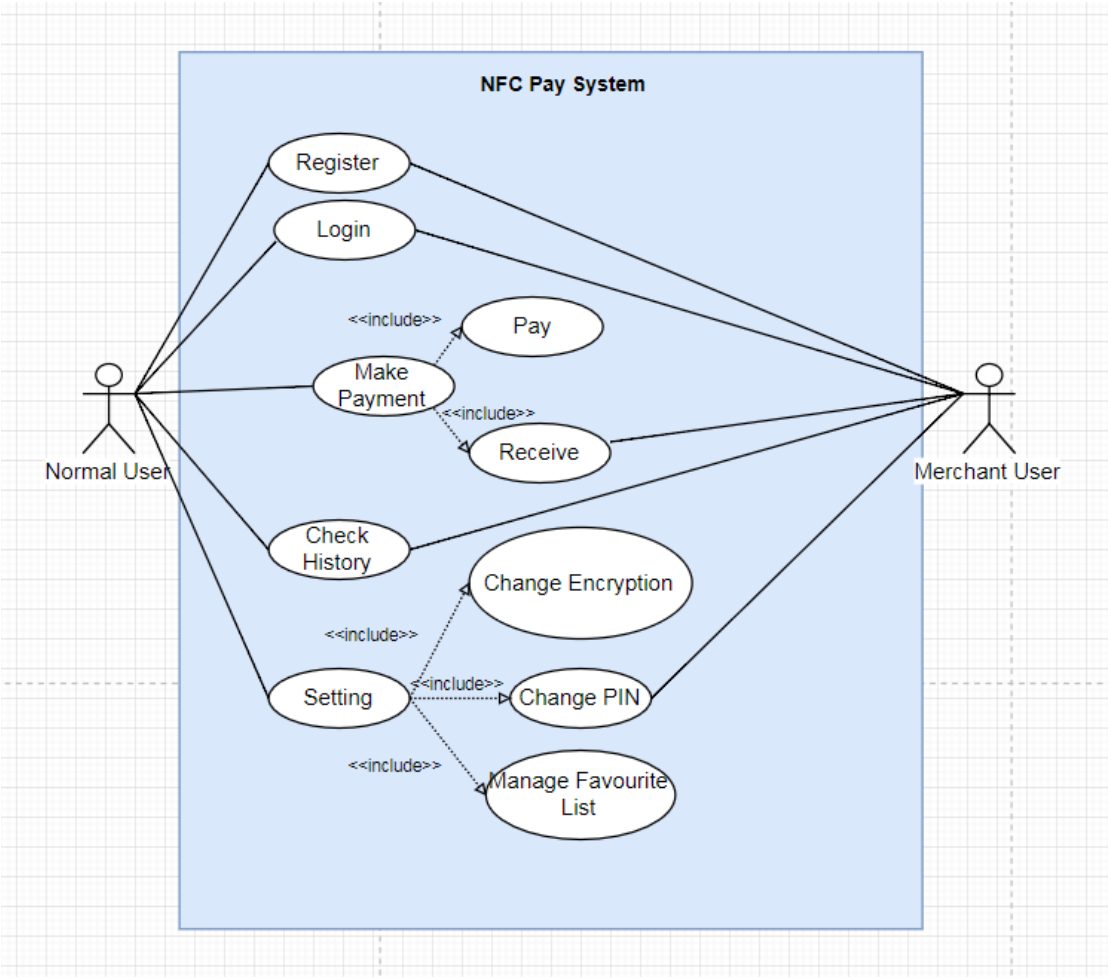

Figure 3.4 Use Case Diagram

The diagram above is the use case diagram of NFC Pay. It shoes the actions that user can do in this app. This app consists of two user, one is normal user and another one is merchant user. Normal user can perform many actions such as register account, login account, make payment like pay money and receive money, check history transaction record, change setting like change encryption method, change pin and manage favourite list. On the other hand, merchant user had some restrictions, since it can only register, login, receive money, check history and change pin.

3.7 Activity Diagram

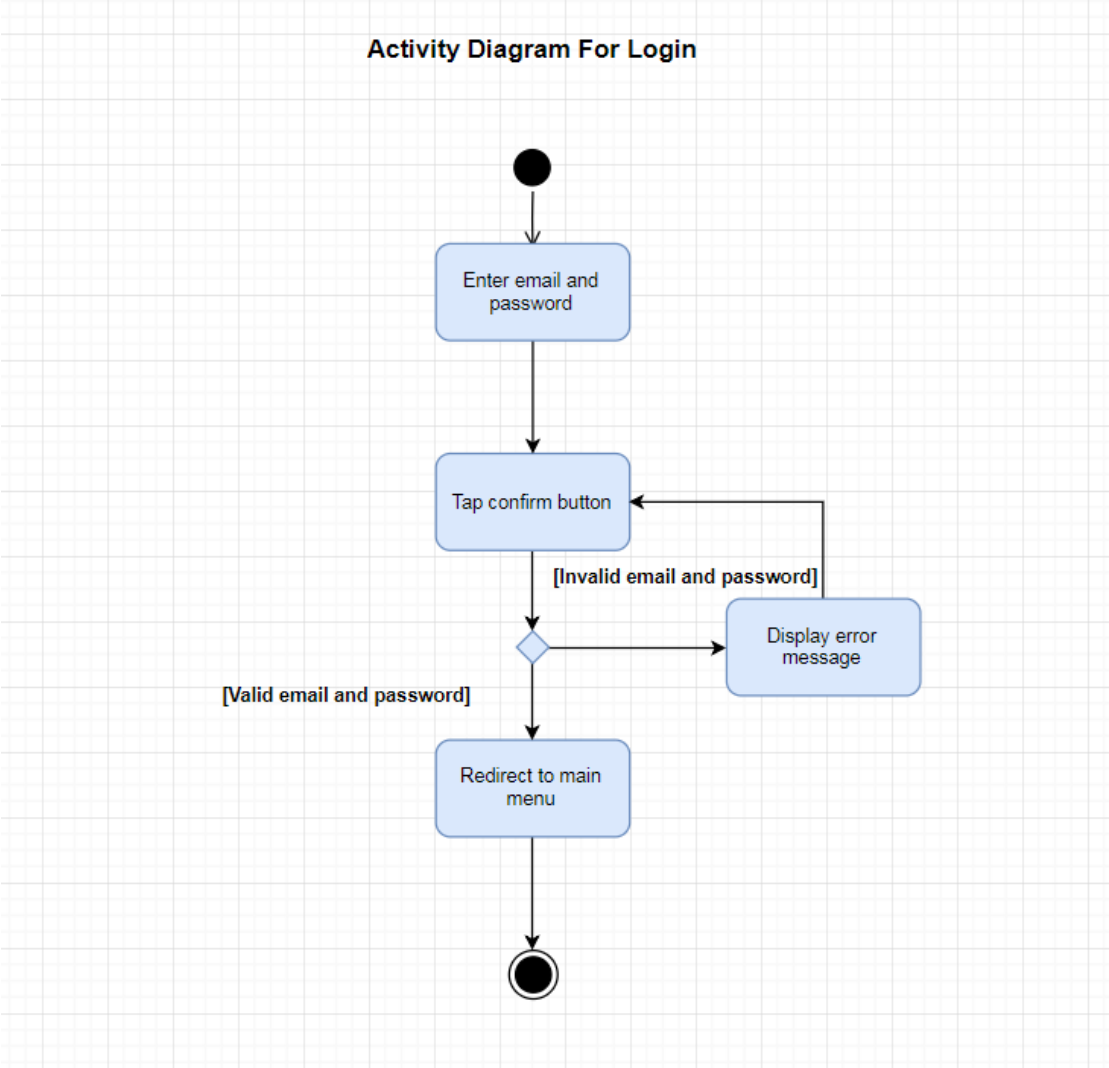

Figure 3.5 Activity diagram for login

This diagram show the whole process of login. First the user need to enter the email and password in the respective field. Next user needs to tap the confirm button to process. These data will be verify at the server side. If the email and password is valid then this user is successful login and redirect to main menu, else the system will display an error message to show that the login is failed.

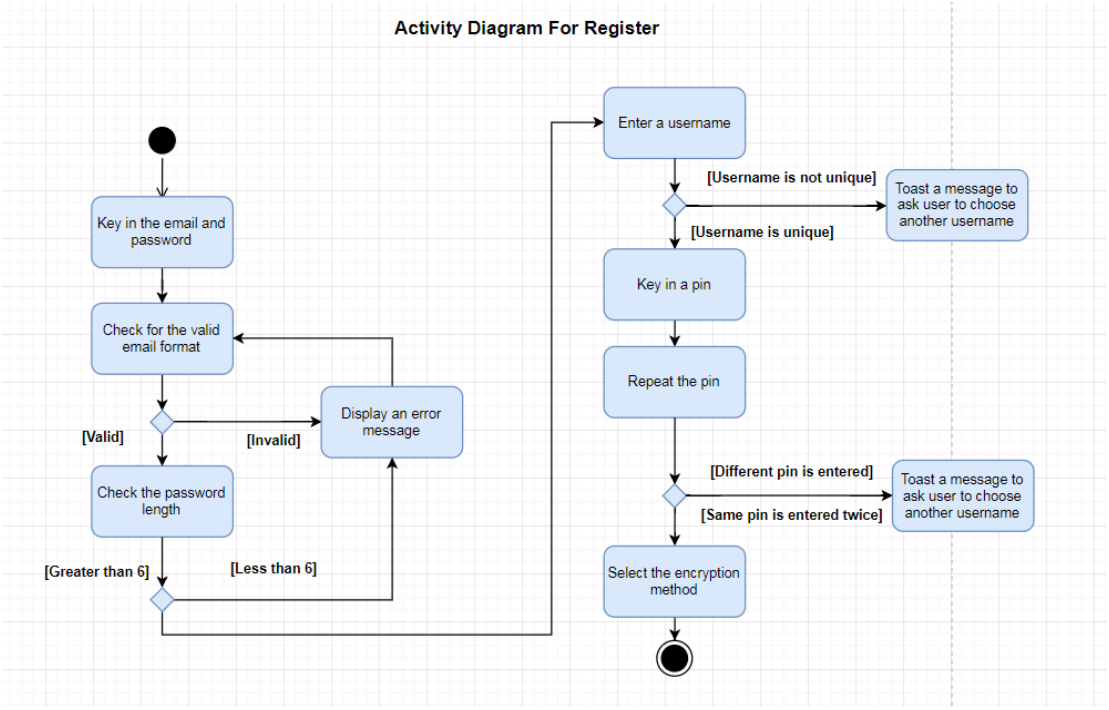

Figure 3.6 Activity diagram for register

For the registration module, first user need to key in the email and password. After tap the confirm button, the data will be sent to server. If the email entered is not in valid email format, an error massage will be shown. Next, the system also will check the length of the password, it should be at least 6 digits long. If less than 6 digits, the system will display an error message. After that, user need to create a username. This username must be unique. If not the system will toast a message to ask user to choose another username. Furthermore, user need to key in a 6 digit PIN twice. If the two PIN are not match, an error message will be shown. Last but not least, for the last registration step, user need to choose an encryption method.

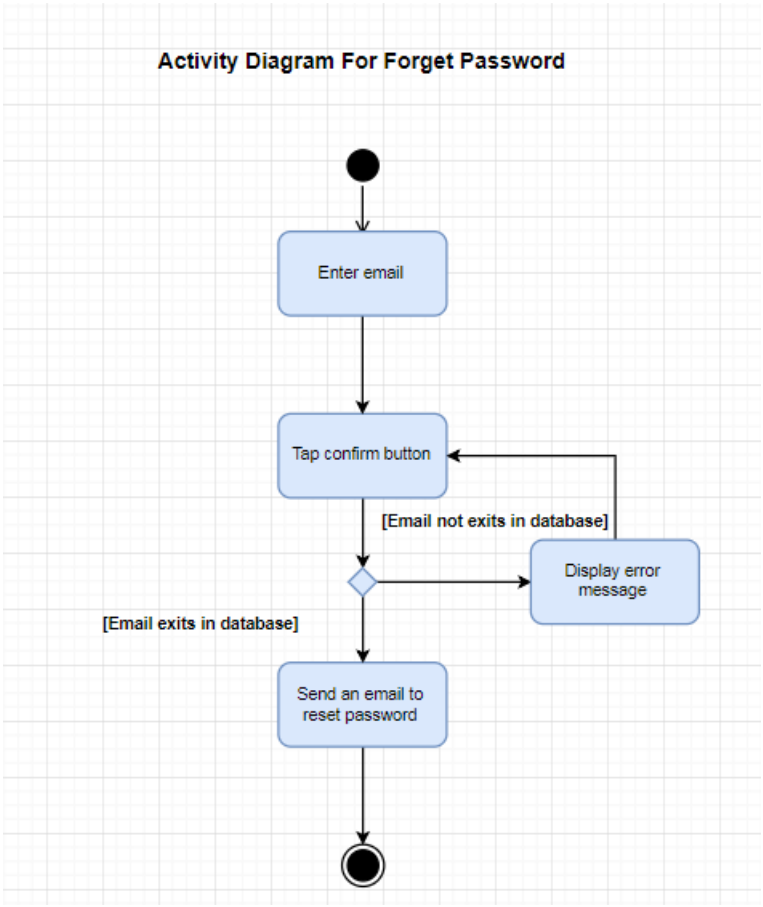

Figure 3.7 Activity diagram for forget password

This is the forget password module. First of all, user need to enter the email. Next, user need to tap the confirm button to process. The data will sent to server and do a verification. If the email is exits in database, an email will be sent to the email address that entered by user just now. If the email is not exist in database, an error message will be shown.

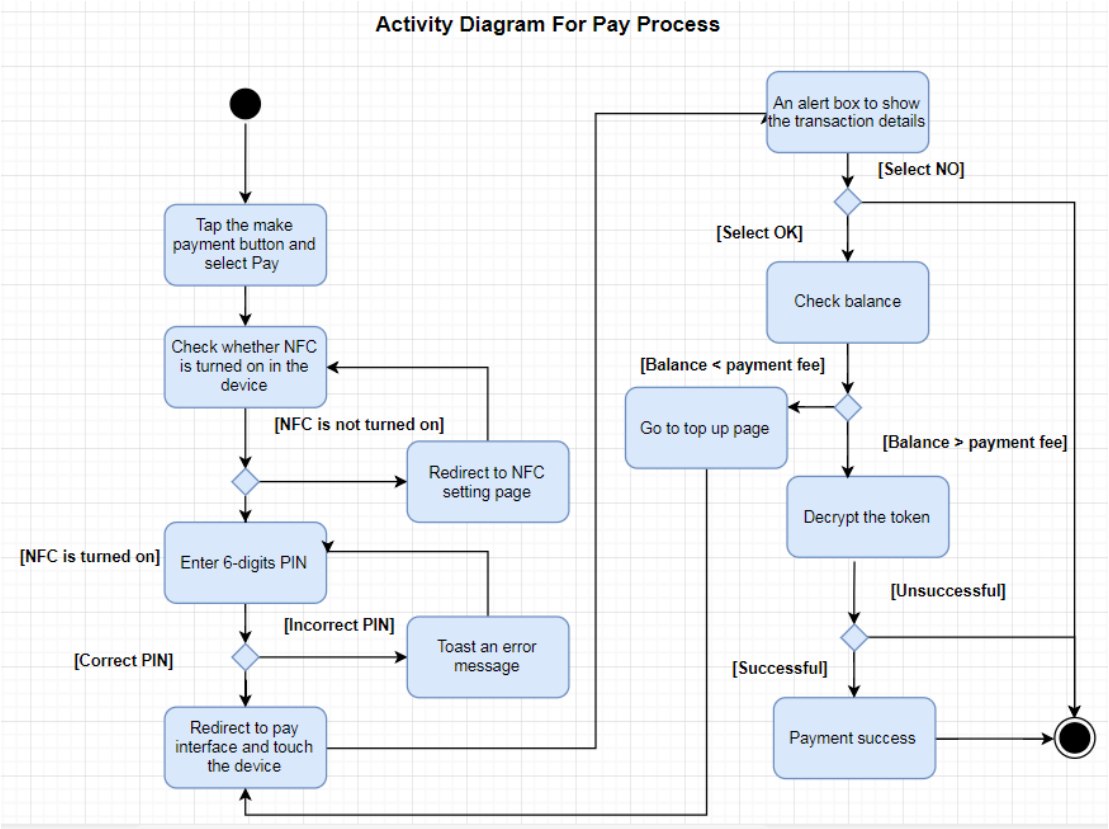

Figure 3.8 Activity diagram for pay process

This is the pay process. To start off, user needs to tap the payment button in the main menu and select pay option. After that, the app will check the phone is turned on the NFC or not. If the NFC is not turn on, an alert box will be shown and redirect to the NFC setting page. If the NFC is turned on, user is required to enter a 6 digits PIN. System will check the PIN whether it matches the one in the database. If correct PIN is entered, it will redirect to pay layout, else the system will toast an error message. Two devices need to touch together in order to let the transfer of data to occur. After get the transaction message, an alert box will pop up to display the transaction details like the payer name and amount. If the information is correct user can tap OK to confirm the transaction. User is also can cancel the transaction by tap the option NO and return back to main menu. After user confirms the transaction, the encrypted token will be decrypted. If the decrypted token is the same as the database, then this transaction is successful, else this transaction is failed.

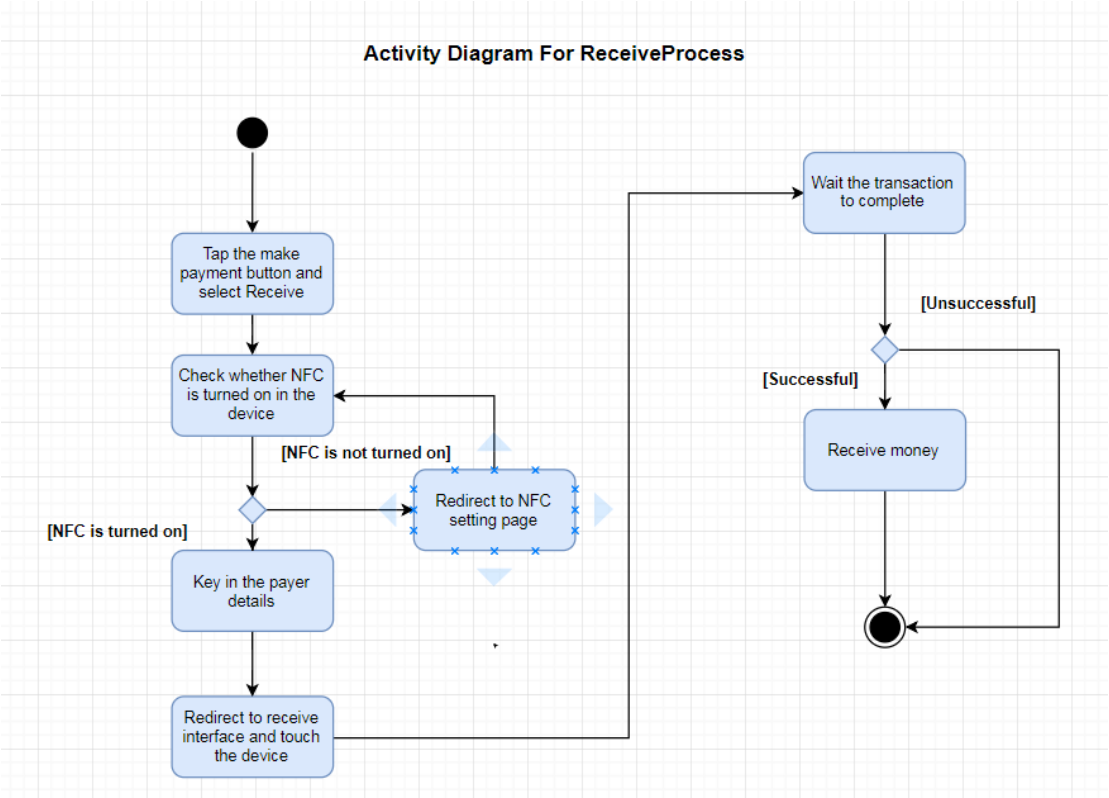

Figure 3.9 Activity diagram for receive process

Diagram above is the receive process. Frist, user needs to tap the payment button in the main menu and select receive option. After that, the app will check the phone is turned on the NFC or not. If the NFC is not turn on, an alert box will be shown and redirect to the NFC setting page. If the NFC is tuned on, it will redirect to the set payer detail page. In the page, user need to fill up the details like the username of payer, the amount and the comment. Then, two devices are touched together. If the transaction is successful, a message will pop up to notice user.

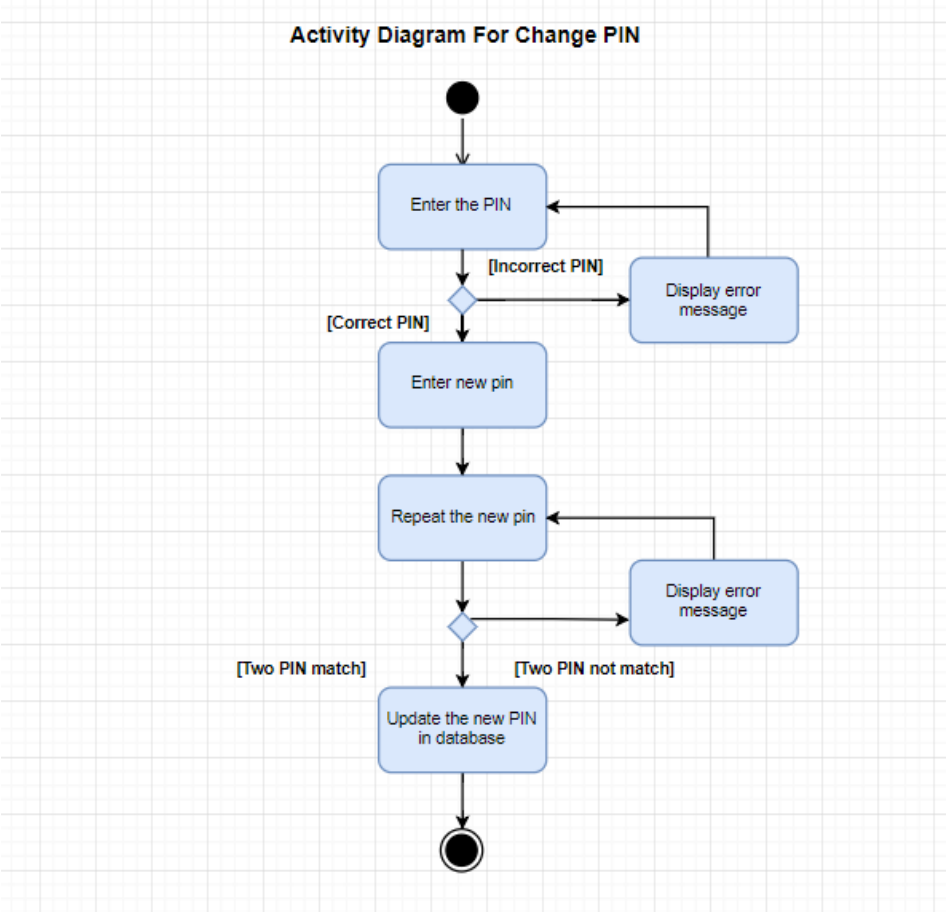

Figure 3.10 Activity diagram for change pin process

Diagram above is the change pin module. First user need to key in the PIN to authentic the real user. If the PIN is not correct, an error message will be shown. Next, user need to enter the new PIN twice. If the two PIN entered is not matched, an error message will be shown, else the new PIN will be updated in the database.

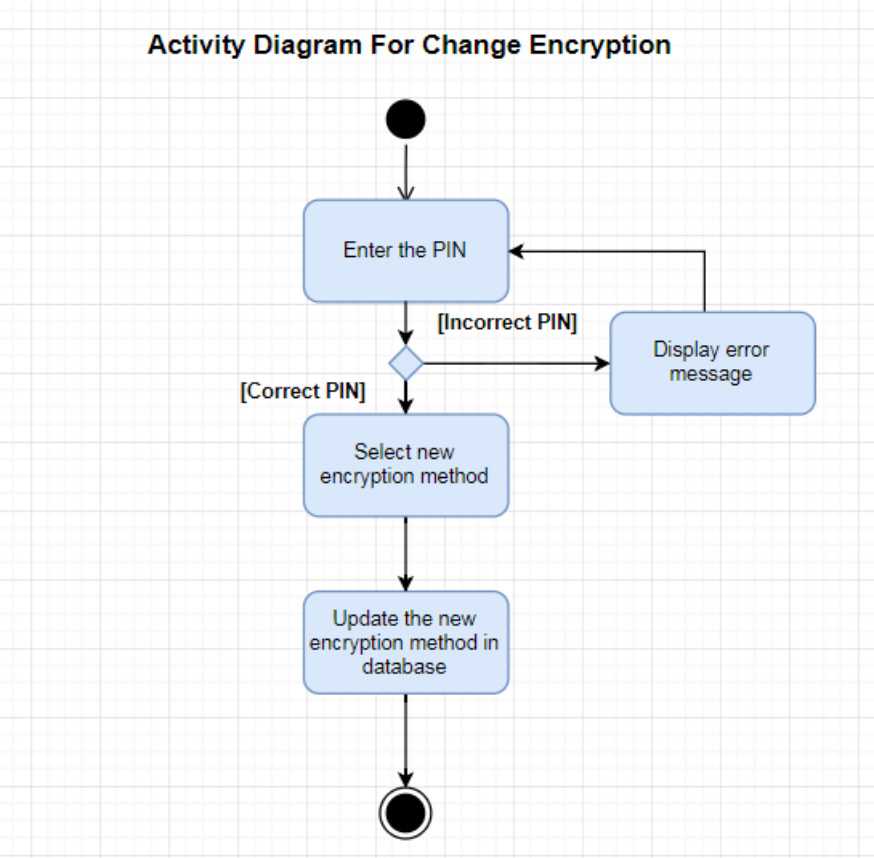

Figure 3.11 Activity diagram for change encryption process

Diagram above is the change encryption module. First user need to key in the PIN to authentic the real user. If the PIN is not correct, an error message will be shown. Next, user need to select the encryption method from a list. Then, the new encryption method will be updated in the database.

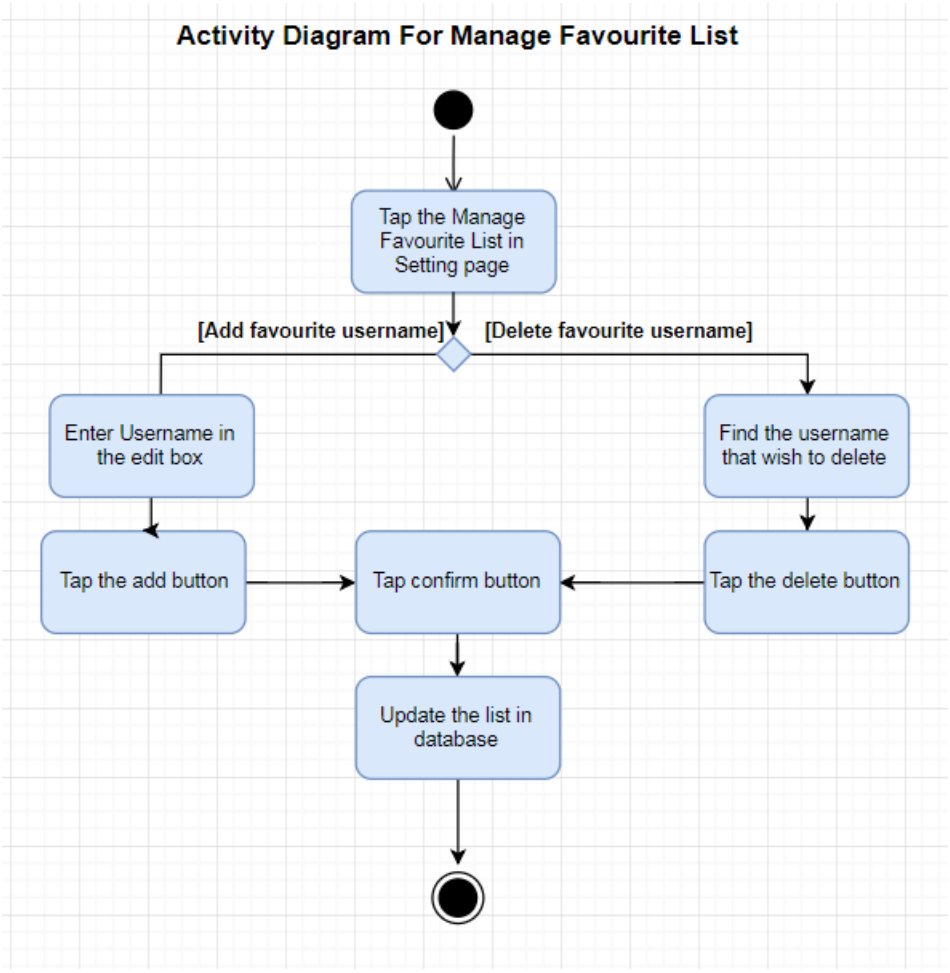

Figure 3.12 Activity diagram for manage favourite list process

Diagram above shows the activity diagram for manage favourite list process. First user need to enter the Manage Favourite List layout by tapping this option in Setting page. If the user wants to add the favourite username, user just need to key in the username in the edit box field and tap the add button. If the user wants to delete the favourite username, user just need to click the delete button next to the username. After that, user needs to tap the confirm button. Last but not least, the list will be updated in the database.

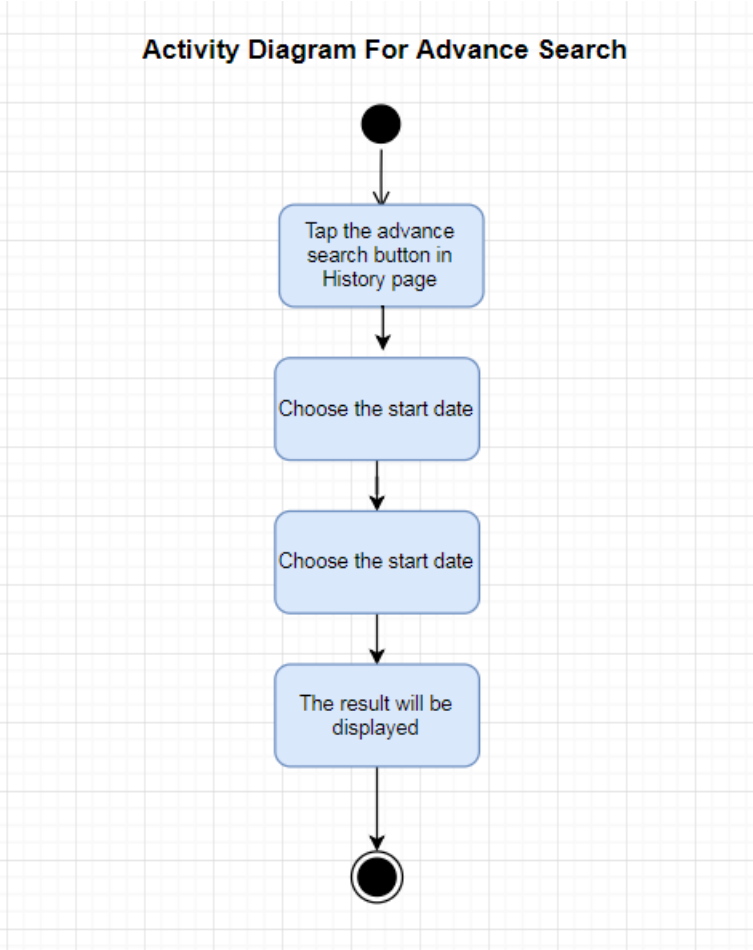

Figure 3.13 Activity diagram for advance search

The diagram above shows the advance search module. First and foremost, user needs to tap the advance search button in History page. Next, start data and end date is selected. After tap the confirm button, the previous transaction records within that time range will be displayed.

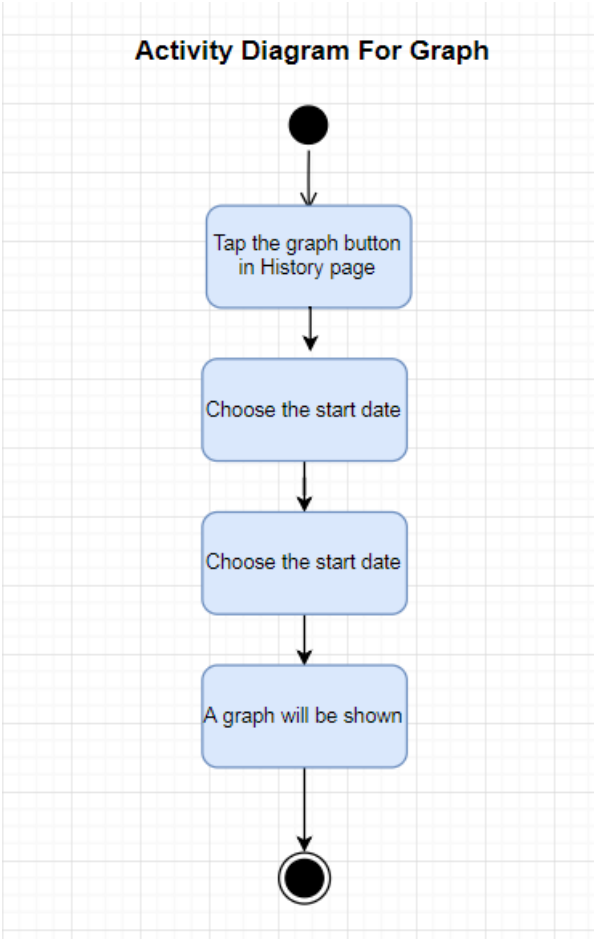

Figure 3.14 Activity diagram for graph

The diagram above shows the graph module for the system. First, the user need to select the graph option in the History page. Next, start data and end date is chosen. After tap the confirm button, a summary pie chart within that time range will be displayed.

3.8 Class Diagram

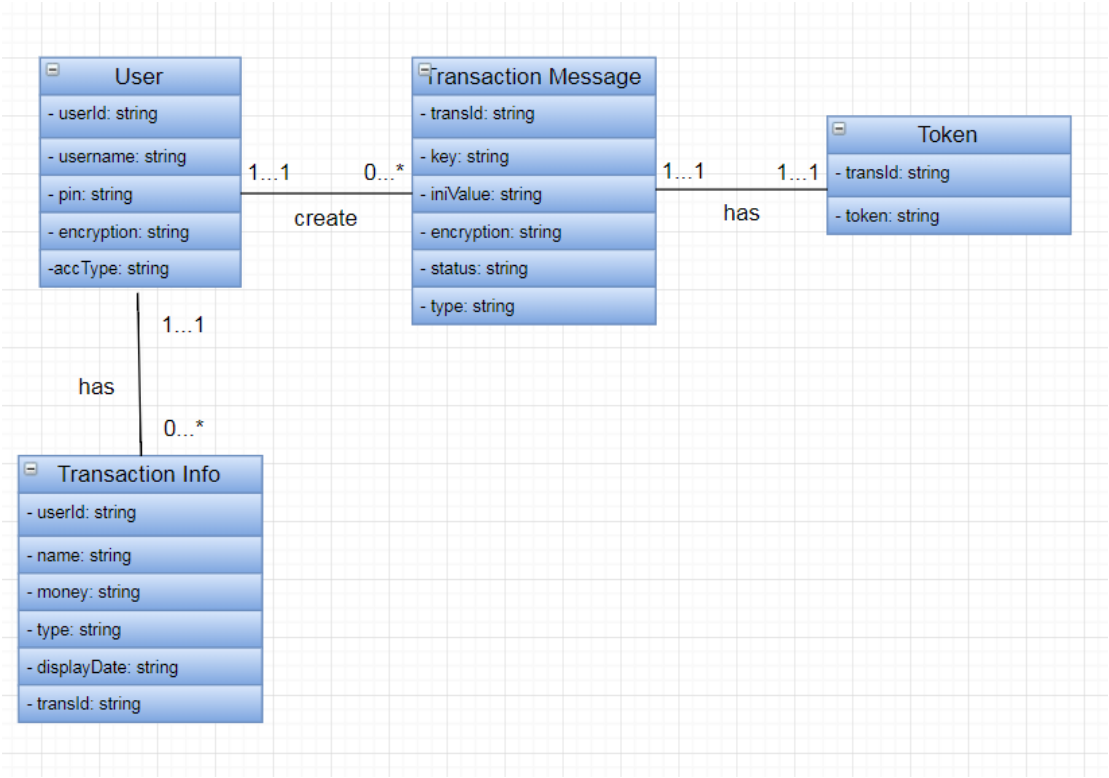

Figure 3.15 Class diagram for NFC Pay

Diagram above is the class diagram. It shows all the class relationship within this system. First, User can create zero or many Transaction Message while each Transaction Message is referred to one User only. Next, Transaction Message has only one Token and at the same time Token also owned by one and only one Transaction Message. Furthermore, User can has zero or many Transaction Info while each Transaction Info is owned by only one User.

3.9 Object Diagram

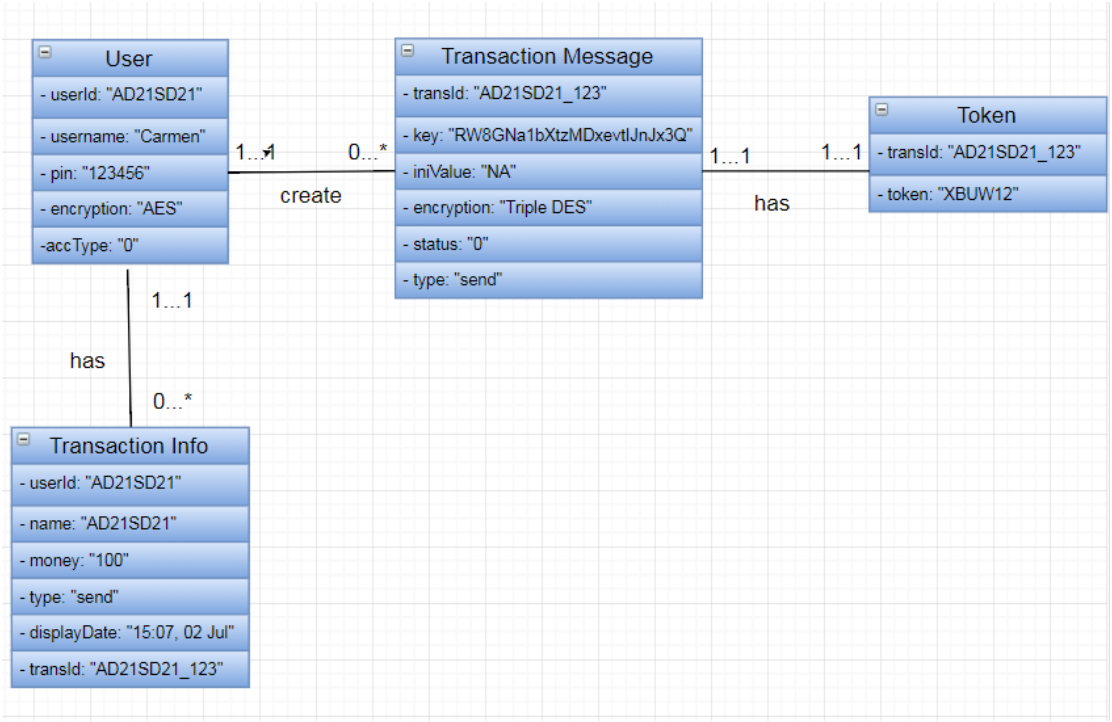

Figure 3.16 Object diagram for NFC Pay

Diagram about show the sample input that stored in these variables.

CHAPTER 4 SYSTEM DESIGN

4.1 Graphical User Interface Design

User Registration Interface Design

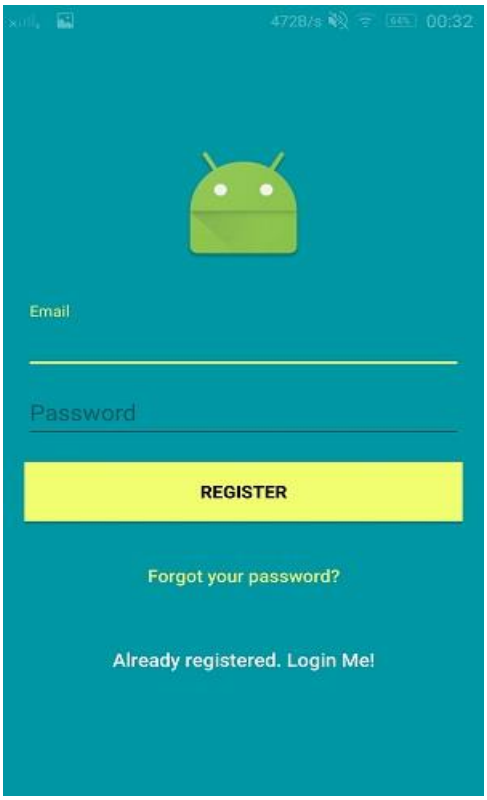

Figure 4.1 Register interface

This layout is for those who is not a member to register an account.

User needs to enter the email and password. After key in those details, user needs to tap the register button in order to register an account. Several conditions are checked. It included the email and password must not be empty, the email entered must has the valid email format, the password length must at least 6 digits and the email must not be registered before. If the condition is not met, an error toast message will be shown.

If the user forget the password, user can retrieve it by tapping the yellow color "Forgot you password" link.

If the user already registered, they can go to the sign in page by tapping the white color "Already registered. Login Me!" link.

User Login Interface Design

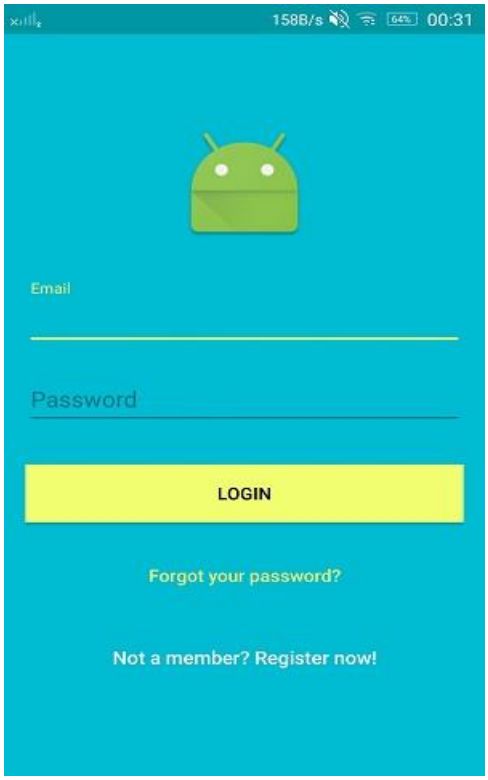

Figure 4.2 Login interface

This is the login layout. User with an account can sign in from here.

User needs to key in email and password they registered. After that, user needs to tap the login button. Same as the user registration interface, several conditions are checked expect the checking of the existing email. An error message will be shown if the condition is not met.

If the user forget the password, user can retrieve it by tapping the yellow color "Forgot you password" link.

If the user not yet registered, they can go to the register page by tapping the white color "Not a member? Register now!" link

Forgot Password Interface Design

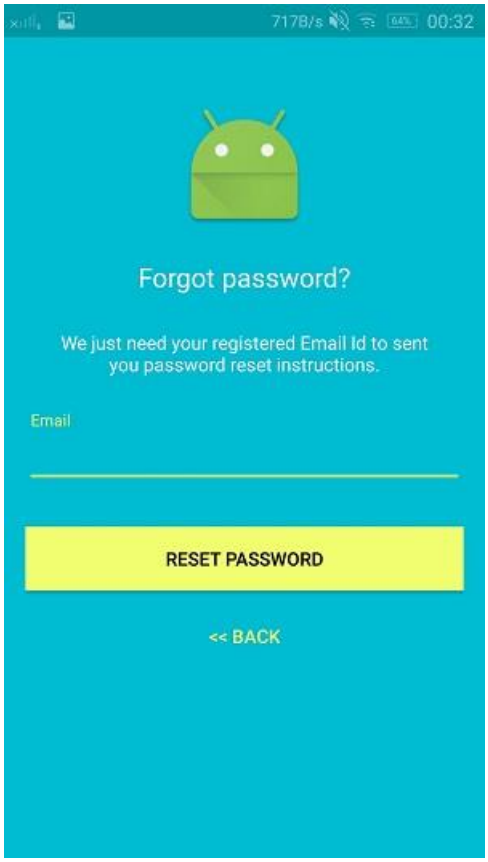

Figure 4.3 Forget password interface

This is the forget password interface.

User needs to enter the email address of their account. Next, user needs to tap the reset password button. After that a reset email will be sent to the email address that key in by the user.

User can choose to return back to the previous page by tap the yellow back link.

Payment Interface Design

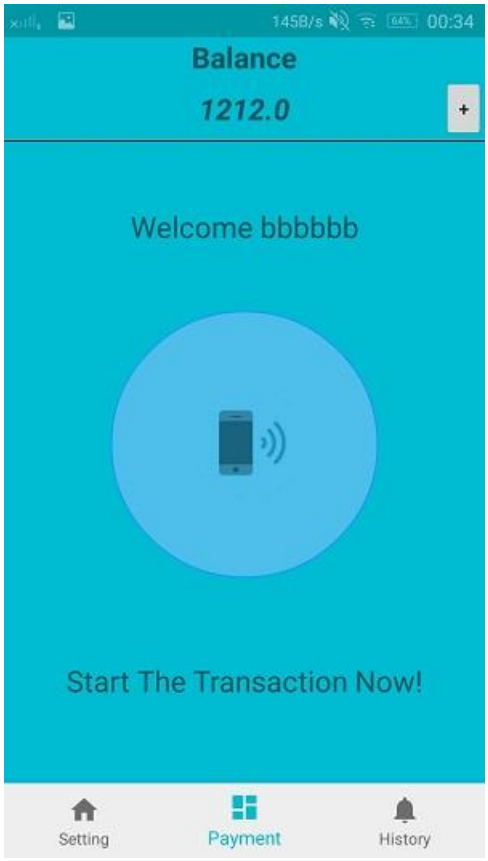

Figure 4.4 Payment interface/ Main menu

This is the payment page or main menu page.

On the most top is the current balance of the user. Next to it is the top up button. User can top up their wallet by tapping the "+" button. Below it is a welcome message is shown along with the username of the user.

If the user wants to make the payment or receive money, user needs to tap the circle button on the center.

Below the circle button, there is a message, "Start the transaction now!" to encourage user to use the wallet.

The bottom is the navigation bar. There are 3 options. Left one is go to the setting page. Middle one is go to the payment page. Right one is go to the history page.

History Interface Design

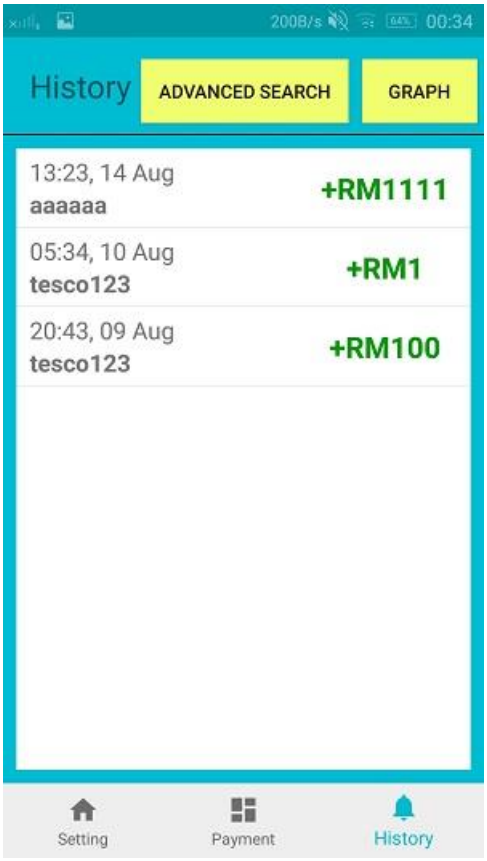

Figure 4.5 History interface

This is the history page. User can view the previous transaction history here.

On the top left side, there are two buttons. One is called advanced search and another one is called graph.

If user taps the advanced search button, user will go to the advanced search page.

If user taps the graph button, user will go to the advanced search page.

Next, under the buttons, there is a list of recent history transaction made by the user. User can tap the transaction list to view the receipt of the transaction.

The bottom is the navigation bar. There are 3 options. Left one is go to the setting page. Middle one is go to the payment page. Right one is go to the history page.

Advanced Search Interface Design

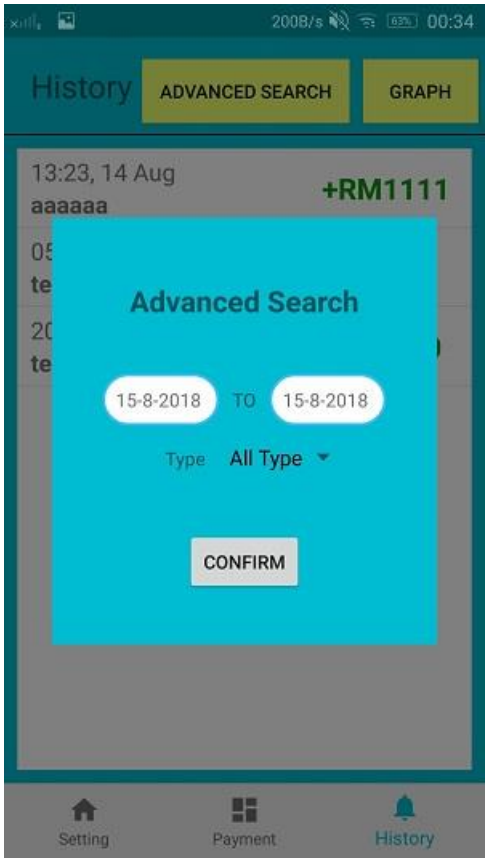

Figure 4.6 Advanced search interface

This is the advanced search interface.

In this interface, user can search the transaction history at any time range. Besides, user also given the option to view the transaction type they selected.

Left one is the start date and right one is the end date.

Next is the drop down list about the types of the transaction. Three options are given here, all type, send and receive.

The bottom is a confirm button.

Graph Interface Design

Figure 4.7 Graph interface

This is the graph interface. For this interface user can have an overview on how much money is spent and received. The details are plotted into a pie chart.

On the top, there is two date. Left one is the start date and right one is the end date. Next to it, it is a search button. User need to tap the button to begin the search.

After that, there are some numerical statistics within the time range selected. The total money, the money sent and the money received.

Below that, it is a pie chart that shows the money in and out within that time range.

Setting Interface Design

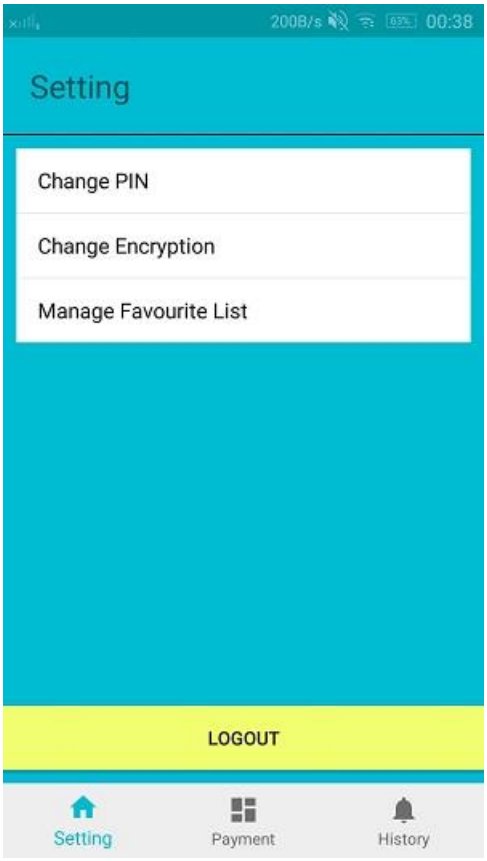

Figure 4.8 Setting interface

This is the setting page. User can change the setting in this page.

On the top of the page, it has a header that shows it is a setting page.

Next, for the current moment, there are only 3 options to let user change. First of all, user can change the pin by tapping the option change pin. Secondly, user can change the encryption method by tapping the change encryption. Thirdly, user can manage the favorite list by tapping manage favorite list.

User can tap the logout button to logout the account.

The bottom is the navigation bar. There are 3 options. Left one is go to the setting page. Middle one is go to the payment page. Right one is go to the history page.

Change Pin Interface/ Confirm Pin Interface

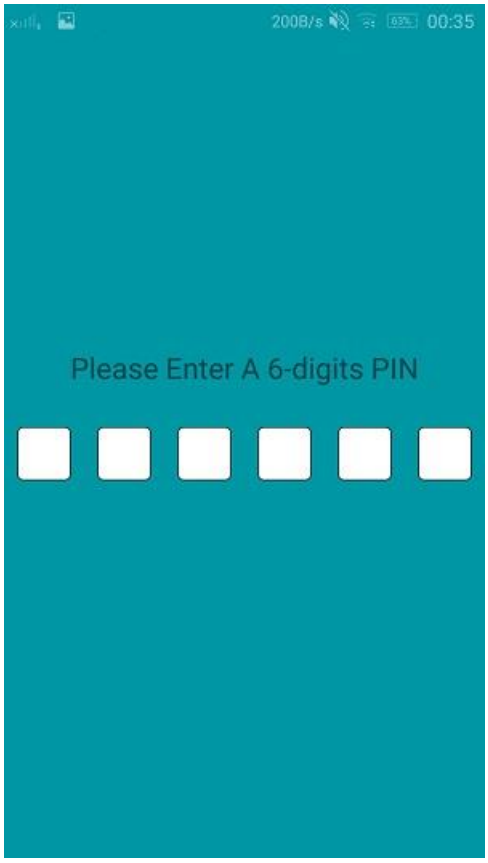

Figure 4.9 PIN interface

There is nothing much different between these two layouts. The only different is the background color and the hint message that displayed.

This interface is allow the user to enter the 6-digits pin.

On the middle there is a hint message. Under that, it is a 6 digit pin view. User need to enter the pin in the pin view.

Select Encryption Interface

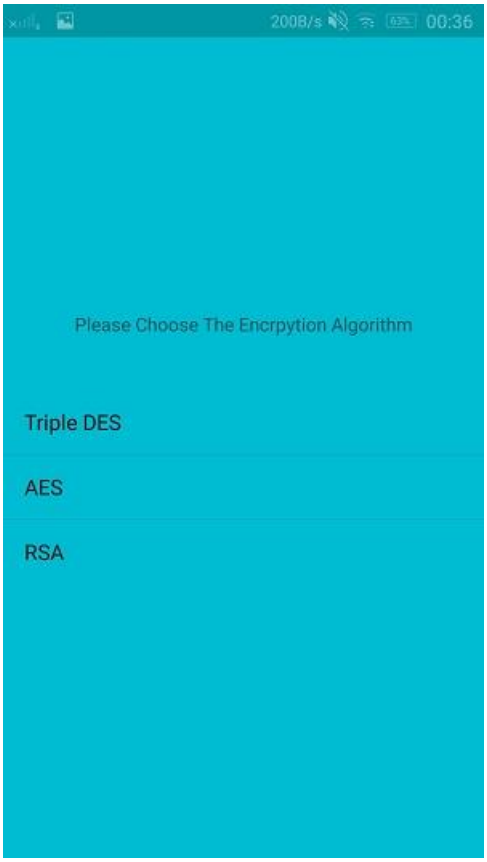

Figure 4.10 Select encryption interface

This is the select encryption interface. This interface provides some encryption method to let user to choose.

It is a simple layout. It consists of two things only. A hint message and a list of encryption method.

User can tap and select the encryption method to want to use during transaction.

Select Transaction Type Interface Design

Figure 4.11 Select transaction type interface

This is the select transaction type interface. User can choose the transaction type in this page, either pay or receive money.

If the user did not switch on the NFC in the phone, an alert message will be popped out and direct the user to switch on the NFC.

Set Payer Details Interface Design

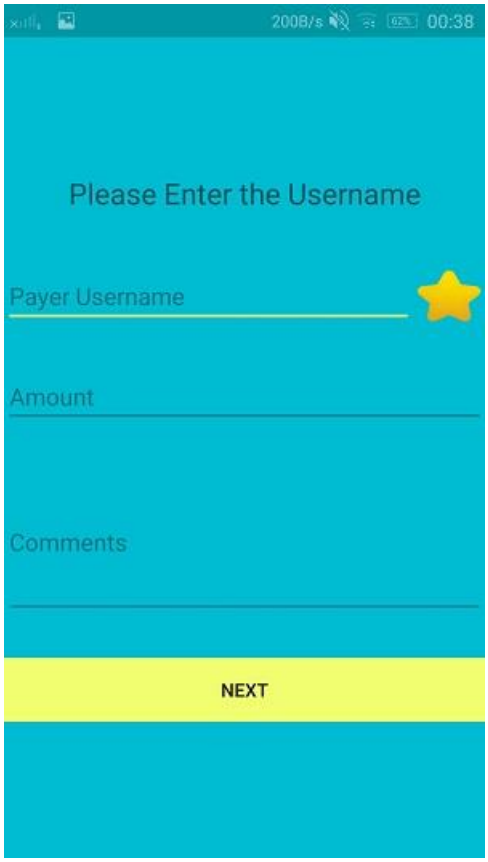

Figure 4.12 Set payer details interface

This is the set payer details interface. In this page, user need to key in the details of the payer, like the payer username, the amount to be pay and the comment of the transaction.

First of all, there is a hint message, “Please Enter the Username”.

Next, user needs to key in the username of the payer. If user saved the payer username into favorite list, user can tap the star icon and just select the username from the favorite list.

Then, user needs to enter the money amount. User may choose to write some comments about the transaction.

User needs to tap the next button to continue the transaction.

Favorite List Interface Design

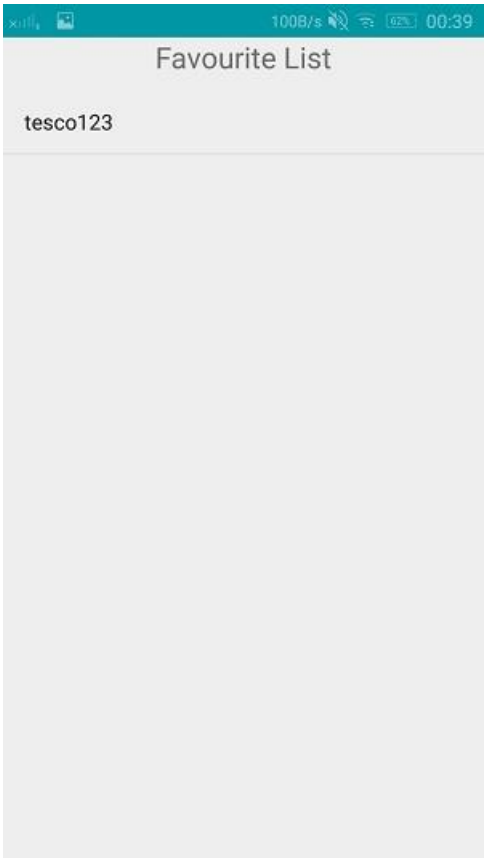

Figure 4.13 Favorite list interface

This is favorite list interface. In this interface user can choose the username from the list and no need to enter the username in Set Payer Details Interface.

Favorite list text is on the middle top of the interface.

Next there is a list of the favorite username that user saved in manage favorite list interface.

Manage Favorite List Interface Design

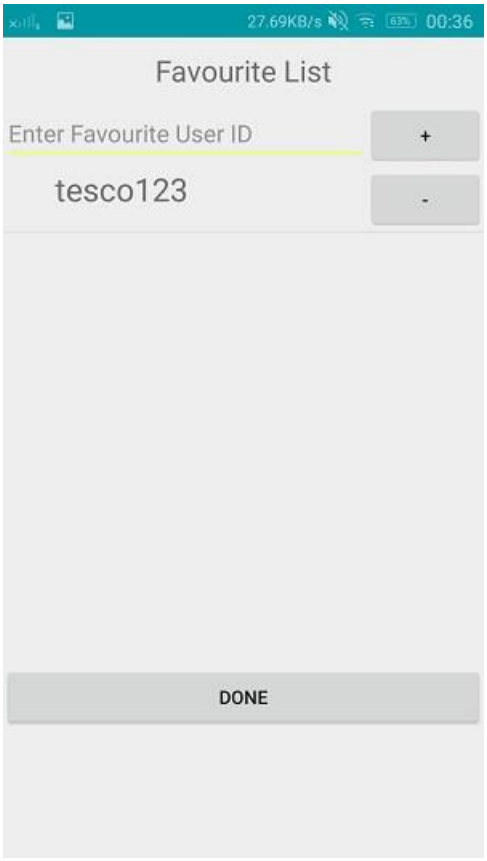

Figure 4.14 Manage favorite list interface

This is manage favorite list interface. In this page, user can manage the favorite username here.

Favorite list text is on the middle top of the interface.

Below it, there is an edit text box and a plus sign button. User can key in the username in the text box and then tap the plus sign button.

Next, there is a list of favorite usernames that saved before. Besides that there is a minus sign, user can delete the username by tapping the minus sign button.

After user finishes the modification, user needs to tap the done button. After all modification will be saved to the database.

Set Username Interface Design

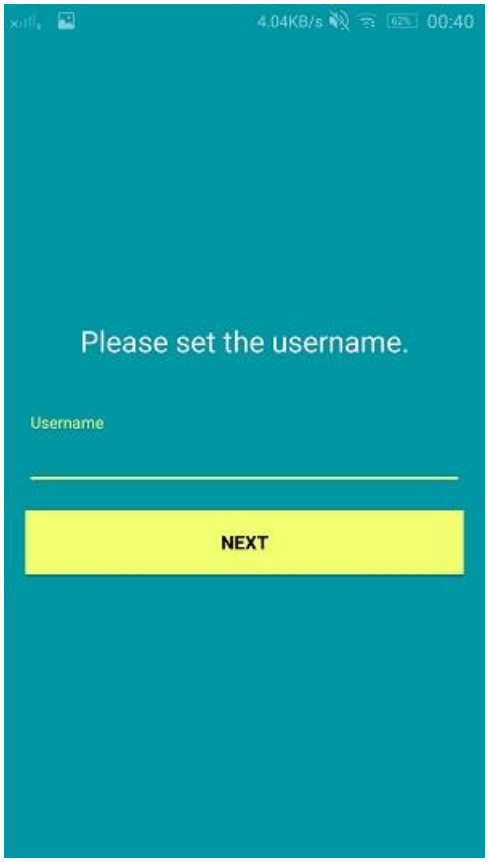

Figure 4.15 Set username interface

This is set username page. After the registration of the email and password, user need to setup a unique username.

User needs to key in the username in the username field. After that user needs to tap the next button.

If the username is already exits, an error message will be shown and user needs to choose another username. Besides that, the username length needs at least 6 digits long.

4.2 Design of Data Storage

The database that this system used is firebase. Firebase is a noSQL database. Thus all the data is not in table form. Below are some data structure of the database.

User Table:

This is used to store the details of user. It stores the accType, balance, encryption, pin and username of the account. The accType is account type. 0 is normal account while 1 is merchant account.

Users:

-userId:

-accType:

-balance:

-encryption:

-pin:

-username:

Below is the exact data in the firebase:

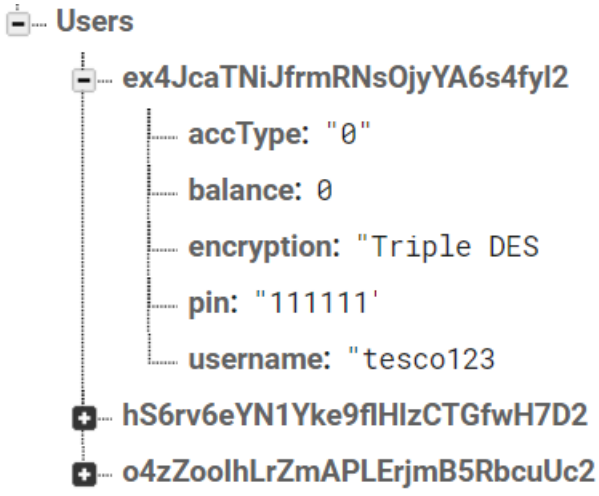

Figure 4.16: Users Table Example Data

TransactionMessage Table:

This is used to store the encryption details of a transaction message. It stores the encryption, iniValue, key and the status. The iniValue is the initialization vector of encryption. Key is the secret key. Status is the transaction status, 0 is waiting, 1 is completed and -1 is failed.

TransactionMessage:

-transId:

- encryption:

-iniValue:

-key:

-status:

Below is the exact data in the firebase:

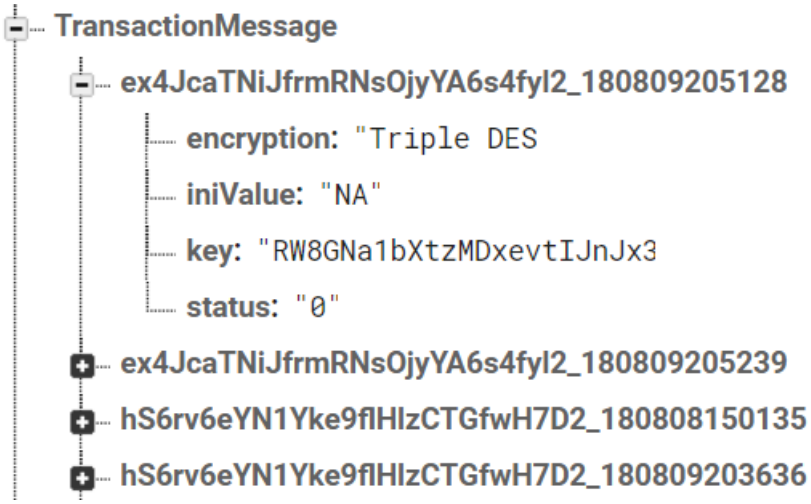

Figure 4.17 TransactionMessage Table Example Data

TransactionInfo Table:

This is used to store the information of transaction. It stores displayDate, money, tranId and type. The displayDate is the date of the completed transaction. The money is the transaction amount. The transId is the transaction Id of the transaction. The type is the type of transaction, either receive or pay.

TransactionInfo:

-userId:

- displayDate:

-money:

-tranId:

-type:

Below is the exact data in the firebase:

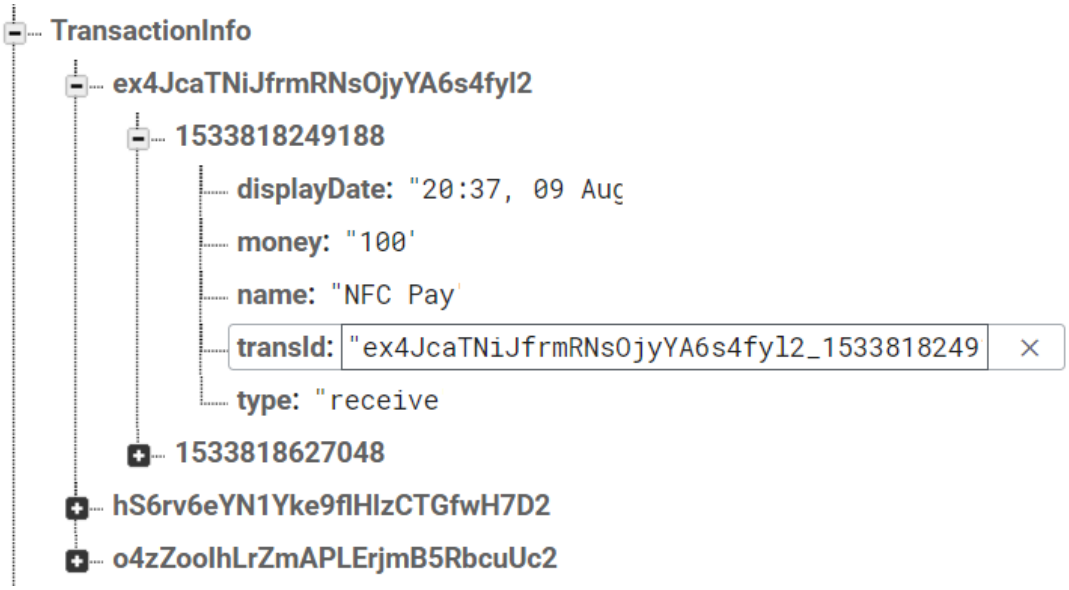

Figure 4.18 TransactionInfo Table Example Data

Token Table:

This is used to store the token. It stores the token with respect to the transaction Id.

Token:

-transId: token

Below is the exact data in the firebase:

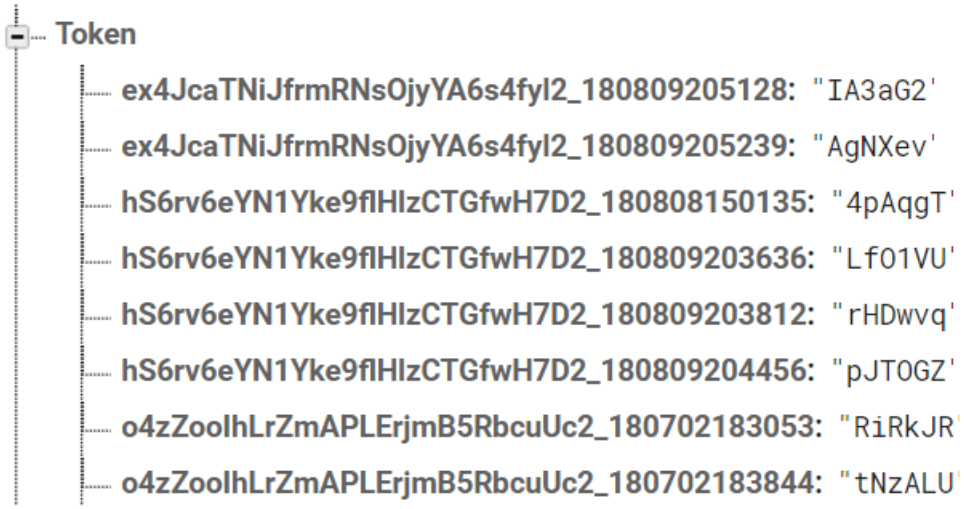

Figure 4.19 Token Table Example Data

Comment Table:

This is used to store the comment. It stores the comment with respect to the transaction Id.

Comment:

-transId: comment

Below is the exact data in the firebase:

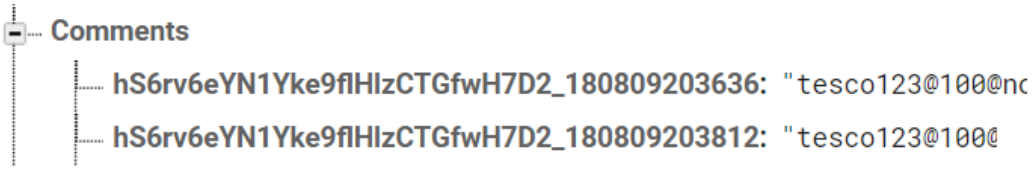

Figure 4.20 Comment Table Example Data

FavouriteList Table:

This is used to store the favourite list. It stores the favourite list with respect to the user Id.

FavouriteList:

-userId:

-list_of_favourite_username

Below is the exact data in the firebase:

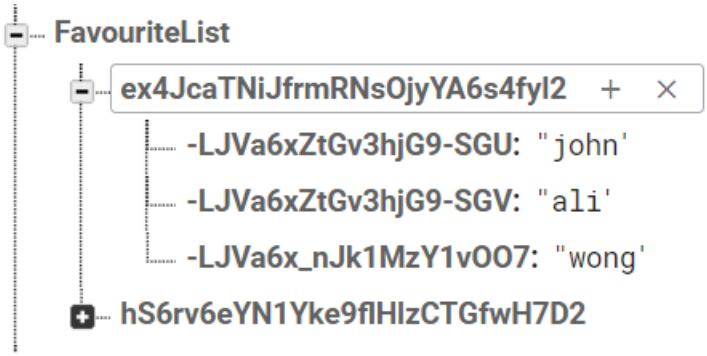

Figure 4.21 FavouriteList Table Example Data

Payer Table:

This is used to store the payer username. It stores the payer username with respect to the transaction Id.

Payer:

-transId:

Below is the exact data in the firebase:

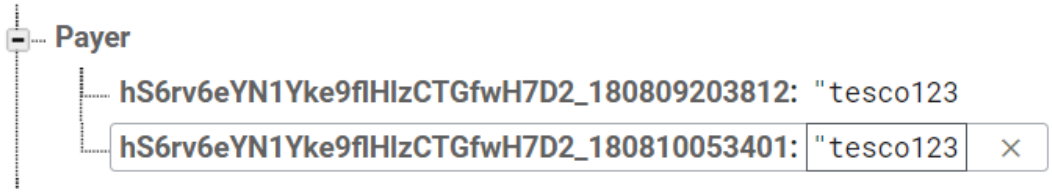

Figure 4.22 Payer Table Example Data

4.3 System Architecture Design

In this project, a 2-tier client-server architecture design is used. The reason why the client-server architecture design is chosen because it has a balance processing between client and server. Besides that, a 2-tier client-server architecture design is used because of this is a small project. This means that the server is responsible for data storage and access while client side responsible for application and presentation logic.

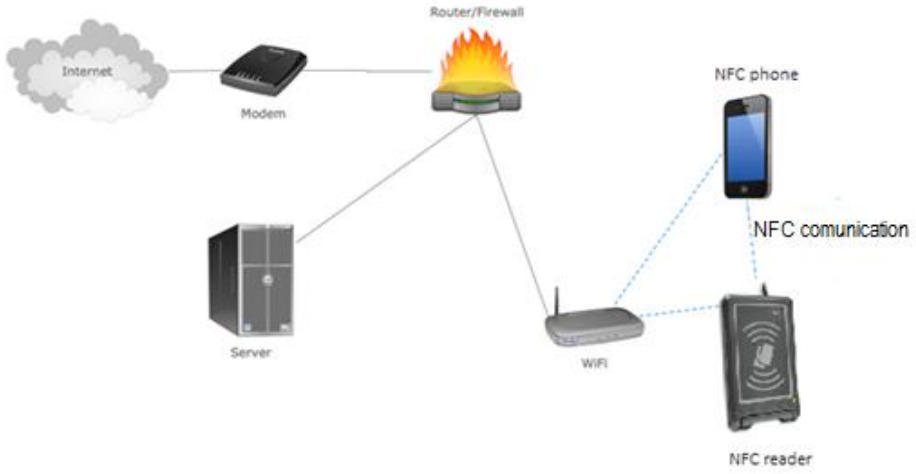

Figure 4.23: Network Diagram of the system

Figure 3.6 shows the network diagram of the system. First of all, the NFC phone will act as sender and send the transaction information to the NFC reader. However this information need to be encrypt first. Thus, the sender will use the public key to encrypt the message. Next, a message will upload to the server. This message includes the file ID and the encryption type chose by user. Furthermore, a handshake will be occurred between two devices. Next when the receiver get the encrypted message, it will get the private key from the server by using the file ID and decrypt it. After that, the pay amount will be deducted from the sender wallet while the receiver will get the money.

CHAPTER 5 SYSTEM TESTING

5.1 System Implementation & Testing

After design phase, implementation phase is started and the system will be installed into two mobile devices. In this chapter, the system will be tested by component testing with several test cases to find out the possible bugs lied within each module. This is very important step to make sure all modules are implemented correctly. After that, an integration testing will be carried out. All the modules will integrate together to evaluate the effective integration among all modules. This is very important to ensure that the full integration system can work together as a whole and integrated way. Last but not least, once all the evaluation of the system is fully satisfied, users will be invited to evaluate on the system. This is to make sure that the system is user friendly and can fulfil their expectations on this application.

5.2 Implementation Challenges

Implementation phase is very crucial in the project development process. In this phase, a product that need to satisfy the requirement of the users need to be developed. Nonetheless, there are some challenges in this phase.

- Database Connection

  Since this is an online mobile application, thus internet connection is a must when using this application. Without the internet connection, user are unable to get the data and access to the online database.

- Unfamiliar with NFC technology
  The learning resource on internet about this NFC technology is quite less. Thus, it increases the difficulty to develop this app.

5.3 Techniques and Tools Used

System development tool

Android studio is used to develop this mobile application. It uses Java programming language as a back end code to operate the system.

Database environment

Firebase is used as the database in this project. It stored data like the user details, the transaction details and so on. The reason Firebase in used is because it is very easy to use and it is an online database, so there is no need to install the server like wamp server.

5.4 System Testing

Several modules will be tested here. If the expected result and actual result is aligned then this module is considered as no bugs.

5.4.1 Modules to Be Tested

The table below showed the modules need to be tested.

Modules ID	**Module**	**Test Priority**
M001	Login Module	High
M002	Register Module	High
M003	Main Menu Module	High
M004	Pay Module	High
M005	Receive Module	High
M006	History Module	High
M007	Change Pin Module	High
M008	Change Encryption Module	High
M009	Manage Favourite List Module	High
M010	Logout Module	High

Table 5.1 Modules to be tested

5.4.2 Test Summary

M001 Login Module

Requirement	Input	Expected Output	Actual Output	Status
The system shall accept the user login with correct email address and password	Valid email address and password	Intent to Payment Page	Intent to Payment Page	Pass
	Invalid email address and valid password	Display error message	Display error message	Pass
	Valid email address and invalid password	Display error message	Display error message	Pass
	Invalid email and invalid password	Display error message	Display error message	Pass

Table 5.2 Test Summary of Login Module

M002 Register Module

Requirement	Input	Expected Output	Actual Output	Status
The system shall accept only correct email address format	Valid email format	Register successfully	Register successfully	Pass
	Invalid email format	Display error message	Display error message	Pass
The system shall accept the password with at least 6 characters long	Valid format	Register successfully	Register successfully	Pass
	Invalid format	Toast an error message	Toast an error message	Pass
The username shall at least 6 characters	Valid format	Process to next page	Process to next page	Pass
	Invalid format	Toast an error message	Toast an error message	Pass
The pin shall be the same	Same pin	Process to next page	Process to next page	Pass
	Different	Toast an error message and enter the pin again	Toast an error message and enter the pin again	Pass
The data shall store into database	All valid inputs	Data saved in database	Data saved in database	Pass

Table 5.3 Test Summary of Register Module

M003 Main Menu Module

Requirement	Input	Expected Output	Actual Output	Status
The system shall display the correct username with respect to the account login	Valid account	Display the correct username	Display the correct username	Pass
The system shall display the correct balance user have	Valid account	Display the correct balance	Display the correct balance	Pass

Table 5.4 Test Summary of Main Menu Module

M004 Pay Module

Requirement	Input	Expected Output	Actual Output	Status
The system display an alert box when NFC is not enabled in the phone	NFC is not enable	An alert box is showed	An alert box is showed	Pass
The system shall allow user to process payment after key in the correct pin	Correct pin	Process to next page	Process to next page	Pass
	Incorrect pin	Toast an error message and enter the pin again	Toast an error message and enter the pin again	Pass
The system shall display a transaction detail in alert box when two devices touch together	Two devices touched together	An alert box that show the payee username and the amount to be paid	An alert box that show the payee username and the amount to be paid	Pass
The system shall notify the user when the balance is not enough to pay the bill	Balance is not enough to paid the bill	An alert box to redirect to top up page	An alert box to redirect to top up page	Pass
The system shall be able to retrieve the secret key from the database and decrypt the transaction token	Retrieve the data from database	Transaction token is successfully decrypted and transaction is completed	Transaction token is successfully decrypted and transaction is completed	Pass

The balance shall deduct with correct amount of money	Pervious transaction amount	The system deduct the correct amount of money from balance.	The system deduct the correct amount of money from balance.	Pass

Table 5.5 Test Summary of Pay Module

M005 Receive Module

Requirement	Input	Expected Output	Actual Output	Status
The system shall return the correct username selected in favourite list	Favourite username	Correct username is showed	Correct username is showed	Pass
The system shall store the details of payer that keyed in in database	Payer details	Data is stored	Data is stored	Pass
The system shall encrypt the transaction token	Transaction token	Transaction token is encrypted	Transaction token is encrypted	Pass
The system shall show an alert box when the payer completed the transaction.	Payer completed the transaction	An alert box show that the transaction is completed.	An alert box show that the transaction is completed.	Pass
The system shall add the correct amount of money received	Transaction amount to be received	Correct amount is added in the balance	Correct amount is added in the balance	Pass

Table 5.6 Test Summary of Receive Module

M006 History Module

Requirement	Input	Expected Output	Actual Output	Status
The system shall display all the information of the previous transaction record	All the previous history record	Display all the information of previous transaction record	Display all the information of previous transaction record	Pass
The system shall allow user to check the detail of one single transaction	Tap the desire transaction record	A receipt of the specific transaction.	A receipt of the specific transaction.	Pass
The system shall allow the user to search the transaction record within some range	A range of date	Correct list of transaction according to the range of date	Correct list of transaction according to the range of date	Pass
The system shall display a pie chart within some range	A range of date	A pie chart about the total spent and receive of money according to the range of date	A pie chart about the total spent and receive of money according to the range of date	Pass

Table 5.7 Test Summary of History Module

M007 Change Pin Module

Requirement	Input	Expected Output	Actual Output	Status
The system shall prompt the user to key in the old pin before the user want to change the new pin	Correct pin	Process to change pin page	Process to change pin page	Pass
	Incorrect pin	Toast an error message and enter the pin again	Toast an error message and enter the pin again	Pass
The system shall allow the user to change the pin	Two same pin are entered	The new pin is updated	The new pin is updated	Pass
	Different pin are entered	Toast an error message and enter the pin again	Toast an error message and enter the pin again	Pass

Table 5.8 Test Summary of Change Pin Module

M008 Change Encryption Module

Requirement	Input	Expected Output	Actual Output	Status
The system shall prompt the user to key in the pin before the user want to change the encryption method	Correct pin	Process to change encryption page	Process to change encryption page	Pass
	Incorrect pin	Toast an error message	Toast an error message	Pass
The system shall allow user to set their new encryption method	New encryption method	New encryption method is updated in database	New encryption method is updated in database	Pass

Table 5.9 Test Summary of Change Encryption Module

M009 Manage Favourite List Module

Requirement	Input	Expected Output	Actual Output	Status
The system shall allow user to add their favourite username in the list	Favourite username	The username is added in the favourite list	The username is added in the favourite list	Pass
The system shall allow save this list to database	List of favourite username	The list in stored in database	The list in stored in database	Pass

Table 5.10 Test Summary of Manage favourite List Module

M010 Logout Module

Requirement	Input	Expected Output	Actual Output	Status
The system shall allow user to logout	User taped the logout button	Logout successfully	Logout successfully	Pass

Table 5.11 Test Summary of Logout Module

5.5 Test Result

This component test is based on testing all the modules on by one. Below is the result after testing all the modules.

Modules ID	**Module**	**Status**
M001	Login Module	Pass
M002	Register Module	Pass
M003	Main Menu Module	Pass
M004	Pay Module	Pass
M005	Receive Module	Pass
M006	History Module	Pass
M007	Change Pin Module	Pass
M008	Change Encryption Module	Pass
M009	Manage Favourite List Module	Pass
M010	Logout Module	Pass

Table 5.12 Test results

CHAPTER 6 SYSTEM EVALUATION AND DISCUSSION

6.1 Chapter Overview

In this chapter, the strength, limitation and the future improvement of the NFC Pay app will be discussed.

6.2 Proposed System Completion

In this section, the previous objectives set will be discuss, to make sure that all the objectives is completely fulfilled in this app.

The first main objective is **to allow the sure to make payment by using NFC**. This is achieved. When two devices touched together, the transaction massage that contains the transaction ID, encrypted token, the amount and the payer username will be sent to the payer's device. This is proven in test case **M004 Pay Module -** The system shall display a transaction detail in alert box when two devices touch together, this shows that the payer is received the message only then this alert box will pop out.

Next, the second object **to enhance the security of the system** is also achieved. Three of its sub objectives are working perfectly in this app. For the first sub objective, **to encrypt the data before transaction,** is achieved in **M004 Pay Module -** The system shall be able to retrieve the secret key from the database and decrypt the transaction token. For the second sub objective **to prompt user to enter PIN when making payment,** is achieved in **M004 Pay Module -** The system shall allow user to process payment after key in the correct pin. For the third sub objective **to show the payee information to the payer before the transaction starts**, is achieved in **M004 Pay Module -** The system shall display a transaction detail in alert box when two devices touch together.

Last but not least, the final objective**, to allow the user to check back the previous transaction history** is also proofed in all the test case in **M006 History Module**. User not only can check all the past transaction record, but can also search the transaction record within a time range in list or a pie chart form.

6.3 System Strength

1. Convenience and fast

This mobile app provides the user another alternative way to make payment. Cashless payment is very good in a few aspects. First of all, this app allows the user eliminate the need to bring the heavy coins to go out. Besides, it is also convenience and fast, just a touch of devices then the payment is success. At the same time, the time to wait for the change of money also saved.

2. Prevent man-in-the-middle attack

The app have several measure to counter the man-in-the-middle attack. First and foremost, this app provides many types of encryption method to use in transaction message encryption. This make the transaction safe. Although someone could able get the transaction message, they cannot decrypt it. Next, this app will show an alert to show the details of the payee before the user makes the payment.

3. Merchant mode for the merchant

In this app, user not only can send money to another user, but they can use this app to make payment. This app provides a merchant mode that special for merchant side. In this mode, they can only receive money and cannot pay money.

4. This app allow user to check the transaction history within specific time range

This application provides two advance options for user to check the previous transaction record in term of listing or a pie chart.

6.4 System limitations

1. Not every phone have NFC feature

Although NFC is a very good technology that can able two devices to transfer data, not every mobile devices have this function.

2. Must have Internet connection

As mentioned before, this is an online mobile application. Thus, it cannot function without the internet connection.

3. Not a Multilanguage system

This application only support English language.

6.5 Future Enhancements

1. Add the real top up function

Due to the some restrictions, this mobile app do not have any real top up function.

2. A better layout and UI interface

UI interface can be more user friend and more attracting to the user.

3. More encryption option

There are many more encryption method that can be implemented in this app. Besides, hash function can be also used.

4. Support Multilanguage

Now in current version, the application just only support English language. Other language like Chinese, Japanese, Korean, and so on can be implemented in the future.

CHAPTER 7 CONCLUSION

In short, NFC is a good technology that can help people to improve the quality of life. In this case we use it to make payment. However there are some drawbacks of this technology. It includes eavesdropping, man in the middle attack, relay attack, data corruption and so on. As the time passed, this technology will surely getting more popular and this will motivate the attacker to expose the vulnerability of NFC. The attack can sniff the transaction message and the attacker might make some changes on it, letting the victims to pay the bill for the attacker. Thus, a protocol to secure the transaction is designed in this project to prevent the successful attack. The aim of this app is to prevent this kind situation to happen. Besides, the second purpose of this app is to provide people another way to make cashless payment instead of just scanning QR code.

There are two account types for this app, one is the normal account and another one is merchant account. User account is just like normal user. It can be used to pay and receive money. Unlike the normal account, merchant account is for merchant. It can only receive money.

Furthermore, this mobile application have many useful features like make payment, receive money, check history transaction, change the pin and so on. Next, the strength of this app is all the transaction message is encrypted by using the preferable encryption by the user.

Weakness of this app is that not all the phone has this NFC feature. Next, this app can only be used in close range due to the nature of NFC technology. Therefore, remote payment is not possible.

In conclusion, there are a lot of improvement can be made in this app. These weaknesses are hoped to be solved in the near future.

Reference

Damme, GV, Karahan, H, Wouter, K, Preneel 2009, *Offline NFC Payments with Electronic Vouchers.* Available from: ACM Digital Library. [16 August 2017].

European Union Agency for Network and Information Security. 2016, *Security of Mobile Payments and Digital Wallets*. Available from: < https://www.enisa.europa.eu/publications/mobile-payments-security >. [10 November 2017].

Ghag, O. 2012, *A Comprehensive Study of Google Wallet as an NFC Application*. Available from: < http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.252.6928&rep=rep1&type=pdf >. [10 November 2017].

Kadambi, KS, Li, J, Karp, AH 2009, *Near-Field Communication-Based Secure Mobile Payment Service.* Available from: ACM Digital Library. [16 August 2017].

Lee, H, Kim, J, Yung, J, Lee, Y, Won, D 2017, *An Enhanced Unlinkable Anonymous Payment Scheme Based on Near Field Commnication.* Available from: ACM Digital Library. [16 August 2017].

Luo, JN, Yang, MH, Huang, SY 2016, *An Unlinkable Anonymous Payment Scheme based on near field communication.* Available from: ScienceDirect. [16 August 2017].

Mendoza, S. 2016, *Samsung Pay: Tokenized Numbers, Flaws and Issues*. Available from: < https://www.blackhat.com/docs/us-16/materials/us-16-Mendoza-Samsung-Pay-Tokenized-Numbers-Flaws-And-Issues-wp.pdf >. [10 November 2017].

Qiao, M, Carpenter, A 2013, *Security of the near field communication protocol: an overview.* Available from: ACM Digital Library. [16 August 2017].

Rouse, M. 2007, *Near Field Communication (NFC)*.Available from: <http://searchmobilecomputing.techtarget.com/definition/Near-Field-Communication>. [16 August 2017].

Xinru, C. 2016, *Information Security of Apple Pay*. Available from: < https://publications.theseus.fi/bitstream/handle/10024/118948/Chen_Xinru.pdf?sequence=1 > . [10 November 2017].

Security of NFC payment on mobile payment application

ORIGINALITY REPORT

4%	1%	1%	3%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Luo, Jia Ning, Ming Hour Yang, and Szu-Yin Huang. "An Unlinkable Anonymous Payment Scheme based on near field communication", Computers & Electrical Engineering, 2016. Publication	1%
2	Submitted to University of Mauritius Student Paper	<1%
3	Submitted to INTI University College Student Paper	<1%
4	Submitted to University of Greenwich Student Paper	<1%
5	Submitted to Griffth University Student Paper	<1%
6	link.springer.com Internet Source	<1%
7	Submitted to 79920 Student Paper	<1%
8	Hakjun Lee, Jiye Kim, Jaewook Jung, Youngsook Lee, Dongho Won. "An enhanced	<1%

	unlinkable anonymous payment scheme based on near field commnication", Proceedings of the 11th International Conference on Ubiquitous Information Management and Communication - IMCOM '17, 2017 Publication	
9	Submitted to Informatics Education Limited Student Paper	<1%
10	Submitted to CSU, San Jose State University Student Paper	<1%
11	Submitted to Rivier University Student Paper	<1%
12	Bernstein, Tony. "The Pandora's box.(United Kingdom. Her Majesty's Revenue and Customs)", Financial Adviser, Sept 30 2010 Issue Publication	<1%
13	Submitted to The University of Manchester Student Paper	<1%
14	Submitted to Johns Hopkins Unversity Student Paper	<1%
15	Submitted to University of Technology, Sydney Student Paper	<1%
16	Submitted to University of Westminster Student Paper	<1%

17	Submitted to University of Maryland, University College Student Paper	<1%
18	tec-in.org Internet Source	<1%
19	eprints.utar.edu.my Internet Source	<1%
20	Nadja Damij, Talib Damij. "Process Management", Springer Nature America, Inc, 2014 Publication	<1%
21	www.imamu.edu.sa Internet Source	<1%
22	Submitted to CSU, Fullerton Student Paper	<1%
23	emerchantbroker.com Internet Source	<1%

Exclude quotes	On	Exclude matches	< 8 words
Exclude bibliography	On		

Security of NFC Payment On Mobile Payment Application

By Wong Wen Teng

Introduction

- People are starting to use the cashless payment.
- It is very convenient to use.
- There are some security issues in NFC technology.
- Design a security protocol in NFC transaction is a must.

PROBLEM STATEMENT

- NFC is vulnerable to these attacks:
  - Eavesdropping
  - Man in the middle
  - Relay attack
  - Data Modification and Insertion
  - Data Corruption

PROJECT OBJECTIVE

- To design a security protocol in payment method using NFC technology.
- To encrypt all the information during transaction.

METHODOLODY

- Develop the app using Android Studio
- Firebase is used to stored the data

CONCLUSION

✓ Design a secure NFC transfer protocol

✓ Make the transaction safer.

✓ An E-wallet that can make payment

Universiti Tunku Abdul Rahman			
Form Title : Supervisor's Comments on Originality Report Generated by Turnitin for Submission of Final Year Project Report (for Undergraduate Programmes)			
Form Number: FM-IAD-005	Rev No.: 0	Effective Date: 01/10/2013	Page No.: 1of 1

FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY

Full Name(s) of Candidate(s)	WONG WEN TENG
ID Number(s)	14ACB07309
Programme / Course	COMPUTER SCIENCE
Title of Final Year Project	SECURITY OF NFC PAYMENT IN MOBILE PAUMENT APPLICATION

Similarity	**Supervisor's Comments (Compulsory if parameters of originality exceeds the limits approved by UTAR)**
Overall similarity index: __4__ % **Similarity by source** Internet Sources: 1% Publications: 1% Student Papers: 3%	
Number of individual sources listed of more than 3% similarity: _____	
Parameters of originality required and limits approved by UTAR are as Follows: **(i) Overall similarity index is 20% and below, and** **(ii) Matching of individual sources listed must be less than 3% each, and** **(iii) Matching texts in continuous block must not exceed 8 words** ***Note: Parameters (i) – (ii) shall exclude quotes, bibliography and text matches which are less than 8 words.***	

Note Supervisor/Candidate(s) is/are required to provide softcopy of full set of the originality report to Faculty/Institute

Based on the above results, I hereby declare that I am satisfied with the originality of the Final Year Project Report submitted by my student(s) as named above.

_____ Signature of Supervisor

Name: _____

Date: _____

_____ Signature of Co-Supervisor

Name: _____

Date: _____

UNIVERSITI TUNKU ABDUL RAHMAN

FACULTY OF INFORMATION & COMMUNICATION TECHNOLOGY (KAMPAR CAMPUS)

CHECKLIST FOR FYP2 THESIS SUBMISSION

Student Id	14ACB03709
Student Name	WONG WEN TENG
Supervisor Name	MR. KU CHIN SOON

TICK (√)	DOCUMENT ITEMS Your report must include all the items below. Put a tick on the left column after you have checked your report with respect to the corresponding item.
√	Front Cover
√	Signed Report Status Declaration Form
√	Title Page
√	Signed form of the Declaration of Originality
√	Acknowledgement
√	Abstract
√	Table of Contents
√	List of Figures (if applicable)
√	List of Tables (if applicable)
	List of Symbols (if applicable)
√	List of Abbreviations (if applicable)
√	Chapters / Content
√	Bibliography (or References)
√	All references in bibliography are cited in the thesis, especially in the chapter of literature review
	Appendices (if applicable)
	Poster
√	Signed Turnitin Report (Plagiarism Check Result - Form Number: FM-IAD-005)

*Include this form (checklist) in the thesis (Bind together as the last page)

I, the author, have checked and confirmed all the items listed in the table are included in my report. _____ (Signature of Student) Date:	Supervisor verification. Report with incorrect format can get 5 mark (1 grade) reduction. _____ (Signature of Supervisor) Date: