

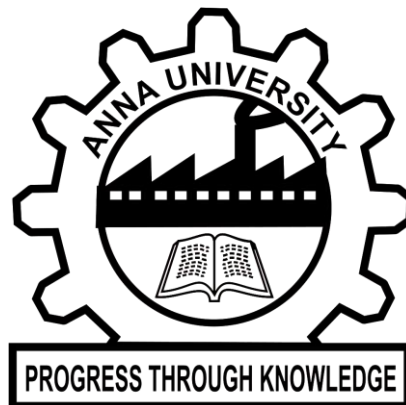
ATM FRAUD DETECTION SYSTEM

A MINI PROJECT REPORT

Submitted by:

DHINAKARAN V (210419205010)

VIJAY S (210419205059)



ANNA UNIVERSITY : CHENNAI 600 025

JUNE 2022



**CHENNAI
INSTITUTE OF TECHNOLOGY**

DEPARTMENT OF INFORMATION TECHNOLOGY

CHENNAI INSTITUTE OF TECHNOLOGY

JUNE 2022

DEPARTMENT OF INFORMATION TECHNOLOGY
CHENNAI INSTITUTE OF TECHNOLOGY
(ANNA UNIVERSITY : CHENNAI 600 025)

CANDIDATE'S DECLARATION

We, Dhinakaran V & Vijay S students of B.Tech (Information Technology), hereby declare that the Project Dissertation titled — “Atm Fraud Detection System” which is submitted by us to the Department of Information Technology, Chennai Institute of Technology, Chennai. This work has not previously formed the basis for the award of any Degree, Diploma, Fellowship or other similar title or recognition.

Place: Chennai

Date: 21/06/2022

Dhinakaran V

(210419205010)

Vijay S

(210419205059)

DEPARTMENT OF INFORMATION TECHNOLOGY
CHENNAI INSTITUTE OF TECHNOLOGY
(ANNA UNIVERSITY : CHENNAI 600 025)

BONA FIDE CERTIFICATE

I hereby certify that the Project titled “ATM Fraud Detection System” which is submitted by Dhinakaran V & Vijay S is a record of the project work carried out by the students under my guidance & supervision. To the best of my knowledge, this work has not been submitted in any part or fulfillment for any Degree or Diploma to this University or elsewhere.

SIGNATURE

Dr.R.SARAVANAN, M.E, Ph.D
(HEAD OF DEPARTMENT)

Department of Information Technology
Chennai Institute of Technology
Kundrathur, Chennai- 600 069.

SIGNATURE

Dr.R.SURENDARAN, M.E, Ph.D
(PROFESSOR)

Department of Information Technology
Chennai Institute of Technology
Kundrathur, Chennai- 600 069.

Submitted for the project viva examination held on_____.

INTERNAL EXAMINER

EXTERNAL EXAMINER

ACKNOWLEDGEMENT

We express our gratitude to our chairman Shri.P.SRIRAM, and all trust members of **Chennai Institute of Technology** for providing the facility and opportunity to do this project as a part of our undergraduate course.

We thank our Principal Dr.A.RAMESH M.E., Ph.D. for his valuable suggestion and guidance for the development and completion of this project.

We sincerely thank our Head of the Department Dr.SARAVANAN, M.E.,Ph.D, Department of Information Technology for having provided us valuable guidance, resources and timely suggestions through our work.

We are overjoyed to express our sincere gratitude to DR.R.SURENDARAN, M.E.,Ph.D., our beloved project guide, for his insightful advice, outstanding encouragement and unwavering support throughout the course of our project.

We wish to extend our sincere thanks to All Faculty members And Lab Instructors of the Department of Information Technology for their valuable suggestions and their kind cooperation for the successful completion of our project.

Abstract

This paper gives the intersection between the cash cards standards followed in the banks and the financial frauds. It undertakes two primary tasks; namely understanding of the traditional standard cash card provided by the banks and a proposed methodology to make them more secure to reduce the cash card frauds. The methodology uses the face detection procedure and online based account activation procedure which plays a prominent role to authenticate the user. This authentication mechanism is useful while transaction to secure cash card from being cloned via skimming device, card trapping. This paper provides a generalized solution for financial fraud by the cash card cloning or trapping that is being done in the field of E-banking.

Table of Contents

Chapter 1: Introduction

Page No.

1.1	Introduction.....	2
1.2	Motivation.....	2
1.3	Objective of the Project.....	2
1.4	Scope of the Work.....	2
1.5	Organization of the Project.....	3
1.6	Summary.....	3

Chapter 2: ATM

2.1	What is ATM?	5
2.2	How it Works?	6
2.3	What is ATM Fraud?	7
2.4	Types of ATM Fraud or Attack.....	8
	2.4.1 Card Skimming.....	8
	2.4.2 Salisi Gang.....	9
	2.4.2.1 How the Salisi Gang Works.....	10
	2.4.2.2 Another Version of This.....	10
	2.4.3 Cash Trapping.....	10
	2.4.3.1 How Cash Trapping Works.....	11
	2.4.4 Card Trapping.....	11
	2.4.5 Fake PIN Pad Overlay.....	12
	2.4.6 Shoulder Surfing.....	12
	2.4.7 Fake Assistance.....	13
	2.4.8 Physical Attack.....	13
2.5	Summary.....	13

3.1	Requirement Analysis.....	15
3.2	Process Specification.....	15
3.3	Functional Requirements.....	15
3.4	Non-functional Requirements.....	15
3.5	Feasibility Study.....	16
	3.5.1 Technical Feasibility.....	16
	3.5.2 Economic Feasibility.....	16
	3.5.3 Operational Feasibility.....	16
3.6	Summary.....	16

Chapter 4: Process Modeling

4.1	Proposed System Overview.....	18
4.2	Waterfall Model.....	18
4.3	Workflow in Waterfall Model.....	18
4.4	System Flowchart.....	19
4.5	Summary.....	20

Chapter 5: System Design

5.1	E-R Diagram.....	22
5.2	Data Flow Diagram.....	22
	5.2.1 DFD Level 0.....	23
	5.2.2 DFD Level 1.....	23
	5.2.3 DFD Level 2.....	24
5.3	UML Design.....	25
	5.3.1 Use Case Diagram.....	25
5.4	Summary.....	26

Chapter 6: Development Process

Page No.

6.1	Development Strategy.....	28
6.2	System Model.....	28
6.3	System Interface.....	29
	6.3.1 Admin.....	29
	6.3.2 Client.....	29
	6.3.3 ATM Machine.....	29
6.4	Summary.....	29

Chapter 7: Development Environment and Testing

7.1	Development Environment and Tools.....	31
	7.1.1 Platform.....	31
	7.1.2 Editor and Productivity Management Tools.....	31
	7.1.3 Required tools and Modules.....	31
	7.1.4 Technology.....	31
7.2	System Introduce and Testing.....	32
7.3	Comparison with Existing System.....	37
7.4	Summary.....	37

Chapter 8: Conclusion and Future Works

8.1	Conclusion.....	39
8.2	Future Works.....	39

List of Figures

	Page No.
Fig 2.1: ATM Machine	6
Fig 2.2: ATM system	7
Fig 2.3: ATM Fraud	8
Fig 2.4: Card Skimming	9
Fig 2.5: Salisi Gang	9
Fig 2.6: Cash Trapping	11
Fig 2.7: Card Trapping	11
Fig 2.8: Fake PIN Pad Overlay	12
Fig 2.9: Shoulder Surfing	12
Fig 4.1: Waterfall Model	19
Fig 4.2: System Flowchart	19
Fig 5.1: E-R Diagram for ATM Transaction	22
Fig 5.2: DFD Level 0	23
Fig 5.3: DFD Level 1	23
Fig 5.4: DFD Level 2	24
Fig 5.5: Use Case Diagram	25
Fig 6.1: Client-Server Model	28
Fig 7.1: Admin Panel	32
Fig 7.2: Client Interface	33
Fig 7.3: Card Entry and Choosing Authentication Method	34
Fig 7.4: Authentication Methods	35
Fig 7.5: Transaction Process	36

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 a request for cheques, deposit cash and others. 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 with a menu and he/she had to enter the option provided in the menu. For example, when the user wants 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 along with the respective argument, then the payment history is displayed on the screen.

The user also must be given the 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 are 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-paced 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 dispensing cash is the result of an amazingly fast burst of the customer never sees, but a trust is being done in a confidential manner.

1.5 Organization of the Project

In “Introduction”, the 1st chapter of the book contains the information about project motivation, the objective of the project and so on.

In “ATM”, the 2nd chapter of the book contains the information about ATM machine and its security threats.

In “Requirement Analysis”, the 3rd chapter of the book contains the information about system specification, requirement analysis, and feasibility study.

In “Process Modelling”, the 4th chapter of the book contains the information about process model in detail and the system flowchart.

In “System Design”, the 5th chapter of the book contains the detail information about system design which includes E-R diagram, Data Flow diagram, Use Case Diagram.

In “Development Process”, the 6th chapter of the book contains the information about development strategy, system models and system interfaces.

In “Development Environment and Testing”, the 7th chapter of the book contains the information about development environment and tools, productivity management tools. This chapter introduces the implemented system and also tells about testing.

In “Conclusion and Future Works”, the 8th chapter of the book shows conclusion as well as tells about future works on this project.

1.6 Summary

This chapter includes that, ATM is most widely used transaction method. There are several ATM threats nowadays. Our goal is to prevent these threats by creating a system which consists multiple authentication procedures to authenticate the real card holder and secure the transaction. At the end of this chapter shows the organization of the project.

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 customer's 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 world's 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 Card Automatic 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.



Figure 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.

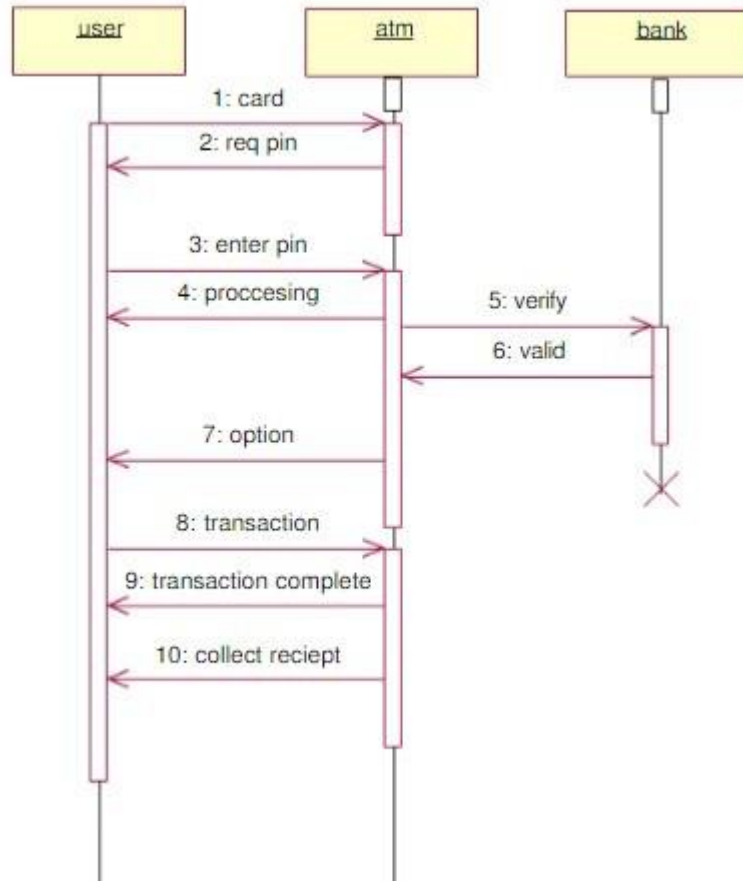


Figure 2.2: ATM system

ATM system works by a sequential process. There is three main module in this system. They are user, ATM and bank. Firstly user enters the card in ATM machine. Then asked a pin number, user input his/her pin number in the system. ATM system then checks the user identity and also verify the user or cardholder. After completing the authentication process ATM system gives the access for the transaction. The 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.



Figure 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 on 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



Figure 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 A M.

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 are 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.





Figure 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.



Figure2.7:Card 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.



Figure 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 backwards.

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 on the internet that installs small cameras to see the actual PIN being keyed-in by the cardholder.



Figure 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.

The best way to prevent this is to transact on ATM machine that is in safe places like banks (inside), malls and other places that have security and well lighted.

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.

2.5 Summary

ATM is Automated Teller Machine which is used for withdrawing, deposit and check balance from an ATM booth. ATM works with the bank by authenticating the cardholder by different types of an authentication procedure for the transaction. In this days ATM technology consists many threats and frauds. These frauds are different types and have different attacking procedure.

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. The user has to send an activation request to the server. Then server side will be responsible for activating the card.

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

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

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

3.3 Functional Requirements

Functional requirements include several parts. These are:

1. Card validation process should work correctly.
2. Card authentication methods such as PIN matching method and Face recognition method must work properly.
3. The transaction process is needed to work fine as above.

3.4 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.

3.5 Feasibility Study

After the requirement analysis, the feasibility study determines whether a proposed system is feasible or achievable, given the organization's 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.

3.5.1 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 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.

3.5.2 Economic Feasibility

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

3.5.3 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 copying with the solution.

3.6 Summary

This chapter includes the project's functional and non-functional requirements to complete this system. We also discussed a feasibility study of different types like technical, economic and operational feasibility.

Chapter 4

Process Modeling

4.1 Proposed System Overview

The following features should be added to 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 Waterfall Model

The Waterfall Model was the first Process Model to be introduced. It is also referred to as a linear-sequential life cycle model. It is very simple to understand and use. In a waterfall model, each phase must be completed before the next phase can begin and there is no overlapping in the phases. The Waterfall model is the earliest SDLC approach that was used for software development. The waterfall Model illustrates the software development process in a linear sequential flow. This means that any phase in the development process begins only if the previous phase is complete. In this waterfall model, the phases do not overlap.

4.3 Workflow in Waterfall Model

System and software requirements: Captured in a product requirements document.

Analysis: Resulting in models, schema, and business rules.

Design: Resulting in the software architecture.

Coding: The development, proving, and integration of software.

Testing: The systematic discovery and debugging of defects.

Operations: The installation, migration, support, and maintenance of complete systems.

Thus the waterfall model maintains that one should move to a phase only when its preceding phase is reviewed and verified.

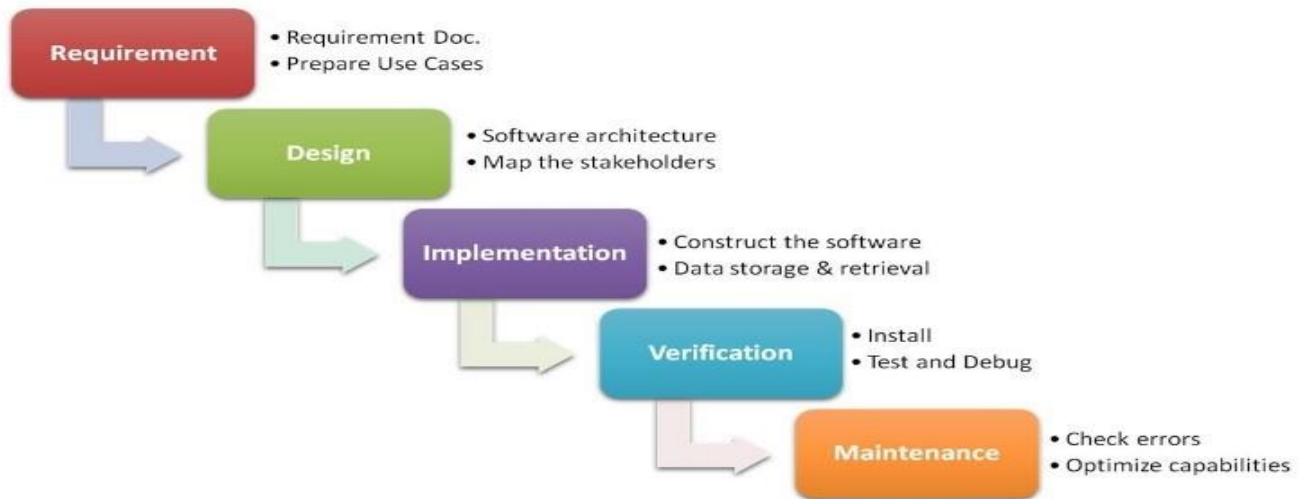


Figure 4.1: Waterfall Model

4.4 System Flowchart

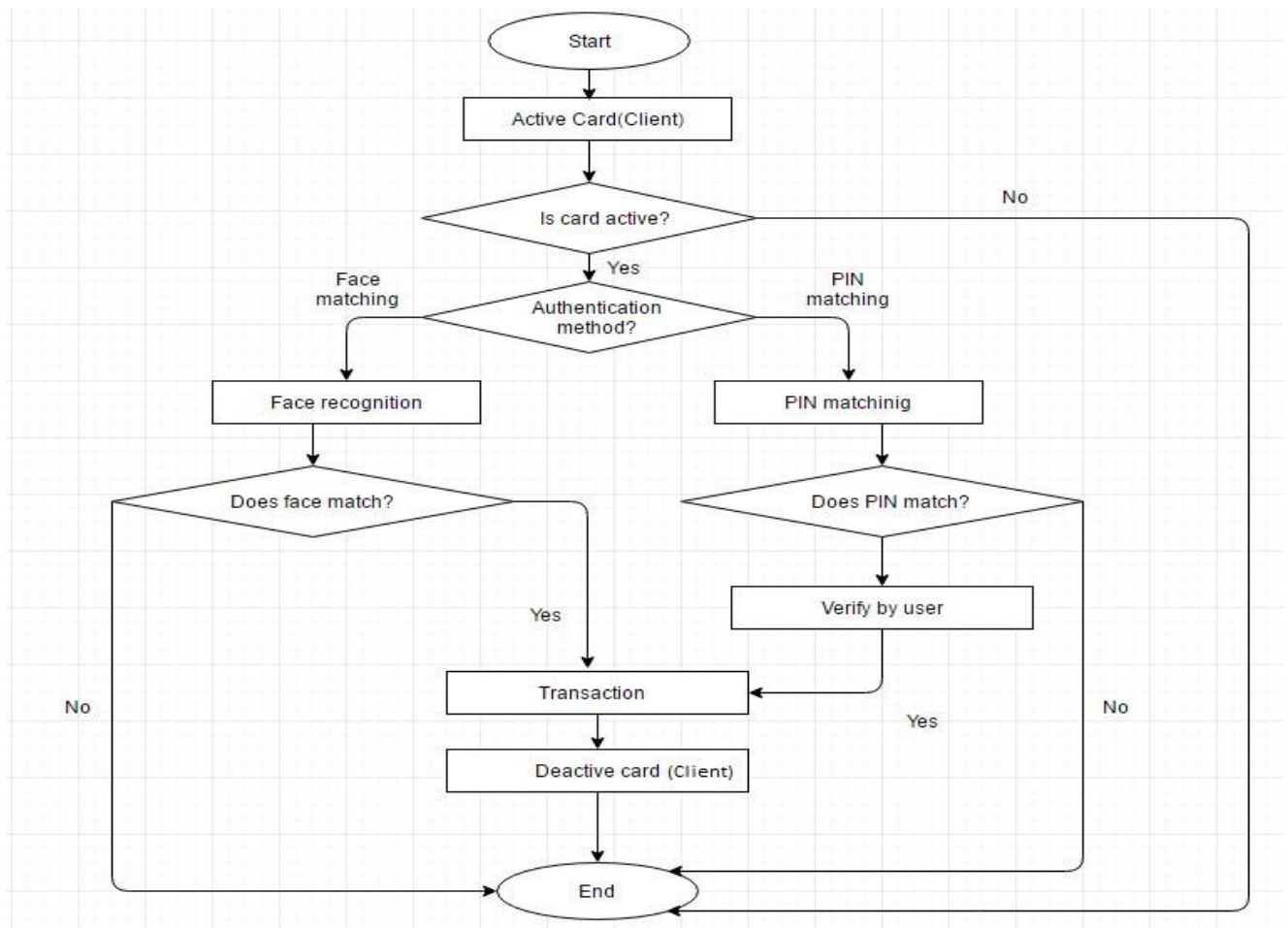


Figure 4.2: System Flowchart

4.5 Summary

This chapter includes the process model that has followed. Waterfall model is followed to complete this project which is very simple to work with. This chapter also shows how the system will work in the figure.

Chapter 5

System Design

5.1 E-R Diagram

In software engineering, an Entity-Relationship Model is an abstract and conceptual representation of data. Entity-relationship modelling is a database modelling 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.

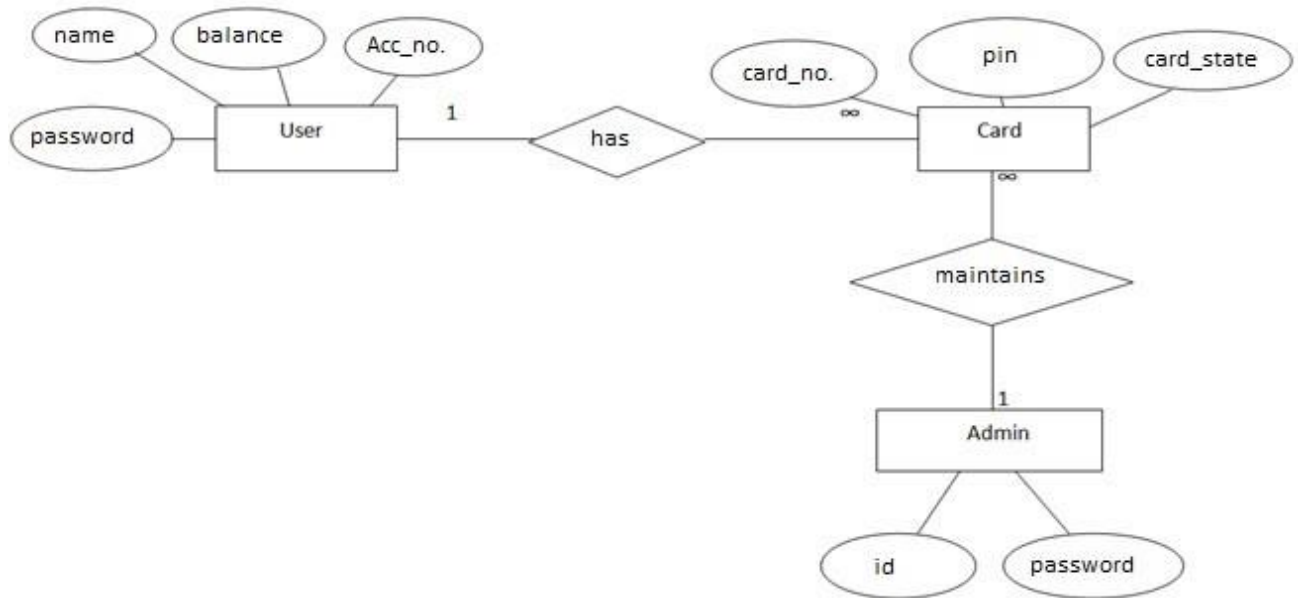


Figure 5.1: E-R Diagram for ATM Transaction

5.2 Data Flow Diagram

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

5.2.1 DFD Level 0

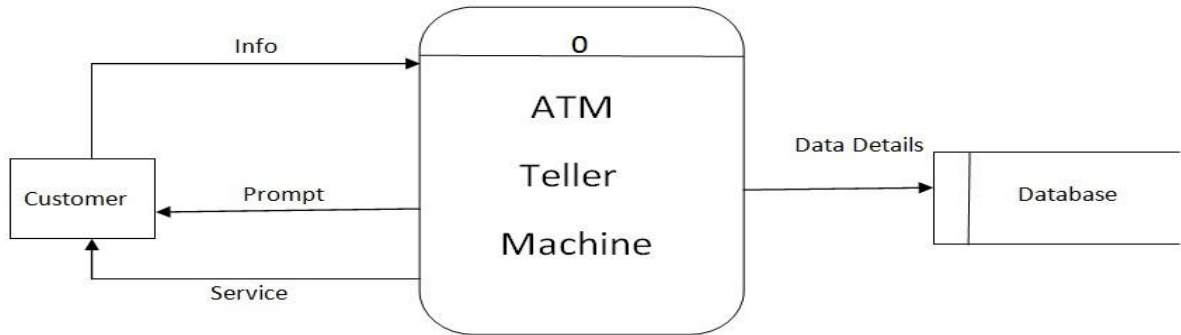


Figure 5.2: DFD Level 0

5.2.2 DFD Level 1

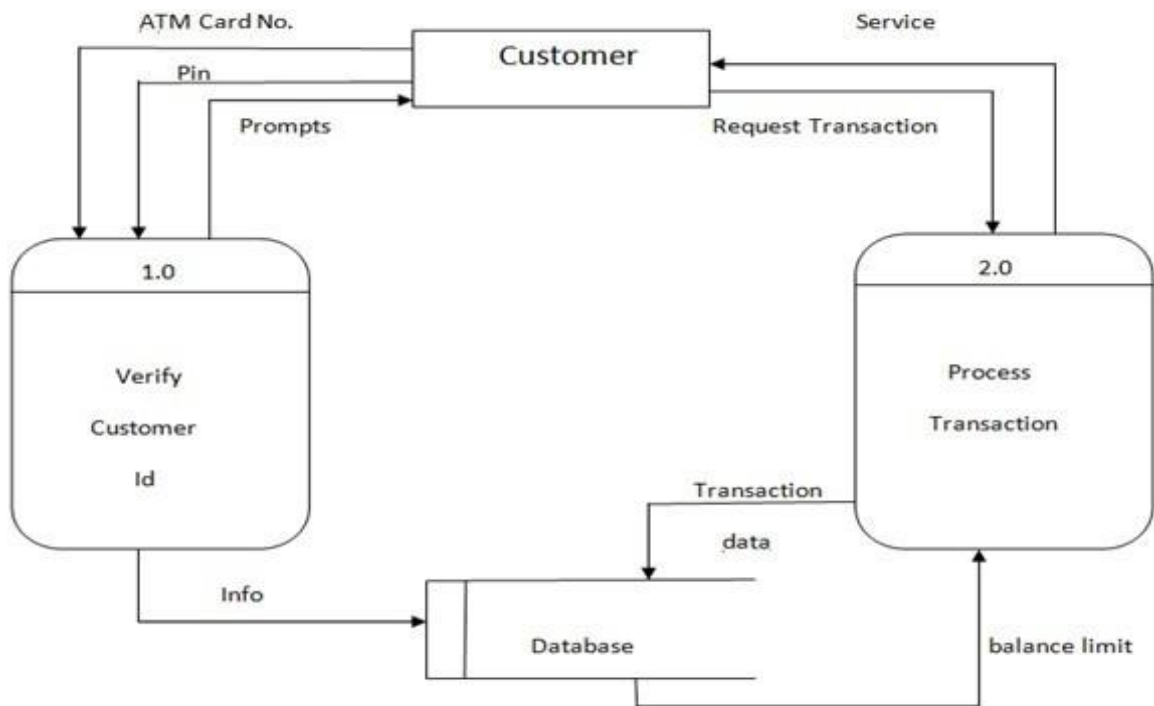


Figure 5.3: DFD Level 1

5.2.3 DFD Level 2

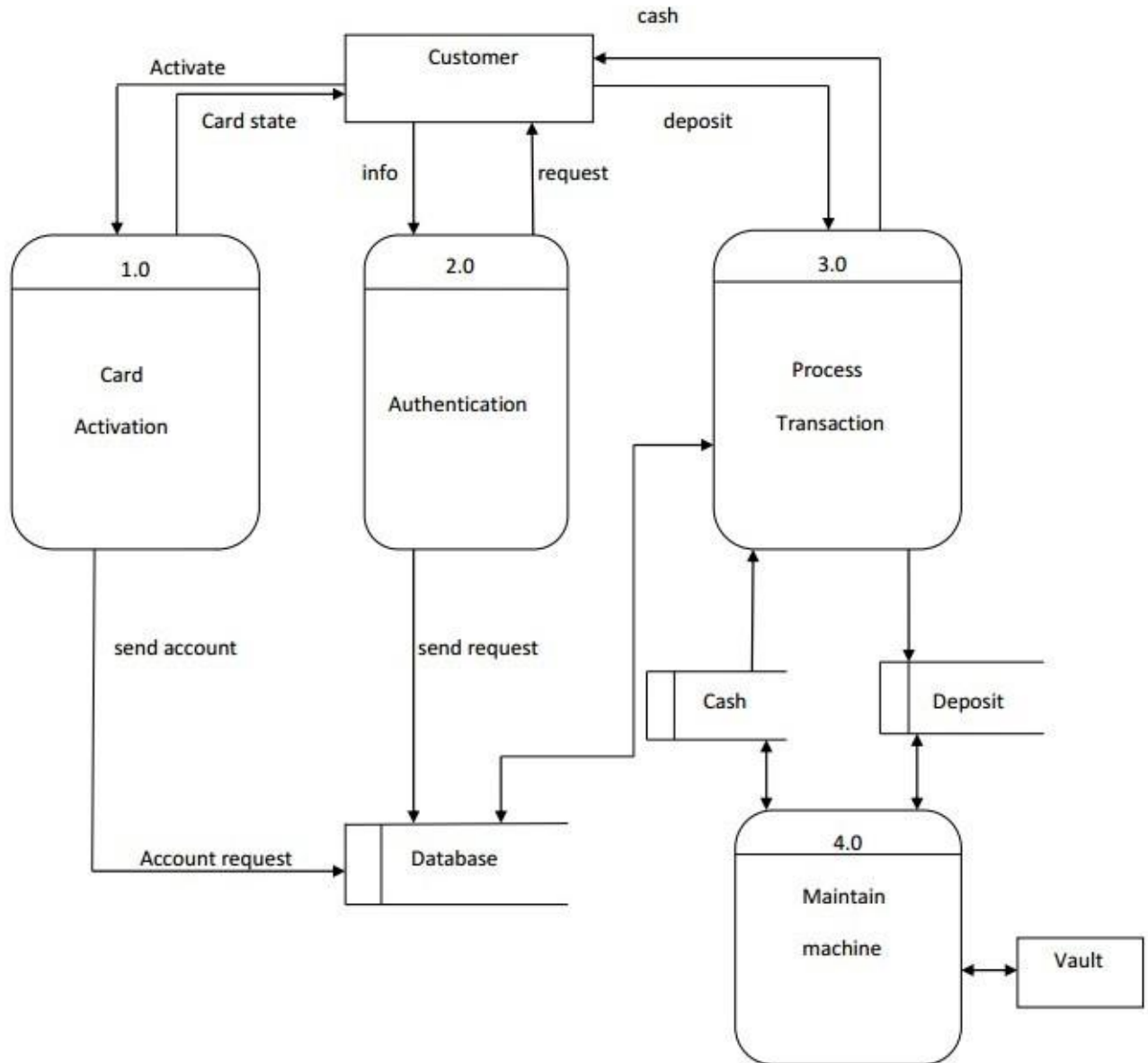


Figure 5.4: DFD Level 2

5.3 UML Design

5.3.1 Use Case Diagram

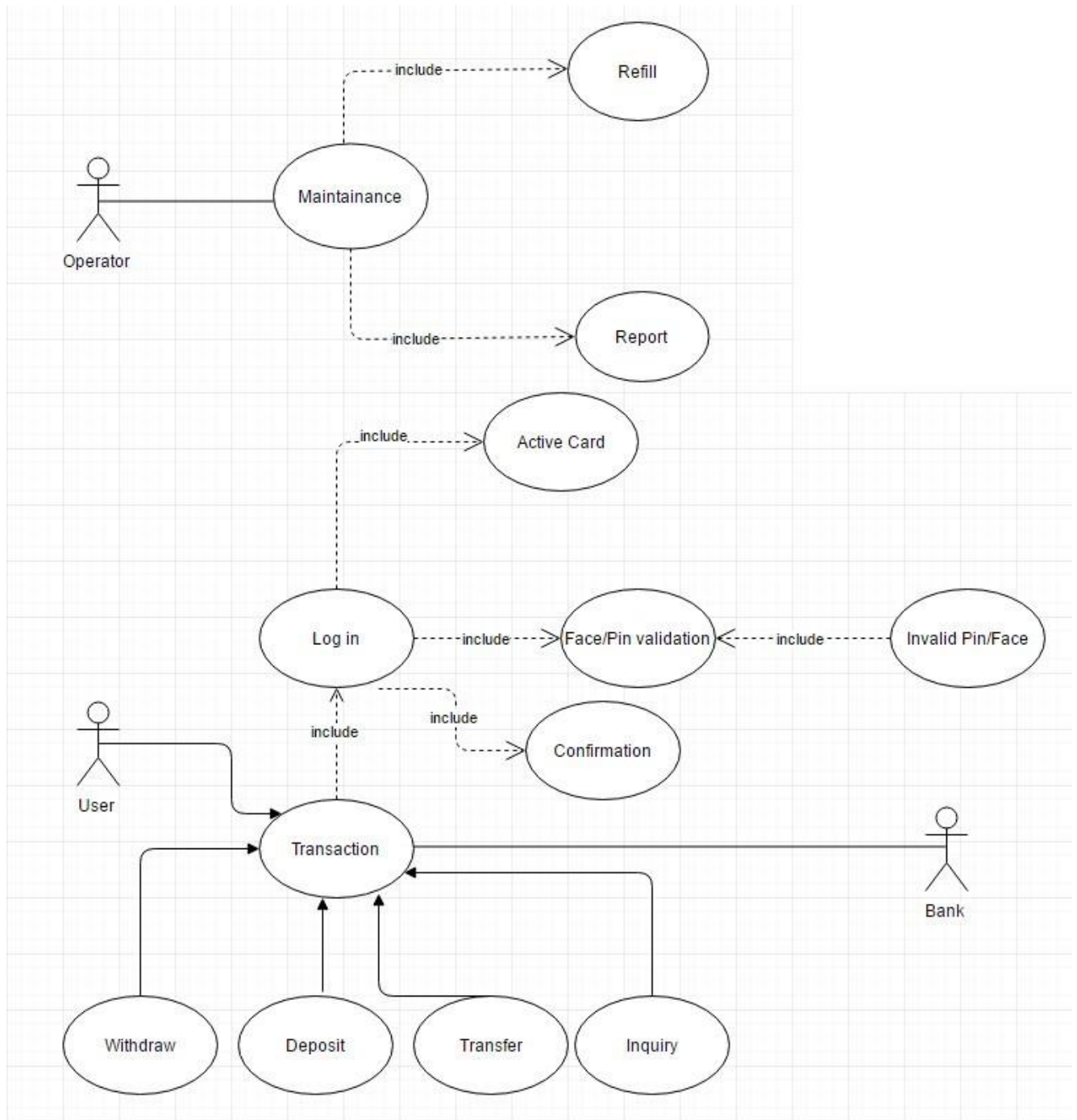


Figure 5.5: Use Case Diagram

5.4 Summary

This chapter shows E-R diagram for showing the entity relation in our database. This chapter discusses data flow diagram for showing the flow of data such as DFD level 0, DFD level 1 and DFD level 2. It also includes use case diagram of the system.

Chapter 6

Development Process

6.1 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.

6.2 System Model

The development model includes server, admin, ATM machine and the user device. The 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 a database. ATM machine device act as usual ATM machine. In other words, it is an automated simulation of real life ATM machine.

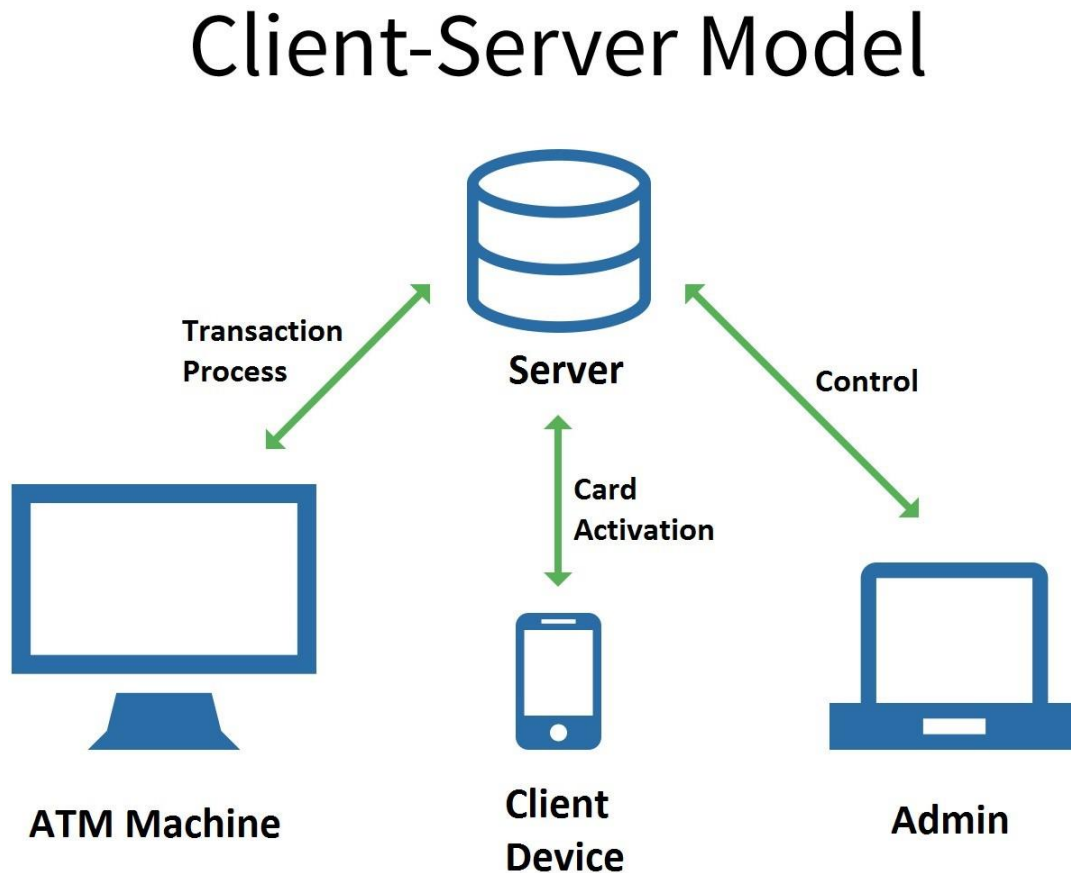


Figure 6.1: Client-Server Model

6.3 System Interfaces

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

6.3.1 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 the 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.

6.3.2 Client

The client can log in his card through the 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.

6.3.3 ATM Machine

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

6.4 Summary

This chapter includes system model and its interfaces. System model shows how the system will interact with different interfaces. There are three interfaces for the system, all of them are well discussed.

Chapter7

Development Environment

And Testing

7.1 Development Environment and Tools

7.1.1 Platform

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

7.1.2 Editor and Productivity Management Tools

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

We used Trello Board as our productivity management tool, Slack for our team management and communications. Git for Version Control System.

7.1.3 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 the image to a numeric array. Python Image Library (PIL) is required to convert normal openCV image to PIL image which is more efficient and convenient to use.

7.1.4 Technology

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

7.2 System Introduce and Testing

The following figure shows Admin panel which will be visible after login as admin. Admin can then perform some action such as Add client, Add card etc.

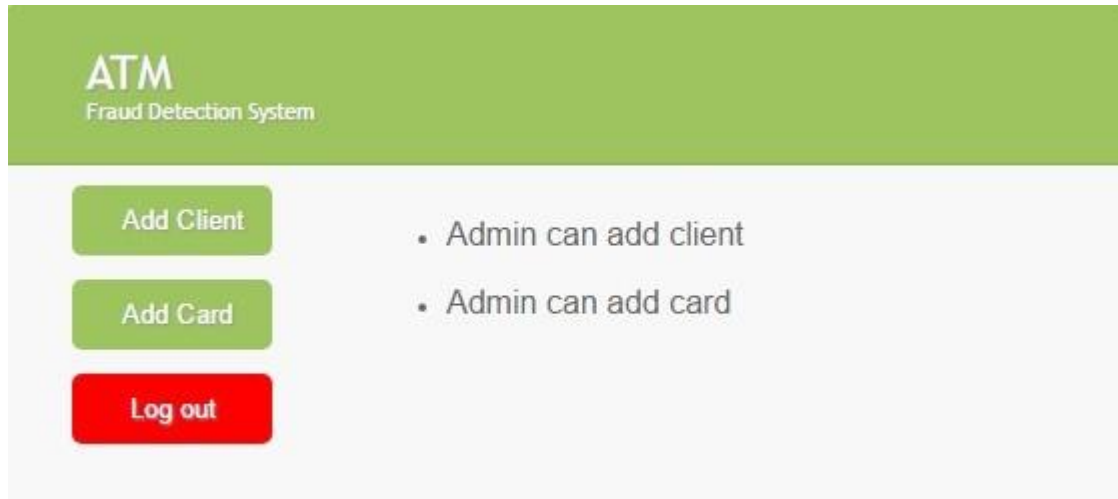


Figure 7.1: Admin Panel

The client should run his application from his device. He should log into Turn On and Turn Off action of the corresponding card.

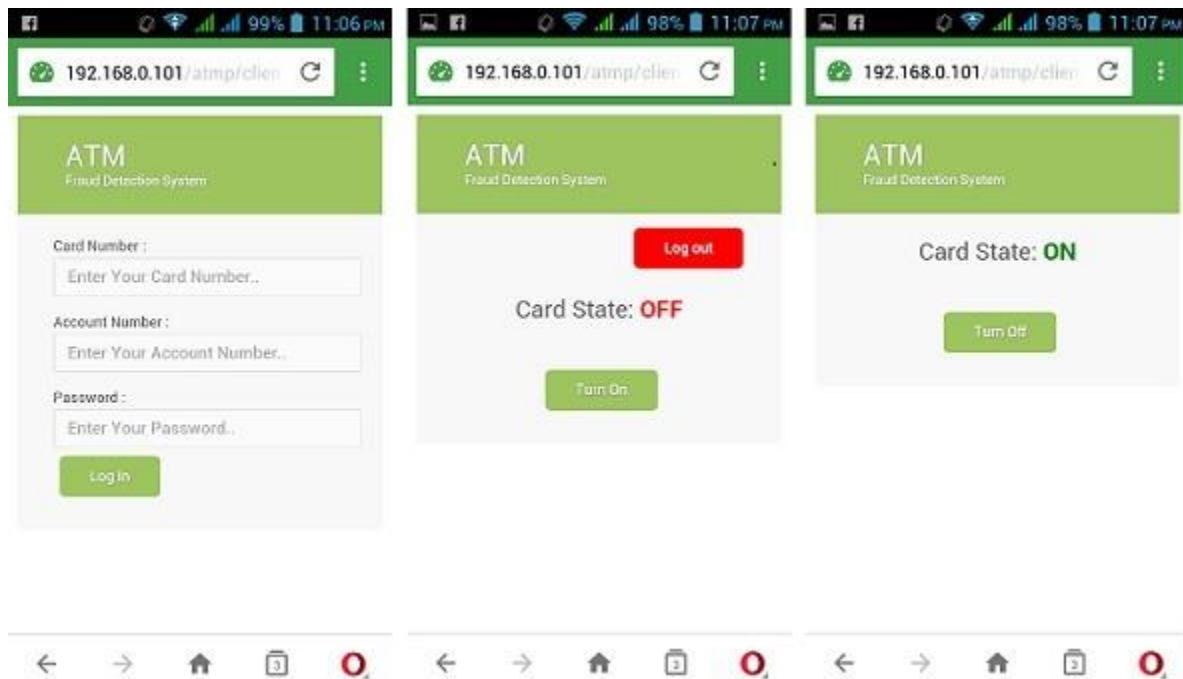


Figure 7.2: Client Interface

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

The figure consists of two vertically stacked screenshots of an ATM interface. Both screenshots have a green header bar at the top with the text "ATM" in large white letters and "Fraud Detection System" in smaller white letters below it.

The top screenshot shows a light gray background with the text "Enter Card Number :" in a dark gray font. Below this text is a white rectangular input field with the placeholder text "Enter Your Card Number..". Below the input field is a green rectangular button with the text "Enter" in white.

The bottom screenshot shows a light gray background with the text "Please choose your authentication method:" in a dark gray font. Below this text are two green rectangular buttons stacked vertically. The top button has the text "Face Recognition" in white, and the bottom button has the text "PIN" in white.

Figure 7.3: 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 the camera. To complete PIN method client should enter the PIN number of the corresponding Card. Then the transaction process start.

The figure displays two screenshots of the ATM Fraud Detection System interface. Both screens have a green header with the text "ATM" and "Fraud Detection System".

The top screenshot shows the face recognition interface. It contains the text "Please press Start button to start face recognition process." and a green button labeled "Start".

The bottom screenshot shows the PIN entry interface. It contains the text "Enter PIN Number :" followed by a text input field with the placeholder "Enter Your PIN...". Below the input field is a green button labeled "Submit".

Figure 7.4: Authentication Methods

These figures show the actual interfaces of transaction method process. The client enters 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 the client and redirect to its default interface.

The figure consists of two vertically stacked screenshots of a web application interface for an ATM Fraud Detection System. Both screenshots have a green header bar at the top with the text 'ATM' in large white letters and 'Fraud Detection System' in smaller white letters below it.

The top screenshot shows the input form. Below the header, there is a label 'Enter Amount :'. Underneath this label is a text input field with the placeholder text 'Enter Your Amount..'. Below the input field is a green button with the text 'Submit' in white.

The bottom screenshot shows the success message. Below the header, the text 'Transaction Succesfull!' is displayed in a large, bold, dark grey font. Below this, the text 'Thank You' is displayed in a slightly smaller, dark grey font.

Figure 7.5: Transaction Process

The system works fine in its initial run. Each and every module is tested well by giving some real and meaningful input. This ensures that unit testing is completed well. The system also ran to test in each integration of modules. Thus the integration testing is completed well. When the project implementation is completed, it ran again to test and find out bugs. After found bugs, we debugged them and ran it. It then ran properly. Hence the system testing process went through different phases and tested well.

7.3 Comparison with Existing System

To figure out the comparison between existing ATM system and this system, we have to know existing ATM system. Existing ATM system prompts the client to enter a card, then it reads the card. It again asks for PIN and read the PIN and match it to the PIN that stored in the database. Finally, the transaction process occurred.

In this system, one has to active his card before use which ensures security to protect several threats. One can choose either face recognition or PIN method as the authentication method. It includes many modern technologies which lead advantage in future works.

7.4 Summary

This chapter tells about our development tools, environment and productivity management tools. It shows the whole system in brief. Several figures are included to understand the system well and determine its functionalities. At the end of this chapter, it figures out the comparison between the existing system and this system.

Chapter8

Conclusion and Future Works

8.1 Conclusion

In ATM Banking a Fraud detection system will run on the bank's server. And it's Function to do the 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 behaviour is recorded and then for the new transaction, it is checked. We have suggested a method for finding the spending profile of cardholders, as well as the application of this knowledge in deciding the value of observation symbols and an 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 the case of internet banking.

8.2 Future Works

Our future plan is to extend the security authentication methods in this system which will lead to meet a great and strong security system. Our initial intention is to work with Irish recognition method. Iris recognition is a method of identifying people based on unique patterns within the ring-shaped region surrounding the pupil of the eye. This authentication method has several advantages, such as very high accuracy of the authentication. There is no way to replicate the eyes. That's why it will be one of the strongest authentication methods. It is also possible to recognize dead human eye, which decreases the physical security threats. Though Irish recognition method will be costly to work with and many research have to do, our clear goal is to deal with it.

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 Stallings, Cryptography and Networks Security.
- [4] Ingemar J. Cox, Mathew L. Miller, Jeffrey A. Bloom, Jessica Fridrich, Ton kalker, Digital Watermarking and Steganography.
- [5] Digital Watermarking, [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: