CREDIT/DEBIT CARD FRAUD DETECTION SYSTEM USING HIDDEN MARKOV MODEL

BY

S. M. ASIFUR RAHMAN

ID: 142-15-3995

AND

NUSRATH JHAHAN

ID: 142-15-3751

This Report Presented in Partial Fulfillment of the Requirements for the Degree of Bachelor of Science in Computer Science and Engineering

Supervised By

Ms. Farhana Irin
Lecturer
Department of CSE
Daffodil International University

DAFFODIL INTERNATIONAL UNIVERSITY

DHAKA, BANGLADESH

MAY 2018

APPROVAL

This Project titled **"Credit/Debit Card Fraud Detection System Using Hidden Markov Model**", submitted by S. M. Asifur Rahman and Nusrath Jhahan to the Department of Computer Science and Engineering, Daffodil International University, has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of B.Sc. in Computer Science and Engineering and approved as to its style and contents. The presentation has been held on 5th May 2018.

BOARD OF EXAMINERS

_____

Dr. Syed Akhter Hossain **Chairman**
Professor and Head
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

_____

Dr. Sheak Rashed Haider Noori **Internal Examiner**
Associate Professor and Associate Head
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

_____

Md. Zahid Hasan **Internal Examiner**
Assistant Professor
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

_____

Dr. Mohammad Shorif Uddin **External Examiner**
Professor
Department of Computer Science and Engineering
Jahangirnagar University

DECLARATION

We hereby declare that, this project will be done by us under the supervision of **Ms. Farhana Irin, Lecturer, Department of CSE,** Daffodil International University. We also declare that neither this project nor any part of this project has been submitted elsewhere for award of any degree or diploma.

Supervised by:

_____

Ms. Farhana Irin
Lecturer
Department of CSE
Daffodil International University

Co-Supervised by:

_____

Rubaiya Hafiz
Lecturer
Department of CSE
Daffodil International University

Submitted by:

_____

S. M. Asifur Rahman
ID: 142-15-3995
Department of CSE
Daffodil International University

_____

Nusrath Jhahan
ID: 142-15-3751
Department of CSE
Daffodil International University

ACKNOWLEDGEMENT

First we express our heartiest thanks and gratefulness to almighty God for His divine blessing makes us possible to complete the final year project successfully.

We really grateful and wish our profound our indebtedness to **Ms. Farhana Irin**, **Lecturer**, Department of CSE, Daffodil International University, Dhaka. Deep Knowledge & keen interest of our supervisor in the field of "*Artificial Intelligence*" to carry out this project. Her endless patience ,scholarly guidance ,continual encouragement, constant and energetic supervision, constructive criticism , valuable advice ,reading many inferior draft and correcting them at all stage have made it possible to complete this project.

We would like to express our heartiest gratitude Prof. Dr. Syed Akhter Hossain, professor and head, Department of CSE, for his kind help to finish our project and also to other faculty member and the staff of CSE department of Daffodil International University.

We would like to thank our entire course mate in Daffodil International University, who took part in this discuss while completing the course work.

Finally, we must acknowledge with due respect the constant support and patients of our parents.

ABSTRACT

The use of credit and debit card has been increased day by day. So the financial fraud or the fraudulent transaction has also increased day by day in today's world because of development of modern technology. With the help of these cards we can make both online and offline payment easily. For online transaction it uses virtual card and for offline transaction it uses physical card. In today's world, credit and debit card provides cashless shopping at every shop. In this fraud detection system (FDS), when a fraudulent transaction is going to be done, it will be detected by this system. A fraud can be detected using Hidden Markov Model (HMM) during transaction. In this project, the sequence of operations in credit card transaction processing system using a Hidden Markov Model and show how it can be used for the detection of fraud. An HMM is initially trained with the normal behavior of a cardholder. If an incoming credit card transaction is not accepted by the trained HMM with sufficiently high probability, it is considered to be fraudulent. At the same time, we try to ensure that genuine transactions are not rejected.

TABLE OF CONTENTS

LIST OF FIGURES

FIGURES **PAGE**

LIST OF TABLES

TABLES **PAGE**

CHAPTER 1

INRODUCTION

1.1 Introduction

At present online transactions are increasing day by day to purchase goods and getting services. A very recent survey stated that 27% of cardholders (debit, credit and prepaid) around the world have faced fraudulent transaction in the last five years [1]. It shows that a high percentage of credit cardholders are in security threat. Credit card can be used in offline and online transaction. It can be classify into two types:

1. Physical credit card transaction.
2. Virtual credit card transaction.

In physical credit card transaction the cardholders has to produce the card to the merchant counter and the merchant will insert the card into EVM (Euro pay, MasterCard and Visa) machine. Fraudulent transaction may happen in this mode. It is very difficult to detect fraud in this type of transaction. If the cardholders does not understand the stealing of card it can cause a vast amount of loss for the issuing authorities.

Virtual credit card transaction is used for purchasing something in online. So, these kind of transactions happens in Internet through some merchant sites payment gateway. To make this kind of transaction happen card holder needs to provide details information such card number, validity CVV number, name of the card holder etc. There is also a huge chance of fraudulent transaction and loss of money in this mode too.

Nowadays hackers are using various techniques to steal the details about card. The most dangerous thing about the fraudulent transaction is that the cardholders doesn't know his/her information about credit card has been stolen until major damage done.

There are different theories or approaches has been given in the past. These are -

Fuzzy-Darwinian Detection, Blast-SSHAHA model, Bayesian and Neural Network, Fusion of Dempster–Shafer theory and Bayesian learning etc.

A Hidden Markov model is a system which is assumed to be a Markov process with hidden states. Each states is linked with probability distribution. A Hidden Markov Model can be represented as the simplest dynamic Bayesian Network.

1.2 Motivation

Now a days people using internet for their daily life transaction like shopping, online banking etc. It will be increased day by day with the development of modern technology. On the other side, financial fraud also increasing day by day with development so every year people loss billion of money. To reduce these type of crime or fraud we build a system using Hidden Markov Model.

1.3 Objectives

It will help the people to keep safe their money from the thief. Now a days most of the transaction happened via card rather than cash. People shopping from online market via their card. This system will provide them an easy and well security so that their money can't take by the thief. It will also provide the more secured online banking system.

1.4 Advantages

1. The proposed project detects fraud much faster.
2. The probability of finding the fraud is much better.
3. The system has less complexity.
4. It will reduce the tedious work of the employees in the bank.

1.5 Report Layout

In this report, we have organized the rest of part as follows, we have discussed about background with related works, related studies, Hidden Markov Model in chapter 2. Then in chapter 3, we described about Business Process Modeling, use case modeling, use case description, design requirements. In chapter 4, we have conversed about design and implementation plan. In this section, we have discussed about front and backend design, Interaction design and UX. After that in chapter 5, we have discussed about Implementation of our fraud detection system and testing implementation. Finally we have concluded the report with future scopes and limitations in chapter 6.

CHAPTER 2

BACKGROUND

2.1 Introduction

In this chapter we will discuss how we can stop credit/debit card fraud. How a consumer will be helpful when they lost or stolen card. Also will be discuss about identity theft. Also about fake and Counterfeit card will be also discuss hear, different kind of technique we will follow on credit card fraud detection system. Here we will discuss about Fuzzy-Darwinian Detection.

Blast-SSAHA model, Bayesian and Neural Network, Fusion of Dempster–Shafer theory and Bayesian learning.in this chapter Hidden Markov Model and Bayesian Network will also discuss.

2.2 Comparative Studies

Several techniques are used in credit/debit card fraud. As the technology is changing faster the techniques of the fraudsters are also changing. Now I am describing about some common techniques –

2.2.1 Lost Or Stolen Card:

When a card is lost or stolen, owner of the card needs to inform the issuing bank. But, it is still possible for thief to make unauthorized purchase and this is the main reason of credit card fraud. Almost 48% damage is done by this way. [7] All credit card has one common security measure and it is called signature. It is very easy for a thief to forge. Some merchants demand photo ID such as driving license, national ID card etc. to identify the original users. But in some law it is illegal. Some credit card company provides photo of the user which is more easy way to breach the security.

2.2.2 Identity Theft:

This reason costs almost 15% fraud. [7] Identity theft can be divided into two parts. These are –

- **Application Fraud:** This fraud takes place when a thief still the information of a person or create fake data to open account. After creating the account with fake information the hacker takes full advantages of it, until he/she get caught.
- **Account Takeover:** In this method criminal may pose as original user and gain control over the account. At first fraudster takes control of the account by providing customers account number or credit card number. Then the fraudster communicates with the card issuer company masquerading as original user and asks for mail to be redirected to a new address. After finishing this steps the fraudster reports that the card is lost and asks for a replacement.

2.2.3 Fake and Counterfeit card:

Fraudsters are continuously finding new and innovative ways for counterfeit cards. Lost or stolen card and the generation of counterfeit cards together creates the biggest threat. Some common techniques of counterfeit cards given below –

2.2.3.1 Skimming:

Most of the cases counterfeit fraud occurs by skimming. In this way thief can produce victim's card using basic methods such as photocopying receipts or using electric device to swipe and store victims card number. Skimming causes 14% credit card fraud. [7]Skimming is the most preferable and fester growing process of credit card fraud. It is found that the employees or cashiers of business establishment are carrying pocket skimming device. It is a battery operated small magnetic stripe reader, in which they swipe the cards very easily and gets the information they need. Skimming occurs unknown to the cardholders and it is very difficult to trace. If the cardholders are unaware it can cause a major damage.

2.2.3.2 Creating Fake Cards:

This is a very common process of credit card fraud. Although it takes a lot of time and skills for the fraudsters to produce. They create a fake card from scratch using sophisticated machine. Recent cards has many features to make it difficult as much as possible. Introduction of hologram in almost every card makes it more difficult to forge.

2.2.3.3 Magnetic Stripe Erasing:

A fraudster can tamper a card by erasing the metallic stripe with powerful electro magnet. Then the fraudster temper with the details of the card so that they match fully with the details of original cards. When a fraudster starts to use the card the cashier will swipe it through terminal several times before understanding the metallic stripe is not working. Then the cashier will manually input the card details into terminal. This is a high risk form of credit card fraud.

2.2.4 Cloning a Site:

In this process the criminal can clone a site completely or just the pages from which we are placing orders. Here the customers haven't any reason to think they are not dealing with the original company they wished to. This cloned site will also send an email after receiving the card details as original. So the customers will not suspect anything. But the fraudster gets the data and able to do whatever he/she want.

2.2.5 False Merchants Site:

These sites are often makes very cheap offers to the customers. This sites requests to the customers to fill up some details to get access in some certain content's. Most of this sites are claim to be free but requires valid credit card details to verify the age. This sites are set up for gathering credit card information as much as possible. They doesn't take charge for any of their services. They are actually a part of large criminal network.

From all the discussion it is very much clear that credit card fraud is a big threat already and if the security process is not enough it will become more dangerous in upcoming future.

2.3 Related Works On Credit Card Fraud Detection System:

Here, I want to discuss about some of the credit card fraud detection techniques briefly which are given in the past. This discussion will contain the advantages and drawbacks of those techniques. These are -

1. Fuzzy-Darwinian Detection.
2. Blast-SSAHA model.
3. Bayesian and Neural Network.
4. Fusion of Dempster–Shafer theory and Bayesian learning.

2.3.1 Fuzzy-Darwinian Detection

Uses genetic programming for developing fuzzy logic. Genetic programming algorithm is used to search the information that is wanted. The accuracy rate of fuzzy system is very high and it also has low false alarm rate. But it slows down the system and very expensive. [1][2]

2.3.2 Blast-SSHAHA model

Is composed by BLAST and SSAHA two algorithms. This two algorithms are capable of sequence aligning to detect credit card fraud. It is also acquainted as BLAH-FDS algorithm. It has two stage of sequence alignment. One is for incoming transactions in the past and another for genuine transactions made in the past. The speed and accuracy of this model is good. But it hasn't got the capability of detecting duplicate transaction or cloned credit card fraud. [3]

2.3.3 Bayesian and Neural Network

Both are suitable approaches for dealing in uncertainty. In general it uses artificial intelligence programming and machine learning methods in neural network and Bayesian network is used for developing particular pattern to understand the spending behavior of customers. Neural network learn by itself. So there is no need to reprogram. It has good accuracy but need a long term training to reduce the slowness. [3]

2.3.4 Fusion of Dempster–Shafer theory and Bayesian learning

Mainly consists of four elements. These are Rule based filter, Dempster–Shafer adder, Transaction history database, Bayesian learner. In this four steps the system analyze customers past and present spending behavior together based on particular purchase. This system has high accuracy and also improves the fraud detection. But it is very expensive and system speed is less. [1].

2.4 Hidden Markov Model:

Hidden Markov Model is a double embedded stochastic process with two hierarchy levels [6]. It is the simplest, easiest and most secure approach to predict something related to time series [4]. The concept of Bayesian network very important to understand Hidden Markov Model. A brief concept of Bayesian network is given below -

2.4.1 Bayesian Network

Represents the casual probabilistic relationship among a set of random variables, their conditional dependencies and it provides a compact representation of joint probability distribution through directed acyclic graph. So it consists of three important parts. These are -

1. Probability.

2. Conditional probability distribution.

2.5 Challenges

Accomplishment challenges are this type of task which is really difficult to overcome. But things can be solved. There are a lots of challenges came ahead to develop the fraud detection system such as clustering, Hidden Markov Model training, transaction process, stores data properly etc.

CHAPTER 3

REQUIREMENT SPECIFICATION

This chapter is based on Business Process Modeling, Use Case Model, Use Case Description, Complete System Diagram and Design Requirements.

3.1 Business Process Modeling

Business process modeling is mapping out regular business process and finding ways to improve them. It is a part of the practice of management. Process modeling software gives an analytical representation of a processes in an organization.

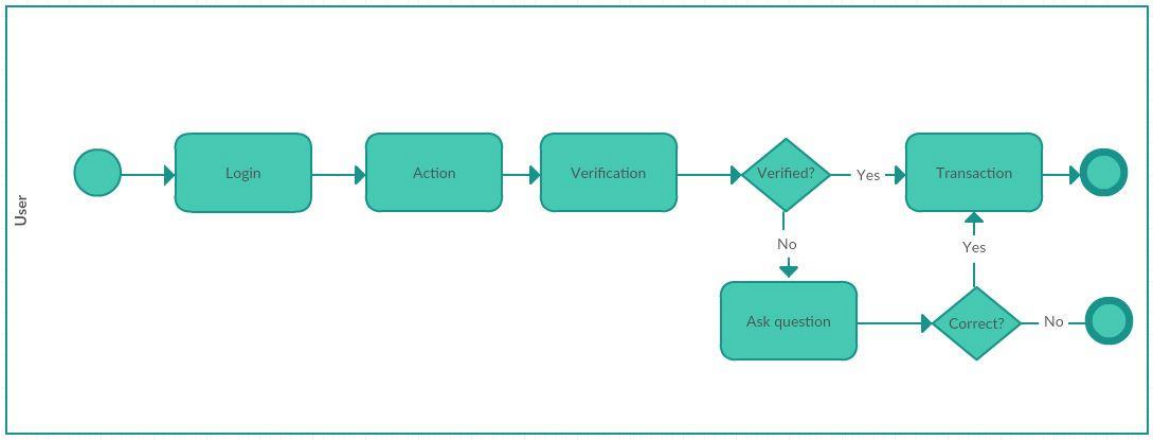

Figure 3.1: Business Process Modeling

Our first step in modeling is actually pen and paper. However, to actually run a business process, we will need to digitize that process in a way that a workflow engine can understand. Business process modeling tools allow us to represent out process in a digital way that can be transferred to a live automated process.

3.2 Use Case Model

The high-level use case diagram is shown in **Figure 3.1**and is discussed below in terms of the functionalities and the relationships between different use cases.

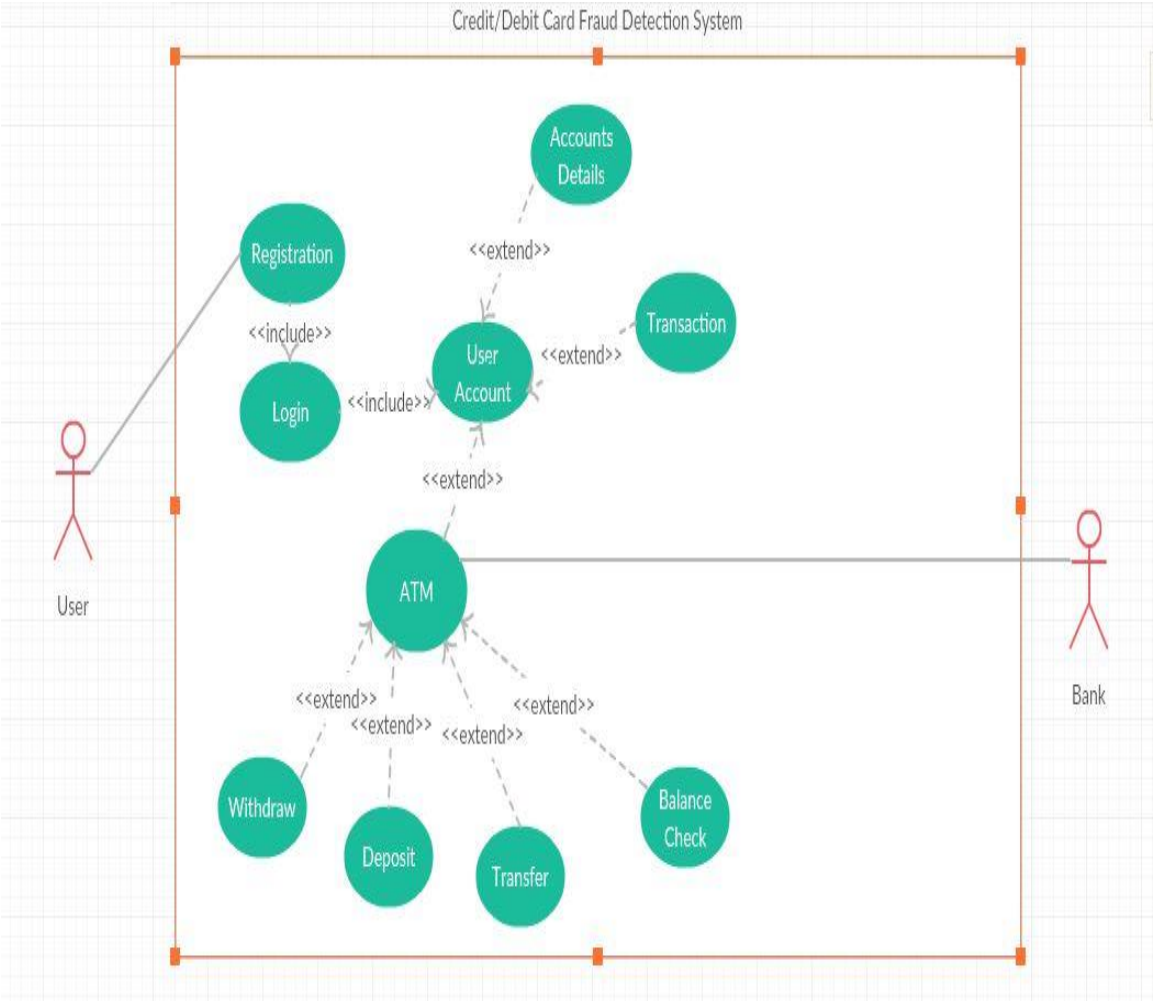

Figure 3.2: Use Case Model Diagram

3.2.1 Use Case Description

In this section we describe some of the use cases of the use case diagram. They are describe below:

3.2.1.1

Use Case ID: UC-01

Use Case: Login

Actor: User

Description: This use case description describe the scenario where the user have to login.

Pre-Condition: If you are new, than registration as a user.

Post Condition: Login, Transaction, Security check.

Normal Flow:

1. Open the home.
2. If you are new user, than at first registration your account.
3. If you already have an account, than just login.

Alternative Flow:

1. User name or Password incorrect.

3.2.1.2

Use Case ID: UC-02

Use Case: Account Details

Actor: User

Description: This use case describes the scenario where the user can know the details of his/her user account.

Pre-Condition: Registration, Login. User Account.

Post Condition: Transaction.

Normal Flow:

1. Enter into the home page.
2. Login in your profile using your user name and password.
3. Click on My Dashboard.
4. Select account details from dropdown.

Alternative Flow: None**.**

3.2.1.3

Use Case ID: UC-03

Use Case: Withdraw.

Actor: User

Description: This use case describes the scenario where the user can withdraw their deposited money.

Pre-Condition: Login, Select ATM

Post Condition: None.

Normal Flow:

1. Open home page.
2. Select login.
3. Enter user name and password for login.
4. Select ATM.
5. Enter your pin number.
6. Select withdraw from options.

Alternative Flow: None.

3.2.1.4

Use Case ID: UC-04

Use Case: Balance Check.

Actor: User

Description: This use case describes the scenario where the user can check their balance.

Pre-Condition: Login, Select ATM, Enter Pin.

Post Condition: none.

Normal Flow:

1. Open the home.
2. Select login.
3. Enter user name and password.
4. Select ATM.
5. Enter Pin Number.
6. Select Balance option.

Alternative Flow: None**.**

3.3 Complete System Diagram

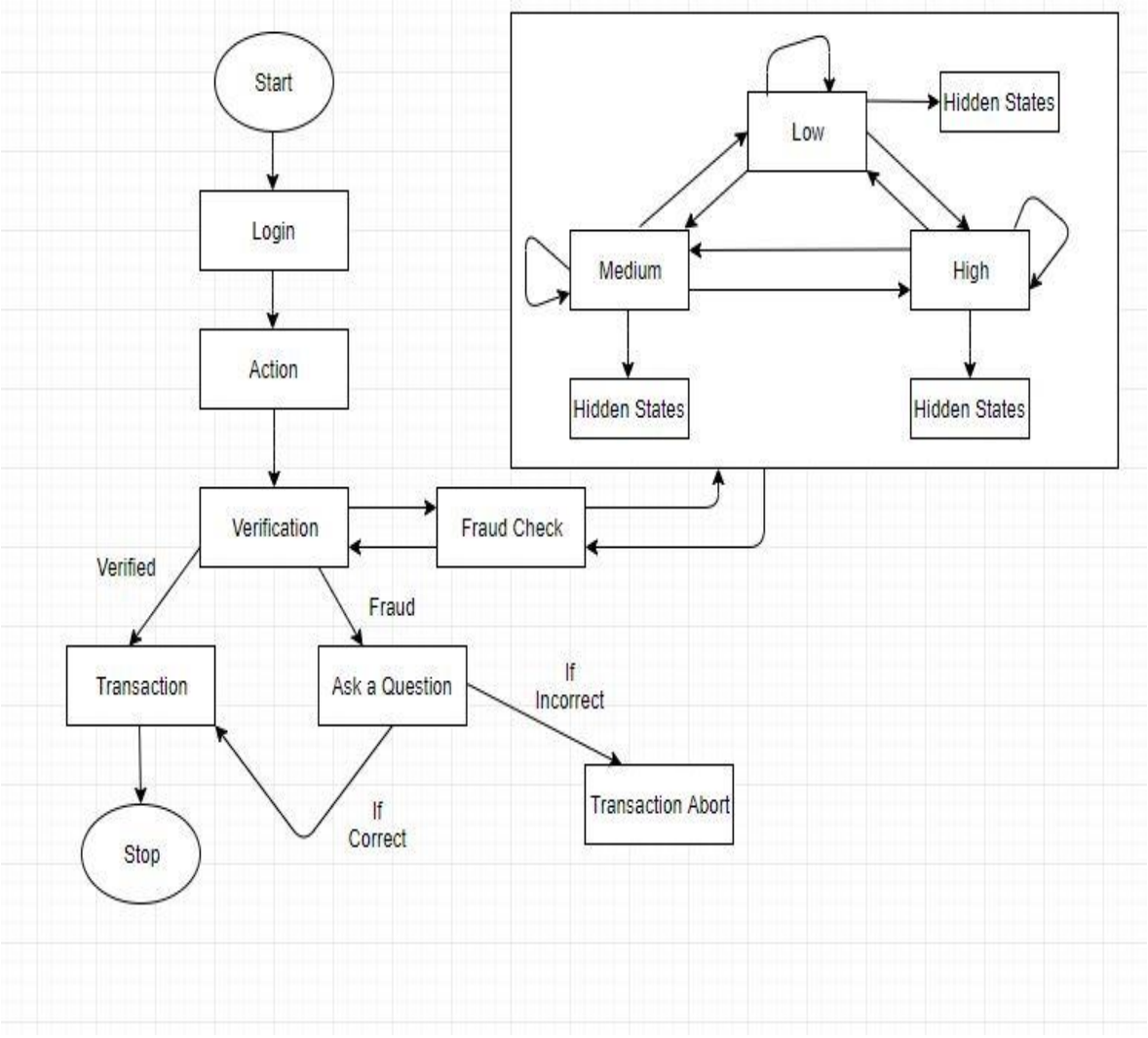

Figure 3.3: Complete System Diagram

The diagram shows complete view of the system. At first user needs to login to do any kind of transaction. Then the user selects the item for purchase or the category of the transaction. After that verification process starts. In verification process there are four categories of user's low, medium and high. From the initial probability which is provided to the system, it calculates the probability of the next transaction based on some hidden states. I have selected the threshold value for the system is 0.5 or 50%. So the system will detect the next transaction genuine if the outcome is 50% or more. If it is less than 50% the system will ask some security question to the user which is only known to the original user. If he/she able to answer those questions, then system will enable the transaction procedure. Otherwise it will stop the transaction and the authority will take the further action.

3.4 Design Requirements

In this system, we used some web programming language such as HTML, CSS, Java Script. We use MySQL database server. This project mainly using JSP and Servlet with core java.

HTML is a markup Language used to structure text and multimedia documents and to set up hypertext links between documents, used extensively on the World Wide Web.

CSS is the language for describing the presentation of web pages, including colors, layout and fonts. CSS is independent of HTML and can be used with any XML-based markup language.

JavaScript is the programming language of HTML and the web. It's easy to learn. It is one of the three core technologies of WWW content production. It is used to make web pages interactive and provide online programs, including video games.

MySQL is the world most used open source relational database management system that runs as a server providing multi user access to a number of database.

CHAPTER 4

DESIGN SPECIFICATION

This chapter is about the design of our project and the methodology. Also about how we implement our project.

4.1. Design

4.1.1 Home Screen

A user when start or open our app, they can see this home screen at first.

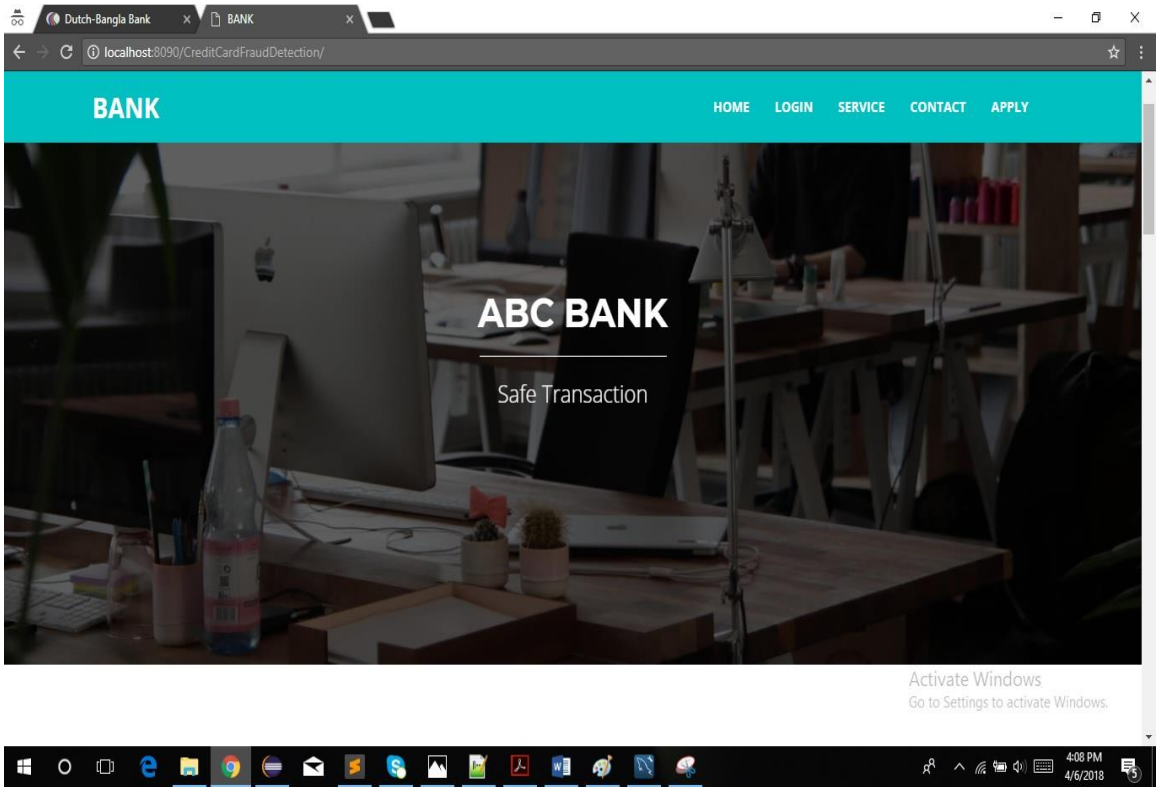

Figure 4.1.1.1: Home Screen

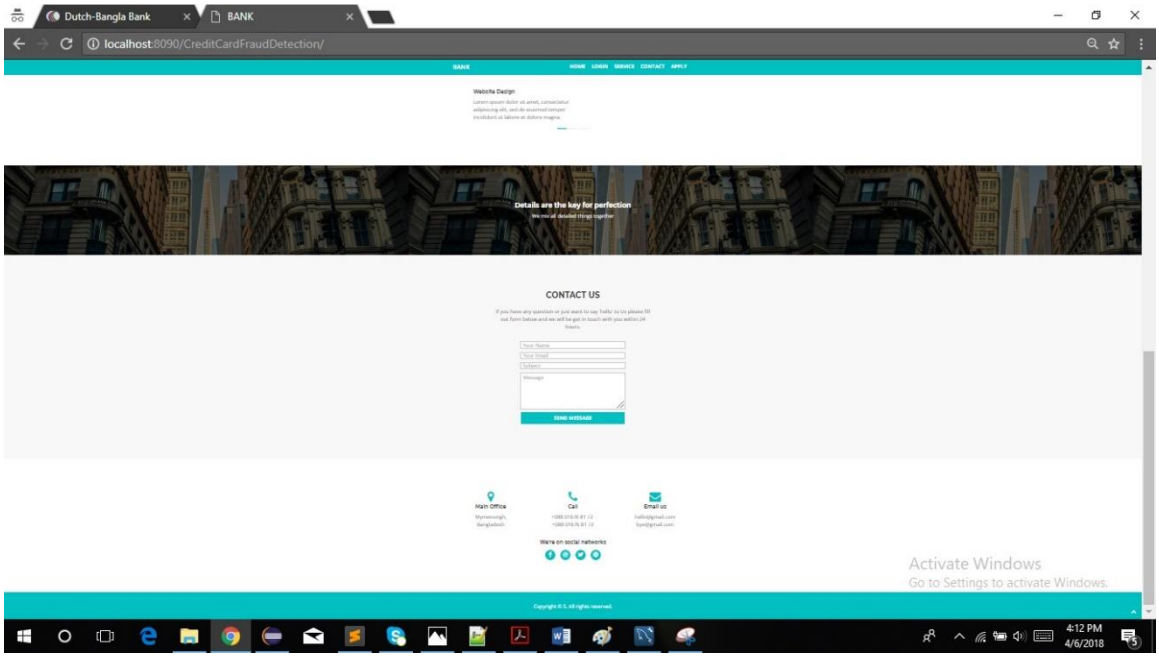

Figure 4.1.1.2: Home Screen

4.1.2 Login Screen

Here user need to login in their account using their user name and password.

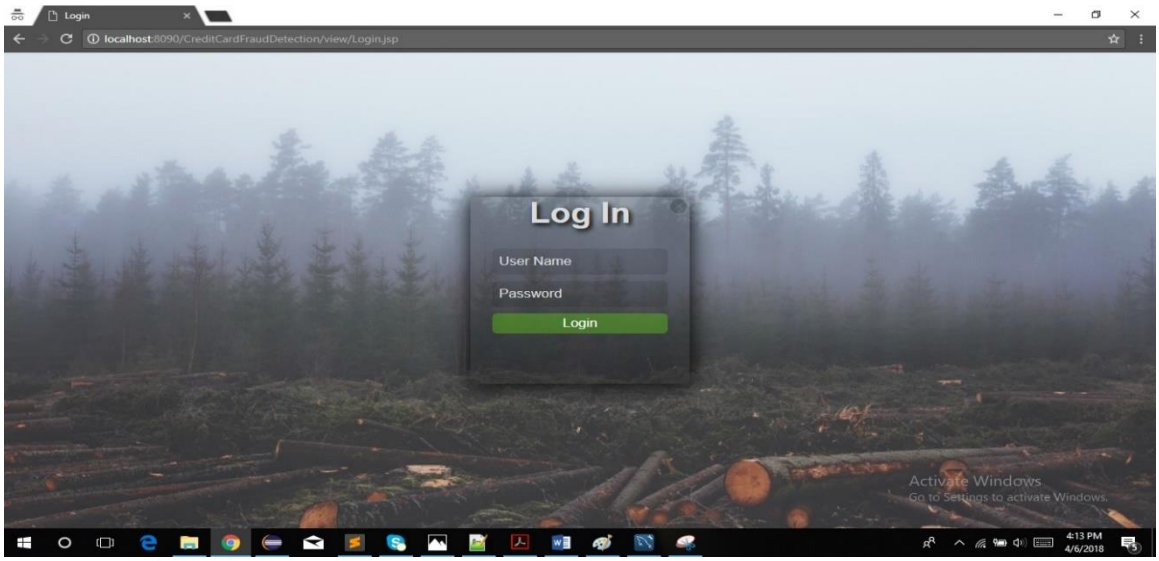

Figure 4.1.2.: Login Screen

4.1.3 User Home Screen

This is the user home screen after login.

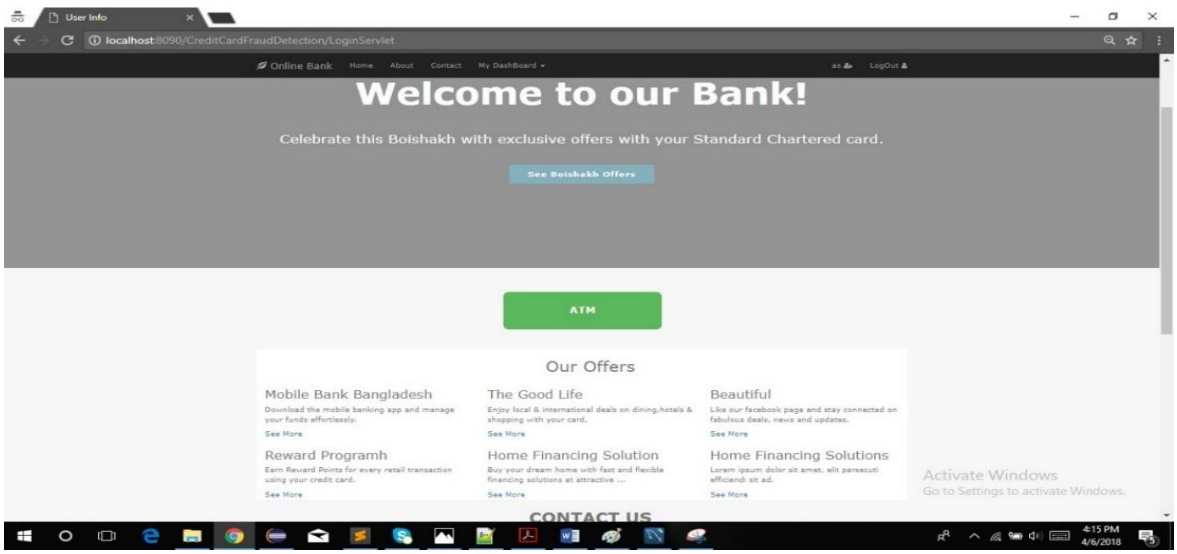

Figure 4.1.3.1: User Home Screen

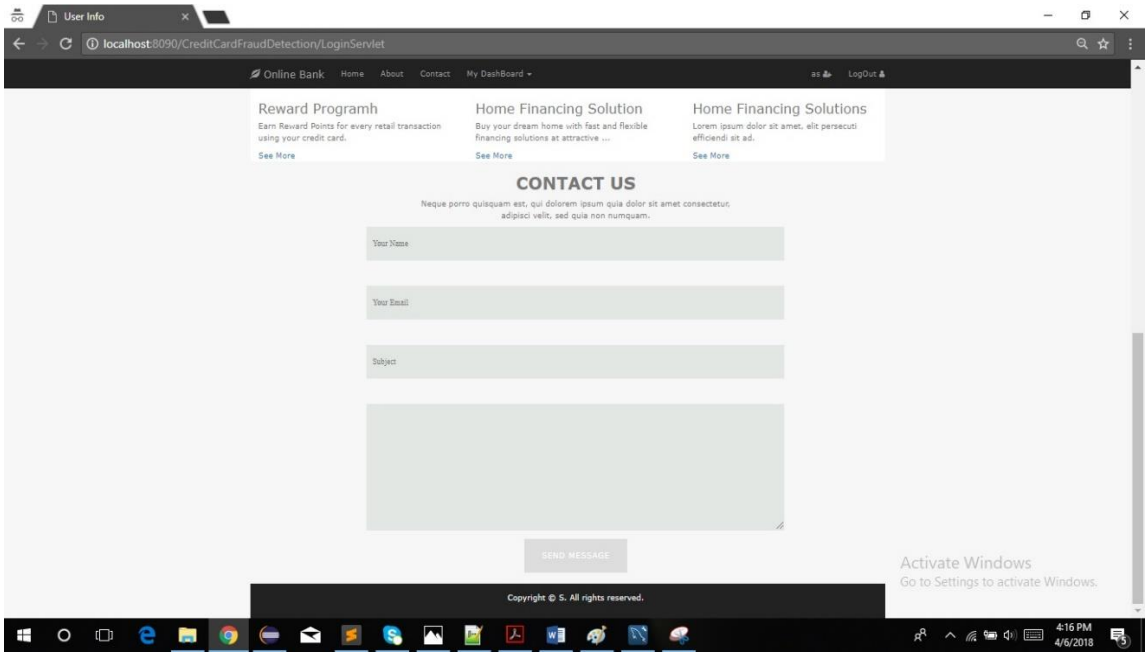

Figure 4.1.3.2: User Home Screen

4.1.4 Account Details Screen

This is the users account details page.

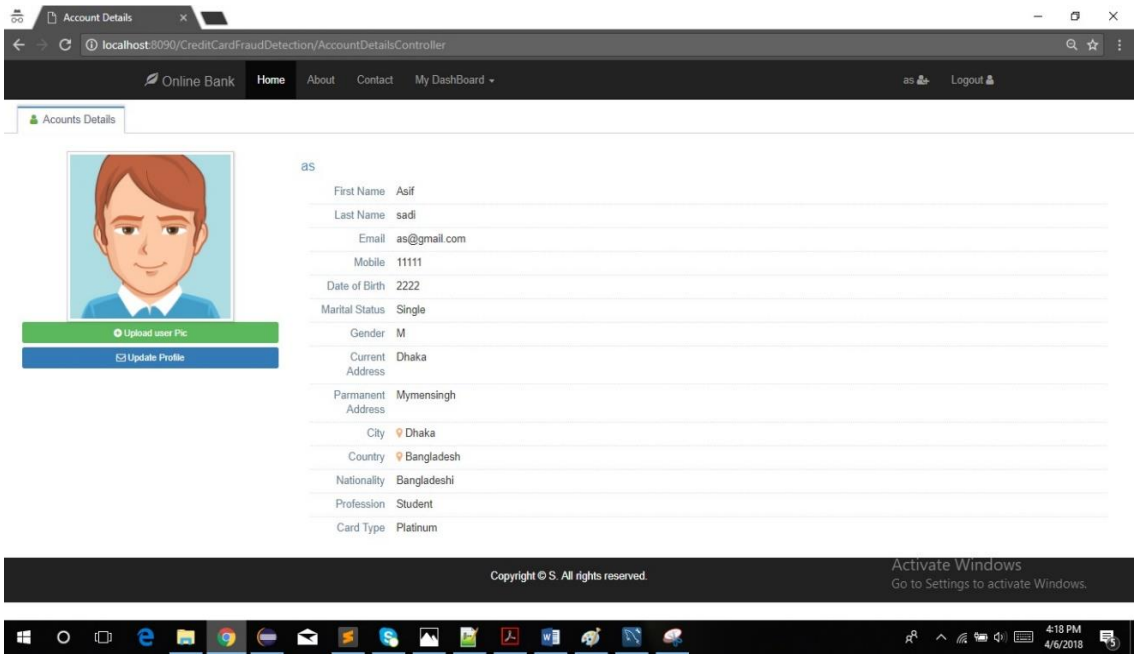

Figure 4.1.4: Account Details Screen

4.1.5 User Transaction History Screen

A user when start or open our app, they can see this home screen at first.

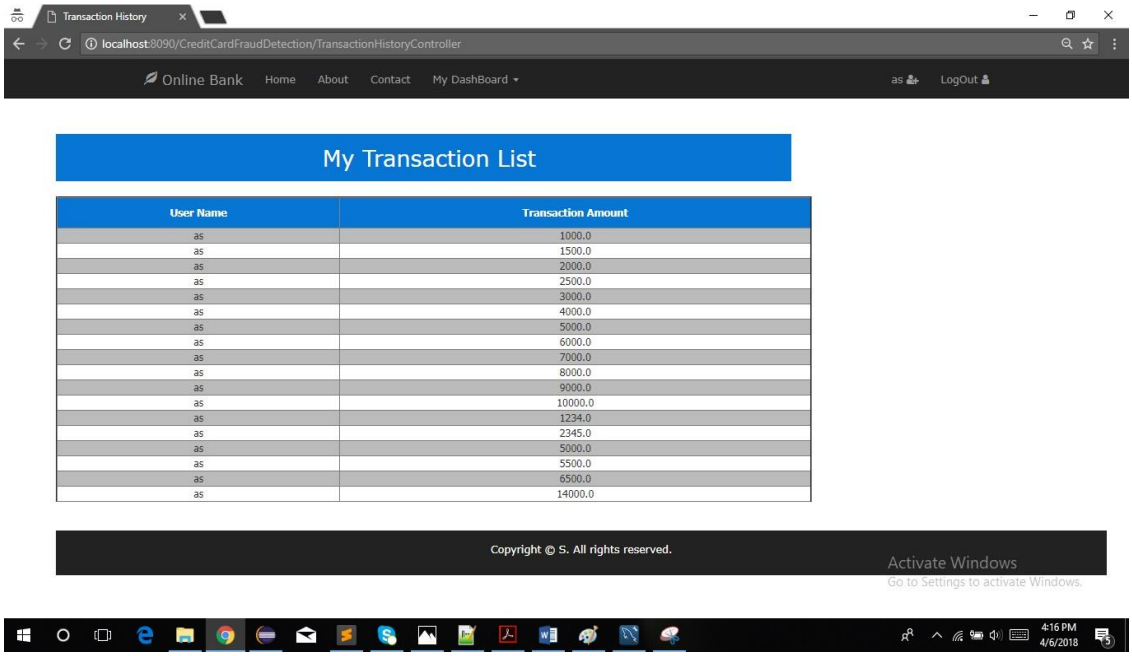

Figure 4.1.5: Transaction History Screen

4.1.6 ATM Screen

This is the ATM starting screen.

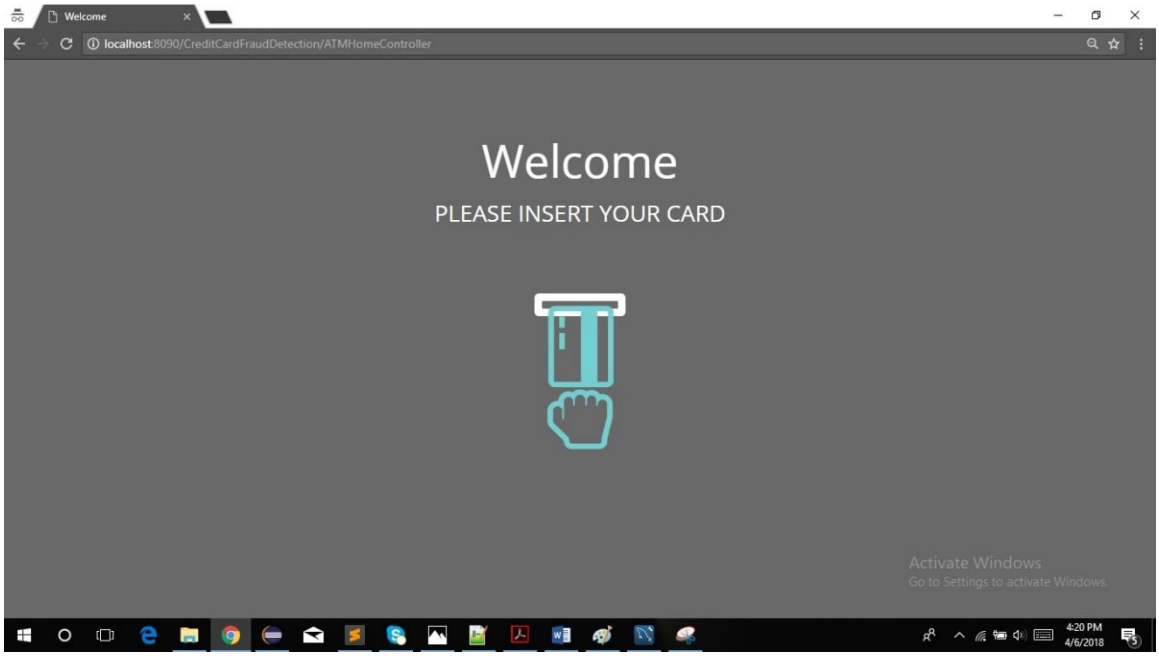

Figure 4.1.6.1: ATM Screen

4.1.6.2 Pin Screen

Here user need to enter his/her card pin number.

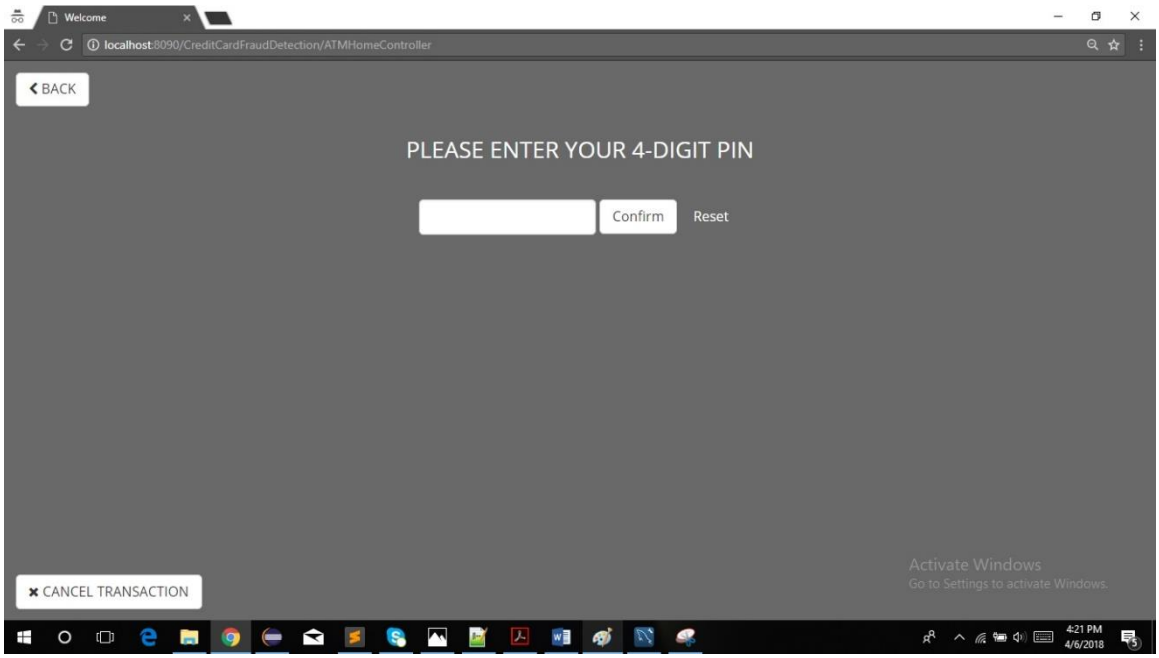

Figure 4.1.6.2: Pin Screen

4.1.6.3 ATM Home Screen

From here user can select an option.

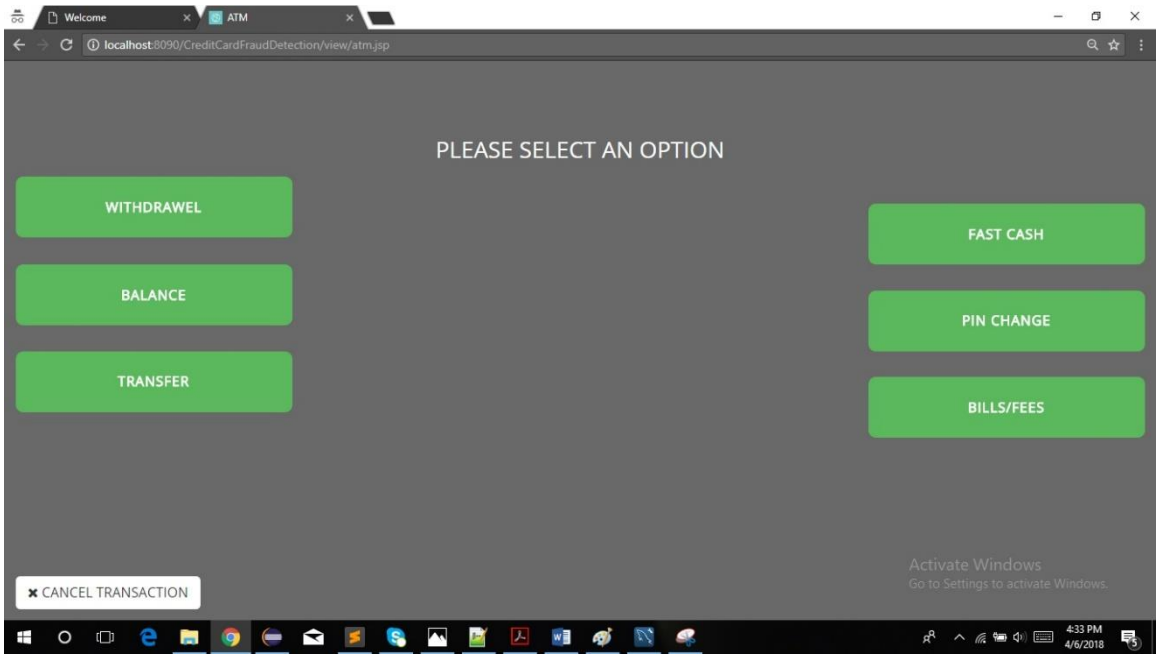

Figure 4.1.6.3: ATM Home Screen

4.1.6.4 Amount Screen

A user enter the amount he want to transact.

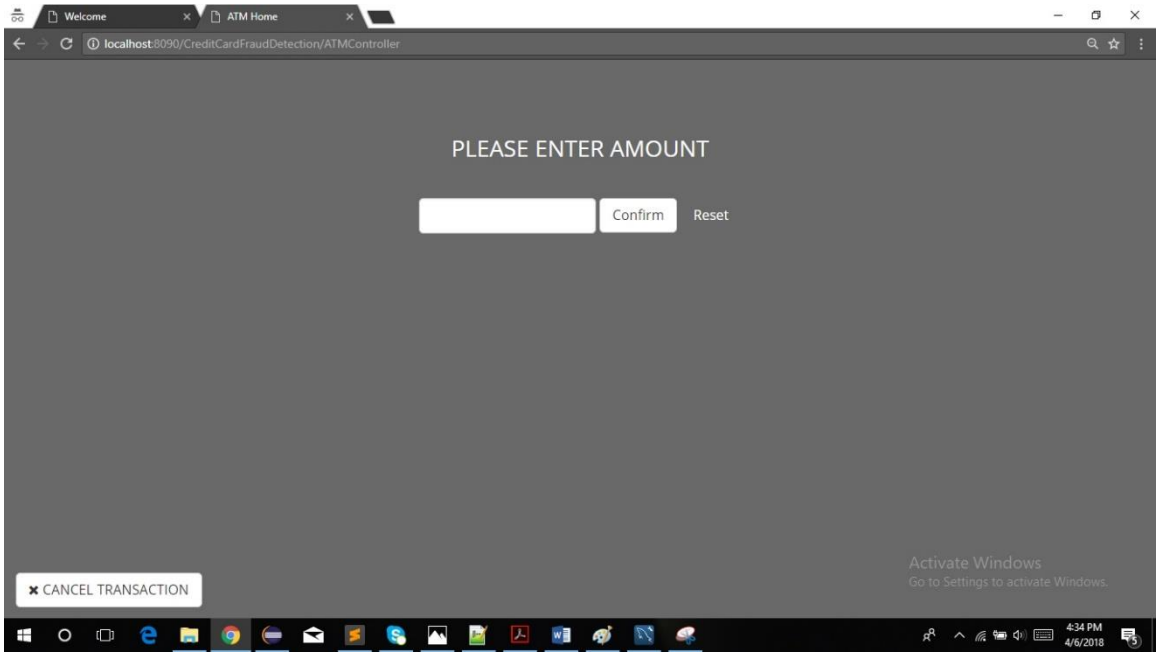

Figure 4.1.6.4: Amount Screen

4.1.6.5 Success Screen

Success screen when there is no fraud founded.

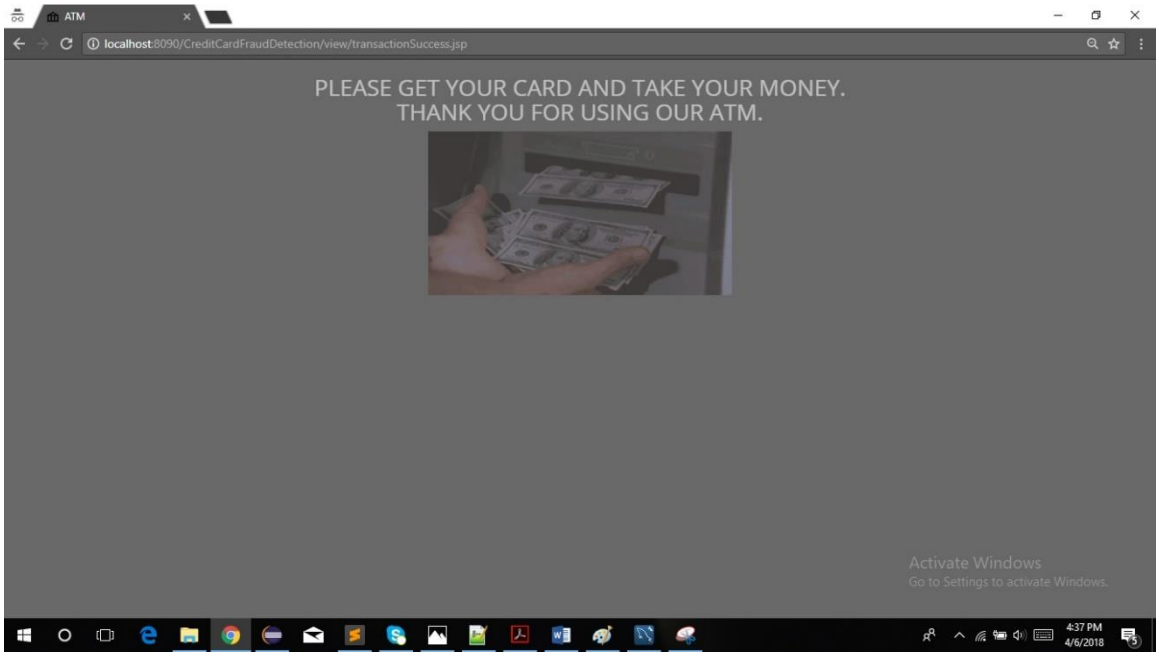

Figure 4.1.6.5: Success Screen

4.1.6.6 Fraud Screen

When system found fraudulent, than the transaction will be canceled.

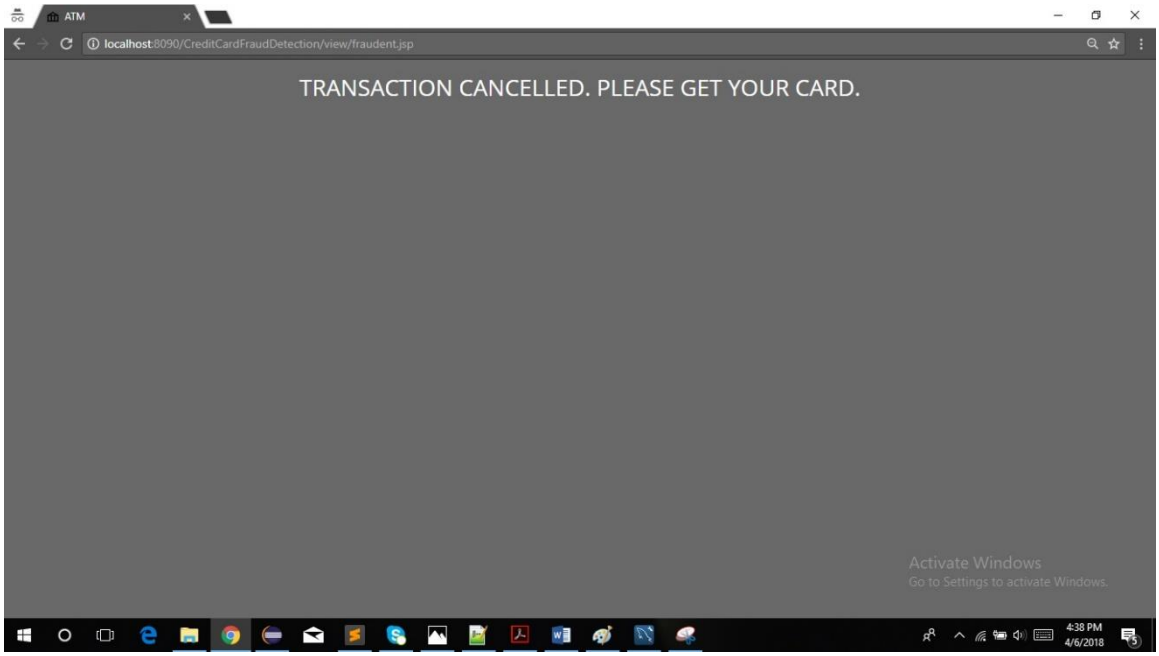

Figure 4.1.6.6: Fraud Screen

4.1.6.7 Security Question Screen

This is the security question page.

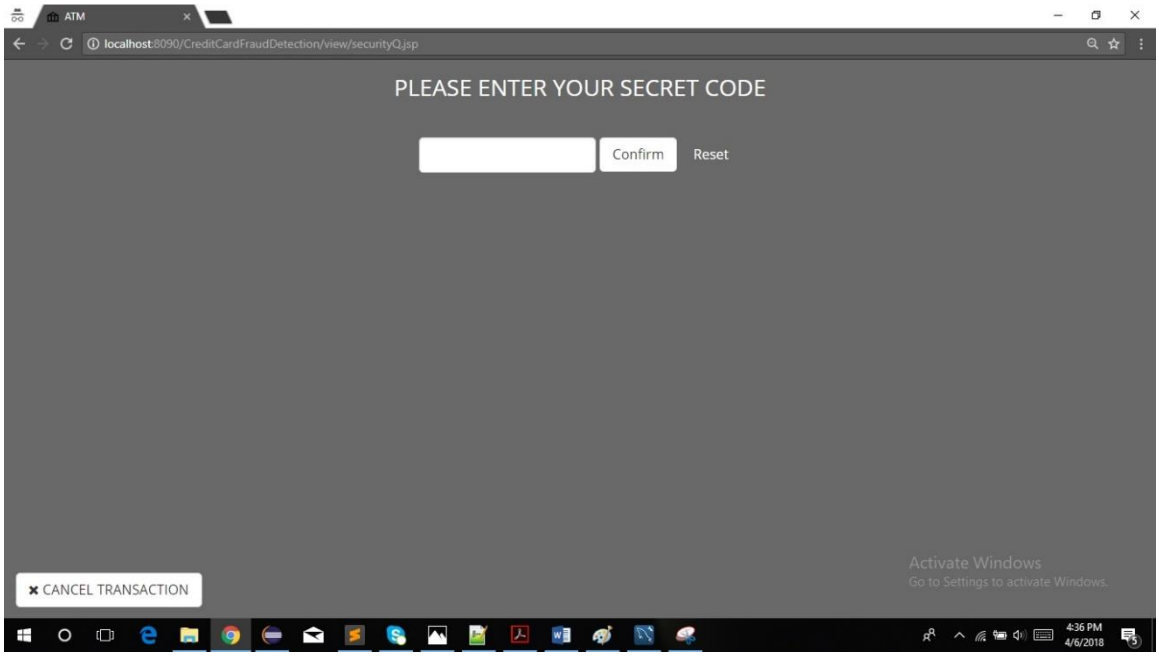

Figure 4.1.6.7: Security Question Screen

4.2 Methodology

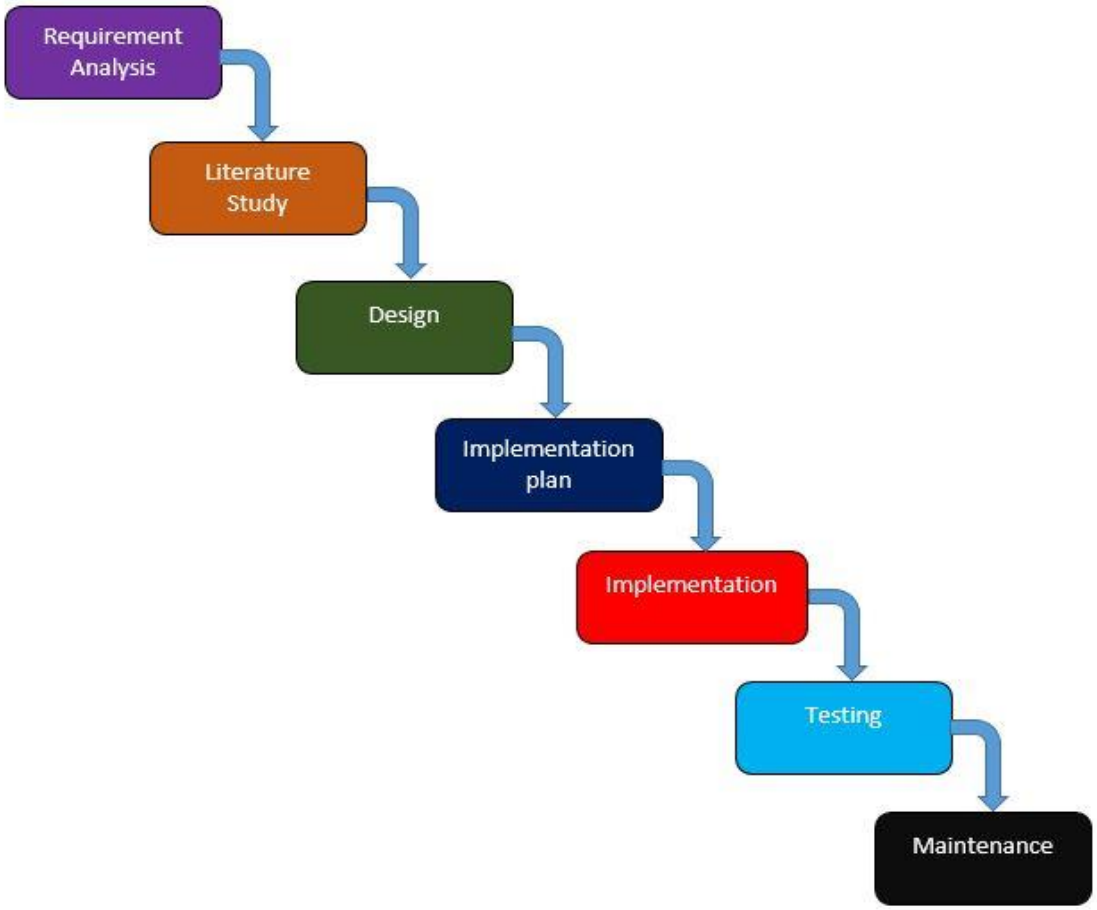

Figure 4.2: Waterfall Methodology.

All of the steps in waterfall methodology are explain below:

1. **Requirement Analysis**: This is the first phase of this methodology, where at first we should identify the problem to solve it and then find out all possible requirements of the system to develop the system.
2. **Literature study**: In this phase, we had to study about the project related work, what is the process to solve it, the better way to solve it. This phase help us to make decision about the proper system to develop a project/system.
3. **Design**: The physical characteristic of the system are designed during this phase. The operating environment, inputs and outputs are defined in this phase. This system design helps in specifying hardware and helps in defining the overall system architecture.
4. **Implementation plan**: In this phase, we worked on the planning of the program execution. Here we thought about how the program implement or execute, which process should be implement first etc. In one word, in this phase we planned about all kind of implementation process to develop our system.
5. **Implementation**: The implementation plan are given in previous phase and the detailed specification produced during the design phase are translated into hardware, communication and executable software. This is an important and major phase for our project system. The system is first developed in small programs called units. Each unit is developed and tested for its functionality, which we called as unit testing.
6. **Testing**: All the units developed in the implementation phase are integrated into a system after testing of each unit. Here user tests the system to ensure that the functional requirements as defined in requirement document are satisfied by the developed or modified system.
7. **Maintenance**: Maintenance is another important phase. The system performance in accordance with user requirements is monitored. Sometimes there are some problem or issues come up in the user environment, to fix those issue, maintenance is very important.

4.3 Interaction Design and UX

User experience design focuses on the overall experience between a user and a product. So Interaction Design is a Subset of UX Design. There's no point in conducting user research and working out what user's want if interaction designers who are responding to those needs are kept at arm's length from research outputs. The simpler the interaction the more beautiful it is. So interaction design isn't the same as user experience design.

4.3.1 Interaction Design

Interaction design is specifically a discipline which examines the interaction (via an interface) between a system and its user. It may also incorporate design focused on how information should be presented within such a system to enable the user to best understand that information though this is often considered to be the separate discipline of "information design" too. [7]

4.3.2 User Experience Design

User experience (UX) design is the process of creating products that provide meaningful and personally relevant experiences. This involves the careful design of both products usability and the pleasure consumers will derive from using it. It is also concerned with the entire process of acquiring and integrating the product, including aspects of branding, design, usability and function.

4.4 Implementation Requirements

HMM consists of three states-

1. Set of finite states.
2. Transition from one state to another.
3. Transition only dependent on current state.

HMM relates each sate of states with probability distribution. Transition from one state to another depends on transition probabilities. For an individual outcome an output or observation can be generated according to an associated probability distribution. It is only an outcome, not any internal states. So, it shows only result not any internal hidden purposes. Hence it is called Hidden Markov Model.[4][5]

Here, I need the concept of Bayesian equation to calculate the transition probabilities. Example of HMM with diagram given below –

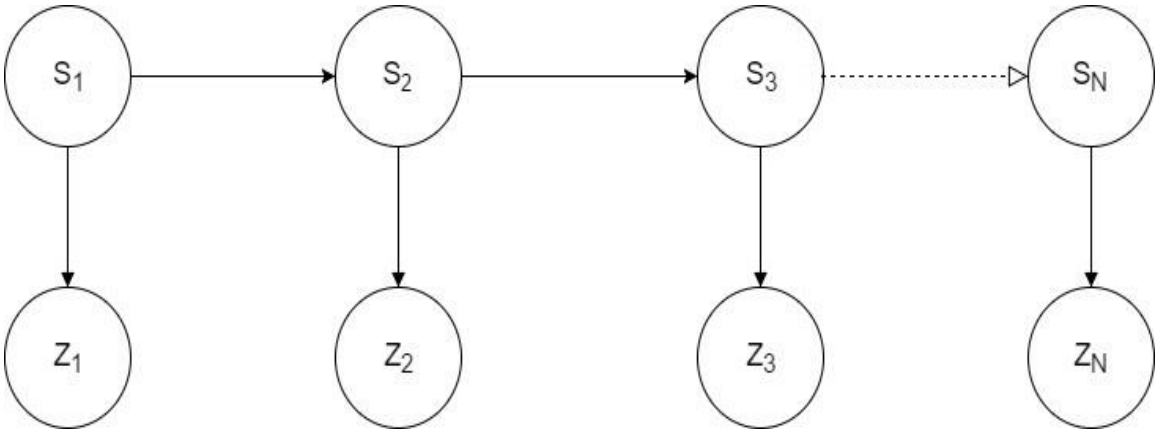

Figure 4.3: State Transition in HMM

In the following diagram S_1, S_2, S_3…SN are some states. Each state has a measurement or Hidden fact (Z_1, Z_2, Z_3…Z_N) which is the specialty of HMM. Transition from one state to another depends on hidden facts.

Based on HMM several applications have maid. Such as speech recognition, bioinformatics and genomics [6].

An HMM can be characterized by the following:

1. Suppose, N is the number of states in an HMM model. So we can demonstrate the set of states as

$S = \{S_1, S_2 \ldots\ldots\ldots S_N\}$.

2. State at random time t is denoted as q_t .

3. The number of observation symbol denoted as M. Observation symbol means the physical output of the model. So, the number of observation symbol set $V= \{V_1, V_2, V_3, \ldots. VM\}$.

4. State transition probability denoted as $A=[a_{ij}]$. Here a_{ij} is the transition probability between the state i and j.

5. Observation symbol matrix stated as $B = [B_{jk}]$.

6. The sequence of observation is $O =O_1, O_2 \ldots\ldots O_N$.

From the following description it is known that an HMM model needs two parameters N and M. After stating these parameters it is possible to do the required calculation.

HMM is the perfect solution for detecting fraud transaction and the extra flexibility. It turns off the number of false transaction at very lower level. This is why I choose HMM based model.

CHAPTER 5

IMPLEMENTATION AND TESTING

In this chapter we are discussed about the implementation, the evolution criteria and the testing part of our project.

5.1 Implementation

A system using Hidden Markov Model is ideal solution for credit card fraud detection. The main benefit of using HMM-based approach is, it decreases the false transaction amount at very low position. It doesn't need any fraud signature to detect the false transaction and still it is able to catch the fraud using some spending behavior. For the proposed system there will be three category according to user spending behavior. These are-

1. High.
2. Medium.
3. Low.

The system uses the deviation in last 10 transactions amount. Initially the system doesn't have the required data. In this phase new user will be asked about some security questions until they have done required amount of transaction. But for the old users system needs to construct a model.

5.1.1 Construction Phase

In this section the system will construct model for the old users. Which means the system will convert the spending amount into observation symbol. This is an internal process and it will not affect the online transaction of others user. K-means clustering algorithm is one of the solutions for building those observation symbols. [7]

This is important phase of the fraud detection system. In this phase HMM training will be start. Training Algorithm follows the following steps:

1. Initialization of HMM parameters
2. Forward procedure
3. Backward procedure

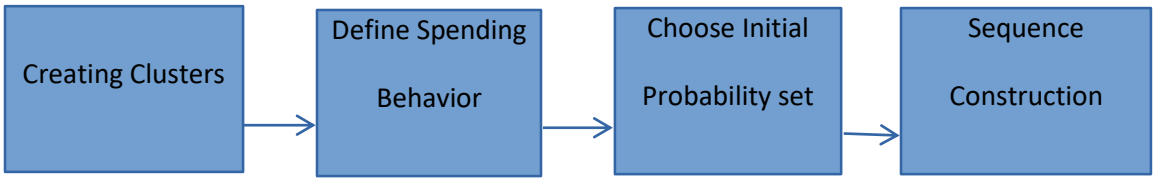

Figure 5.1: Construction Phase

5.1.2 Detection Phase

After completing the construction phase the system is well known about the observation symbols and its sequences which is O_1, O_2 .....O_N. So when a new transaction occurs the system will add it to observation symbol O_{N+1} and it will delete the first transaction. The system will work with last 10 transactions of the users. If any unexpected probabilistic deviation occurs during the transaction the system will detect it as a fraudulent transaction.

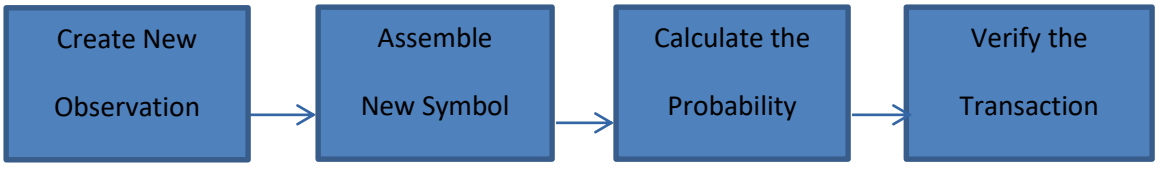

Figure 5.2: Detection Phase

5.2 Working with random data

It is not possible to do simulation on real time transaction data. Banks are not providing any dataset because of security issues. I have used several data sets of random numbers for testing the proposed system. One example is given below in table:

Table 5.1: Transaction List Details.

Transaction No	Amount	Category
1	7500	Medium
2	2500	Low
3	1000	Low
4	9000	Medium
5	8000	Medium
6	12000	High
7	1500	Low
8	11500	High
9	6500	Medium
10	13000	High

From sequence of category we have found required initial probabilities. Those are:

Table 5.2: Initial Probabilities.

Category	Transition	Value
Low	L | L	1/3
	L | M	1/3
	L | H	1/3
Medium	M | M	¼
	M | L	¼
	M | H	½
High	H | H	0
	H | L	½
	H | M	½

5.2.1 Discussion on the result

In my proposed system I have shown that the system initially checks the probability of upcoming transaction being genuine or fraud. It is much faster and simple comparing to the others and also reduces the probability of fraud transaction in vast amount. The threshold value for my system will be 50%. So, when the probability of next transaction based on some states less than 50%, the system will detect it as a fraudulent transaction.

For the proposed system I have used several data sets, which are generated by a random number generator. It is not possible to find out real world data set for security reason. So the proposed system has the limitation of not using the real data sets. It is possible to give more correct answer if the analysis on transaction is increases to more than 10. But it is more important to ensure the security of users. Because if the system takes more time to analyze on users transaction patterns, on the other hand users will be in security less more time. Sometimes it may happen that the user is genuine, but the probability of that transaction is below threshold value. So, the user needs to answer some questions.

5.3 Evaluation Criteria

Evaluation of our results will be crucial to the project's success. As we obtain a better understanding of the algorithms and their implementations, we are better prepare to intelligently design our evaluation method. It is important to note that the evaluation is the primary objective of this project. The integration of the most accurate algorithm into the final application is secondary. We will consider this project a success when we are confident that we have properly gather all information and help the people. Besides these, more possible information can be added in future. But this time those cases are covered which are most important.

5.4 Testing Implementation:

Table 5.3: Test result.

No. of test	Test Case Description	Expected Result	Actual Result
1.	Start the application properly and shown the design representation.	Start properly and shown	Successful
2.	Proper using of local host	Properly used	Successful
3.	Check the data passing system	Properly passed	Successful
4.	User registration system.	Successfully done	Successful
5.	Showing users all information.	Showed successfully	Successful
6.	All kind of transaction	Done successfully	Successful
7.	Fraud Detection System	Properly worked	Successful
8.	Update all the information	Properly updated	Successful

CHAPTER 6

CONCLUSION AND FUTURE SCOPE

6.1 Conclusion:

In this project I have discussed the common ways of credit card fraud and I have used HMM based system which will help to detect the fraud transactions of credit card. The system will calculate the probability of next transaction being fraud or genuine based on some facts. To sort out the facts I have made three categories low, medium and high for the users. The types of purchase or spending behavior will be the hidden states. Here I have also build a method for building the patterns automatically which is clustering algorithm. The system is also saleable for handling large volume of data. The future work for this system can be figure out more common human behavior to make this system more secure.

6.2 Limitations:

There are some limitation of our system beside lots of advantage. We need to update functionality of the database system. It is not possible to find out real world data set for security reason. So the proposed system has the limitation of not using the real data sets.

6.3 Future Scope:

We have some plan for the future. We can make the system more dynamic and secured. It's only the beginning of this project. Subsequently there are some arrangements too to develop it later. We are going to combine this system with the Neural Network so that it will work more efficiently.

References

[1] Singh, Divya, and Asst Prof Rakesh Pandit. "Credit Card Fraud Detection Using Hidden Markov Model." (2015).

[2] Zareapoor, Masoumeh, K. R. Seeja, and M. Afshar Alam. "Analysis on Credit Card Fraud Detection Techniques: Based on Certain Design Criteria." International Journal of Computer Applications 52.3 (2012).

[3] Narekar, Mr Yogesh M., and Mr Sushil Kumar Chavan. "A Review On Credit Card Fraud Detection Using BLAST-SSAHA Method."(2015)

[4] Stamp, Mark. "A revealing introduction to hidden Markov models." Department of Computer Science San Jose State University (2004).

[5] Rabiner, Lawrence R. "A tutorial on hidden Markov models and selected applications in speech recognition." Proceedings of the IEEE 77.2 (1989): 257-286.

[6] Gade, Vaibhav, and Sonal Chaudhari. "Credit card fraud detection using Hidden Markov Model." International Journal of Emerging Technology and Advanced Engineering 2 (2012).

[7] Bhatla, Tej Paul, Vikram Prabhu, and Amit Dua. "Understanding credit card frauds." Cards business review 1.6 (2003).

[8] Bhusari, V., and S. Patil. "Application of Hidden Markov Model in credit card fraud detection." International Journal of Distributed and Parallel Systems 2.6 (2011): 203.

[9] Khan, MohdAvesh Zubair, Jabir Daud Pathan, and Ali Haider Ekbal Ahmed. "Credit card fraud detection system using hidden markov model and K-clustering." International Journal of Advanced Research in Computer and Communication Engineering 3.2 (2014): 5458-5461.

[10] Learn about Baum-Welch Algorithm, available at << https://en.wikipedia.org/wiki/Baum%E2%80%93Welch_algorithm>>, last accessed on 03-04-2017 at 09:10pm.

[11] Learn about Hidden Markov Model, available at << https://en.wikipedia.org/wiki/Hidden_Markov_model>>, last accessed on 03-04-2017 at 11:00pm.