Chapter 1

Introduction

1.1 Introduction

Automated Teller Machine enables the clients of a bank to have access to their account without going to the bank. This is achieved only by development the application using online concepts.

When the product is implemented, the user who uses this product will be able to see all the information and services provided by the ATM, when he enters the necessary option and arguments. The product also provides services like request for cheques, deposit cash and other advanced requirement of the user. The data is stored in the database and is retrieved whenever necessary. The implementation needs ATM machine hardware to operate or similar simulated conditions can also be used to successfully use the developed product.

1.2 Motivation

As the number of ATM units increase, the machines are prone to hacker attacks, fraud, robberies and security breaches. In the past, the ATM machines main purpose was to deliver cash in the form of bank notes and to debit a corresponding bank account. However, ATM machines are becoming more complicated, and they serve numerous functions, thus becoming a high priority target to robbers and hackers. So I want to prevent these problems by using different approaches for a secured transaction.

1.3 Objective of the project

To develop this ATM system the entire operation has been divided into the following step:

- Account Activation.
- Verification process.
- Banking services.
- Transactions.
- Special services.

The program is designed in such a way that the user has a card and pin number. Once verified, he is provided a menu and he/she had to enter the option provided in the menu. For example, when user want to view the list of payment history than he/she had to enter the option for payment history provided in the main menu. When the option is entered alone with the respective argument, then the payment history is displayed on the screen.
The user also must be given option to browse through the pages like previous page, next page, etc. The user may experience a delay in retrieving or viewing the data, when there many users logged on to the same bank branch system.

1.4 Scope of the work

Millions of times per day around the globe people are instantly withdrawing money at automatic teller machines (ATMs). Given the fast-pace of the world today, it is not surprising that the demand for access to quick cash is so immense. The power of ATMs would not be possible without secure connections. The final act of ATM dispending cash is the result of an amazingly fast burst of the customer never sees, but a trust is being done in a confidential manner.

Chapter 2

ATM

2.1 What is ATM?

ATM stands for; Automated Teller Machine. It is also referred to as a cash machine, a cash dispenser and 'the hole in the wall' among other names. The ATM is an electronic computerized telecommunications device that allows financial institutions (e.g. bank or building society) customers to directly use a secure method of communication to access their bank accounts. The ATM is a self-service banking terminal that accepts deposits and dispenses cash. Most ATM's also let users carry out other banking transactions (e.g. check balance). ATM's are activated by inserting a bank card (cash or credit card) into the card reader slot. The card will contain the customers account number and PIN (Personal Identification Number) on the cards magnetic stripe. When a customer is trying to withdraw cash for example, the ATM calls up the banks computers to verify the balance, dispenses the cash and then transmits a completed transaction notice.

The idea for an ATM originally was to simply replace or reduce the workload of a bank teller (i.e. the person in the bank who gives out money to customers). The ATM would help reduce banks overheads as wages would be decreased. As for who created the first ATM or where it was first used is a topic of much debate. Basically what answer you get when the question 'who invented the ATM?' is asked depends on who you ask. Miller (2006) presents the facts as he knows it about the history and invention of the ATM. The notion of having a bank machine which automatically dispensed cash to customers came about in the 1930's. A Turkish born inventor working in America called George Simijan started building an earlier and not-so-successful version of an ATM in the late 1930's. He registered the related patents. Simijan came up with the idea of a 'hole-in-the-wall' machine which would allow customers to make financial transactions. However, at the time this idea was well ahead of its time and was met with great doubt. Simijan registered 20 patents related to the device and persuaded an American bank to trial it. However, after 6 months the bank reported little demand in the service and it was withdrawn. It was not until the 1960's that the idea of the ATM was looked at again. John Shepherd-Barron, an inventor from the UK, had an idea in the 1960's for a 24/7 cash dispenser. At the time Shepherd-Barron was the managing director of a company called De La Rue Instruments which today still manufactures cash dispensers. People who believe John Shepherd-Barron invented the ATM argue that the worlds first ATM was installed outside a north London branch of Barclays in 1967.

In 1965 a Scottish man called James Goodfellow was given a project to develop an automatic cash dispenser. Goodfellow was a development engineer with a UK company called Smiths Industries Ltd. He designed a system which accepted a machine readable encrypted card and had a numerical keypad used to enter a PIN. This design is covered in patents in both the UK and USA among other countries. This patent still describes the basic ATM function 40 years later (i.e. the design was patented in 1966). Goodfellow's machines were marketed by Chubb Ltd and installed throughout the UK during the late 1960's and early 1970's. Don Wetzel, then the Vice President of Product Planning of the American Corporation Docutel, claims he applied for a patent on an ATM in 1968. In fact some people believe Wetzel to be the inventor of the ATM. However, an ATM design patented in 1973, stating the Docutel Corporation as the assignee, states John D White as the inventor. White claims he started working on ATM system in 1968 and he installed the first ATM in 1973. This machine was called the 'Credit CardAutomatic Currency Dispenser'. Evidence suggests it was White who received the patent and not Wetzel. There is also a statement in the patent which supports the idea of the modern ATM – "Both the original code and the updated code are scrambled in accordance with a changing key". This is basically what happens today. ATM's have security keys programmed into them. The code changes and is scrambled to prevent access to credit and ATM card numbers between the ATM, the bank and the network processor. It is clear that the topic of ATM invention is quite a controversial one. However, the combined effort of all the inventors surely has helped create today's ATM. Anyone who worked on ATM

design from the 1930's until today has contributed something to the modern ATM designs. The purpose of this research is to investigate existing ATM design and to design a 'best of breed' ATM user interface design.

Fig 2.1: ATM Machine

2.2 How it works?

Here we look at the design of the proposed ATM 'best of breed' menu system in relation to the potential users who could use the system. *Error! Reference source not found..2* shows a sequence diagram for a complete operational ATM system. The proposed 'best of breed' ATM system does not need to worry about factors such as, insufficient cash or invalid card, as it only concentrates on simulating an ATM navigation menu system.

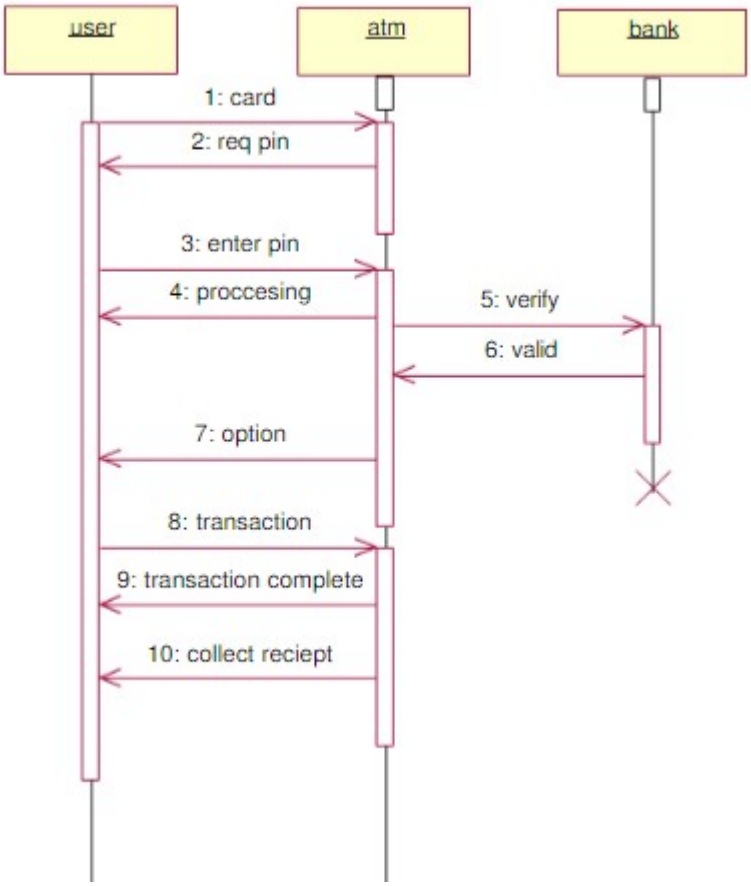

Fig 2.2: ATM system

ATM system works by a sequential process. There are three main module in this system. They are user, ATM and bank.Firstly user enter the card in ATm machine. Then asked a pin number, user input his/her pin number in the system. ATM system then check the user identity and also verify the user or card holder. After completing the authentication process ATM system gives the access for transaction. Card holder can also deposit amount and check balance in the ATM.

2.3 What is ATM Fraud?

ATM fraud refers to fraud with the use of an ATM card whereby the perpetrator of the crime uses the card to immediately withdraw funds from a consumer account using PIN based transactions at the ATM.

For instance, a perpetrator who manages to get an ATM pin number will use the ATM card at any automatic teller machine (ATM) to withdraw money from an innocent user’s bank account. Through ATM fraud, a perpetrator can even access the line of credit that is attached to an account. The common method adopted to get an ATM card by such perpetrator is to steal a customer's card. However the new technique adopted is to trap the card inside the ATM's card reader with a device called a lebanese loop. When the customer gets frustrated by not getting the card back and walks away from the machine, the perpetrator of the crime will remove the card and withdraw cash from the customer's account.

Fig 2.3: ATM Fraud

2.4 Types of ATM Fraud or Attack

2.4.1. Card skimming

This is done by using a card reader that can capture the data in the magnetic strip of a card. One bold move done by these criminals includes installing a card reader right on top of the ATM's card slot.

With this device, once a card is inserted, data will automatically be captured. Such card readers, measuring 1″ x 1″ are being sold in the internet for a very low price and with complete instructions.

This scheme, though, is more popular in credit cards because the 'take' is higher compared to ATM cards.

Fig 2.4: **Card skimming**

2.4.2. Salisi gang

Fig 2.5**: Salisi Gang**

Another type of ATM fraud is called the Salisi Gang aka Ipit Gang or LaglagBarya Gang. This is fairly common during paydays when there is a long line of cardholders at the ATM.

2.4.2.1 How the salisi gang works

When the cash being withdrawn is about to be dispensed by the ATM, a member of the gang will drop several loose bills and then point to the unsuspecting cardholder for help.

Once the cardholder tries to pick up the bills, another gang member will immediately get the cash waiting at the cash out shutter and then disappear out of sight as fast as he can.

It will be too late when the cardholder realizes what actually happened when he/she tries to get the money being withdrawn.

2.4.2.2 Another version of this

When the cardholder is about to retrieve his/her ATM card right after withdrawal, one of the gang members will cut-off, get the card coming out of the card slot, and replace it with a similar looking card.

All of these will happen in just a split second. The unsuspecting cardholder, without realizing what had just happened, will get his/her '*card*' and immediately leave.

The gang member, who had already seen the PIN during withdrawal, will then use the stolen card in other ATMs and try to withdraw the remaining balance before the card is reported as '*stolen*'.

2.4.3 Cash Trapping

The proliferation of fraud and crimes committed in the ATM's have surfaced a new and become more sophisticated and the perpetrators bolder than before.

The most common is the so-called cash trapping perpetrated by the notorious group called Ruler Gang. They were given that name because of the device they use in trapping the cash that looks like a ruler.

In the U.S., the device is called the False ATM Presenter.

Fig 2.6**: Cash Trapping**

2.4.3.1 How cash trapping works

A member of the gang will install a specially fabricated "*ruler*" device onto the cash out shutter of the ATM and leaves it there. This device looks exactly like the cash out shutter of the machine.

When an unsuspecting cardholder tries to withdraw, the cash will be trapped inside (it is actually glued at the back of the device).

After a while, the cardholder, thinking there is something wrong with the machine or with his/her transaction, will leave frustrated and disappointed.

Thereafter, the gang will remove the device with the cash still glued on it using their special prying tool.

2.4.4 Card Trapping

Normally relatively low value, the fraudster will use a device to physically trap the cash that is dispensed and come to collect once the customer has left the ATM location.

Fig 2.7: Cash Trapping

2.4.5 Fake PIN Pad Overlay

A device similar to the machine's keypad is placed right on top of the ATM keypad and captures the PIN entered by the cardholder. Before you transact to the ATM machine, kindly inspect anything that is suspicious on the machine itself.

Fig 2.8: **Fake PIN Pad Overlay**

2.4.6 Shoulder surfing

That's why it is very important to be aware of the person or people around the ATM machine when you transact. If a person or people is too near to you when you transact you can advise them to move a little bit backward.

This is literally looking over the shoulder of the cardholder to see the PIN as it is being keyed in. This compromises the PIN of the cardholder without his/her knowledge.

There is a high-tech, knowledgeable group which is popular in the internet that installs small cameras to see the actual PIN being keyed-in by the cardholder.

Fig 2.9: Shoulder surfing

2.4.7 Fake assistance

"*May I Help You?*" is another ATM fraud employed by notorious elements preying on the elderly and those new in having an ATM card.

Once these perpetrators spotted one, they will appear to be very helpful and offer assistance to the unsuspecting cardholder but in truth, these perpetrators are already memorizing the card number and PIN.

With the card number and PIN, the gang can easily transfer the funds to their own bank account using the internet or mobile phone or a clone ATM card.

There are other fraud and crimes committed in the ATM because of the fact that it is where the money is. Listed below are other fraud and crimes, although not as popular as those discussed above, which are committed at the ATMs:

2.4.8 Physical Attack

A scheme that is similar in a way to the one above but here, the cardholder is held-up at gunpoint or with a knife by a hold-upper after withdrawing from the ATM. This is very common ATM fraud here in the Bangladesh.

This usually happens in paydays like 15th and 30th of the month. We need to be aware of this to help prevent happening to us.

Best way to prevent this is to transact on ATM machine that are in safe places like banks (inside), malls and other places that has security and well lighten.

Now that we know the different types of ATM fraud and crimes, this will really help us be aware of our activity when transacting thru the ATM. This information can help us identify and detect ATM fraud activities and take necessary action.

Chapter 3

Requirement Analysis

3.1 Requirement Analysis

Requirement Analysis is the third step of System Development Life Cycle (SDLC). This step is very much important and inseparable part of a project.

Requirement Analysis is concerned with discovering and deciding what the new system is required to do?

3.2 Process Specification

Card activation: The card should be activated by the user before committing a transaction. This will be done by user mobile phone. User has to send activation request to the server. Then server side will be responsible to activate the card.

Face detection/PIN: After card activation, user will be authenticated by the system through face detection strategy or PIN may be instead that. If user is not verified then he/she won't able to complete a transaction.

Confirmation: A simple confirmation message will be send to the user smart phone if he/she uses PIN method. If face detection method is followed then user won't have to follow this step.

Card access: After three tier authentication, user will get access to the card. Then he/she will be able to do transaction such as withdraw, deposit, transfer, check balance etc.

Card deactivation: After complete transaction, the card state will be deactivated automatically to avoid security attacks. Whenever it needs to do a transaction, user will have to activate it again.

3.3 Non-functional Requirements

The non-functional requirement is bellowed.

- The ATM network has to be available 24 hours a day.
- Each bank may be processing transactions from several ATMs at the same time.
- The ATM must be able to use several data formats according to the data form that are provided by the database of different banks.

3.4 Feasibility

After the requirement analysis the feasibility study determines whether a proposed system is feasible or achievable, given the organizations resources and constraints. That is why feasibility studies are must for any new and expanding project. This study takes a brief look at the major factor that will influence the ability of the

system. It is independent of my initial research, analysis or overall review of any new venture. The three major area of this study is technical feasibility, economical feasibility, and operational feasibility. According to the requirements of the designing of ATM system, it is clear that a large amount of data is to be handled. To maintain all information for all the components a well-designed computerized system is needed. By implementation the system processing data consistency is improved.

3.4.1 Technical Feasibility

In this part, it is ensured whether the existing technical resources – hardware, software etc. It will support the design of the proposed system. During the component analysis it was found that the all Bank uses computers. These computers work under a Local Area Network (LAN) based system. Therefore, it can be concluded that the proposed system is technically feasible.

3.4.2 Economic Feasibility

After analyzing the technical feasibility, the economic feasibility has to be considered. It is very important to take under consideration the cost effect of the system.

3.4.3 Operational Feasibility

In this part, the existing managerial and organizational framework was studied. It was done in order to see whether the proposed system would change the working environment or not. The system, which was going to be implemented, obviously will change the working environment but that must not be drastic and the users must feel comfortable handling and coping with the solution.

Chapter 4

Process Modeling

4.1 Proposed System Overview

The following features should be added for a proposed system:

- An account holder should be able to deposit amount in his/her account through ATM.
- An account holder should be able to transfer funds from his/her account to any person located anywhere in the world.
- An account holder should be able to check his recent or past bank statements e.g. online credit card purchases.
- An ATM should be equipped with a security system which should add face detection technique for the account holder before he had entered the pin code. This will make ATM transaction more secure.
- An ATM should be two layer user authentication and verification process.

4.2 E-R Diagram

In software engineering, an Entity-Relationship Model is an abstract and conceptual representation of data. Entity-relationship modeling is a database modeling method, used to produce a type of conceptual schema or semantic data model of a system, often a relational database, and its requirements in a top-down fashion.

Diagrams created using this process are called entity-relationship diagram or E-R Diagram or ERD.

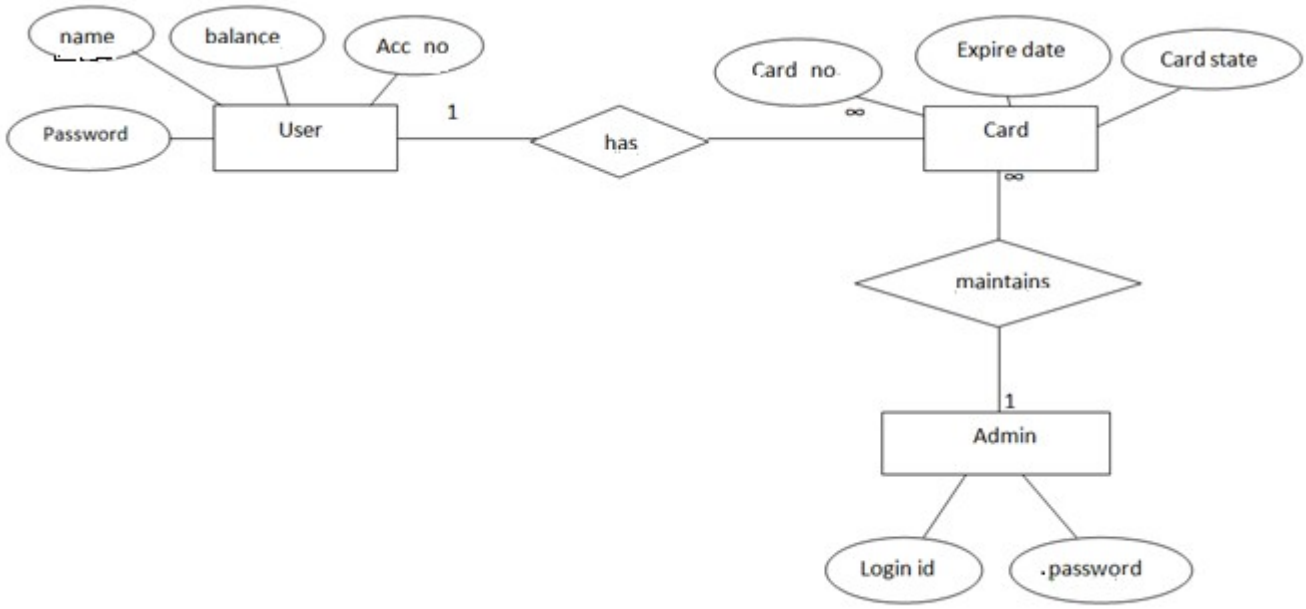

Fig 4.1: **E-R Diagram for ATM Transaction**

4.3 Data Flow Diagram

A data flow diagram is a graphical depiction of flow of data through intended software system and is used as 1st step to create an overview of system. It's really useful as it provides overview of data as well as functionally to software designers.

4.3.1 DFD Level 0

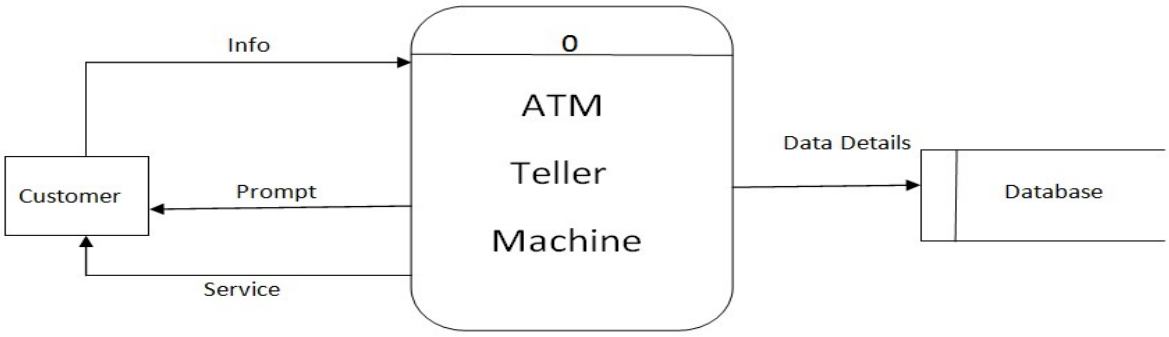

Fig 4.2: DFD Level 0

4.3.2 DFD Level 1

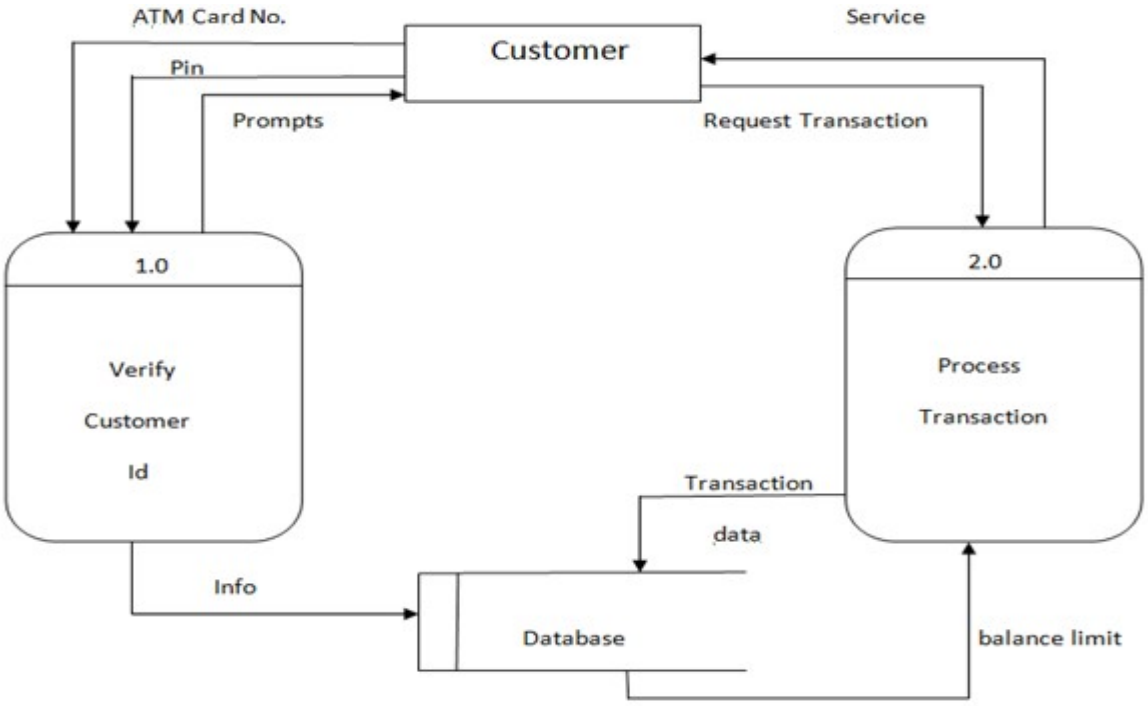

Fig 4.3: DFD Level 1

4.3.3 DFD Level 2

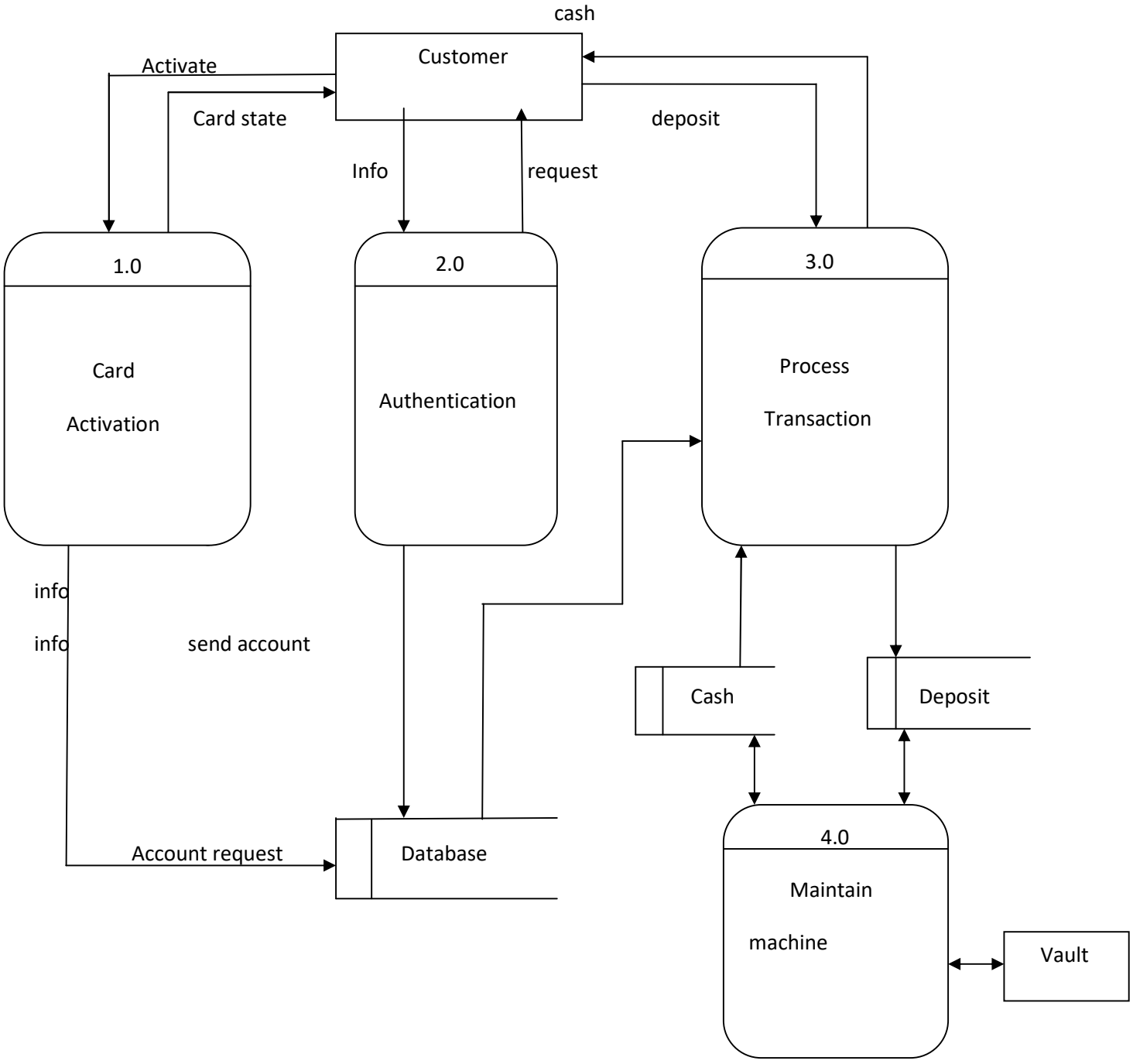

Fig 4.4: DFD Level 2

4.4 UML Design

4.4.1 Use case Diagram

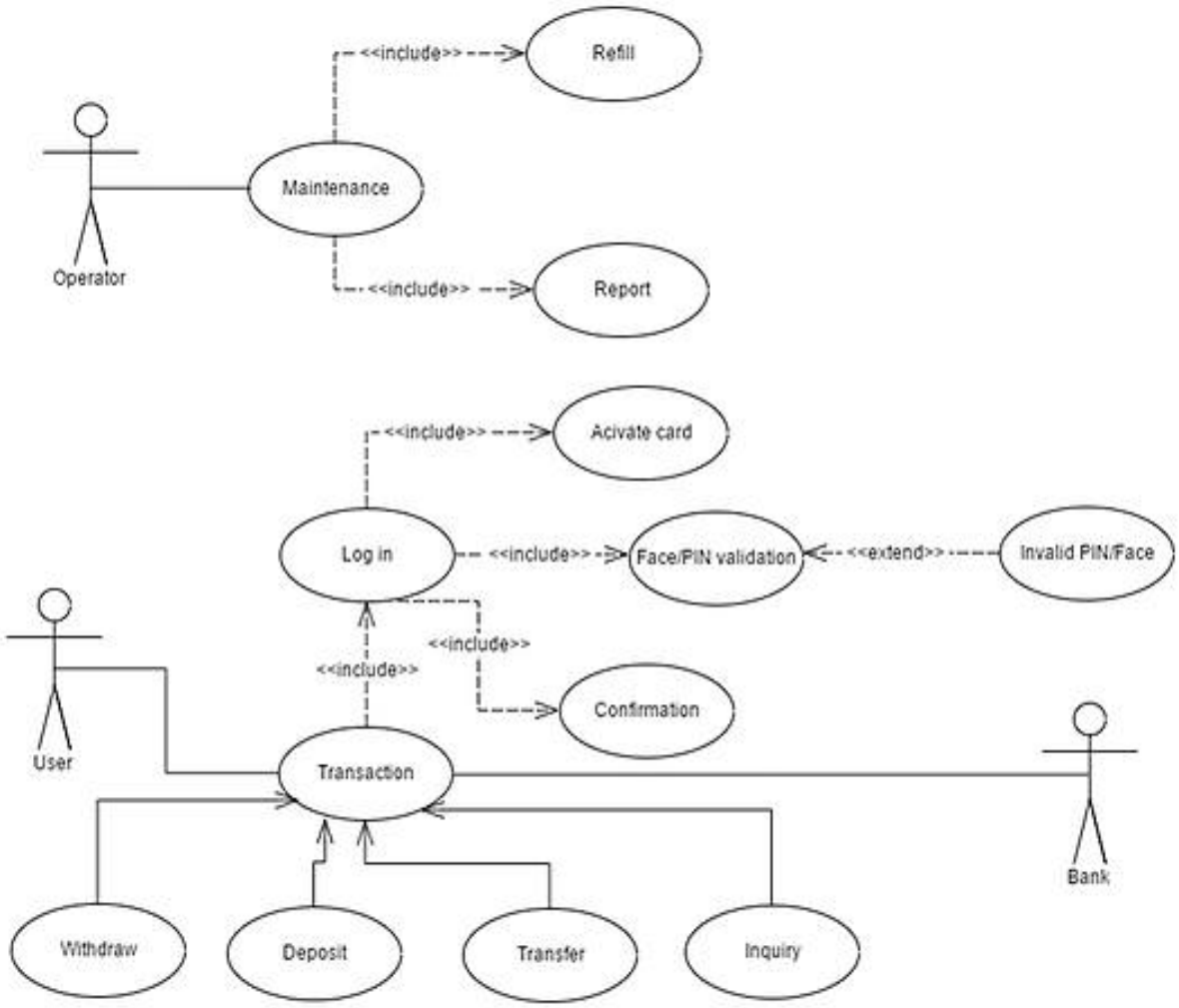

Fig 4.5: Use Case Diagram

4.4.2 System Flow chart

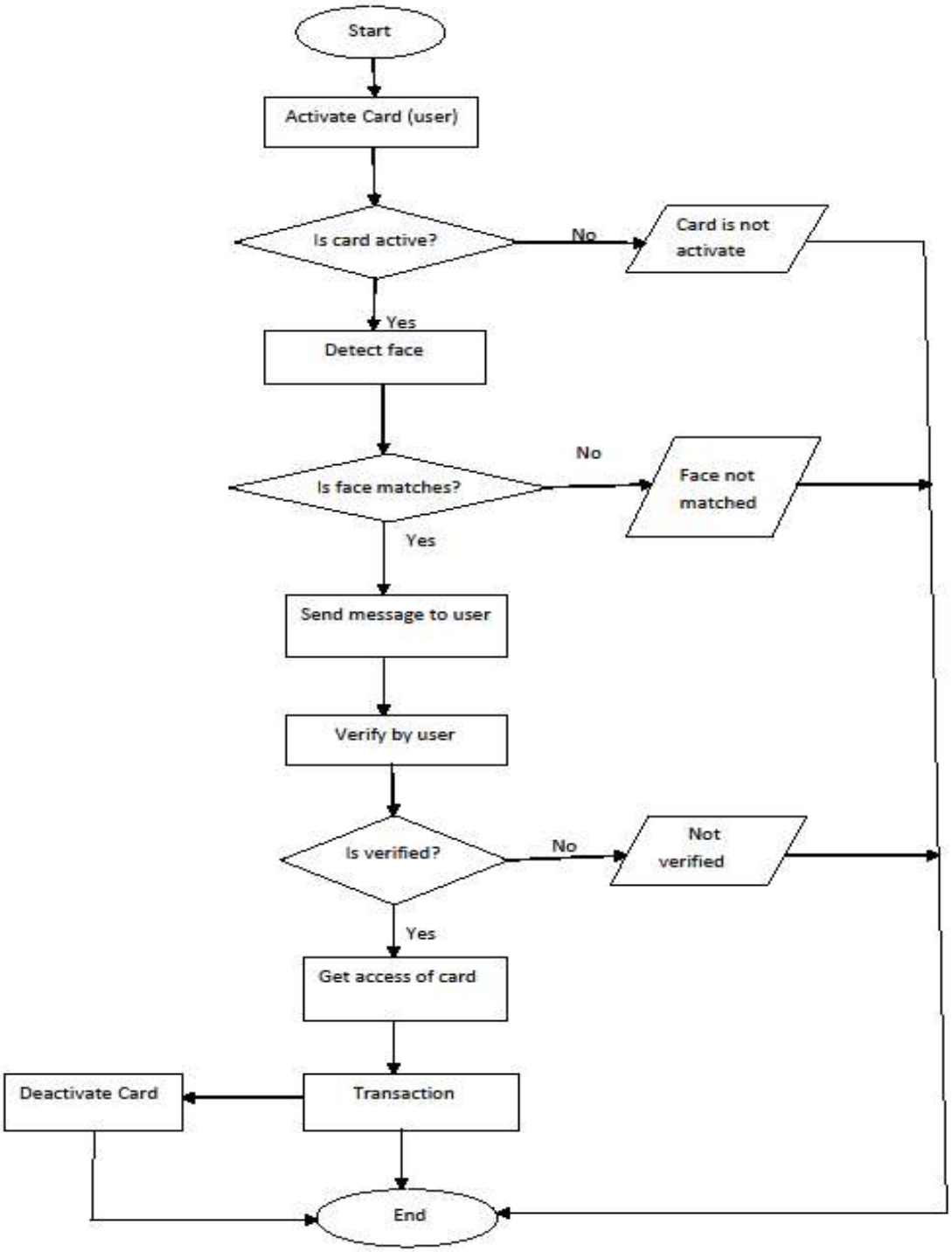

Fig 4.6 System Flowchart

Chapter: 5

Development Process

5.1 Development Strategy

The Development consists of paper prototyping of rough ideas and sketches which later translated into real implementation. Workflow efficiency is the most when a clear concept is ready and in front of the eye. That way development process goes much faster.

5.2Process Model

The development model includes server, admin, ATM machine and user device. User needed to activate his card to start his transaction procedure. After completing the process he deactivates his card. Admin is responsible for controlling system and its components such as database. ATM machine device act as usual ATM machine. In other words, it is automated simulation of real life ATM machine.

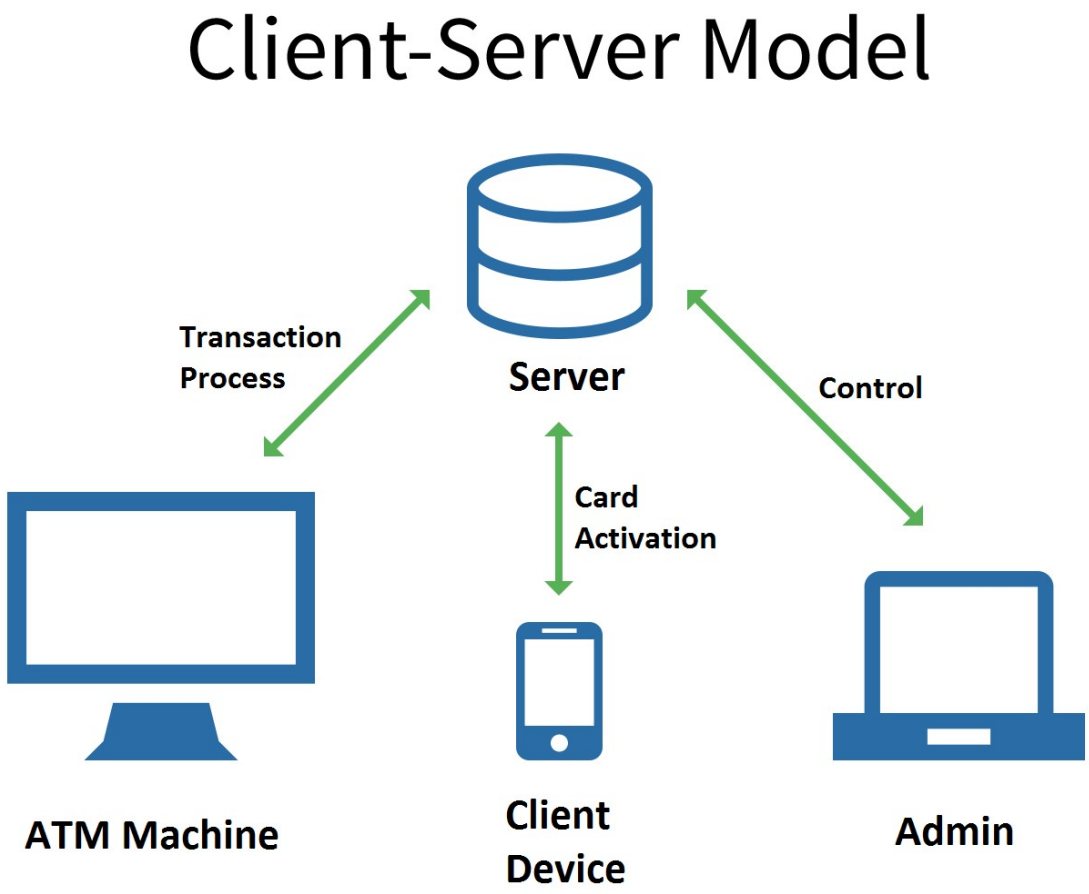

Fig 5.1: Client Server Model

5.3 System Overview

The system generally works with three main interfaces. One for admin, second one for ATM machine and last one for Client.

5.3.1 Admin

Admin can add Client by submitting a form that contains Client name, account number, password etc. To complete this process admin need to scan face of Client which will be added in the system files. Admin also can add a Card by submitting a form that contains Card number, account number, PIN.

5.3.2 Client

Client can log in his card through client interface. He needs to submit his account number and password to log in. He can activate, deactivate and log out as well. Activation and deactivation process communicate with the server.

5.3.3 ATM Machine

ATM machine interface is a automated interface. By default one can see interface which prompts to enter card number. It goes with several processes such as card validity check, card mode check, PIN matching, face recognition and so on. After these authentication one can complete his transaction.

Chapter: 6

Development Environment And Testing

6.1 Development Environment and Tools

6.1.1 Platform

The system is cross platform. Files of the system works fine in several operating systems, such as Windows, Linux and Android. The development process and testing process is performed in Windows Operating system.

6.1.2 Editor

To code PHP and Javascript programs, Sublime Text 3 is used. Pycharm community edition is used to write code and run python codes.

6.1.3 Required Tools and Modules

The system requires two important tools to run its face recognition module. One of them is Python 2.7.13 and another one is OpenCV 2.4.

The system also requires some python modules to run defined above part. Numpy or Numeric python is used to convert image to numeric array. Python Image Library (PIL) is required to convert normal openCV image to PIL image which is more efficient and convenient to use.

6.1.4 Technology

Several scripting languages are used such as PHP is used to communicate with server and modify database. Mysql is used for database. Python and OpenCV is used to run face recognition modules. Javascript is used to make more interactive user interface. JSON served bridge between PHP and Python scripts.

6.2System Introduce and Testing

Following figure shows Admin panel which will be visible after log in as admin. Admin can then perform some action such as Add client, Add card etc.

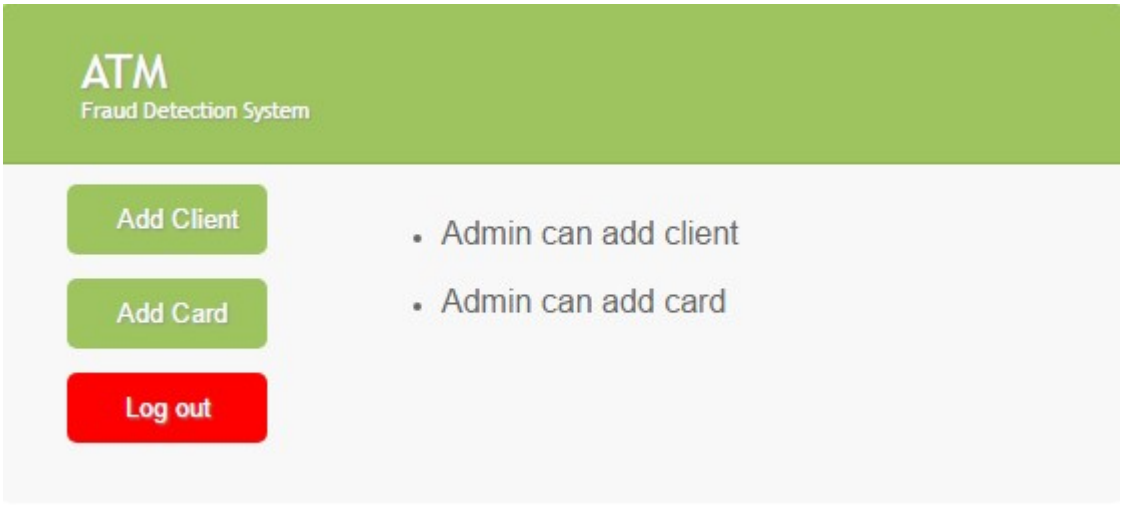

Fig 6.1: Admin Panel

Client should run his application from his device. He should log in to Turn On and Turn Off action of corresponding card.

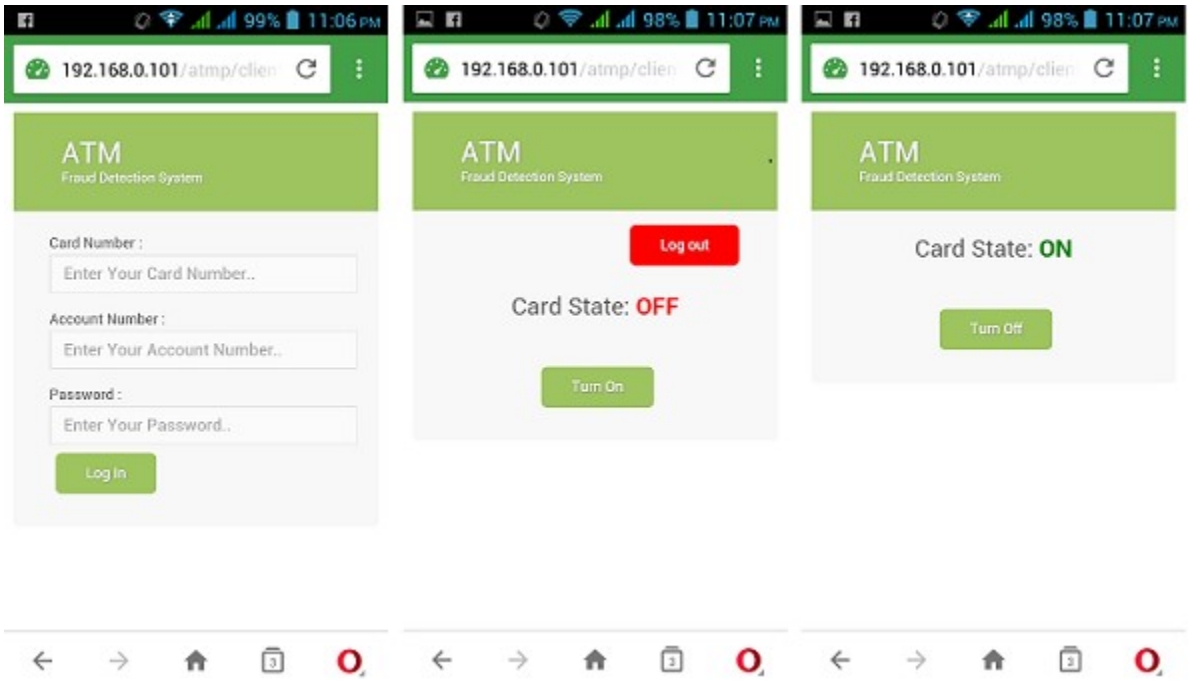

Fig 6.2: Client Interface

ATM machine shows its interface which tells client to enter card and allows client to choose authentication method. There are two available methods of authentication. These are face recognition and PIN method.

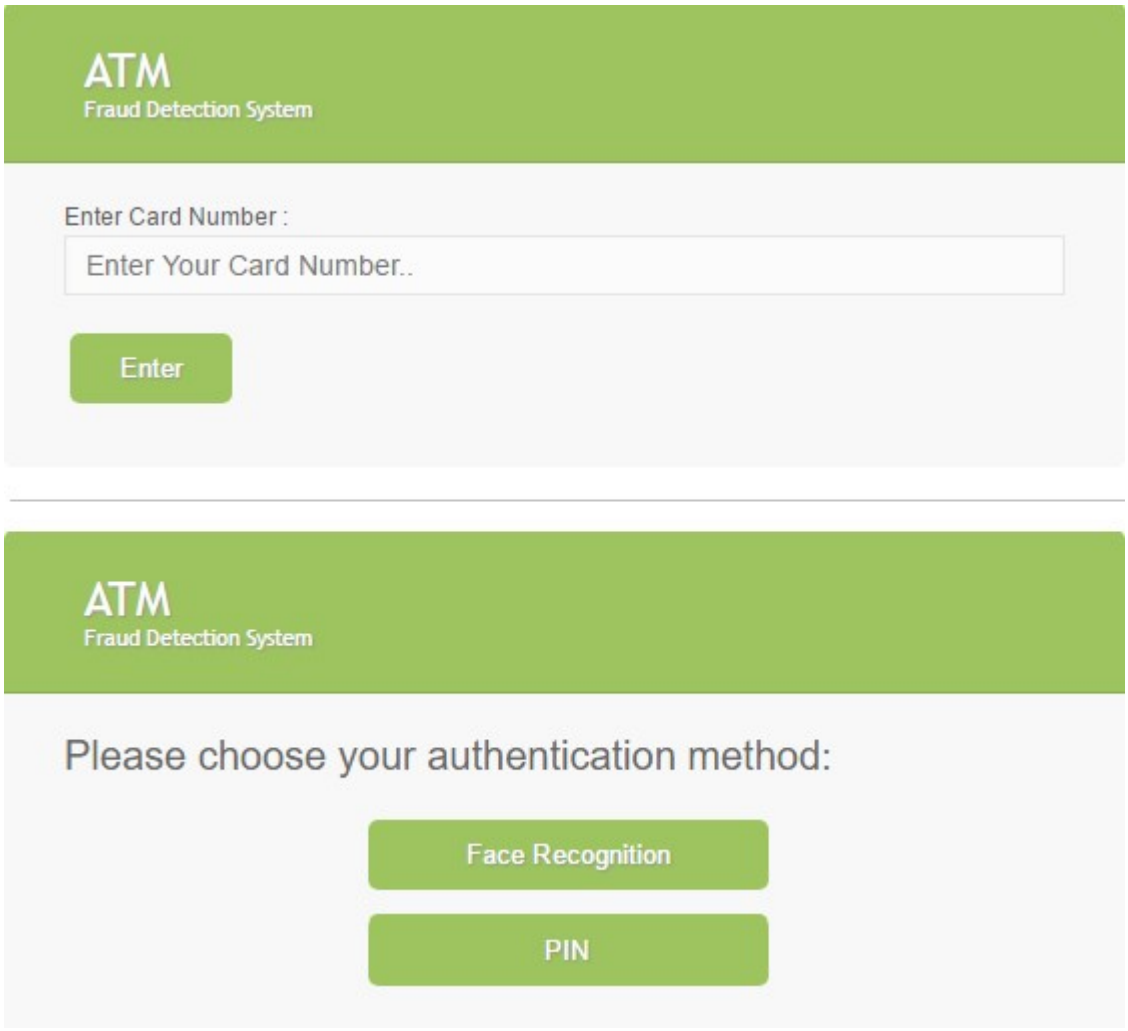

Fig 6.3: Card entry and choosing Authentication method

Following figures show the interface of the face recognition module and PIN method module. To perform face recognition one should press the “Start” button and stand in front of camera. To complete PIN method client should enter the PIN number of corresponding Card. Then the transaction process start.

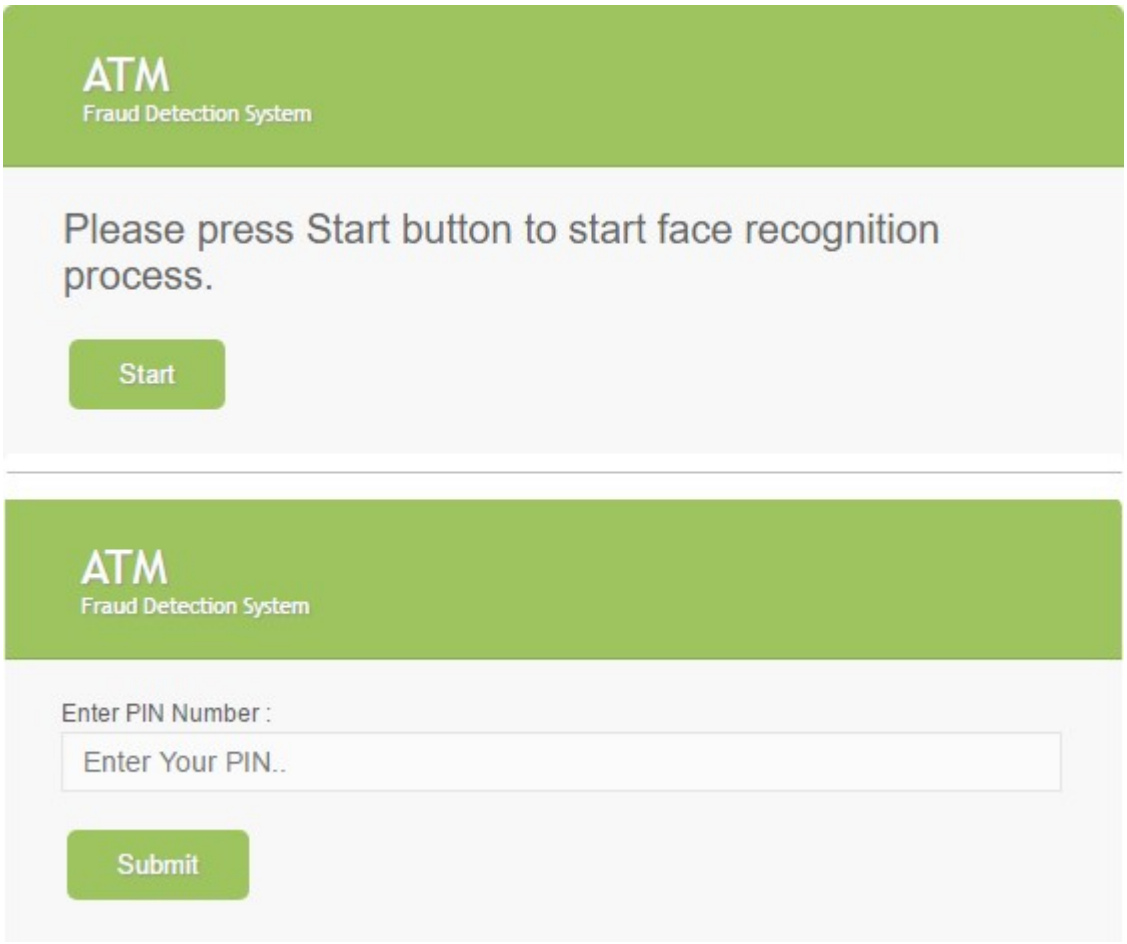

Fig 6.4: Authentication methods

These figures show the actual interfaces of transaction method process. Client enter the amount that he wants to withdraw and then submit the amount. Then the transaction process performed and the system then gives a message to client and redirect to its default interface.

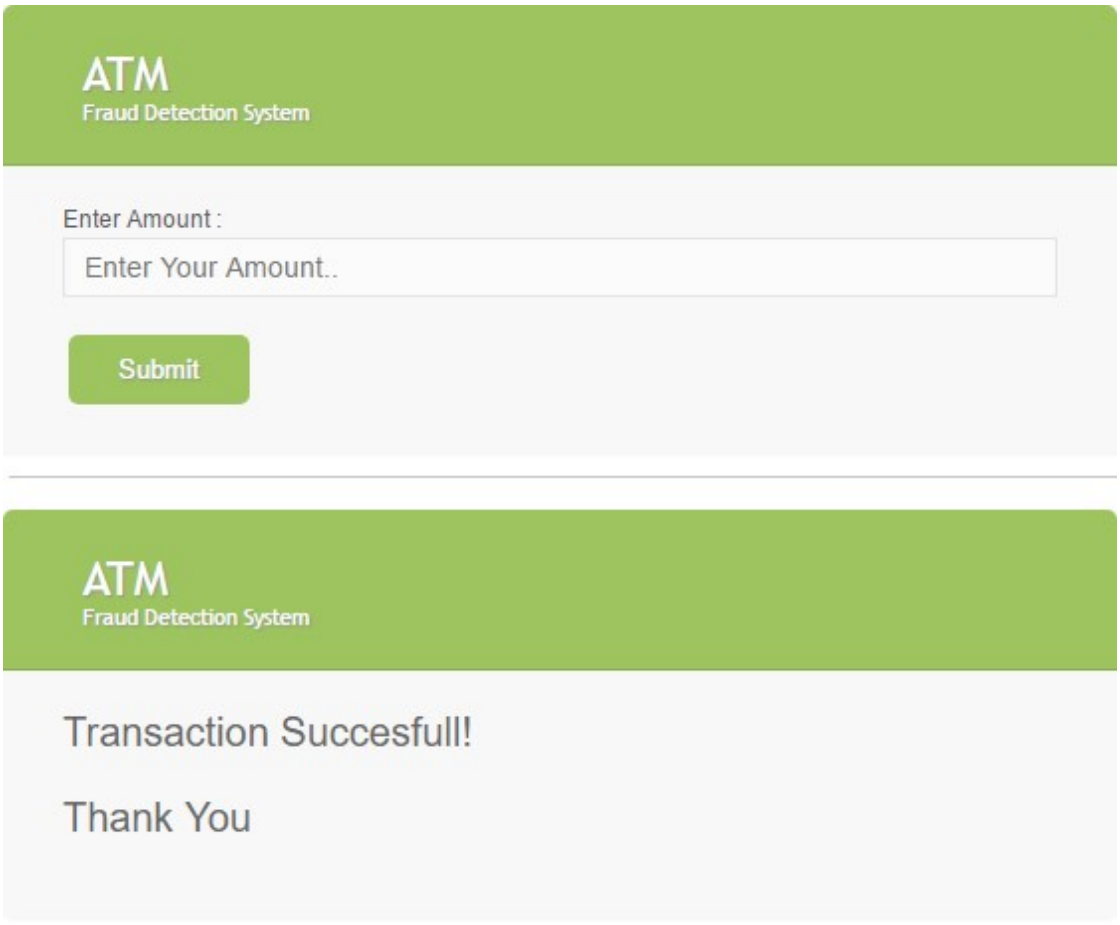

Fig 6.5: Transaction Process

Chapter: 7

Conclusion

7.1 Conclusion

In ATM Banking a Fraud detection system will run at the banks server. And it's Function to do financial transaction without any fraud. It is considered under Prediction system. A method to attack card activation and face detection based online banking methods is to manipulate the used software in a way, that correct transactions are shown on the screen and faked transactions are signed in the background. First user behavior is recorded and then for new transaction it is checked. We have suggested a method for finding the spending profile of cardholders, as well as application of this knowledge in deciding the value of observation symbols and initial estimate of the model parameters. The system is also scalable for handling large volumes of transactions. The proposed methodology is aimed at detecting fraud in case of internet banking

REFERENCES

[1] Hong Guo,Bojin, Forensics analysis of skimming device for credit fraud detection.

[2] Yun Yang, Jia Me, ATM terminal design is based on fingerprint recognition

[3] William Stalling, Cryptography and Networks Security.

[4] Ingemar J. Cox, Mathew L. Miller, Jeffrey A. Bloom, Jessica Fridrich, Ton kalker, Digital Watermarking and Steganography.

[5] DigitalWatermarking, [Online] Available: http://en.wikipedia.org/wiki/Digital_watermarking

[6] Credit card cloning, [Online] Available: http://www.wired.com/threatlevel/2009/03/washington

[7] Kerberos Security, [Online] Available: http://krebsonsecurity.com/2010/06/police-arrest-178-in-u-seurope- raid-on-credit-cards-cloning-labs/

[8] Credit Card Theft, [Online] Available: http://creditcardsnewsindia.blogspot.com/2010/05/money-stolenby-cloning-credit-cards.html [9] Credit Card Fraud, [Online] Available: