ISBN 978-93-5156-328-0
International Conference of Advance Research and Innovation (ICARI-2014)

Fraud Detection in Online Banking Using Hidden Markov Model

Samruddhi Belan*, Sujata Mane, Tejas Patani
Department of Computer Engineering, SIEM, Nashik, India

Article Info

Article history:
Received 2 January 2014
Received in revised form
10 January 2014
Accepted 20 January 2014
Available online 1 February 2014

Keywords

Hidden Markov Model
Transaction
Credit Card
Fraud Detection
Online Shopping,
Internet
E-Commerce
Security.

Abstract

As online banking becomes the most popular mode of payment for both online as well as internet based transaction, cases of fraud associated with it are also rising. In this paper we model the sequence of operations in internet banking transaction processing using a Hidden Markov Model (HMM) and showing how it can be used for the detection of frauds. If an incoming online banking transaction is not accepted by the trained HMM with sufficiently high probability, it is considered to be fraudulent. At the same time, we will try to ensure that genuine transactions are not rejected.

1. Introduction

Today world online banking service is the most popular and provides a fast and easy way to make transactions. As increasing online transaction, the number of fraud transaction is also increased by various thefts. In this paper, we design a model with sequence of operations in online transaction by using Hidden Markov Model (HMM) and decides whether the user act as a normal user or fraud user. The HMM is initially trained with customer's last few transactions. In the trained system, the new transaction is evaluated with transition and observation probability. Depends upon the observation probability, system finds the acceptance probability and decides the transaction will be declined or not. Normally existing fraud detection system for online banking will detect the fraudulent transaction after completion of the transaction. It is additional burden to and fraudulent after transactions. This causes the economic loss and makes the bank name as unsecured. Our model predicts the fraudulent during the transaction time and prevents the money transfer. The main objective is to ensure that the genuine transactions should not be rejected. [4]

Corresponding Author,
E-mail address: belansamruddhi@gmail.com

1.1 Online banking

In today's world of emerging technologies, enterprises are moving towards the Internet for businesses. People are rushing towards the e-commerce applications for their day-today needs, which in turn are making the Internet very popular. Online Banking has given both an opportunity and a challenge to traditional banking. In the fast growing world, banking is a necessity, which in turn takes a lot of time from our busy schedule. Going to a branch or ATM or paying bills by paper check and mailing them out, and balancing check books are all time-consuming tasks. Banking online automates many of these processes, saving time and money. For all banks, online banking is a powerful tool to gain new customers while it helps to eliminates costly paper handling and manual teller interactions in an increasingly competitive banking environment. Banks have spent generations gaining trust of their customers. [1]

1.2 Fraud detection system

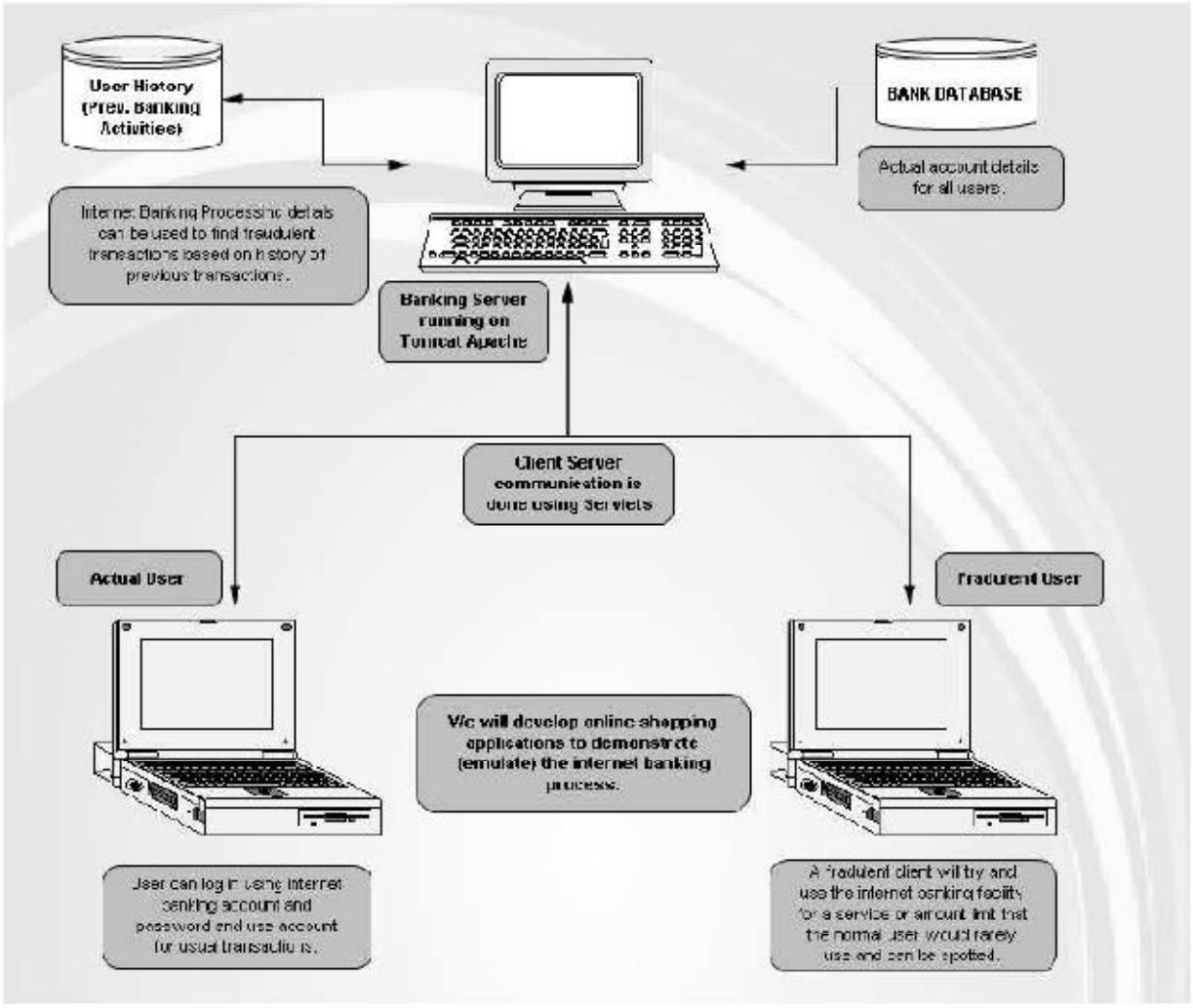
All the information about credit card (Like Credit card number, credit card CVV number, credit card

ISBN 978-93-5156-328-0

ISBN 978-93-5156-3

Expiry month and year, name on credit card etc.) will be checked with credit card database. If User entered database is correct then it will ask Personal Identity number (PIN). After matching of Personal Identity number (PIN) with database and account balance of user's credit card is more than the purchase amount, the fraud checking module will be activated. The verification of all data will be checked before the first page load of credit card fraud detection system. If user credit card has less than 10 transactions then it will directly ask to provide personal information to do the transaction. Once database of 10 transactions will be developed, then fraud detection system will start to work. By using this observation, determine users spending profile. The purchase amount will be checked with spending profile of user. By transition probabilistic calculation based on HMM, it concludes whether the transaction is real or fraud. If transactions may be concluded as fraudulent transaction then user must enter security information. If transaction will not be fraudulent then it will direct to give permission for transaction. If the detected transaction is fraudulent then the Security information form will arise. It has a set of question where the user has to answer them correctly to do the transaction. These forms have information such as personal, professional; address, date of birth etc are available in database. If user entered information will be matched with database information then transaction will be done securely. And else user transaction will be terminated and transferred to online shopping website. [6]

2. System Architecture



ISBN 978-93-5156-328-0

ISBN 978-93-5156-3

Fig: 1. System Architecture

System architecture contains following modules. They are as follows:

- **Client Server Interaction:** A module using Java Networking shall be built that will allow the client application to call Servlets.
- **Client GUI:** Using AWT / Swing. This GUI shall allow the user to log in and transact online using internet banking enabled account.
- **Client Side Item / Service Browser:** A module that will allow the client to browse through all available items/services available on internet. Client can select any of these items/services and opt to buy them online Client
- **Transaction Module:** A module that will allow clients to enter their credentials / authentication information and proceed with a transaction. This module also presents the client with transaction report (success /failure / etc.)
- **Servlets:** Client § Server communication is achieved through a series of Servlets. These Servlets will be hosted using Tomcat Apache on the server.
- **Account Database:** A database containing account information of all clients is maintained on bank's server. The details may include account number, log in, password, available balance, etc.
- **Transaction Database:** A database containing history of client's online transactions will also be maintained on server. The databases shall be maintained using Object Serialization.
- **Fraud Detection Using HMM:** A module implemented using Hidden Markov Model algorithm that will try to find out if the ongoing transaction is fraudulent or not will be implemented on server side.
- **Server GUI:** Server side application GUI will be developed suing AWT/Swing. This module shall allow the administrator to log in and view account details of a specific client as well as add a new client to accounts database.[1]

3. Methodology

There are three phases in Methodology. They are as follows:

Phase 1: Database Development

Phase 2: Cluster Formation

Phase 3: Fraud Detection

3.1 Phase 1: Database development

Create an application for fraud detection in online application that contains the home page and the transaction details. Home page provides the user to know about log in - id, password, user-name, security questions and transaction details. After entering user name and password details in the home page the server validates the information and redirect to reservation page.

3.2 Phase 2: Cluster formation

The second module of the project to cluster the customer accounts into low, high, middle depending upon the spending profile of the customer. The clustering process based on the K-means clustering. Euclidean Distance is the most common use of distance. In most cases will refer to Euclidean distance. Euclidean distance or simply 'distance' examines the root of square differences between coordinates of a pair of objects. [4]

Fig: 2. Block diagram of cluster formation

3.3 Phase 3: Fraud Detection

To implement the fraud detection by using the Hidden Markov Model (HMM). We use the states and transition probability between them. The outcome of the HMM will be the observation symbols (Oi). The observation symbols are the low, high; medium depends on the transaction amount. It can be determined by clustering process. After the HMM parameters are learned, we take the symbols from a cardholder's training data and form an initial sequence of symbols. Let O1, O2 . . . OR be one such sequence of length R. This recorded sequence is

ISBN 978-93-5156-328-0

ISBN 978-93-5156-3

formed from the cardholder's transactions up to time t. We input this sequence to the HMM and compute the probability of acceptance by the HMM. Let the probability be α1, which can be written as follows α1= P (O1, O2, O3 . . . OR |λ) Let OR+1 be the symbol generated by a new transaction at time t+1. To form another sequence of length R, we drop O1 and append OR+1 in that sequence, generating O1,O2,O3 . . .OR,OR+1 as the new sequence.

We input this new sequence to the HMM and calculate the probability of acceptance by the HMM. Let the new probability be α2= P (O2, O3, O4. . . OR+1 |λ). Let Δα=α1-α2 If Δα value is greater than threshold value then the transaction could be a fraud with low probability. If the transaction be a fraud then the model asks the user to answer the security questions (after ten transactions).The customer answers were checked by the FDS (Fraud Detection System) and decides whether the user be the genuine user or the fraud user. If the customer be a genuine the ticket will reserved otherwise the transaction will be declined.

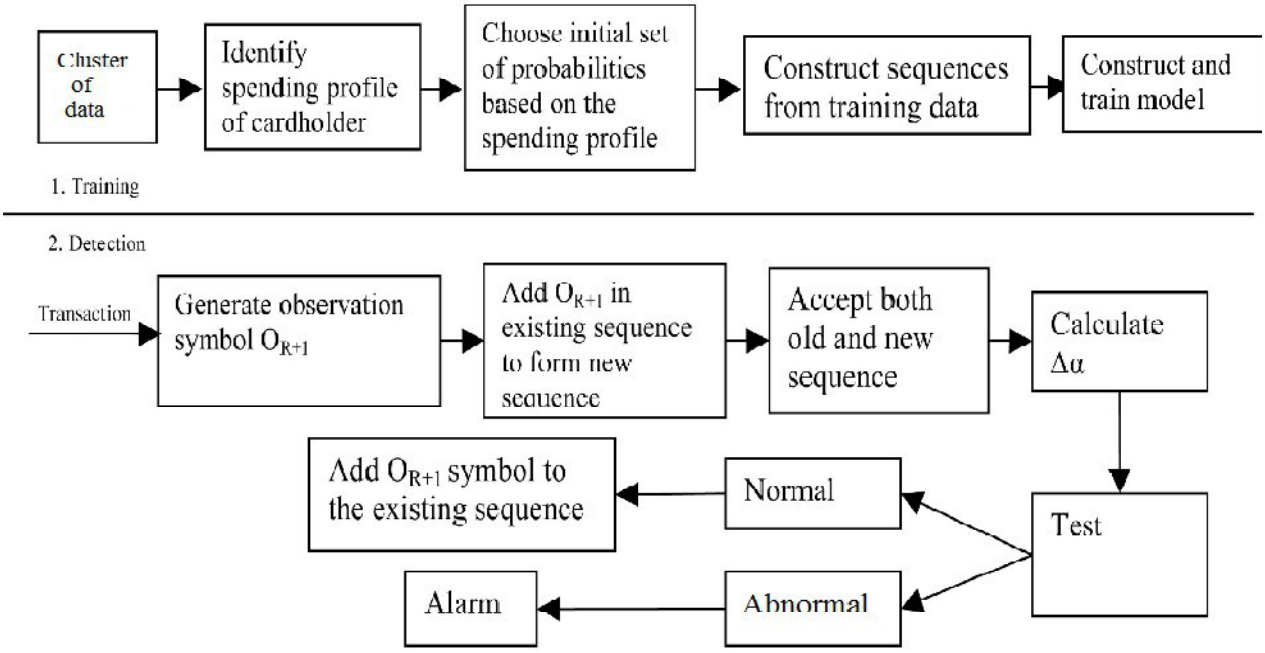


Fig: 3. Training and detection

4. Conclusion

The proposed methodology is aimed at detecting fraud in case of online banking. In online 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 signature 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. Hidden Markov Model is used to track the user behaviour. First user behaviour is recorded and then for new transaction it is checked.

References

[1] Sunil Mhamane, L. M. R. J Lobo, "Fraud Detection in Online Banking Using HMM", International Conference on Information and Network Technology, 2012

[2] A. Srivastava , A. Kundu , S. Sural, "Credit Card Fraud Detection Using Hidden Markov Model", IEEE Transaction, January-March 2008

[3] Shailesh S. Dhok, "Credit Card Fraud Detection Using Hidden Markov Model", International Journal of Soft Computing and Engineering, 2012

[4] S. Esakkiraj, S. Chidambaram, "A Predictive Approach for Fraud Detection Using Hidden Markov Model", International Journal of

Engineering Research & Technology, January-2013

[5] V. Bhusari and S. Patil, "Study of Hidden Markov Model in Credit Card Fraudulent Detection", International Journal of Computer Applications, April 2011 .

[6] S. M. Varghese, R. B. Jadhav, "Online Banking Fraud Detection by Hidden Markov Model", International Journal of Educational Administration, 2013