Multi-Layer Security Analysis and Implementation of Smartphone Based ATM

Imran Farid **15341025**

RabbyZaman **14301143**

IffatJahan Emmy **13141005**

Supervisor: **Dr. Amitabha Chakrabarty**

Department of Computer Science and Engineering
BRAC University

DECLARATION

We hereby declare that this thesis is a presentation of our original work. Materials of work found by other researchers are mentioned with due reference to the literature and acknowledgement of collaborative research and discussions.

The work is done under the guidance of Dr. Amitabha Chakrabarty, at the Department of Computer Science and Engineering, BRAC University, Dhaka.

Date of Submission: 14th December, 2016

Signature of the supervisor

_____

Dr. Amitabha Chakrabarty

Assistant professor

Department of Computer Science and Engineering

BRAC University

Dhaka,Bangladesh

Signature of Author

_____

Imran Farid

_____

Rabby Zaman

_____

Iffat Jahan Emmy

Acknowledgement

We have been supported by numerous people during our research work. A few words' mention here cannot adequately capture all our appreciation.

We are very thankful to our thesis coordinator Dr.Amitabha Chakrabarty, Assistant Professor, Department of Computer Science and Engineering, BRAC University for guiding us throughout our thesis work. Due to his endless support and patience, we were able to achieve our goals. We will always be grateful to him, for his kind words, his belief in us, his immense support and guidance.

We are also grateful to Shauvik Shadman, Shondipon Paul, Students of BRAC University and Samiul Islam, CCSE Lab Assistant of IUBfor being with us throughout the thesis work.

Last but not least, we would like to thank our parents, our brothers and sisters, for all their enduring support and always believing in us.

Abstract

Smartphone penetration was 10% in 2015 and is expected to grow in coming years. Card based ATMs (automated teller machine) are being updated or replaced by modern card-less ATMs in developed countries. The purpose is to improve security and prevent fraud. In this thesis we are going to introduce a new authentication process for smartphone based transaction by including code cards.

CONTENTS

CHAPTER 1

INTRODUCTION

Technology is always improving. In the recent years it has risen in an exponential rate. Technology makes everything easier and simpler. In the banking system we noticed technology sweeping in and taking over making it easier to deposit and retrieve money. With the advancement of technology, frauds and exploits in the banking system has increased as well. The need for security and safety of the banks and the retrieval of money has become of utmost importance.

Since the advancement of technology, one of the most important devices that have become inseparable from our life is the advent of the mobile phones. Nearly everyone has a cell phone nowadays. In our thesis we have pitched an idea which incorporates cell phones in the banking system considering and emphasizing on the security measures and improving on the present security that the banks have on the ATM machines and making it nearly impossible to steal money even if credentials are stolen.

Bangladesh being a developing country needs to look into the security measures as technology takes over every sector including the banks before thieves and hackers can exploit the people more than they already have. We have accounts of ATM threats constantly rising and in recent times it is only increasing.In Bangladesh there are accounts of fraudulent methods already persistent. In the vision to Digital Bangladesh this is an alarming issue and therefore we have proposed an idea which, although sophisticated may very well making ATM transactions easier and much more secure than the present scenario.

1.1 MOTIVATION

While we were thinking of the banking system as a whole, we discussed how it is now that we have a lot of banks, and how technology has shaped it. Now a day there is a lot of credit cards and debit cards and other membership cards that it is a hassle to maintain them. Adding to this we also thought of the security perspective of the system and realized that in a developing and populous country like Bangladesh it is necessary to maintain the security because there is a growing threat to the people and banks.

In recent times there were a lot of attacks and theft of money through ATM scamming and it is on the rise. In Bangladesh alone there were multiple accounts of theft of the ATMs. This is a matter of personal and also a national security. We care about the security of money of every person and so we have thought of improving this.

Here lays our motivation to form a system which will be infallible and impenetrable. Then we also thought how we could make the system easier to handle. In a world of technology an easy and secure transaction is of sheer importance.

We planned to provide just that using simple everyday used mobile phones and put forward a way to easily transact with the banks and make it safe and secure.

1.2 Scope

This thesis is targeted towards all the people who have a bank account and need to transact with the banks very frequently. We have designed the system using tools and security measures which are respectively easy to use and cannot be broken. Using only a cell phone and codes we can easily transact securely and without hassle. Users do not have to worry about money being stolen from them, as this method is very safe and secure.

1.3 Contribution

This thesis report improves on an outdated system of money transactions. The need for having a good, secure and easy method is very high. So, from the users perspective, they only have to carry their cell phones and the ATM machines need to have an NFC enabled module. These are our contributions.

1.3.1 Problem Statement

Deputy Inspector General of Bangladesh Police, told journalists on 15th February 2016, Monday in a press briefing that some 36 customers have found their money was stolen from their bank accounts by the skimming card gang since January. One Facebook user and founder of his own company posted in his Facebook that Tk 22,000 was drawn from his Eastern Bank Limited account without his knowledge on 13th march 2016 while his credit card was with him. There are around 24 depositors who, similarly, were victims of this ATM forgery.

EBL has fully compensated its clients who suffered financial losses due to ATM cards forgery. The bank has given a total Tk17.53 lakh among these 24 depositors (Source bdnews.com). Seven customers of UCBL suffered from similar problems and UCBL had to pay their customers a total of Tk 1.26 lakh. Head of Fraud Control and Dispute Management from UCB's Branches Control and Development Division of cards said that a man entered a UCB ATM booth at Banani on Feb 7, 2016 telling the security guard that he was there to fix technical glitches in the machine. He entered the booth that day at 10:42 AM and several other times to plant the skimming device which copies the card data from the computer of the ATM.

This unknown culprit later used advanced illegal technology to enter the ATM computer's system and carry out transactions with the stolen data. Data of many clients of other banks were also stolen in the same manner [3]. The frauds planted video cameras and skimming devices inside the ATM to steal card information and watch people enter their PINs on the entry pad. Recently, four credit card frauds have been arrested in Bangladesh.

This thesis work tackles the modern day problem of safe and secure monetary transaction problems. In recent years ATM scamming has become very dominant and needs to be stopped. Also, with so many credit cards it's difficult to handle. Hence, in our thesis we are proposing the introduction of a new payment system where the traditional RFID based ATM machines are replaced by NFC based ATMs [4].

1.3.2 SOLUTION

To solve this problem we have come up with an infallible system which ensures that there can be no scam. We use a cardless ATM system using NFC (Near Field Communication) on the mobile phones, and a few codes to ensure proper transaction and no fraud.

The procedure we have used has different layers of security. Using encryption algorithms and real time code generation and processing we have tried to make a failsafe of everything scenario.

1.3.3 METHODOLOGY

We have used almost a mini computer which is known as an arduino uno. This is a credit card shaped object which can be programmed to do certain tasks has been programmed by us to make use of an NFC shield which is an external device that can be mounted on the arduino uno and can be used to pass data and information to other NFC compliant devices.

We have set the thesis up in a way so that we can emulate our work and we have done so by connecting the arduino uno along with the NFC shield and connecting it with the computer which acts as the CPU and also the server of the bank.

We have made an android application which can be used by the user to request a transaction. We have used android studio to program the application and we made it all work.

We studied encryption algorithms and the concept of keys where we broke up a key and one half of the key will always be changing so we made that possible. These are our methodologies.

1.4 GOALS

Our goal is very simple. We wanted to revolutionize the ATM machine industry and revamp the security measures that are in use in the ATM machines today.

Our primary goal is to provide the security of those ATM machines and make the transaction lines secure. We tried to prevent anyone from taking control of anyone's account number or their PIN numbers.

Our secondary goal was to provide a smooth card less transaction. Now a day the card less transaction has become very widespread in foreign countries and so we think that is the way to go. Since our aim was to go card less it would be made easier with a cell phone. **Simplicity** is also something we planned to achieve.

1.5 THESIS OUTLINE

In chapter 1 we give a brief introduction of the whole topic. We introduce it and set our motives.

Chapter 2 deals with the current literature in play at this moment in time.

Chapter 3 mentions the specifications of the hardwires and software’s we used do our thesis.

In Chapter 4, we have tried to explain the working principle of our work.

Chapter 5 talks about the architecture of the whole system.

In Chapter 6 the analysis of the system is provided where we show the practical interfaces and our simulation.

In chapter 7 we conclude our report.

CHAPTER 2

LITERATURE REVIEW

During our literature review we came to know about two papers focused on Automated Teller Machine in Bangladesh [6] and NFC-enabled Automate Teller Machine[7]. Our primary concern for this thesis is security as our thesis involves transaction. The existing ATM systems in Bangladesh use contactless RFID (Radio-frequency identification) cards. There are two classes of the contactless bank cards: magnetic stripe data and contactless EMV. The RFID cards in Bangladesh use magnetic stripe data for transactions. The RFID cards store the user's account number and expiry date in the card. The user has to insert the card in the ATM machine and the ATM requests for 4 digits PIN after verifying the card. The user can then proceed with the transaction with a few steps.

Fig 2.1: A Traditional ATM

The magnetic stripe cards are vulnerable to theft. Any magnetic stripe card reader can read the data stored in the card. As a result someone can easily clone the card. The 4 digits pin is used for security purpose. But there have been numerous events in the past where the PIN number was stolen. Usually in ATM frauds the thief implants a magnetic stripe card reader over the ATM's reader and also mounts a stand-alone camera over the keypad so that the PIN can be seen. After collecting the information, the thief clones the contactless cards and uses the PIN to steal money from the ATM. We have also gone through the working procedure of NFC based atm. the model uses host card emulation in NFC enabled smart phones. Thus the ATM machine can recognize the smart phone as a virtual ATM card. The data from smart phone to ATM card were assumed to be a secure exchange, because the data exchange distance is only 4 cm max. Later it was found that a fake NFC reader can be implanted nearby the smart phone and the account information can be hacked. So lack of security was a big challenge here. We showed our interest to know about the data exchange security. When we were looking for more information, we found a paper named "NFC-enabled Automated Teller Machines" by Fabian Tamas.

Fig 2.2: An NFC Based ATM

In his work he has talked about the implementation of NFC based ATM and the exchange security. He proposed encrypted data exchange. We adopted his idea from there and thought to make it better.

CHAPTER 3

SPECIFICATIONS

In this chapter we will talk a bit about the hardware and the software that we have used in this thesis. There are two parts and several components that we have put to use. In the next sections, we have explained the hardwires and the different softwires that we used and give a brief explanation of their use and implementations.

3.1 HARDWARE SPECIFICATIONS

Here we will give a brief of the hardware components that we used to simulate the ATM machines and we used arduino to be an intermediary device.

3.1.1 ARDUINO UNO

The Uno board and version 1.0 of Arduino Software (IDE) were the reference versions of Arduino, now evolved to newer releases. Arduino/Genuino Uno is a microcontroller board based on the ATmega328P (datasheet). It has 14 digital input/output pins (of which 6 can be used as PWM outputs), 6 analog inputs, a 16 MHz quartz crystal, a USB connection, a power jack, an ICSP header and a reset button. It contains everything needed to support the microcontroller. [8,9]

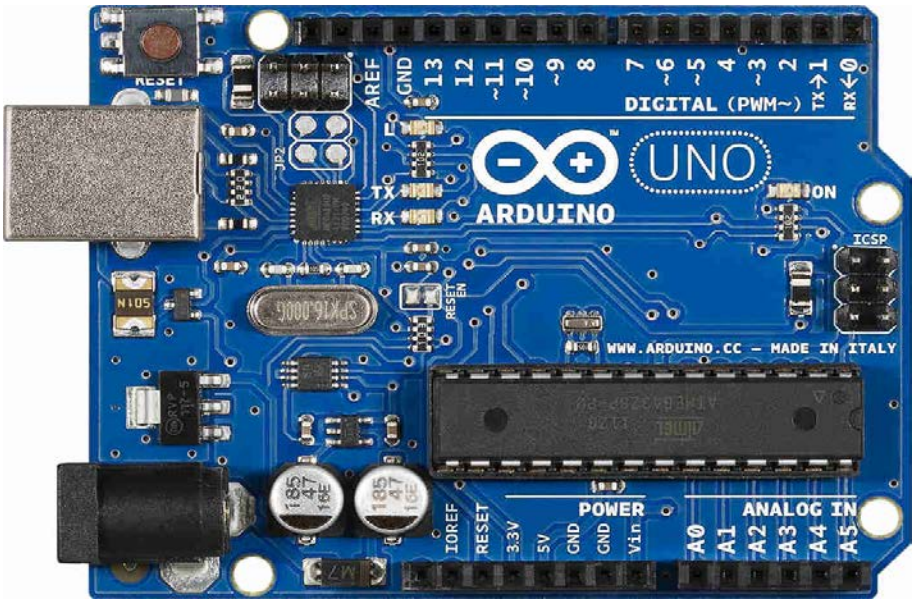

Fig 3.1: An Arduino Uno

3.1.2 ARDUINO NFCSHIELD

NFC Shield is a Near Field Communication interface for Arduino build around the popular NXP PN532 integrated circuit. NFC is a short-distance radio technology that enables communication between devices that are held close together. NFC traces its roots in RFID technology and is an open platform technology standardized in ECMA-340 and ISO/IEC 18092. NFC communication range is up to 10 cm. But, this is limited by the antenna and power radiation design. Most devices work within a range of 10mm. NFC Shield antenna is designed to work within a range of 1cm. NFC Shield provides all necessary circuitry for PN532 like 27.12 MHz crystal, power supply. It also beaks-out the I/O pins of PN532 for easy access. The communication between Arduino and NFC Shield is via SPI.[8,9]

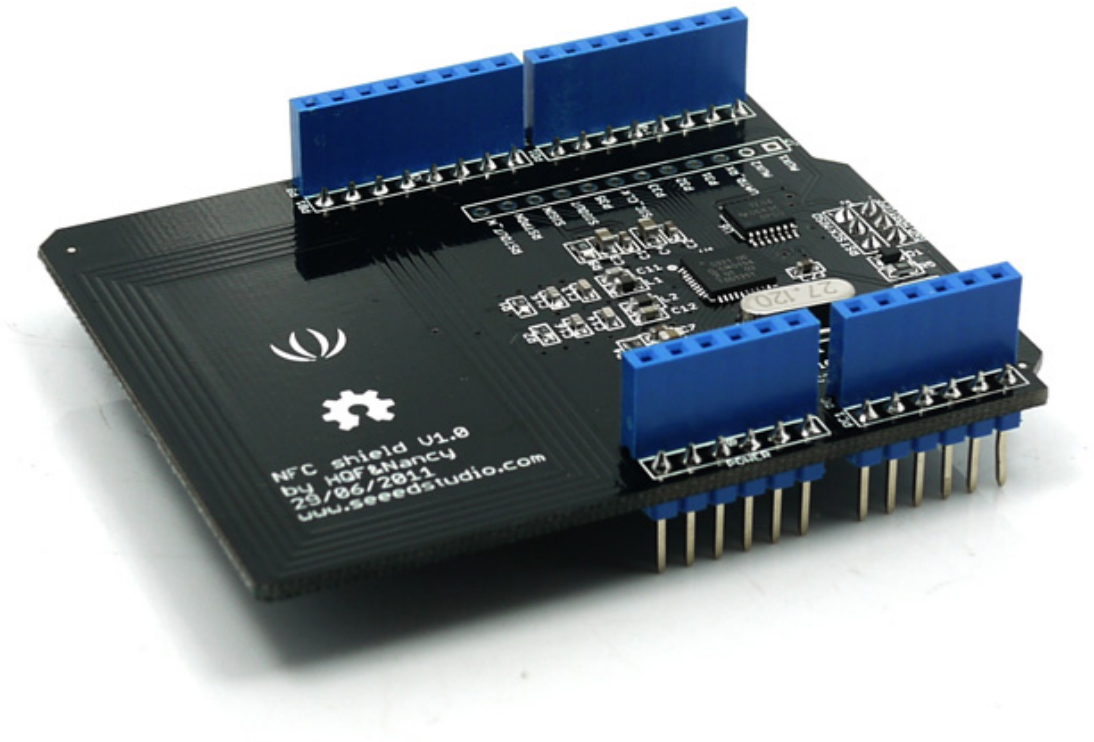

Fig.3.2: An NFC shield

3.2 Software Specifications

The softwares that we used are explained in this section. We will mention where we have coded and used the help of all the softwares used in this thesis.

3.2.1 Android enabled device

We used an android phone to use the application, as the application is developed in Android. Any android phone will suffice as long as it supports android apps.

Fig.3.3:Android phone

3.2.2 NETBEANS:

NetBeans is a software development platform written in Java. The NetBeans Platform allows applications to be developed from a set of modular software components called *modules*. Applications based on the NetBeans Platform, including the NetBeans integrated development environment (IDE), can be extended by third party developers. The NetBeans IDE is primarily intended for development in Java, but also supports other languages, in particular PHP, C/C++ and HTML5. NetBeans is cross-platform and runs on Microsoft Windows, Mac OS X, Linux, Solaris and other platforms supporting a compatible JVM. [10]

Fig.3.4: Netbeans Logo

3.2.3 ANDROID STUDIO:

Android Studio is the official integrated development environment (IDE) for Android platform development. We used Android studio to build the integrated application.

Fig.3.5: Android Studio Logo

Based on Jet Brains' IntelliJ IDEA software, Android Studio is designed specifically for Android development. It is available for download on Windows, Mac OS X and Linux, and replaced Eclipse Android Development Tools (ADT) as Google's primary IDE for native Android application development. [11]

3.2.4 MySQL:

MySQL is an open-source relational database management system(RDBMS).This is used to build the database of the application. [12]

Fig.3.6: MySql Logo

3.2.5 Arduino software:

The open-source Arduino Software (IDE) makes it easy to write code and upload it to the board. It runs on Windows, Mac OS X, and Linux. The environment is written in Java and based on Processing and other open-source software. [8,9]

Fig.3.7: Arduino Software

CHAPTER 4

PROPOSED METHOD OF WORKING

Here in this chapter we will discuss the new and improved method of working procedure of the ATM machine. We will discuss in complete details on how the system works, on the flow of work and how authentication is achieved. In details and with the help of diagrams and figures we will try to state our case.

4.1 WORK-FLOW

Our proposed method of transaction requires the user to have an android enabled device and a bank account. Using a well planned method and also using cryptographic algorithms we have formed a safe and secure channel to data transfer. The data includes card ID, Password, half key. They are sent through an intermediary device which we used arduino uno and an NFC shield. This acts as an intermediary device between the ATM computer and the cell phone device.

Next we have set up two servers namely a web server to control the application authentication and a bank server to handle user authentication and validation of request.

The ATM ensures authenticity of the user by generating a half key which is then used by the client device to encrypt the data. The half key is then also sent to the bank server so that they can form the full key and decrypt the data.

The data is then used by the bank server to authenticate the user by searching through the MAC address which is sent separately with the encrypted data. If the correct data is found then it waits for a code card input which is dynamically generated and sent to the user. There is another process of getting the code card which is static code cards which will be provided to the user.

After the correct code card is input then the user will be allowed to transact with the ATM.

4.2 FLOWCHART

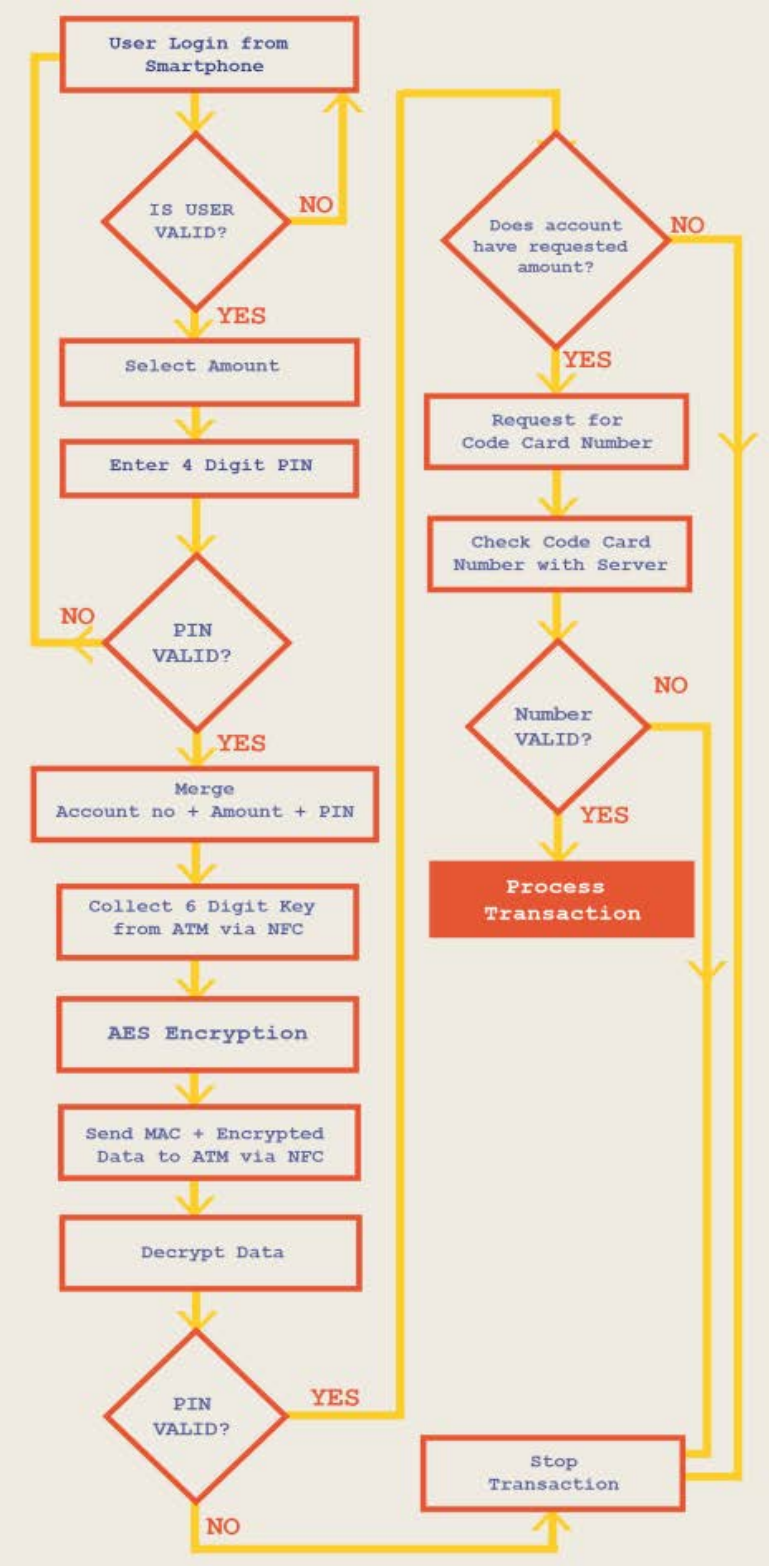

Fig.4.1: Flowchart of Working procedure

4.3Client Device

The client device is an android supported device which will have NFC built in and is used in this aspect. The client device can be from Sony, Samsung or any other brand as long as it supports android and preferably an android of a version greater or equal to 4.0.

4.3.1 First time use

The android application will be given to the client by the bank once they set up a bank account with information. The application must be provided with a password which will be saved and must be entered every time client opens the application. This password will be set the first time the client opens the application. Then the PIN must also be set and the application saves the PIN number for further use. This application also saves the MAC address of the device to use it in the future. It sends the MAC address only for the first time to the bank so that it can save it in accordance with the user ID and password. This process only happens for the first time and this will be done by the bank.

4.3.2 Application lock password

The application must be provided with a password to unlock and this can be anything the user chooses. When the client wants to make a transaction then he or she must provide this password every time he or she opens the application. The application password will be checked with the web server through an internet connection of the phone.

4.3.3 PIN of account

The app password is first authorized by the web server and only then will the next step may be shown. If the application password matches the user ID password in the database then the app will prompt for a PIN code. This PIN code is the PIN code of the bank account that is given to the user. This PIN code does not change ever, unless the client contacts the bank and changes it.

4.3.4 Form full key

The data that will be sent to the bank must be encrypted. Hence we will need a key to encrypt the data and a key on the bank server side to decrypt the data. But if the key is the same it might be prone to hacking and data stealing. Moreover, once it is hacked it can be used over and over again.

Therefore, we have thought of a process to change the key every time. The key will be broken in half and the half key will be present in the client device and also in the bank server. But the other half of the key will be generated in the ATM machine every time a client uses the NFC module. Once the app authentication is complete the half key will be generated and will be sent to the client application.

As soon as the application has the half key, the app will form the full key and encrypt the data. The data includes the account number, amount of money and PIN number. This information are encrypted. They will send the encrypted data through the NFC of the phone to the NFC shield of the arduino.

4.3.5 Encrypt Data

The encryption of the data is done by the app of the client device. The data to be encrypted are account number, amount of money and the PIN number. This is done using AES encryption algorithm. This is done automatically by the client device after the application is accepted. If they are not the user is banned from transaction.

This encryption process helps the user protect against attacks and moreover since it is sent through NFC,it is very safe. Even if the encrypted data is stolen it will be impossible to get the actual data. Moreover, if the half key is stolen, it cannot be decrypted. Since, the half key changes every time so it is quite impossible to get the key.

4.3.6 Send to intermediary device

The encrypted data is then sent to an intermediary device which is in the ATM machine. The intermediary device is comprised of the arduino uno and the NFC shield.

Also the MAC address and the half key is sent to the intermediary device. Which acts as a bridge between the ATM machine and the client device. The device receives the data and passes it on to the computer inside for further work.

One string is sent to the intermediary device which is comprised of the encrypted data, MAC address, and the half key. They are concatenated to form a single stream of data.

sent data=half_key+MAC_address+encrypted_data

4.4 Intermediary device

The intermediary device is the device which is in between the client device and the computer in the ATM machine. It is a part of the ATM machine; its work is to validate the transaction by keeping in contact with the servers.

It is formed of two devices including an arduino uno and an NFC shield which are very cheap and easily ingrate able. Also it is easily programmable.

4.4.1 Accept phone data

The primary duty of the Arduino Uno and the NFC shield is to accept phone data. At first the application password is authenticated which does not require the Arduino, but after that the generation of the half key is done. Once the half key is generated it is sent to the phone.

The work of the accepting data means accepting encrypted data, MAC address and the half key. The client device sends the encrypted data to the NFC shield by tapping when the prompt is made.

4.4.2 Send phone data

The encrypted data after reception is then sent to the ATM machine. The MAC address is not encrypted because it is already very big and it is impossible to be put to use. The MAC address is sent normally. Also the half key which is very dynamic is sent back to the ATM machine which then begins an authentication process.

4.5 Automated Teller Machine

The automated teller machine or the ATM machine is the device which interacts with the arduino and the bank server. It has the most work in all the devices. After authentication it will provide the client with the money and the receipt.

4.5.1 Interact with intermediary device

The ATM machine interacts with the intermediary device to get the data from the phone and to send data back to the phone. Firstly it initiates a number to give to the intermediary device, then receives data from the device, and after authentication tells the intermediary device to prompt for a code card number, then accepts a code card number.

4.5.2 Generate half key

One of the responsibilities of the ATM machine is the generation of a half key. It generates a half key every 10 seconds. It picks a random 6 digit number. As soon as it picks a number it waits for a device to be connected with the NFC shield.

As soon as it connects to an android device it gives the half key which is then used by the client device.

4.5.4 Interact with the bank server

The ATM machine interacts with the bank server as it sends the encrypted data along with the half key and the MAC address. The bank server then provides the ATM machine instructions and the next steps to do.

4.6 Code Card

The ATM contacts the bank server for authentication and the bank server after authentication, waits for the entry of a code card number.

The code card will be sent to the client and it is used as an extra layer of security. The code card are of two types. First is a static code card which will be given to the client on a monthly or weekly basis. Second is a dynamic code card which will be given to the client as soon as he is validated. That will be the primary code card which needs to be used.

4.6.1 Generation of Code Card

The code card will be generated by the bank server and then passed to the client through a text message, in that way the presence of the client is detected and even if the PIN and other data are compromised this will stay in the way.

4.6.2 Static Code Card

10 static code card numbers will be given to the user in a weekly or monthly basis. The users can use these codes to enter and it will work the same way.

4.6.3 Dynamic Code Card

The code that is generated instantly after bank server authentication is called the dynamic code card. That is sent by the bank to the user's phone number. And then waits for the user to input the code card.

4.7 Validation

Once the transaction is confirmed and also the code card is correct, the ATM machine will receive orders to carry out the transaction. Lastly it will prompt the process which will send the money out so that the client can receive it.

4.8 Server-Side

The server side means the side which is not present in the ATM. The server side holds the database and the required options to decrypt and validate data. There are two servers which we have used.

The web server and the bank server are used. They are two independent servers with no relation to each other. They work with the client device and also with the ATM device to help with the transaction.

4.8.1 Web server

The web server, serves the client device. The client device must have an internet connection to get the application working. It receives request for a lookup of data and then replies accordingly.

4.8.1.1 Receive

The web server receives a request for a look up of user information. There is a database the server maintains and as soon as the server gets a request for data it starts processing. It receives data from client devices and acts accordingly. It receives the account number of the user and the password that the user has inserted.

4.8.1.2 Lookup

After receiving the request it does a look up which essentially means a search. If it finds a match it then it checks if the provided password is a match. It searches from the database. We have used firebase as our database and it searches from there to give a result.

4.8.1.3 Send

After the lookup it sends the information if they found a match or not. If there is no record or the password is incorrect then it sends a block message which blocks the user into transacting again.

4.8.2 BANK-SERVER

The bank server is the server which connects to the ATM machine. It corresponds with the ATM machine and accepts data and sends data to the ATM machine. It can also decrypt the data received from the ATM machine. We have used Java code and mysql to simulate the bank server and we have used simple mysql search queries to implement our system.

4.8.2.1 SEPARATION

At first the server accepts a request for a client trying to transact with the ATM machine. It accepts the request and then it receives a data which is a string. This string contains encrypted data, MAC address and a half key.

The first task of the bank server is to separate the encrypted data, MAC and the half key. It separates them character wise and then processes them. Two activities happen after this, firstly, the decryption method is initiated and secondly, the PIN number is searched using the MAC address that was sent.

4.8.2.2 FORM KEY

After separation it takes the half key and then forms the full key which will be needed. The bank server will already have the other half of the key. Once both the keys are concatenated it will form the full key and then this key may be used to decrypt the data that was sent.

4.8.2.3DECRYPTION

The decryption starts as soon as the full key is formed. The key is then used to decrypt the data that was sent. Using the AES algorithm the bank server decrypts the data.

After the decryption the account number and the PIN code is found. They are used in the look up.

4.8.2.4 LOOKUP AND WAIT

After the data is decrypted, the MAC address is used to search for the users account number and the PIN number. We have used mysql to emulate the bank server and used mysql queries to do the task of look up and wait.

Once the account number and the associated PIN number is retrieved then it is checked with the account number and the PIN number provided in the encrypted data. If the correct PIN was provided then the server sends a code card to the clients preferred cell phone number and waits.

As it waits it connects to the computer module of the ATM machine and asks for a code card, either the one that is sent to the phone or one of the 10 unused static code card given to the client.

4.8.2.5 VALIDATE

The bank server waits for the code card entry from the client. After the code card is pressed the bank server checks it.

If the code card is correct the response to the ATM machine is positive and it prompts the ATM machine to give the client the money.

Otherwise, if the code card is faulty then the client is blocked for a varied amount of time.

4.9 SUMMARY

To summarize, the transaction is of three steps. Firstly, the application password is checked which solves the problem of stolen credit cards. Even if the phone is stolen the app password will not be known.

In the second step the PIN number is requested from the client and also the amount to be withdrawn. The PIN number, account number and the amount is encrypted and sent. This encryption is done using AES algorithm on the client phone using a key. Half of that key is received from the ATM itself. Since, the data is encrypted and the full key is not same every time it is less unlikely it can be stolen and decrypted.

Thirdly, if the bank server makes sure of the account number and the PIN code then it waits for a code card number which will be provided to the client weekly or monthly. This is the last step of the verification of the transaction.

In this way the client is verified and the transaction is done. There is very little possibility of the credentials to be stolen and even if they are stolen the dynamic and changing keys and code card numbers prevent this.

CHAPTER 5

SYSTEM ARCHITECTURE

In this chapter we will discuss the System Architecture in details and how the full system works. We will go over the tasks of each of the components of the system and how they come together to form the full system. We will also show how it is secured and the different layers which make it secure.

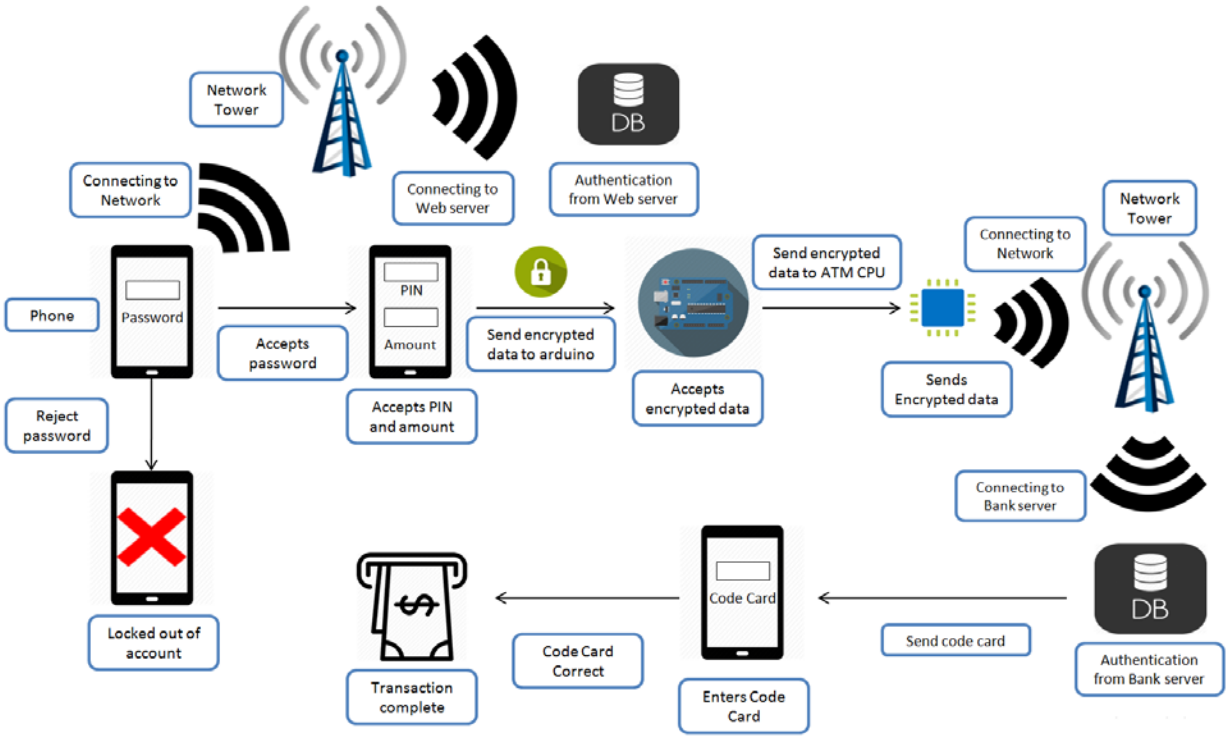

Fig.5.1: System Architecture of our thesis.

The system of this process is not very difficult but the different layer of security makes it much more tough to beat. It uses NFC and other methods to send and receive data. The data which is sensitive is not send without encryption. Therefore, it is almost impossible to penetrate.

As the diagram suggests, the application on the phone when opened requires the user to provide a password. Upon providing the password the phone sends to the network and the network

connects to the database of the web server. The web server accounts for the password that was provided and sends back a signal either accepting or rejecting the request to use the application.

Next up is the communication with the Arduino. We have used an NFC shield with the arduino module for our purposes. The NFC shield is a Near Field Communicator which only works on other devices which have NFC. Since, NFC comes built in with most android devices we tried to capitalize on that.

The client enters a PIN number which is the PIN number of the bank. The client also enters the amount he need. That information is then put on hold. The client's cell phone is tapped once with an area of the NFC module. The client device then quickly grabs the half key and encrypts the account number, PIN and also the amount to be transacted. The NFC then sends the data to the arduino again. When this process is done comes the next step.

The next step is the CPU which is encased with the arduino which is responsible to connect to the bank server. The CPU connects to the bank server and sends the half key, encrypted data, the MAC address and the account number. The processing of data begins in the next segment.

The bank server separates the half key from the string sent to the server and then forms the full key and then decrypts the data to get the account number, PIN number and amount. The MAC address which was separated is then used to query the users account number and also the PIN number. If it exists and matches with the sent data, then the server requests a code card number.

The code card number is then inserted and if it is correct the transaction is done. The CPU prompts the machine to take out the money from the various trays the machine contains.

The transaction and the whole process may feel like a lot but the speed is very fast. Encryption and decryption is very fast as well. It is done in milliseconds and the client will not even know the difference. The extra layers of security measures other than only a magnetic strip and a PIN code was necessary for a long time and we could provide that.

CHAPTER 6

ANALYSIS OF THE SYSTEM

Here in this chapter we will provide a brief analysis of the system. We will show why we need this system and why although it will mean changing physically every ATM, it is necessary. We have then mentioned the application interface and what screens the user will see. We have shown both the application interface and the ATM screen which we have emulated using Java code.

6.1 COST ELEMENT

The system that we have put forward is very cost effective. Given the circumstances of the current scenario of the world, fraud and hacking are increasing and the accounts of the theft are increasing day by day. To enforce a good system and to stop the theft we feel it is very necessary to implement this on a domestic or maybe someday a global scale.

Our system implements only using an arduino uno and an NFC shield on top of it. The cost of an Arduino Uno in the market during the time of writing this is 15$ or 1200taka. This cost is very low compared to the amount of money that can be looted from the ATM machines. The integration to the CPUs of the ATM can also be fairly simple.

One more device that we use with the arduino uno is the arduino NFC shield. The NFC shield costs 25$ or 2000taka. So the total cost might be around 35$ or 3200taka per ATM booth. THis amount is very less compared to the standards of the ATMs that we use at this moment in time.

Considering the cost it will bear, we can say that it is very feasible to integrate this to our ATMs all around the country. It will save a lot of money from being in the hands of wrongdoers. Moreover this can be used for advertisement of the banks so that the users can feel more secure.

6.2 USER VIEW OF THE ANDROID SYSTEM

When the application is first opened then the user sees this screen. This is the log in screen. Here they need to put their username and the password to begin their transactions.

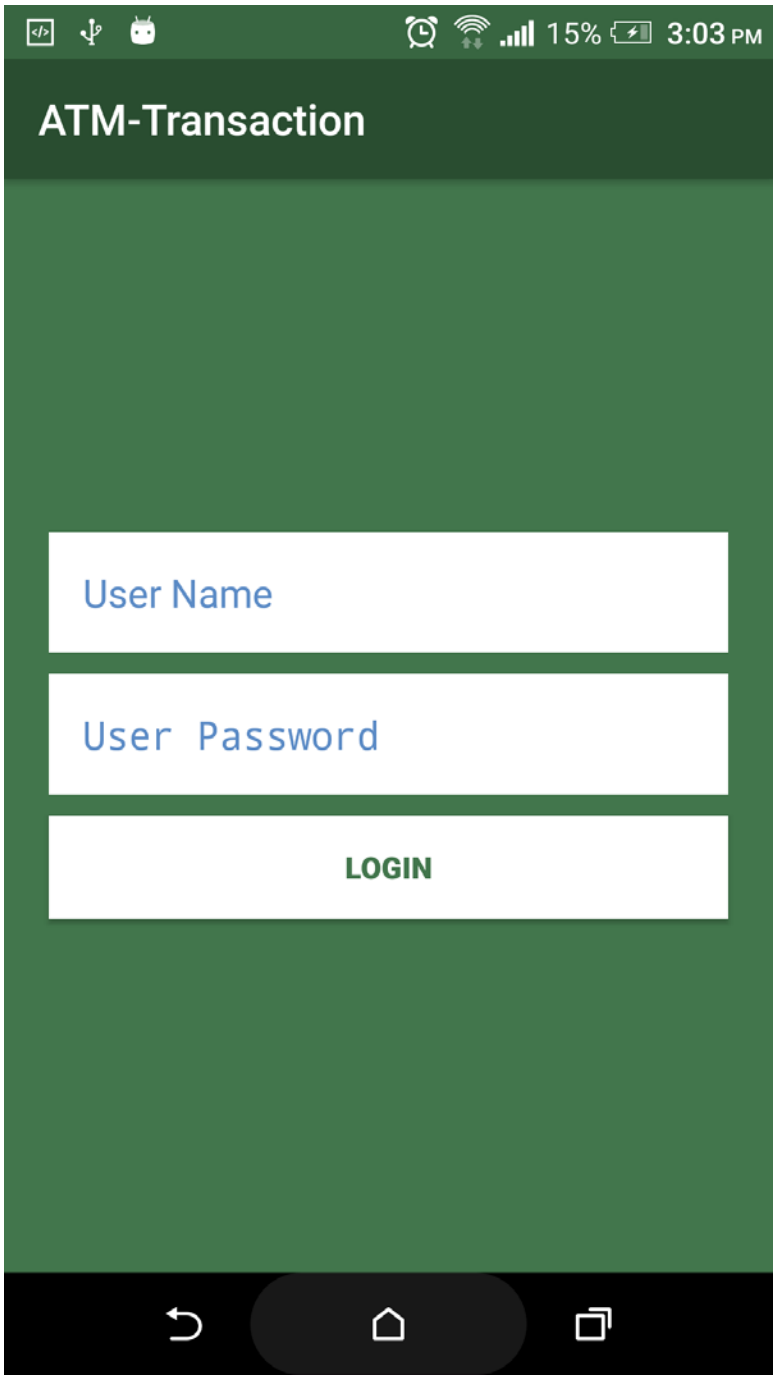

Fig.6.1: Opening page GUI

This is a mock data that we have used as log in to begin the transaction procedure. Here the user needs to provide the correct password. Or else he might be blocked.

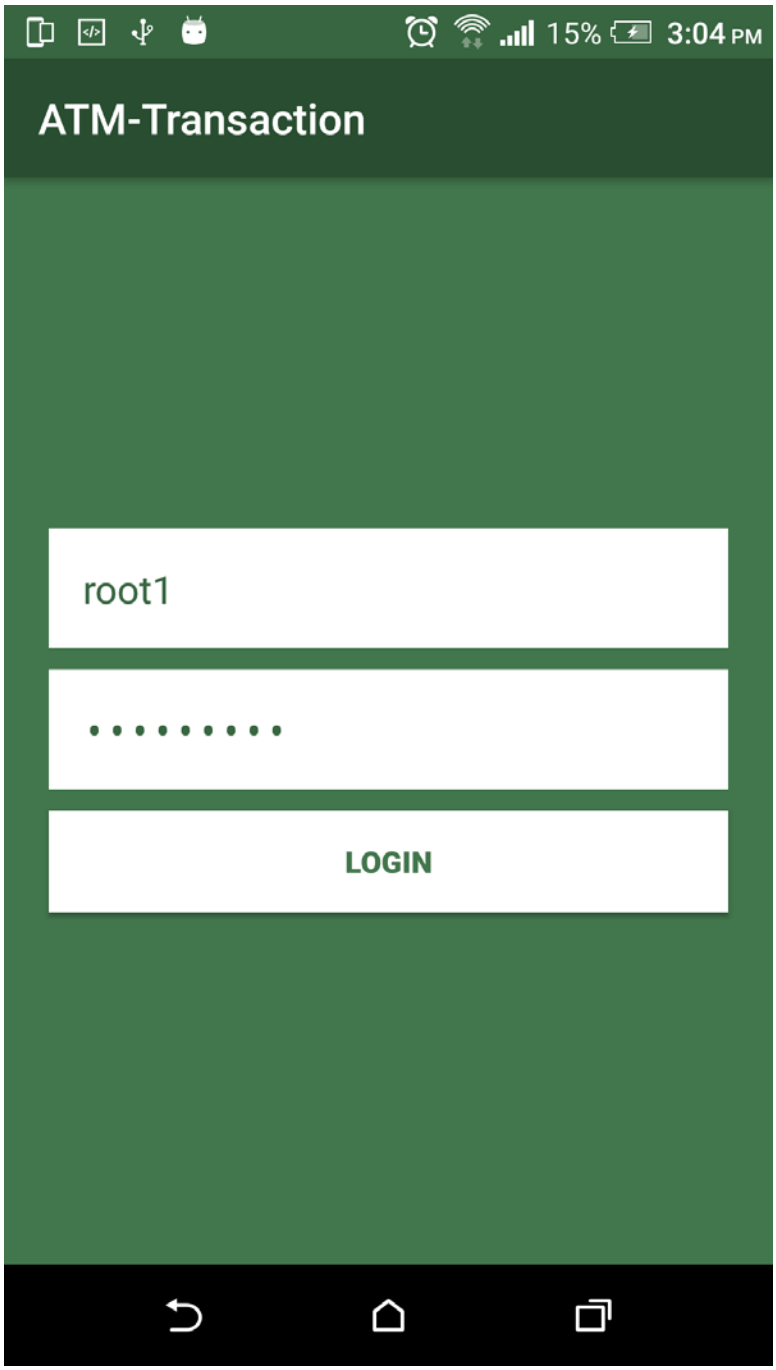

Fig.6.2: Login page GUI

On successful entry of the username and the password the user is then taken to see this screen. Here the user can see a list of amount to select from. Here, the users need to select the amount of money they want to transact.

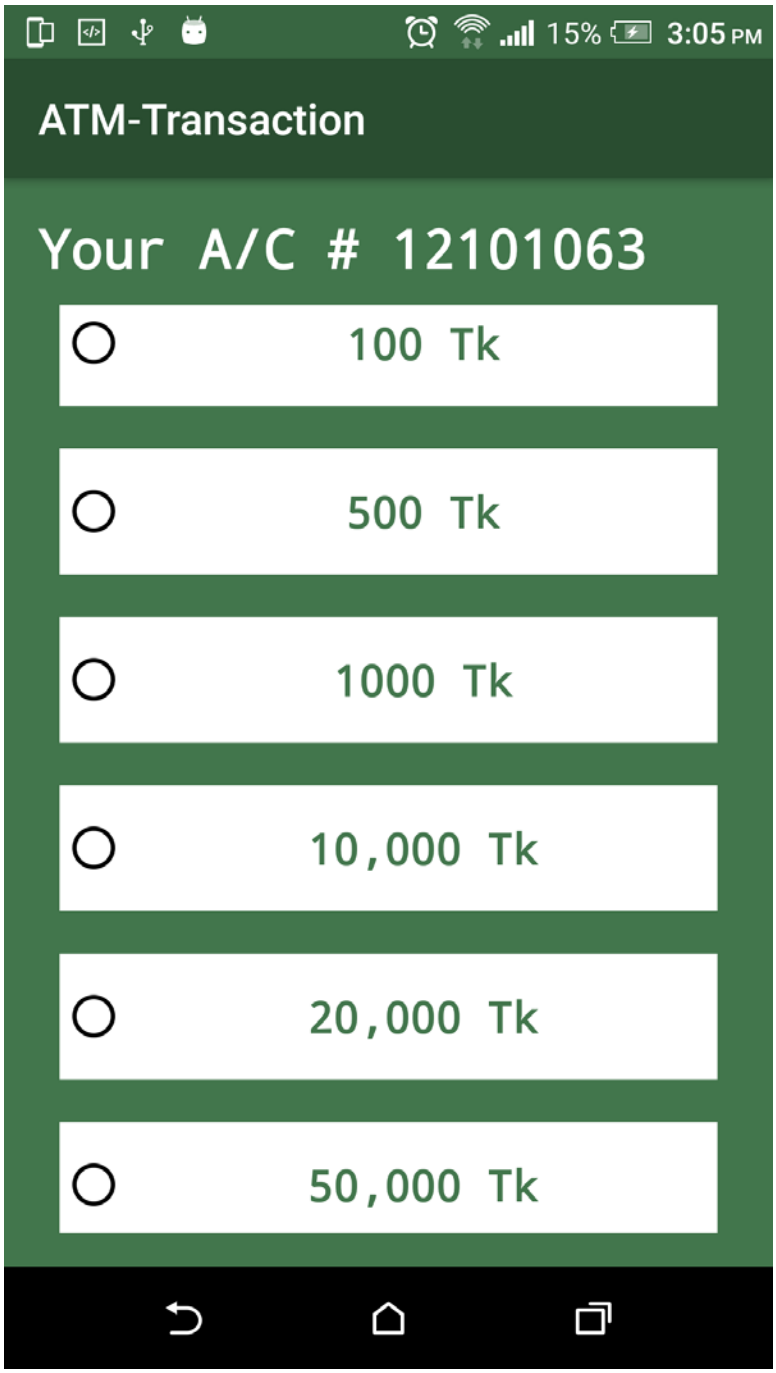

Fig.6.3: Select amount page GUI

The next interface the user sees is this. Here they need to put in the PIN number which is the most important part of the whole process. The PIN is 4 digits.

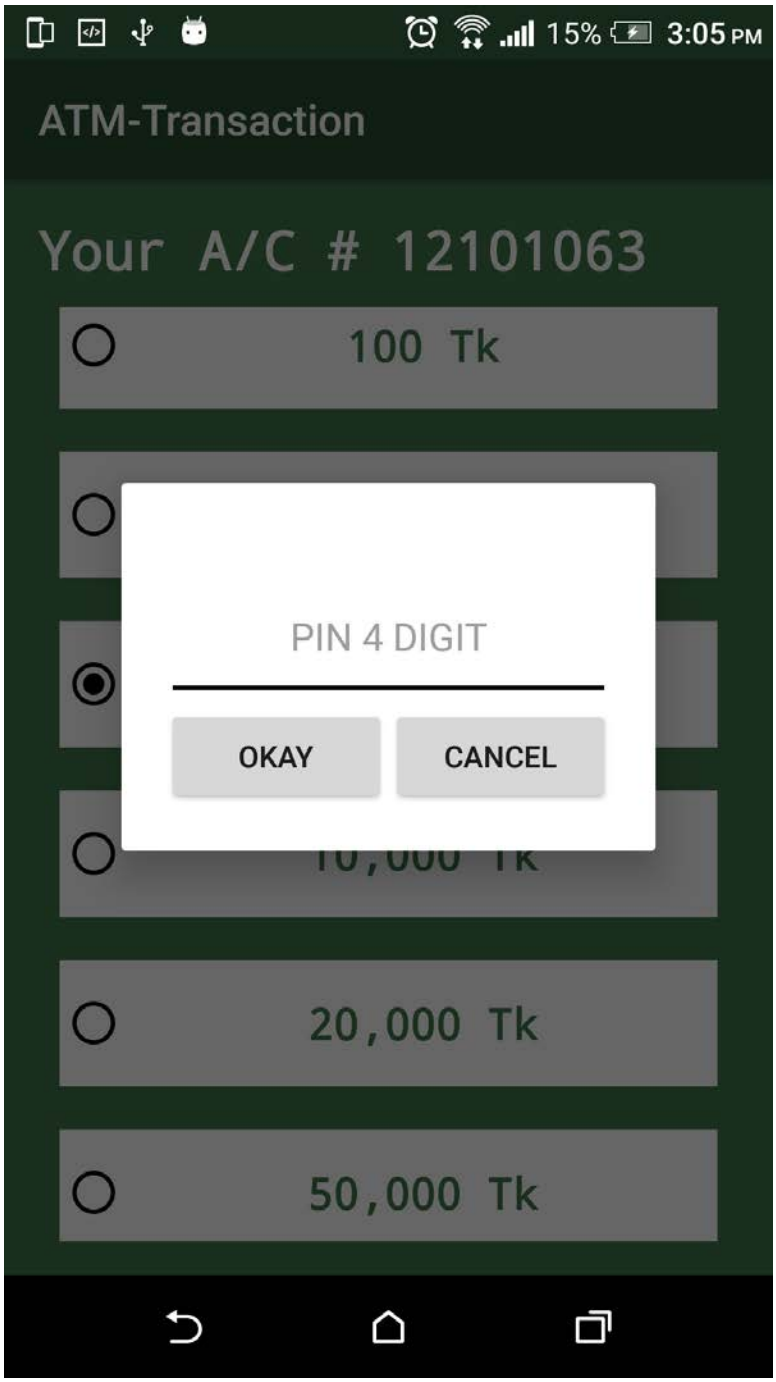

Fig.6.4: Enter PIN page GUI

The PIN number needs to be correct. This is because as soon as the okay button is pressed it will be saved for encryption. If this is wrong the user will be banned from entering anymore and would have to fix it by going to the bank.

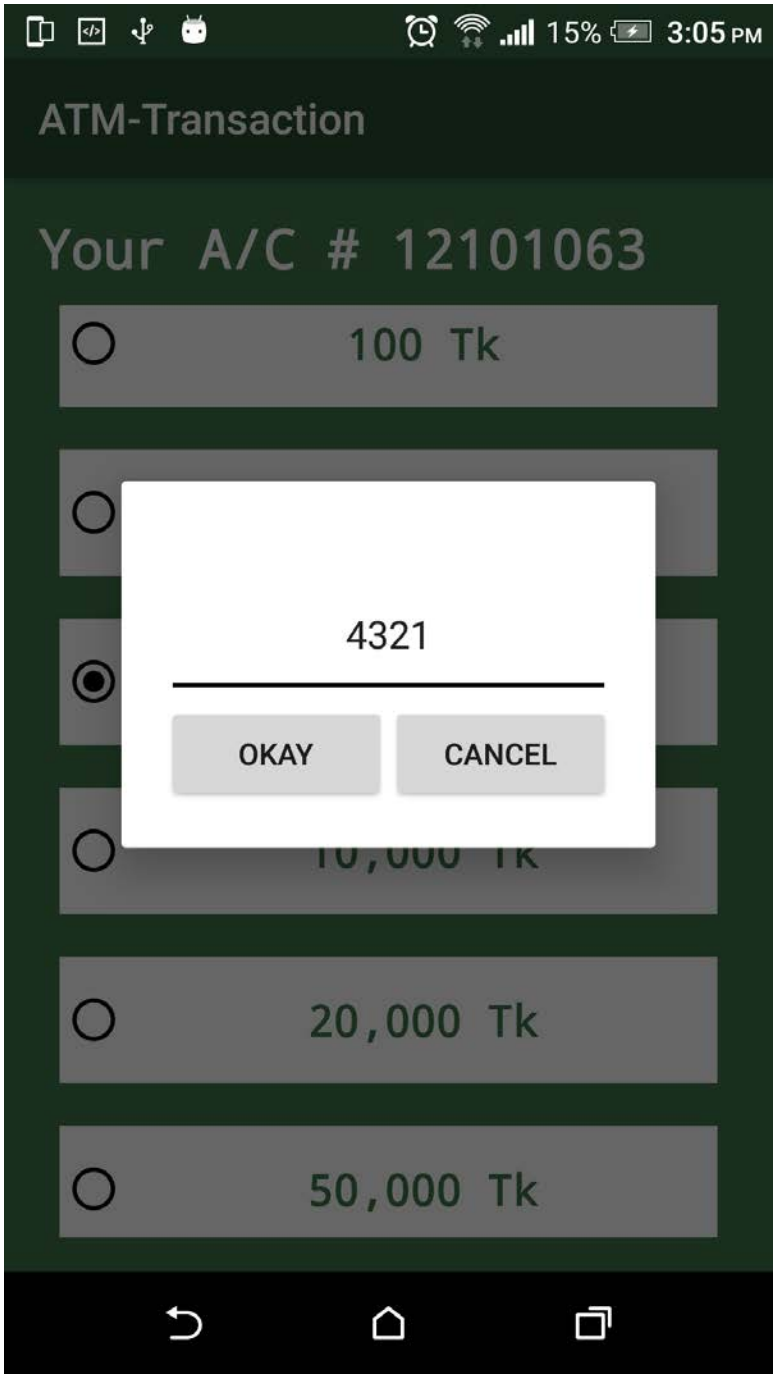

Fig.6.5: Entered PIN page GUI

Here we can see the used account number and also the PIN number which was used. After the PIN number was entered the user needed to have put this close to the NFC part of the ATM and

it would have acquired a half key. Using that half key the application will generate an AES. The AES will not be shown in the application but we showed it here.

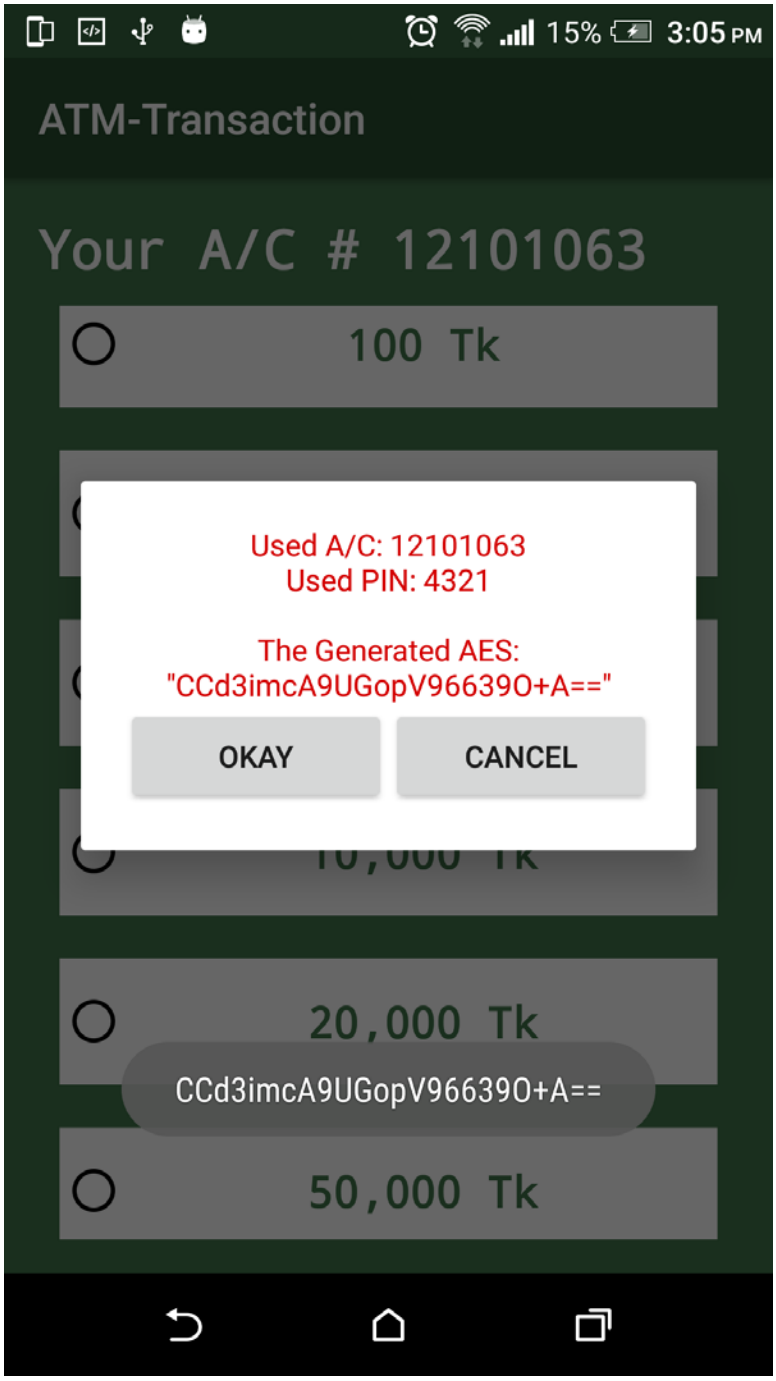

Fig.6.6: Showing the encrypted message to be sent

The AES along with the MAC and half key is sent to the ATM. The Arduino receives a string concatenated with this three strings and passes it on to the CPU. The CPU sends it to the bank server.

6.3 User view of the ATM interface

We have tried to emulate the ATM machine by connecting the Arduino with a computer and writing a java program which will do the work of the ATM. In this section we have provided some screenshots of the ATM screen that the user will see.

Here is the first screen of the ATM machine we will see. The ATM will have a place to tap the phone once he follows the instructions in the ATM. The ATM will take care of the rest.

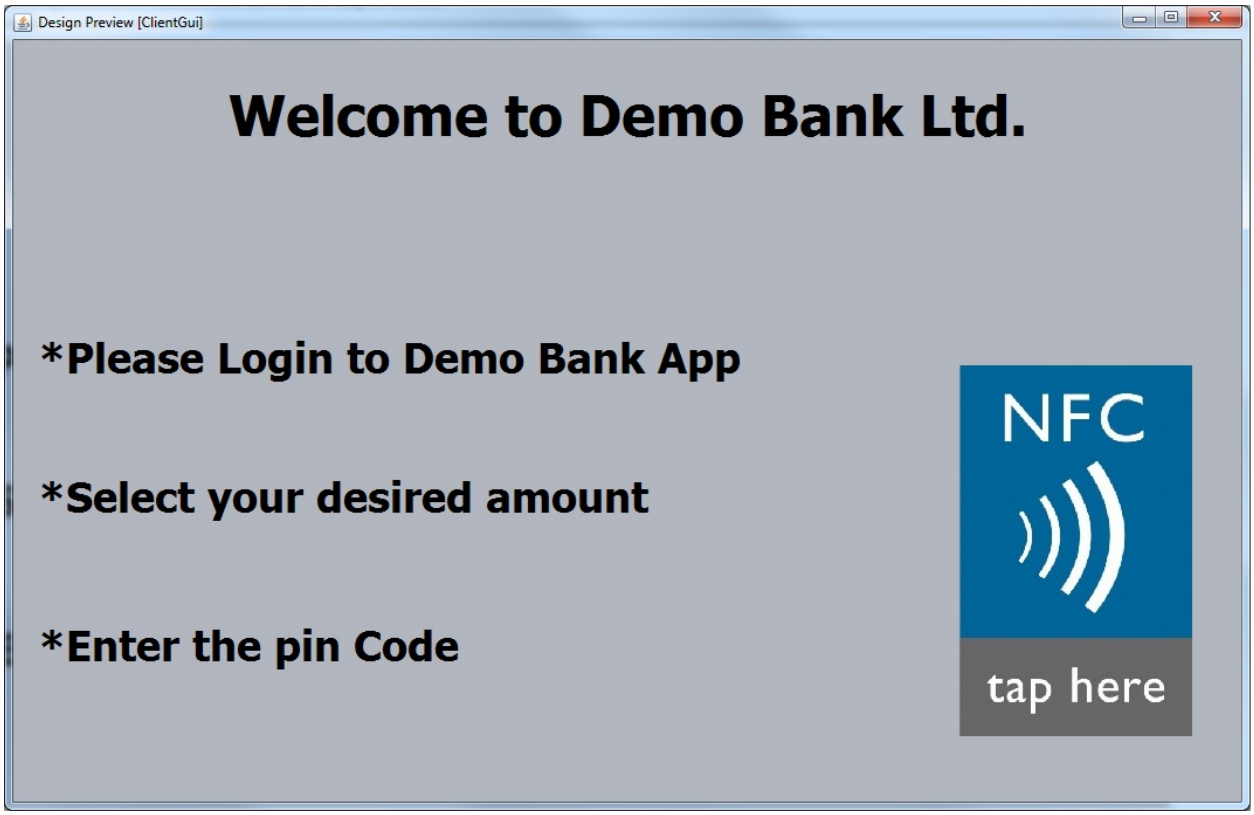

Fig.6.7: GUI of Opening page of ATM

After tapping into the NFC and during the bank server is processing the transaction this screen is shown.

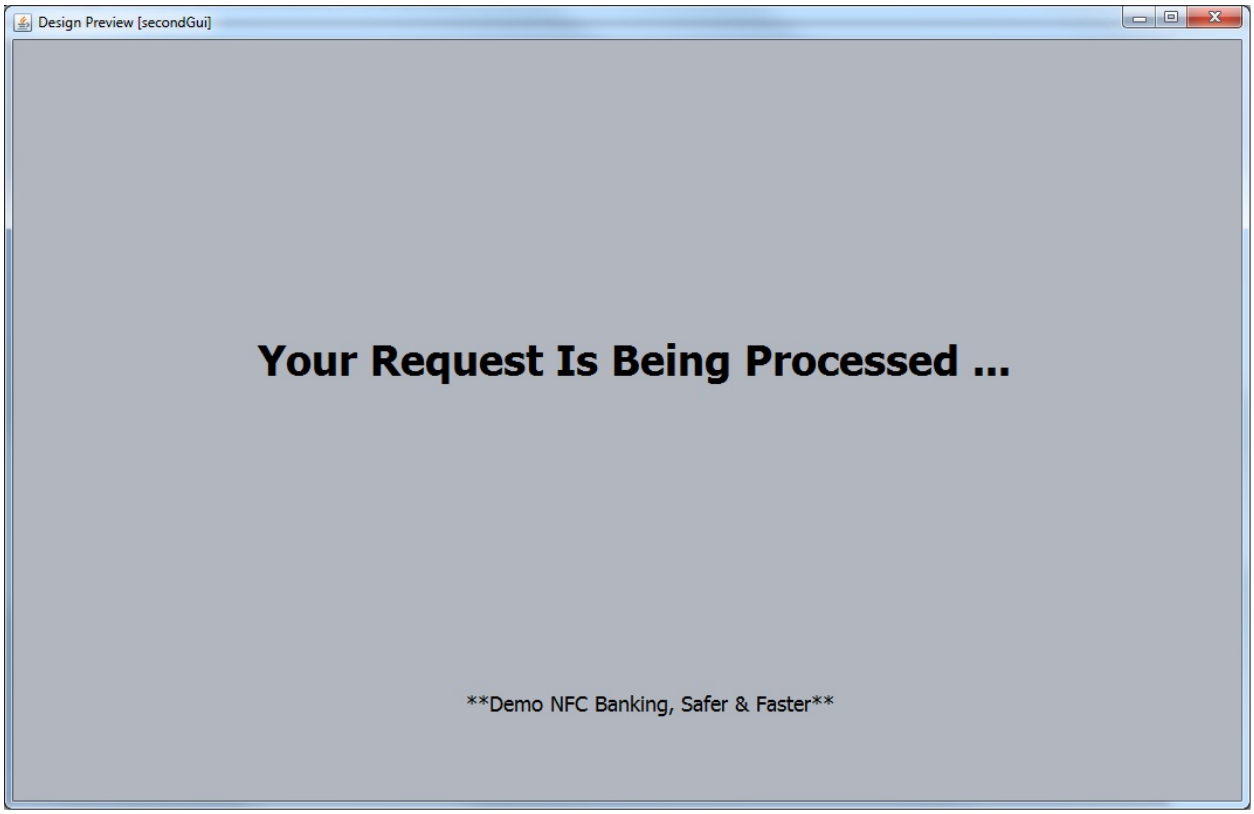

Fig.6.8: GUI of processing page of ATM

This takes a while because of a number of reasons. The bank server might be busy because the bank server has to process information of thousands of requests. It has to decrypt and the processing might be slowed down.

This is seen if the user has provided the incorrect PIN number. The PIN number needs to valid and verified. If it is incorrect then the users card is banned for making further transactions.

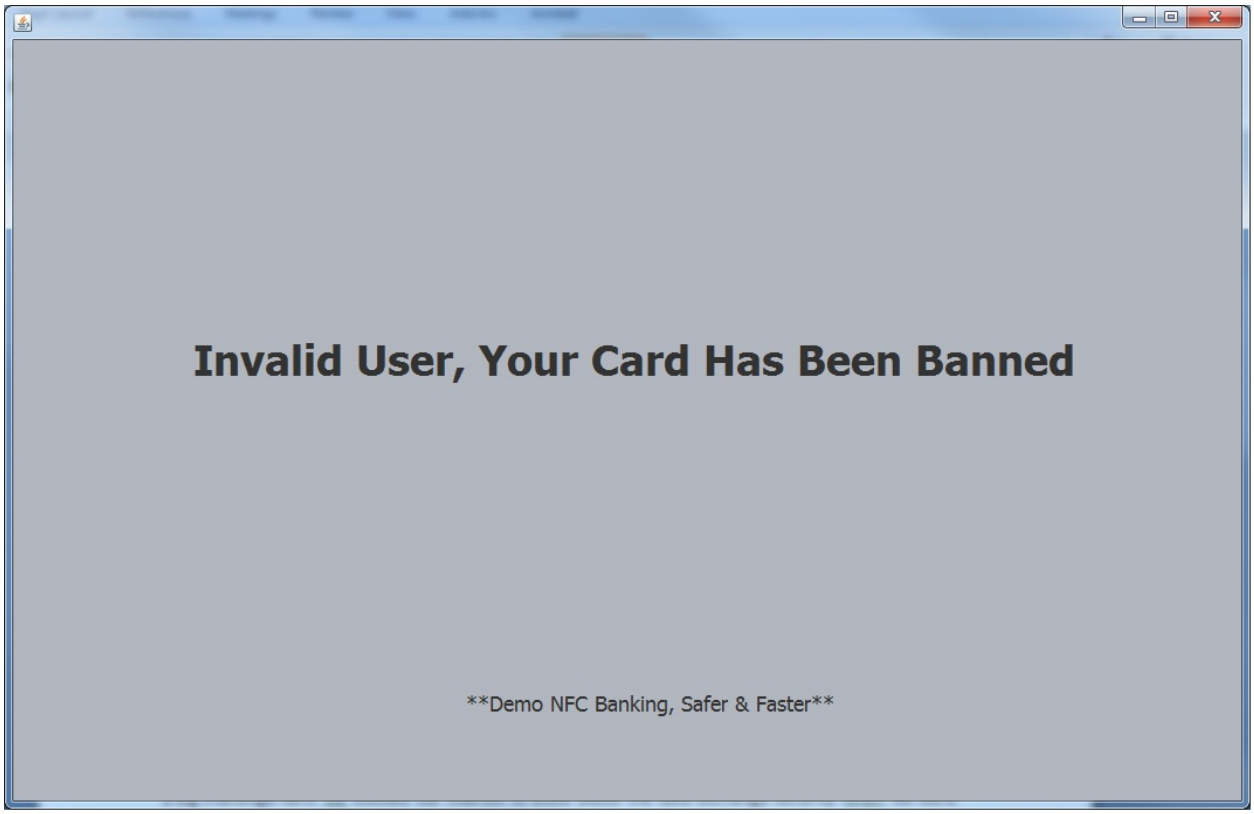

Fig.6.9: GUI of reject page for wrong PIN of ATM

Once a user is banned the ATM screen goes back to the original screen and waits for another transaction while the other user was just banned and needs to contact the bank.

This screen may be seen if the account is seen to be valid. A code card request will be seen. This is that screen. The user needs to input the code card.

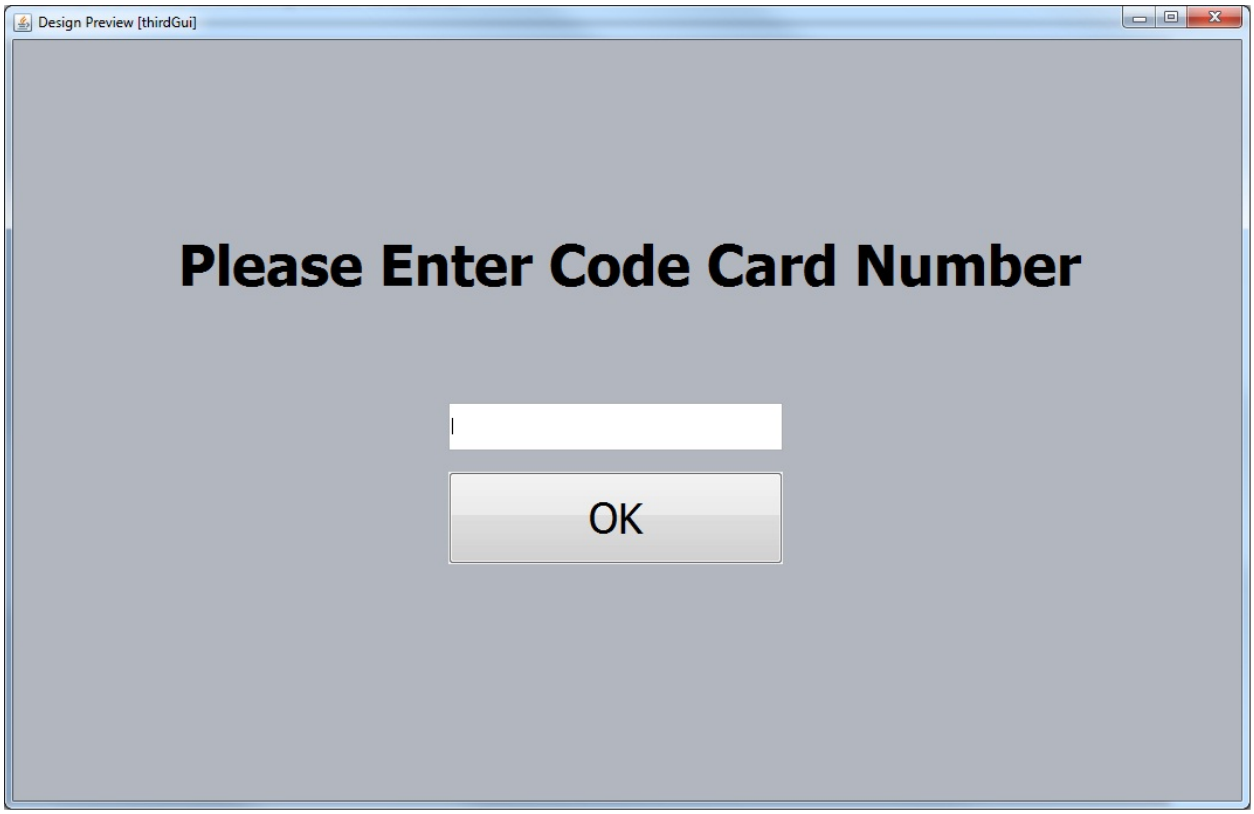

Fig.6.10: GUI of Code card request page of ATM

In the next step either the user enters a wrong code card or correct code card. If the user enters a wrong one, he will be banned again. For example like this.

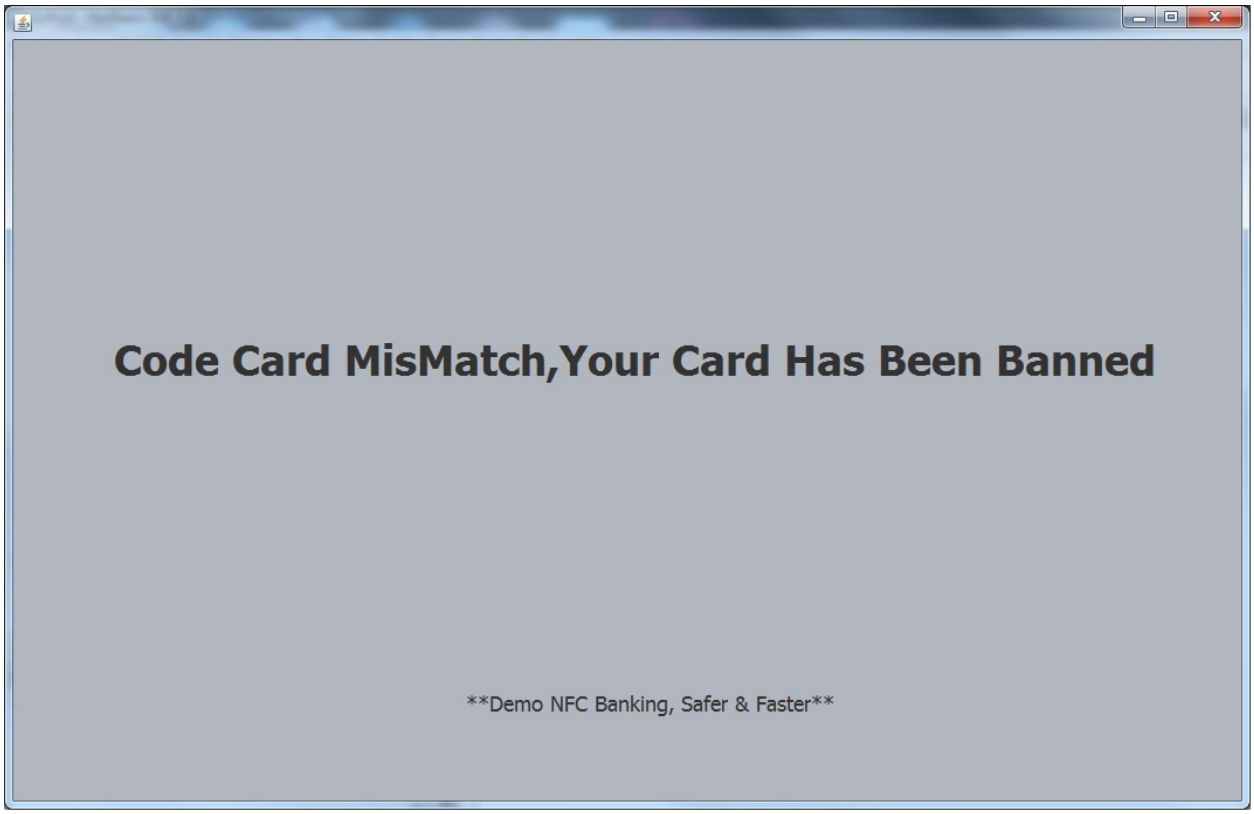

Fig.6.11: GUI of Rejected code card of ATM

On the other hand if the code card is correct. Then the transaction will be completed and he will be given the money.

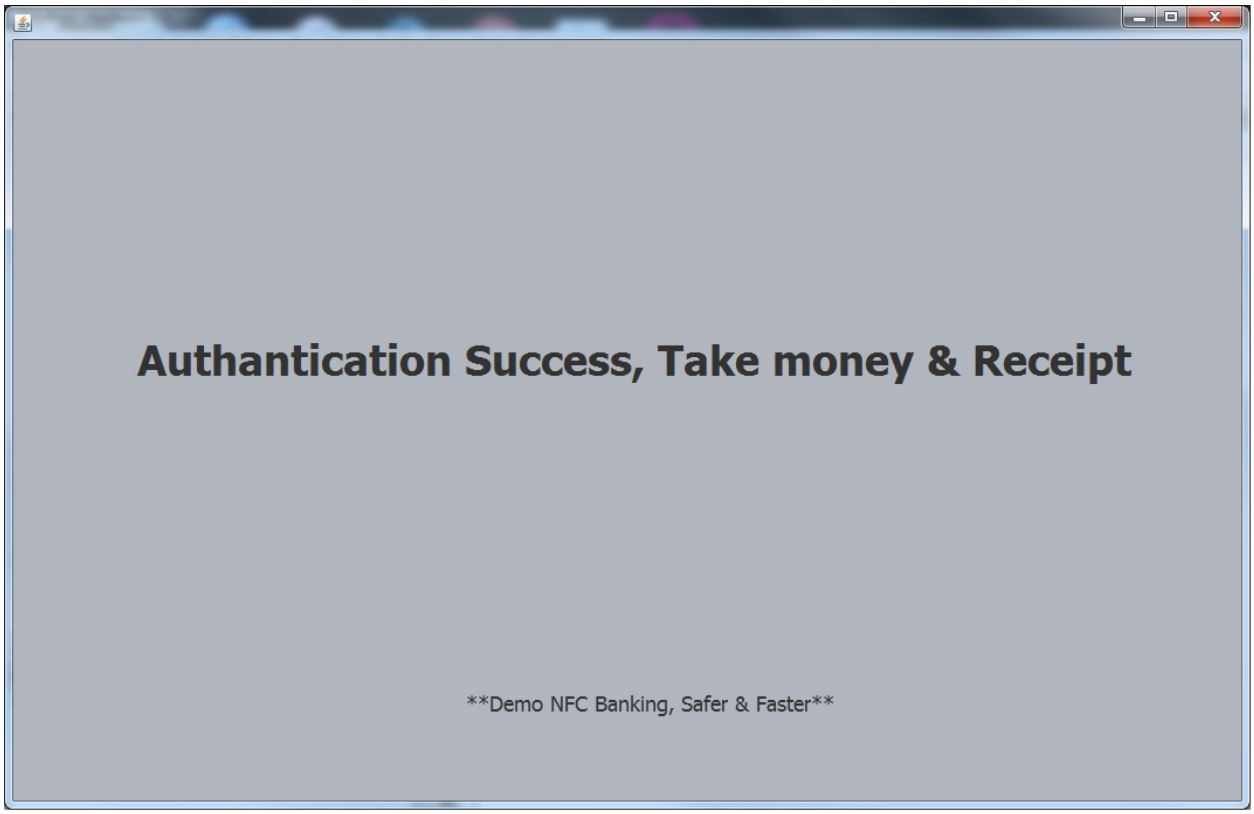

Fig.6.12: GUI of success of ATM transaction

We would like to conclude our analysis part here where we tried to show exactly how the process will work.

6.4 Real Live Demo

Below are some images of the real live working of our thesis. Here we see an arduino connected to an NFC shield which we acquired and tried to work. An ethernet cable is also connected to the arduino to connect to the CPU.

Fig.6.13. NFC connected to arduino

In the next image we can see an NFC module which carries some data to be sent to the phone. We used this to emulate the ATM which will send some specific data. This is called the Nfc device ACR122U which we used to receive data.

Fig.6.14: Nfc device ACR122U in real life

CHAPTER 7

CONCLUSION AND FUTURE WORK

In this chapter we present the conclusion and the future scope of research in this area and how to improve upon it. But first we will discuss a major drawback that we faced during our thesis.

7.1 DRAWBACK

In our thesis we tried to perform the work with and NFC device but this is not available in Bangladesh. Therefore we had to order the NFC shield and the Nfc device ACR122U from abroad. The first time we used it was broken and unusable.

Then we ordered it from Canada again and that too did not work. Since, we did not have much time we used a bluetooth module along with the arduino and transferred data through the bluetooth of the cell phone. Fig 6.15 is a working picture of a bluetooth module working.

We also bought an NFC module from Bangladesh and then we tried to use that but that too did not work due to some difficulties.

Unfortunately we were not able to implement the thesis with the NFC module, but we used and implemented it using a bluetooth module.

7.2 FUTURE WORK

On this thesis we have tried to accumulate as much information we could on encryption. The application password and authentication must be made better. There is a scope to make that better by using encryption algorithms there as well.

Moreover, the application must have built in processes where it might know when it is being hacked or trying to break. As soon as it senses it will shut down.

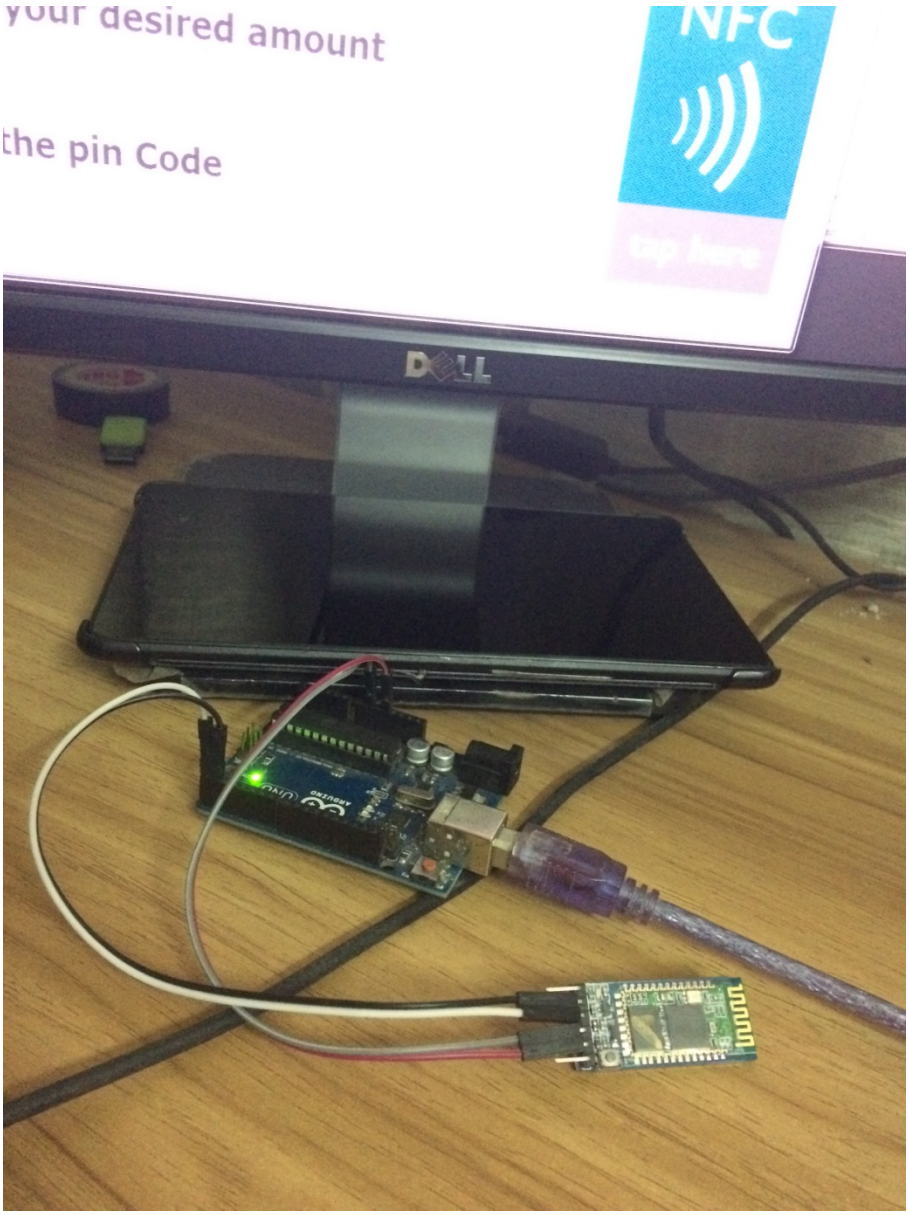

Fig 7.1 Bluetooth module hc-05 with arduino

In case of a robbery or theft there should be a process in order where the thief will not know the police has been informed and maybe the bank will seize the thief.There are possibilities to make it much more secure. These might be pursued in the future.Also, since we could not finish the task we would like to work on this with another NFC device and try to use NFC to implement it.

7.3 CONCLUSION

To conclude we would like to say that although our process may not seem to be simple it really is, the inner working of the system is purely automatic and it takes less time.

According to our process there is a 3 layer security system in place. It will be difficult for anyone to break into our phone and steal our credentials. So, we can claim that our thesis work solves the problem of security in the ATM sector where it is in dire need.

CHAPTER 8. REFERENCES

[1] Paczkowski, L. W., Parsel, W. M., Persson, C. J., &Schlesener, M. C. (2014). U.S. Patent No. 8,881,977. Washington, DC: U.S. Patent and Trademark Office.

[2] Kadambi, K. S., Li, J., & Karp, A. H. (2009, August). Near-field communication-based secure mobile payment service.In Proceedings of the 11th international Conference on Electronic Commerce (pp. 142-151).ACM.

[3] Liu, A., & Berglund, L. A. (2013). Fire-retardant and ductile clay nanopaperbiocomposites based on montmorrilonite in matrix of cellulose nanofibers and carboxymethyl cellulose. European Polymer Journal, 49(4), 940-949.

[4] Du, H. (2013). NFC technology: Today and tomorrow. International Journal of Future Computer and Communication, 2(4), 351.

[5] Madlmayr, G., Langer, J., &Scharinger, J. (2008). Near field communication based mobile payment system. Proc. Mobile und UbiquitäreInformationssysteme-Technologien, Prozesse, Marktfähigkeit, 81-93.

[6]Rezwanul, B., &Mosabber, H., (2006). Understanding of ATM (Automated Teller Machine) inBangladesh.

[7]Fábián T., (2013). NFC-enabled Automated Teller Machines

[8] “Arduino”, Wikipedia: The Free Encyclopedia. Retrieved November 12, 2016; from https://en.wikipedia.org/wiki/Arduino

[9] “List of Arduino boards and compatible systems”, Wikipedia: The Free Encyclopedia.Retrieved November 12, 2016; from https://en.wikipedia.org/wiki/List_of_Arduino_boards_and_compatible_systems

[10] “NetBeans”, Wikipedia: The Free Encyclopedia.Retrieved November 12, 2016; from https://en.wikipedia.org/wiki/NetBeans

[11] “Android Studio”, Wikipedia: The Free Encyclopedia.Retrieved November 12, 2016; from https://en.wikipedia.org/wiki/Android_Studio

[12] “MySQL”, Wikipedia: The Free Encyclopedia.Retrieved November 12, 2016; from https://en.wikipedia.org/wiki/MySQL