Resilient Identity Crime Detection Using HMM and TESLA

Mr. Rahul Derle
Department of Computer Science & Engg.
Institute of Engg. & Technology
Alwar,Rajasthan,India.
derle.rahul@gmail.com

Prof. Rohit Singhal
Associate prof. & H.O.D.Dept. of CS/IT.
Institute of Engg. & Technology
Alwar,Rajasthan,India.
mtechrohit@gmail.com

***Abstract*-ATM cum Debit card transactions continuously grow in number, taking an ever-larger share of the Indian payment system and leading to a higher rate of stolen account number send subsequent losses by banks. Improved fraud detection thus has become essential to maintain the viability of the Indian payment system. In this paper, we model the sequence of operations in ATM cum Debit card transaction processing using a Hidden Markov Model (HMM) and show how it can be used for the detection of frauds. An HMM is initially trained with the normal behavior of a cardholder. If an incoming ATM cum Debit card transaction is not accepted by the trained HMM with sufficiently high probability, it is considered to be fraudulent. Hidden Markov Model helps to obtain a high fraud coverage combined with a low false alarm rate. At the same time, we try to ensure that genuine transactions are not rejected. We present detailed experimental results to show the effectiveness of our approach and compare it with other techniques available in the literature.**

***Index Terms*— ATM cum Debit card fraud, online shopping problem, ATM cum Debit card, e-commerce security, fraud detection, Hidden Markov Model.**

I. INTRODUCTION

In today's increasingly electronic society and with the rapid advances of electronic commerce on the Internet, the use of ATM cum Debit cards for purchases has become convenient and necessary .ATM cum Debit card transactions have become the reality standard for Internet and Web based e- commerce. ATM cum Debit-card-based purchases can be categorized into two types: 1) physical card and 2) virtual card. In a physical-card based purchase, the cardholder presents his card physically to a merchant for making a payment. To carry out fraudulent transactions in this kind of purchase, an attacker has to steal the ATM cum Debit card. If the cardholder does not realize the loss of card, it can lead to a substantial financial loss to the ATM cum Debit card company. In the second kind of purchase, only some important information about a card (card number, expiration date, secure code) is required to make the payment. Such purchases are normally done on the internet or over the telephone. To commit fraud in these types of purchases, a fraudster simply needs to know the card details. Fraud detection based on the analysis of existing purchase data of cardholder is a promising way to reduce the rate of successful ATM cum Debit card frauds.

II. LITERATURE REVIEW

Chiu and Tsai have proposed Web services and data mining techniques to establish a collaborative scheme for fraud detection in the banking industry.Getting real-world fraud data is one of the biggest problems associated with ATM cum Debit card fraud detection. Also, these approaches cannot detect new kinds of frauds for which labeled data is not available.[2]

HMM-based approach is a drastic reduction in the number of False Positives (FPs)—transactions identified as malicious bans FDS although they are actually genuine. In contrast, we present a Hidden Markov Model (HMM)-based ATM cum Debit card FDS, which does not require fraud signatures and yet is able to detect frauds by considering a cardholder's spending habit. [1][2]

III. HMM BACKGROUND

Hidden Markov models are widely used in science, engineering and many other areas (speech recognition, optical character recognition, machine translation, bioinformatics, computer vision, finance and economics, and in social science).

HMM is a statistical process that is completely dependent on the probability occurrence of random states from a set of states. Using the probability distribution technique outputs is generated, and only the outputs are made available to the user not the state.

An HMM can be characterized by the following:

1. N is the number of states in the model. We can denote the set of stateas S = {S1, S2 … Sn}. The state at time instant t is denoted by qt.
2. M is the number of distinct observation symbols per state. The observation symbols correspond to the physical output of the system being modelled.
3. The state transition probability matrix A= [Aij].
4. The observation symbol probability matrix B =[Bjk].
5. The observation sequence O = O1, O2…. On
6. N is the number of hidden states. [3].

A. Transaction Processing

This system works in two phases as

1. Training phase
2. Detection phase

1) Training Phase

This is important phase of the fraud detection system. In this phase HMM training will start. Training Algorithm is used to identify the behaviour of user and sets his transaction acceptance true probability i.e. A1.[3]

Initialization of HMM parameters For training the HMM, transaction amount is converted into observation symbols and form sequences from them. At the end of the training phase, we get an HMM corresponding to each cardholder. [2]This step is offline so it does not affect the performance of transaction processing.

2) Detection Phase

After initialising the HMM parameters, detection phase gets its input. This phase actually work in real time means at the time of actual transaction. For every time of new transaction, it calculates new acceptance probability (A2) and subtracts it from the true probability (A1) to get mean (A), depend upon that it checks whether the transaction it true or fraud.

If transaction is found to be malicious, then the issuing bank does not approve the transaction, and the FDS discards the symbol. Otherwise, new transaction is added in the sequence permanently by discarding very first one, and the new sequence is used as the base sequence for determining the validity of the next transaction.

IV. SYSTEM DESIGN

Our application consist of following modules:

1) ATM cum Debit card Information
2) Fraud check / Verification
3) Transaction

When user will try to do any transaction using ATM cum Debit card he will automatically send to FDS.

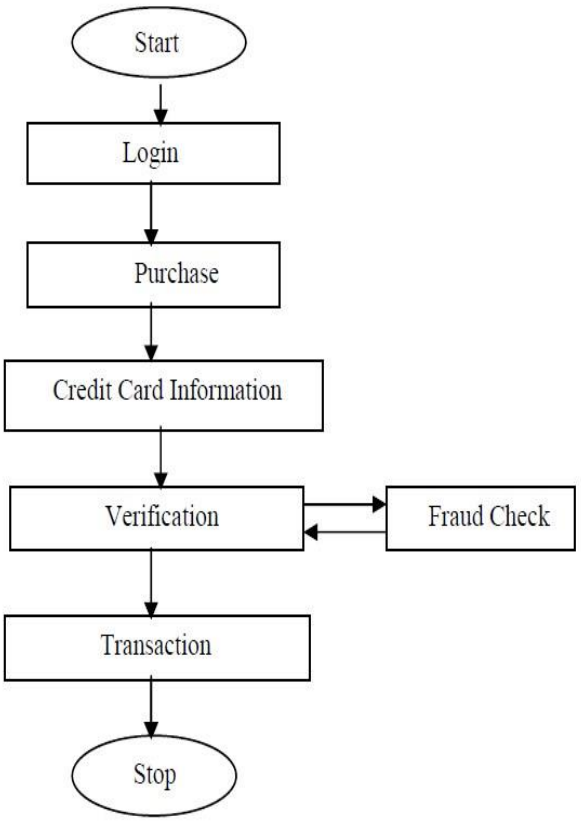

Fig1: Flowchart of the system for ATM cum Debit card fraud detection

Our system will be placed in between the client and bank. There HMM starts its working. Depending on the information provided by the client to system, it will analyse the transaction and take appropriate actions.

1)ATM cum Debit card Information:

Here system will ask for the card holder's information say card no, CVV no, Expiry date etc. But the problem is, everything is there on the card so depending upon the transaction amount FDS will declare transaction as fraud or not.

2)Fraud detection

In this phase system will compare his last 10 transaction with the previous. As FDS knows the cardholder's behavior it will take new transaction amount with the set

of 10 transaction and generate the acceptance probability as A2.

Initial scenario

A1= P (O1, O2…O10)

New transaction scenario (11^{th})

A2= P (O2, O3…O11)

System will calculate the difference between them as A.
A= A1-A2
If A<0 means 11^{th} transaction is maximum and which can be fraud with high probability. And if A>0 means 11^{th} transaction is minimum which also can be fraud but with low probability. So in both the system will transfer user to verification phase.

3)Verification Phase

In this phase user will be asked some personal questions and pin nos. This information is already with the system when user was creating account. If user gives correct answer to those questions then a call is made to user by which he/she can confirm the transaction. If he fails there then the transaction will not be possible. And warning will be sent to user's mail and message about misuse forced to block the card. After confirmation from user, he will be sent to transaction phase and new value will be added to threshold.

4)Transaction

If A=0 then the user will not be taken to verification phase. User will just require to type the verification code send by FDS and then the transaction will be possible.

V. CONCLUSION

The different steps in ATM cum Debit card transaction processing are represented as the under lying stochastic process of an HMM. Used the ranges of transaction amount as the observation symbols, whereas the types of item have been considered to be states of the HMM. And have suggested a method for finding the spending profile of cardholders, as well as application of this knowledge in deciding the value of observation symbols and initial estimate of the model parameters. It has also been explained how the HMM can detect whether an incoming transaction is fraudulent or not. Experimental results show the performance arid effectiveness of our system and demonstrate the usefulness of learning the spending profile of the cardholder.

References

[1] Srivastava A, Amlan K, "ATM cum Debit Card Fraud Detection Using Hidden Markov Model", IEEE transaction on secure computing, January 2006.
[2] Dhok S., "ATM cum Debit Card Fraud Detection System Using Hidden Markov Model", IJSCE, March 2012.
[3] Gade V, "ATM cum Debit Card Fraud Detection System Using Hidden Markov Model", IJETAE ,July 2012.
[4] C. Chiu and C. Tsai, "A Web Services-Based Collaborative Scheme for ATM cum Debit Card Fraud Detection," Proc. IEEE Int'l Conf. e-Technology, e-Commerce and e Service, pp. 177-181, 2004.
[5] C. Phua, V. Lee, K. Smith, and R. Gayler, "A Comprehensive Survey of Data Mining-Based Fraud Detection Research," http:// www.bsys.monash.edu.au/people/cphua/, Mar. 2007.
[6] SoheilaEhramikar, Jan 2010, The Enhancement of ATM cum Debit Card Fraud Detection Systems Book.
[7] David A. Montague, 2010, Fraud Prevention Techniques for ATM cum Debit Card Fraud.