Credit Card Fraud Detection UsingHidden Markov Model

Divya Singh, Asst. Prof. Rakesh Pandit

Abstract— As in present scenario the credit cards or netbanking is very popular and most preferred mode of transaction.The security of these transaction is also a major issue.In this paper we have given the theory to use three key factors of check on any transaction which is firstly trained by the HMM.This is to make the transactions more secure than the previously given theories.We firstly create the behavioural pattern of any user using HMM,afterwards if the transaction is not accepted by the given model than we consider it as security threat or fraud and send an alert to user to verify.

Index Terms — Online fraud detection, Credit card frauds, HMM, frauds.

1 INTRODUCTION

ONE of the recent survey finds that 27% of cardholders (debit, credit and prepaid) around the world have experienced fraud in the past five years. Rates of fraud vary across countries but in Mexico and the United States are more prone to fraud with 44% and 42% of respondents there saying they've experienced card fraud.

The report from Aite Group and ACI Worldwide, which surveyed over 5,000 consumers in 17 countries, notes that U.S. consumers are heavy card users–"more card use means a greater likelihood for card fraud."

As per a survey by Google on credit card frauds in the world, Pune suffered the most in India with Mumbai coming second.

There are various ways like phishing, pharming, skimming and dumpster diving by which money can be extracted from your credit card. Due to lack of awareness, people submit personal details and credit card information to fraudulent emails. Sometimes, fraudsters steal credit card information.

The use of credit card is increasing day to day not only in shops ,malls or others places but also in online shopping, ticket bookings etc. because it provides the cashless mode of payment to the user. As the increase of its popularity the rate of frauds in credit card transaction have also increased.

Credit card can be used in two ways:

1. When the user is present physically with the card during the transaction, it can be categorized as Physical purchasing.
2. When a user uses the card virtual like in online shops on internet that only requires the card information for transaction.

If a cardholder doesn't realize loss of his card, then a fraudulent transaction can take place and sometimes is comes as a substantial loss of amount for bank or the authority.

The virtual card transactions can be done on internet or telephones for making payment. It requires only the information on the card like CVV no. expiry date etc.

Important information has been hacked by the hacker on internet for example phishing sites or fake sites. It can also create problem for user as this information can be easily used by the hacker for making fraudulent transactions, which will be a financial loss for the cardholder.

As the existing fraud detection systems are not sufficient to detect the fraud during the transaction.

The only way to detect this kind of fraud is to analyze the spending patterns on every card and to figure out any inconsistency with respect to the "usual" spending patterns. Fraud detection based on the analysis of existing purchase data of cardholder is a promising way to reduce the rate of successful credit card frauds. Since humans tend to exhibit specific behaviorist profiles, every cardholder can be represented by a set of patterns containing information about the typical purchase category, the time since the last purchase, the amount of money spent, etc.

Here it is shown that how HMM can be used to create a secure transaction system because it is trained with the normal behavior of the user of that card and uses that pattern to detect whether the transaction being made is fraud or not.

2 RELATED WORKS

2.1 Literature Survey

There are different theories and approaches have been given before for learning and fraud detection which are-

1. Fusion Approach using Dempster- shafer and Bayesian learning.
2. BLAST - SSHAHA Model.
3. Fuzzy-Darwinian Detection.

- *Divya Singh is currently pursuing masters' degree program in information technology from Patel College of Science & Technology Indore, University- Rajiv Gandhi Proudyogiki Vishwavidyalaya, India, PH- 09424172527. E-mail: singh.divya.787@gmail.com*
- *Rakesh Pandit is currently workingas Asst. Prof. in Information Technology Dept. Patel College of Science & Technology Indore, India, PH- 09826911228. E-mail: rakesh_pandit@yahoo.com*

4. Hidden Markov Model.
5. Bayesian and Neural Network.

DEMPSTER SHAFER theory introduced a fraud detection system in which the present as well as the past behavior of a customer is observed together and the behavior is said to be the customer's particular purchasing pattern or expenditure.An activity profile based upon the behavior is created for every customer.It provides high accuracy, speed and less number of false alarms, but the only disadvantage is its expesive cost [2].

In second approach i.e. BLAST SSHAHA, a hybrid model of two BLAST and SSHA algorithms is given .This is known as BLAH FDSalgorithm,It is a two stage sequence alignment algorithm used to analyze the behavior of a customer upon their spending.It provides good performance, speed and accuracy.It is used in Telecommunication and banking systems[2].

In third approach, a fuzzy system using genetic programmming for evolving fuzzy logic is used .It uses genetic programming search algorithm and a fuzzy expert system.It gives very high accuracy and low false alarms but it can not be used for online transactions and also a very expensive and low speed system.

In fourth approach Baum Welch algorithm is used with K-means algorithm.Baulm Welch is used for training the model on customer behavior a three price ranges low, medium and high and clustering is used to store data in thhe ranges.This FDS checks the transaction being processed is genuine or not.So a log file is maintained by HMM.

Baysian and Nueral Network ,is a type of artificial intelligence programming with various methods including machine learning supervised and datamining for reasoning.Neural network learn by itself , it don't need to be reprogrammed for different situations.It gives high accuracy and speed.

Web services and data mining technique screen draft for detecting fruads in banking Industry was proposed by Chiu and Tsai.In this system the grouped banks share the knowledge of frauds on the part of the distributed environment.

A metalearning system for fraud detection was proposed by Stolfo et al.It was trained on frankincense metaclassifiers.After that they worked model depended upon the costs to detect the fraud [3].

Gosh and Reilly proposed the neural network for detecting such fraud by the system, it is trained on account transactions.

2.2 Hidden Markov Model

A Hidden Markov Model is a finite learnable stochastic automate.It can be summarized as a kind of double stochastic process with the two followed aspects [2].

i. The first process is a finite set of a state, where each of them is generally associated with multidimensional probability distribution.The transition between the different states are statistacally organized by a set of probabilities called transition probabilities.

ii. In second process, in any state an event can be observed.That means we observe and analyze an event without knowing at which state it occurred.So the states are called "hidden"as they are hidden to the observer.

The Hidden Markov Model is defined by states, state probabilities, transition probabilities, emission probabilities and initial probabilities.

The five main elements of Hidden Markov Model are defined here which are used in our work {1}

1. The N states of a model is defined by

$$S= \{S_1, S2\ldots\ldots S_n\}$$

2. The M observational symbols per state are-

$$V= \{V_1, V2\ldots.. Vn\}$$

We are considering two price ranges minimum and maximum.So here the M=2 second observation is made upon location of the customer that is previous location and current location.The third observation istime taken to give detail entries.

3. The state transition probability are the fixed probability for making a translation from state i to j.It is denoted by t (i, j).For initial state y, we denote the initial probabilities as

$$Pyn+1=j|yn=i,\ yn-1=in-1...\ y1=i1=Pyn+1=j|yn=i=ti,\ j$$

4. The probability that the nth observation will be $x_n = x$ depends only on the underlying state y_n, hence

$$Pxn=x|yn=i,\ yn-1,\ xn-1...=Pxn=x|yn=i=ex|i$$

For all possible observations x ∈O, all state i ∈S, and all n this is called the emission probability of x at state i, and we denote it by e(x | i). The three probability measures t (i, j), ɪɪ (i), and e(x | i) completely specify an HMM. For convenience, we denote the set of these parameters as Θ.

The main problems that we have to consider before using HMMs in practical applications are [1].

Scoring Problem- computing the probability P {x|O} is a natural way of scoring a new observation sequence x, its underlying state sequence is not directly observable and there can be many stable sequence that yields x.Therefore one way to compute the observation possibility is to consider all possible state sequences for the given x and sum up the probabilities as follow-

$$Px|\Theta=\sum yPx,\ y|\Theta.$$

However, this is computationally very expensive, since there are M^L possible state sequences. For this reason, we definitely need a more efficient method for computing $P\{\mathbf{x} \mid \Theta\}$. There exist a dynamic programming algorithm, called the *forward algorithm*, that can compute $P\{\mathbf{x} \mid \Theta\}$ in an efficient manner. Instead of enumerating all possible state sequences, this algorithm defines the following *forward variable*

$$\alpha n,\ i=Px1...xn,\ yn=i|\Theta.$$

This variable can be recursively computed using the following formula

$$\alpha n,\ i=\sum k\alpha n-1,ktk,iexn|i,$$

For n = 2... L. At the end of the recursions, we can compute $Px|\Theta=\sum k\alpha L,\ k$. This algorithm computes the observation probability of **x** with only O (LM^2) computations. Therefore, the amount of time required for computing the probability increases only linearly with the sequence length L, instead of increasing exponentially.

Another practically important problem is to find the optimal state sequence, or the optimal path, in the HMM that maximizes the observation probability of the given symbol sequence **x**, among all possible state sequences **y**, we want to find the

state sequence that best explains the observed symbol sequence. This can be viewed as finding the best alignment between the symbol sequence and the HMM, hence it is sometimes called the *optimal alignment* problem. Formally, we want to find the optimal path $\mathbf{y}^*$ that satisfies the following

$$y*=\text{argmax}_y P(y \mid x, \Theta)$$

Note that this is identical to finding the state sequence that maximizes $P\{\mathbf{x},\mathbf{y} \mid \Theta\}$, since we have

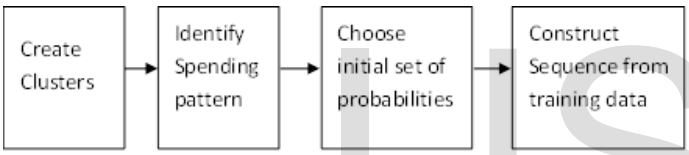
$$P(y \mid x, \Theta) = P(x, y \mid \Theta) / P(x \mid \Theta).$$

Finding the optimal state sequence $\mathbf{y}^*$ by comparing all M^L possible state sequences is computationally infeasible. However, we can use another dynamic programming algorithm, well-known as the *Viterbi algorithm.*

3 Proposed System

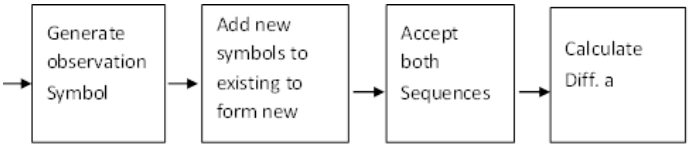
3.1 Training Phase

For training the HMM, we convert the cardholder's transaction amount into observation symbols and form sequences out of them. At the end of the training phase, we get an HMM corresponding to each cardholder. Since this step is done offline, it does not affect the credit card transaction processing performance, which needs online response.



3.1 Detection Phase

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 formed from the cardholder's transactions up to time t. First input this sequence to the HMM and compute the probability of acceptance by the HMM.



4 Expected Outcome

The different steps in credit 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.

5 Research Objective

There is no such method has been implemented by the banking systems to detect the frauds during the transactions to prevent it from taking place. This is an appropriate method to stop such frauds. As many researches have been done in this area but methods have drawbacks too. The problem with most of the mentioned approaches is that they require labeled 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 labeled data is not available. In contrast, a Hidden Markov Model (HMM)-based credit card FDS, which does not require fraud signatures and yet is able to detect frauds by considering a cardholder's spending habit. We model a credit card transaction processing sequence by the stochastic process of an HMM.

The different steps in credit 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.

6 Conclusion

In present scenario where online mode of payment and fraud associated to it drastically increasing, the need of a security system is highly required which can detect the fraud before it can take place.Some of the systems which had been proposed are studied here.In this paper we have observered various approaches already present and tried to propose a system that is an advancement of previously given system for Fraud detection using HMM.

7 References

[1] LAWRENC R. RABINER, 2012. A Tutorial on Hidden Markov Models and Speech Recognition. http://www.cs.cornell.edu/Courses/cs4758/2012sp/materials/hmm_paper_rabiner.pdf

[2] Abhinav Srivastava, Amlan Kundu, Shamik Sural, Arun K. Majumdar."Credit Card Fraud Detection using Hidden Markov Soheila Ehramikar, Jan 2010, The Enhancement of Credit Card Fraud Detection Systems Book.

[3] S. Stolfo and A.L. Prodromidis, "Agent-Based Distributed Learning Applied to Fraud Detection," Technical Report CUCS-014-99, Columbia Univ., 1999.

[4] S.B. Cho and H.J. Park, "Efficient Anomaly Detection by Modeling-Privilege Flows Using Hidden Markov Model," Computer and Secu-

rity.

[5] David A. Montague, 2010, Fraud Prevention Techniques for Credit Card Fraud.

[6] JERMY QUITTNER. "AVOIDING CREDIT CARD FRAUD". http://abcnews.go.com/business/financialSecurity/Story?id=89746&page=12004.

[7] S. Benson Edwin Raj, A. Annie Portia "Analysis on Credit Card Fraud Detection Methods". International Conference on Computer, Communication and Electrical Technology – ICCCET2011, 18th &19th March, 2011.