ATM Fraud Detection Using Hidden Markov Model

Study of HIDDEN MARKOV MODELand its application

[I]Shrutanjay Kulkarni, [II]Sanket Murkute, [III]Prateek Nangare, [IV]Sameer Metkar
Guided by Prof. R S Mote
[I,II,III,IV]NBN Sinhgad School of Engg., Pune, Maharashtra, India

Abstract
ATM card fraud was causing many losses for the card payment industry. Now a days most accepted payment mode is Debit card for both online and also for regular purchasing; hence frauds related with it are also growing. To find the fraudulent transaction, we implement an Advanced Security Model for ATM payment using Hidden Markov Model (HMM), which finds the fraud by using customers behavior. This Security Model is primarily focusing on the normal spending behavior of a cardholder and some advanced securities such as Location, how much money we takes from machine, Time and Sequence of transactions. If the trained Security model identifies any misbehavior in upcoming transaction, then that transaction is permanently blocked until the user enter High Security Alert Password (HSAP). This paper provides an overview of frauds with ATM card statistics and the definition of ATM card fraud. The main outcome of the paper is to find the fraudulent transaction and avoids the fraud before it happens.

Keywords
Hidden Markov Model, Advanced Fraud Detection System.

I. Introduction

It is the need of era and many challenges faced by banking system to provide good and secured facilities of E-transaction. For that our banks provide us a Magnetic Chip, we called it is as ATM card. The model proposed in these applications is all about recognizing and understanding various transactions patterns of the user. It helps in maintaining and updating a database that will describe the operational behavior of the specified user in the form of a pattern. This model totally depends on the pattern evaluating and recognizing Forward-Backward algorithm

II. Background

In the existing fraud detection system, fraud is detected after fraudulent transaction is processed. Due to which the card holder faces a lot of problems before the investigation finish. The existing system does not consider the spending behavior of cardholder as the key element to detect the fraudulent transaction. Hence the crime plays an important role to investigate the fraud. Due to such a long investigation process, the existing fraud detection system is time consuming process. Hence it affects the business processing of fraud detection system. So in this business processing we prefer to the Hidden Markov Model. Now a day's many of transactions are made with ATM/debit card so we don't know the person who is using the card, we just capture the image or record the video for authentication purpose.

III. Major Frauds in ATM

1. Lost or Stolen Card

In this fraud technique fraudsters stole the actual information of customer. This information they can use for making the anonymous transaction

2. Card Not Present

In this fraud, the transaction will be done without using actual card. Here the fraudster does not need a physical card to make a transaction. Because of this disadvantage, Card Not Present (CNP) is becoming more popular than other frauds

IV. Literature Survey

In Abhinav Shrivastava and team proposed, "Credit Card Fraud Detection Using Hidden Markov Model"1 March 2008. They explains in that the problem with most of the previous approaches is that they require labelled data for both genuine, as well as fraudulent transactions, to train the classifiers. Getting real-world fraud data is one of the biggest problems associated with credit card fraud detection. Also, these approaches cannot detect new kinds of frauds for which labelled data is not available.

In Ashish Gupta ,Jagdish Raikwal, " Fraud Detection in credit Card Transaction Using Hybrid Model" 1 Jan, 2014.They proposed survey number of technique for credit card fraud detection and basis on that we will propose a strong literature of Hybrid Markov Modelwhich is a combination of Bayesian Classifier and Hidden Markov Model, based system which will consist of the process of all the surveyed technique and result in better fraud detection than all previous proposed system of fraud detection.

In Fabio Cuzzolin and Michael Spanienza , "Learning Pullback HMM Distances "IEEE Trans, August 2013.They proposed general framework for learning distances function of generative dynamical model, given a training setof labelled videos. The optimal distances function is selected among of family of pullback ones, induced by a parameterised automorphism of the spacemodel. They focus here on HMM models and their models spaces and design.

V. Advanced Security Model

In our advanced security model there are four input parameters.

1. Location

This input parameter will be checked at the time of user login. To calculate this parameter we have to go through following steps,
Step1: First we calculate the Latitude and Longitude of previous transaction.
Step 2: Then we calculate the upcoming transaction's Latitude and Longitude.
Step 3: We calculate one threshold value of location parameter from last 20 transactions, we compare this threshold value with the difference of step1 and step 2 values.If that difference is greater than our threshold then the upcoming transaction may fraud. This input parameter will start the checking from the beginning when

user enters an ATM pin. If our advanced security model founds fraud then he will block the transaction and send a HSAP on user's registered mobile number.

2. Sequence of Transaction

This input parameter is depending on user's behavior, how he withdraws the money. For example, consider one user who having the habit like first he checks the account balance and then he withdraw the money and vice versa. Like this every user have their different patterns of doing transaction. We consider such previous 20 transactions patterns, and that patterns are forwarded to our FDS system as an input parameter.

3. Time Taken for Transaction

Here we consider the time taken for doing the transaction right from the moment a user enters a password to user enter an amount and presses the confirmation button of withdraw money. Here the major role of our FDS system is to calculate the current transaction spending time and compare this time with the previous 20 transactions before giving out the money. If current time deviates with our previous record then we block the transaction.

4. Amount

The amount is most important factor for our fraud detection system. Here we consider previous 20 transactions amounts for finding the fraud.

VI. High Security Alert Password

This facility will get enabled when our fraud detection system got any fraudulent transaction. So as it occurs system will send a High Security Alert Password (HSAP) on user's registered mobile number. As user got this password, user has to enter this password on screen of HSAP to continue the transaction. The time limit to enter the High Security Alert Password is 2 minutes. After 2 minutes the password will get expired. You have to regenerate the new HSAP. If the current user is fraudulent one then the transaction would remain unblocked and the original user get a High Security Alert Password through SMS service and realize that the someone unauthorized user has accessed his/her account so he/she need to block his ATM card as soon as possible.

VII. Observation & Result

It is very difficult task to test debit card fraud detection system using real data set. Bank do not shares their data with the researchers. There is also no possibility of avail such data set for experimentation. Therefore, numbers of transactions were performed to test the efficiency of the system. A simulator is used to generate a mix of genuine and fraudulent transactions. The genuine transactions are generated according to the cardholder's profiles. The cardholders are classifieds into three categories i.e. low, medium, high price transactions respectively. The effects of spending group and the percentage of transactions that belong to the low, medium, and high price range cluster. Then set of experiments were carried out to determine the correct combination of HMM design parameters namely, amount of transaction, time of transaction and the sequence of transaction.

VIII. Conclusion

From the study of the ATM fraud detection using HMM we conclude that the systems gave desired outcomes to some extent. An optimum recognition system can be created by using the suggested advance system.

IX. Future Scope

From the development point of view, improvements to the existing system can be made by adding features like, the logs of system can be sent to the system administrator. Also if a system fails to identify a certain person for more than certain number of time, an immediate message is sent to the administrator warning him of a potential security breach.

X. Acknowledgment

We express our gratitude to out guide Prof. Mote Sirfor his valuable guidance, unwavering support and encouragement that he gave us. During the long journey of this study, hesupported us in every aspect. He was the one who helped and motivated us to propose research in this field and inspired us with his enthusiasm on research and experience in the field.

References

[1] *"Credit Card Fraud Detection Using Hidden Markov Model" Abhinav Shrivastava, Amlan Kundu, Shamik Sural, Senior Member, IEEE, and Arun K. Majumdar, Senior Member, IEEE Transactions, VOL 5, No. 1, JanMar 2008.*

[2] *"Credit Card Fraud Detection Using Hidden Markov Model" by Divya Iyer, IEEE Conference. 2011*

[3] *"Distributed Data Mining in Credit Card Fraud Detection" by Phili K. Chan, IEEE Intelligent Systems, Nov-Dec 1999. [4] S. Ghosh and D.L. Reilly, "Credit Card Fraud Detection with a Neural-Network," Proc. 27th Hawaii Int'l Conf. System Sciences:Information Systems: Decision Support and Knowledge-Based Systems,vol. 3, pp. 621-630, 1994.*

[5] *"Theft Prevention ATM Model using Dormant Monitoring for Transactions" by Prof. V. V. Jog, IEEE Conference. 2012.*

[6] *"HMM Based Enhanced Security System for ATM Payment" by Prof.V.V.Jog and Prof.A.A.Deshmukh, IRACST, ISSN No. 2250-3498, Vol 2 No 2, April 2012*

[7] *L.R. Rabiner, "A Tutorial on Hidden Markov Models and Selected Applications in Speech Recognition," Proc. IEEE, vol. 77, no. 2, pp. 257-286, 1989.*

[8] *"Statistics for General and On-Line Card Fraud," h [7] L.R. Rabiner, "A Tutorial on Hidden Markov Models and Selected Applications in Speech Recognition," Proc. IEEE, vol. 77, no. 2, pp. 257-286, 1989.*

[9] *"Online Banking Fraud Detection Based on Local and Global Behavior" by Stephan Kovache and Wilson Vicente Ruggiero, The Fifth International Conference on Digital Society, 2011.*

[10] *"Plastic card fraud goes back up". BBC. March 12, 2008. http://news.bbc.co.uk/2/hi/business/7289856.stm. Retrieved January 2, 2010.*