Application of Hidden Markov Model in Credit Card Fraud Detection

V. Bhusari[1], S. Patil[1]

[1]Department of Computer Technology, College of Engineering,
Bharati Vidyapeeth, Pune, India, 400011
Email: vrunda1234@gmail.com

ABSTRACT

In modern retail market environment, electronic commerce has rapidly gained a lot of attention and also provides instantaneous transactions. In electronic commerce, credit card has become the most important means of payment due to fast development in information technology around the world. As the usage of credit card increases in the last decade, rate of fraudulent practices is also increasing every year. Existing fraud detection system may not be so much capable to reduce fraud transaction rate. Improvement in fraud detection practices has become essential to maintain existence of payment system. In this paper, we show how Hidden Markov Model (HMM) is used to detect credit card fraud transaction with low false alarm. An HMM based system is initially studied spending profile of the card holder and followed by checking an incoming transaction against spending behavior of the card holder, if it is not accepted by our proposed HMM with sufficient probability, then it would be a fraudulent transaction.

Keywords

Credit card, Hidden Markov Model, fraud transaction

1. Introduction

In day to day life, online transactions are increased to purchase goods and services. According to Nielsen study conducted in 2007-2008, 28% of the world's total population has been using internet [1]. 85% of these people has used internet to make online shopping and the rate of making online purchasing has increased by 40% from 2005 to 2008. The most common method of payment for online purchase is credit card. Around 60% of total transaction was completed by using credit card [2]. In developed countries and also in developing countries to some extent, credit card is most acceptable payment mode for online and offline transaction. As usage of credit card increases worldwide, chances of attacker to steal credit card details and then, make fraud transaction are also increasing. There are several ways to steal credit card details such as phishing websites, steal/lost credit cards, counterfeit cards, theft of card details, intercepted cards etc [3]. The total amount of credit card online fraud transaction made in the United States itself was reported to be $1.6 billion in 2005 and estimated to be $1.7 billion in 2006 [4].

Credit card can be used to purchases goods and services using online and offline transaction mode. It can be divided into two types: 1) physical card and 2) virtual card. In the physical card based purchase, card holder has to produce the card at the merchant counter and merchant will sweep the card in the EMV (Europay, MasterCard and Visa) machine. Fraud transaction can be happened in this mode, only after the card has been stolen. It will be difficult to detect fraud in this type of transaction. If the card holder does not realize loss of the card and does not report to police or card issuing company, it can give financial loses to issuing authorities. In the second method of purchasing i.e. online, these transactions generally happen on telephone or internet

DOI : 10.5121/ijdps.2011.2618

and to make this kind of transaction, the user will need some important information about a credit card (such as credit card number, validity, CVV number, name of card holder). To make fraud transaction to purchase goods and services, fraudster will need to know all these details of card only then he/she will make transactions. Most of the time, the cardholder may or may not know that when or where any person will be seen or stolen card information. To detect this kind of fraud transaction, we have proposed a Hidden Markov Model which is studying spending profile of the card holder. An HMM is to analyze the spending profile of each card holder and to find out any discrepancy in the spending patterns. Fraud detection can be detected on analyzing of previous transactions data which helps to form spending profile of the card holder. Every card holder having unique pattern contains information about amount of transactions, details of purchased items, merchant information, date of transaction etc. It will be the most effective method to counter fraud transaction through internet. If any deviation will be noticed from available patterns of the card holder, then it will generate an alarm to the system to stop the transaction. Various techniques for the detection of credit card fraud transaction have been proposed in last few years, are briefly explained some of them in section 2.

2. Other credit card fraud detection techniques

Credit card fraud detection has received an important attention from researchers in the world. Several techniques have been developed to detect fraud transaction using credit card which are based on neural network, genetic algorithms, data mining, clustering techniques, decision tree, Bayesian networks etc.

Ghosh and Reilly [5] have proposed a neural network method to detect credit card fraud transaction. They have built a detection system, which is trained on a large sample of labeled credit card account transactions. These sample contain example fraud cases due to lost cards, stolen cards, application fraud, stolen card details, counterfeit fraud etc. They tested on a data set of all transactions of credit card account over a subsequent period of time.

Bayesian networks are also one technique to detect fraud, and have been used to detect fraud in the credit card industry [6]. This techniques yield better results but having large cycle time to detect fraud. However, the time constraint is one main disadvantage of this technique, especially compared with neural networks.

Another algorithm that has been suggested by Bentley [7] is based on genetic programming. A Genetic algorithm is used to establish logic rules capable of classifying credit card transactions into suspicious and non-suspicious classes. Basically, this method follows the scoring process in which overdue payment was checking against last three month payment. If it is greater than that of last three month, then it will be considered as suspicious or else it will be non suspicious.

The idea of a similarity tree using decision tree logic has been reported in 1997 by Kokkinaki [8]. A decision tree is defined recursively; it contains nodes and edges that are labeled with attribute names and with values of attributes, respectively. All of these satisfy some condition and get an intensity factor which is defined as the ratio of the number of transactions that satisfy applied conditions over the total number of legitimate transaction. The advantages of the method are easy to understand and implement. However, disadvantages of the methods are that a long time period and check each transaction one by one.

The next is clustering technique proposed by Bolton and Hand in 2002 [9]. In this technique, clustering of two algorithms have used for behavioral fraud detection. The proposed system was identified those accounts that are behaving differently from others at the particular moment whereas they were behaving the same previously. Those accounts are treating as suspicious ones and fraud analysis is to be done only on these accounts. If break point analysis can identify suspicious behavior such as sudden transaction of high amount and high frequency, then card will be identified as fraudulent.

The data mining technique has been using from 1990. This technique was very time consuming and difficult process to detect fraud transaction. Since there are millions of transactions processed everyday and their data are highly skewed. The transactions are more legitimate than fraudulent. It requires highly efficient technique to scale down all data and also try to identify fraud transaction not legitimate transactions. Black Box technique has proposed by Chan in 1999 [10]. In this data mining technique, they have divided the whole data into subgroups and apply mining technique to generate classifiers. These classifiers treat as black box and applied variety of algorithms to these black boxes to detect fraud transactions.

3. Hidden markov model (HMM)

Hidden Markov Model is probably the simplest and easiest models which can be used to model sequential data, i.e. data samples which are dependent from each other. An HMM is a double embedded random process with two different levels, one is hidden and other is open to all.

The Hidden Markov Model is a finite set of *states*, each of which is associated with a probability distribution. Transitions among the states are governed by a set of probabilities called *transition probabilities.* In a particular state an outcome or *observation* can be generated, according to the associated probability distribution. It is only the outcome, not the state visible to an external observer and therefore states are "hidden" to the outside; hence the name Hidden Markov Model [11, 13].

HMM has been successfully applied to many applications such as speech recognition, robotics, bio-informatics, data mining etc [10-12].

In order to define an HMM completely, following elements are needed.

- The number of states of the model, *N*. We denote the set of states $S = \{S_1; S_2; S3; . . S_N\}$, where i =1; 2; . . .; N, is a number of state and S_i, is an individual state. The state at time instant t is denoted by q_t.
- The number of observation symbols in the alphabet, *M*. If the observations are continuous then *M* is infinite. We denote the set of symbols $V = \{V_1; V_2; . . . V_M\}$ where V_i, is an individual symbol for a finite value of M.

$$\Lambda = \{a_{ij}\}$$

- A set of state transition probabilities.

$$a_{ij} = P\{q_{t+1} = S_j \mid q_t = S_i\},\ 1\leq i, j \leq N,$$

where q_t denotes the current state,

Transition probabilities should satisfy the normal stochastic constraints,

$$a_{ij} \geq 0,\ 1 \leq i, j \leq N$$

And

$$\sum_{j=1}^{N} a_{ij} = 1,\ \ 1 \leq i \leq N,$$

- The observation symbol probability matrix B,

$$B = \{b_j(k)\}$$

A probability distribution in each of the states,

$$b_j\,(k) = P\{a_t = V_k \mid q_t = S_j\},\ 1 \leq\ j \leq N,\ 1 \leq k \leq M$$

where, V_k denotes the k^{th} observation symbol in the alphabet, and a_t the current parameter vector.

Following stochastic constraints must be satisfied.

$$b_j(k) \geq 0,\ 1 \leq j \leq N,\ 1 \leq k \leq M$$

And

$$\sum_{k=1}^{M} b_j\,(k) = 1,\ 1 \leq j \leq N$$

If the observations are continuous then we will have to use a continuous probability density function, instead of a set of discrete probabilities. In this case we specify the parameters of the probability density function. Usually the probability density is approximated by a weighted sum of *M* Gaussian distributions $\mathcal{N}$,

$$b_j(a_t) = \sum c_{jm}\,\mathcal{N}(\mu_{jm}, \sum jm, a_t)$$

where, c_{jm} = weighting coefficients,

μ_{jm} = mean vectors,

$\sum jm$ = Covariance matrices

c_{jm} should satisfy the stochastic constrains,

$$c_{jm} \geq 0,\ 1 \leq j \leq N,\ 1 \leq m \leq M$$

And

$$\sum_{m=1}^{M} c_{jm} = 1,\ 1 \leq j \leq N$$

- The initial state distribution, $\Pi = \{\Pi_i\}$,

where,

$$\Pi_i = P\{q_i = S_i\},\ 1 \leq i \leq N$$

$$\sum_{i=1}^{N} \Pi_i = 1$$

Therefore we can use the compact notation

$$\lambda = (\Lambda, B, \Pi)$$

to denote an HMM with discrete probability distributions, while

$$\lambda = (\Lambda, c_{jm}, \mu_{jm}, \sum jm, \Pi)$$

to denote one with continuous densities.

- Hidden Markov Model assumes that current output (observation) is statistically independent of the previous outputs (observations). We can formulate this assumption mathematically, by considering a sequence of observations,

$$O = O_1, O_2, O_3, \ldots.. O_R,$$

$$Q = q_1, q_2, q_3 \ldots\ldots q_R,$$

where R, is a number of observation in the sequence and Q, is a one particular sequence.

- Then according to the assumption for an HMM, probability that O is generated from this state sequence is given by

$$P\{O|q_1,q_2,q_3,\ldots q_R, \lambda\} = \prod_{t=1}^{R} P(O_t|q_t, \lambda)$$

$$P(O|Q,\lambda) = b_{q1}(O_1).b_{q2}(O_2)......b_{qR}(O_R).$$

The probability of the state sequence Q is given as

$$P(Q|\lambda) = \pi_{q1}.a_{q1q2}.a_{q2q3}......a_{qR-1qR}$$

Thus, the probability of generation of the observation sequence O by the HMM with respect to λ will be written as follows:

$$P(O|\lambda) = \sum_{\text{All } Q} P(O|Q, \lambda).P(Q|\lambda).$$

Calculation of probability P(O|λ) is an intensive computing process. Hence, a forward-backward algorithm [13] is used to calculate probability P(O|λ).

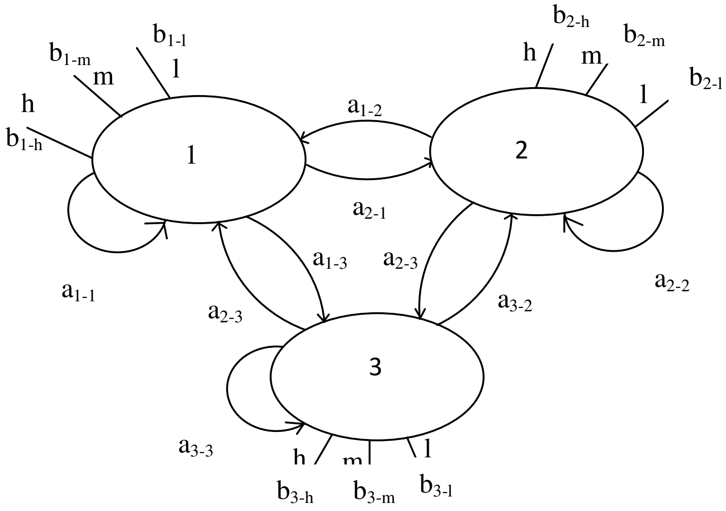

Fig. 1: Transition of different states

4. Application of HMM in credit card fraud detection

In this section, we present credit card fraud detection system based on Hidden Markov Model, which does not require fraud signatures and still is able to detect frauds just by bearing in mind a cardholder's spending habit. The important benefit of the HMM-based approach is an extreme decrease in the number of False Positives transactions recognized as malicious by a fraud detection system even though they are really genuine.

As we have shown that How HMM is useful for interstate transition in section 3. In this fraud detection system, we consider three different spending profiles of the card holder which is depending upon price range, named high (h), medium (m) and low (l). In this set of symbols, we define V = {l, m, h} and M =3. The price range of proposed symbols has taken as low (0, \$100], medium (\$100, \$500] and high (\$500, up to credit card limit]. After finalizing the state and symbol representations, the next step is to determine different components of the HMM, i.e. the probability matrices A, B, and π so that all parameters required for the HMM is known. These three model parameters are determined in a training phase using the forward-backward algorithm [13]. The initial choice of parameters affects the performance of this algorithm and, hence, it is necessary to choose all these parameters carefully. We consider the special case of fully connected HMM in which every state of the model can be reached to every other state just in a single step, as shown in Fig. 1. 1, 2, 3 etc., are names given to the states to denote different purchase types such as bill payment, restaurant, electronics items etc.

In the figure 1, it has been shown that probability of transition from one state to another (for example from 1 to 2 and vice versa, represented as a_{1-2} and a_{2-1}, respectively) and also probabilities of transition from a particular state (1, 2, or 3) to different spending habits h, m, or l (for example, $b_{1\text{-}h}$, $b_{1\text{-}m}$, etc.).

The most important thing is to estimate HMM parameters for each card holder. The forward-backward algorithm starts with initial HMM parameters and converges to the nearest likelihood values.

After deciding HMM parameters, we will consider to form an initial sequence of the existing spending behavior of the card holder. Let O_1, O_2, O_R be consisting of R symbols to form a sequence. This sequence is recorded from cardholder's transaction till time t. We put this sequence in HMM model to compute the probability of acceptance. Let us assume be this probability is α_1, which can be calculated as

$$\alpha_1 = P\ (O_1, O_2, O_3, \ldots O_R \mid \lambda),$$

Let O_{R+1} be new generated sequence at time t+1, when a transaction is going to process. The total number of sequences is R+1. To consider R sequences only, we will drop O_1 sequence and we will have R sequences from O_2 to O_{R+1}.

Let the probability of new R sequences be α_2

$$\alpha_2 = P\ (O_2, O_3, O_4, \ldots .O_{R+1} \mid \lambda),$$

Hence, we will find

$$\Delta\alpha = \alpha_1 - \alpha_2,$$

If $\Delta\alpha > 0$, it means that HMM consider new sequence i.e. O_{R+1} with low probability and therefore, this transaction will be considered as fraud transaction if and only if percentage change in probability is greater than a predefined threshold value.

$$\Delta\alpha/\ \alpha_1 \geq \text{threshold value},$$

The threshold value can be calculated empirically. This Fraud detection system if finds that the present transaction is a malicious, then credit card issuing bank will regret the transaction and FDS discard to add O_{R+1} symbol to available sequence. If it will be a genuine transaction, FDS will add this symbol in the sequence and will consider in future for fraud detection.

5. Results and discussion

It is very difficult to do simulation on real time data set which is not providing from any credit card bank on security reasons. In Table 1, it is shown that a random data set of all transactions happened is categorized according to their types of purchase. With the help of this, we calculate probability of each spending profile (h, l and m) of every category (1, 2 and 3). Fraud detection of incoming transaction will be checked on last 10 transactions.

Table 1, list of all transactions happened till date

No. of Transaction	Category	Amount	No. of Transaction	Category	Amount
1st	1	140	10th	1	55
2nd	3	125	11th	1	210
3rd	2	120	12th	3	550
4th	2	40	13th	3	160
5th	1	15	14th	2	695
6th	3	10	15th	2	342
7th	1	520	16th	1	28
8th	2	74	17th	2	507
9th	2	190	18th	2	610

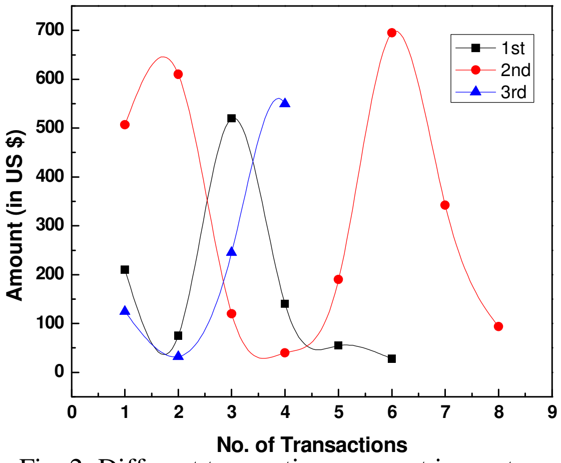

Fig. 2: Different transactions amount in a category

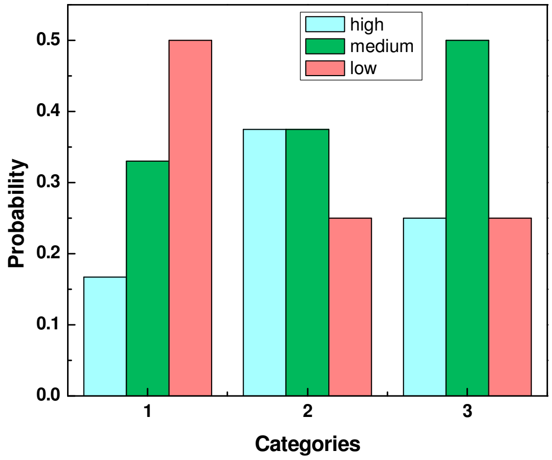

Fig. 3: Probabilities of different spending profiles of each category

In Fig. 3, it is shown that the amount of purchased items or services in different categories such as 1st for restaurant, grocery etc., 2nd for bill payment, balance transfer etc. and 3rd for ticket reservation, electronic devices etc., with respect to their number of transactions.

We have simulated several large data sets; one is shown in Table 1, in our proposed fraud detection system and found out probability mean distribution of false and genuine transactions. In Fig. 4, it is noted that when probability of genuine transaction is going down, correspondingly probability of false transaction going up and vise versa. If the percentage change in probability of false transaction will be more than threshold value, then alarm will be generated for fraudulent transaction and credit card bank will decline the same transaction.

6. Conclusion

In this paper, we have discussed that How Hidden Markov Model will be useful to detect fraudulent online transaction through credit card. The proposed Fraud Detection System is also scalable for handling vast volumes of transactions data processing. The HMM based credit card fraud detection system is not having complex process to perform fraud check like the existing system. Proposed Fraud detection system gives genuine and fast result than existing system. The Hidden Markov Model makes the processing of detection very easy and tries to remove the complexity.

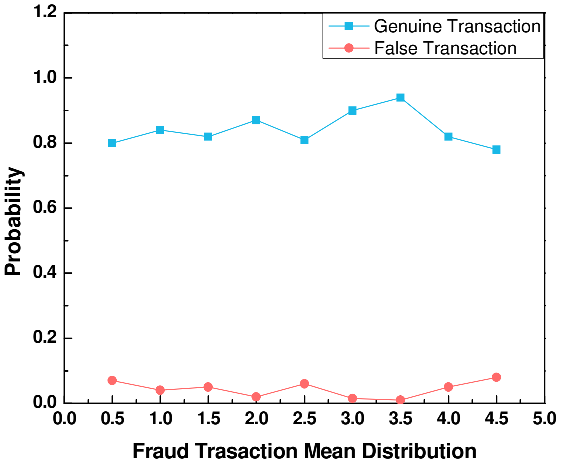

Fig. 4: Fraud Transaction Mean Distribution

In this paper, we have shown that HMM initially checks the upcoming transaction is fraudulent or not. It also takes decision to add new upcoming transaction to existing sequence or not which will be dependent on percentage change in probabilities of old and new sequence. It will decide whether this transaction is genuine or fraudulent depending on threshold values. We have categorized different types of items and services such as restaurant, bill payment etc. These different categories have been considered as three different states of the Hidden Markov Model. In each category, we have further divided into three different groups, high, medium and low based on different ranges of transaction amount. These groups were considered as observation symbols. This technique helps to find the spending behavioral habit of cardholders and purchasing of different items. The most important application of this technique is to decide initial value of observation symbols, probability of transition states and initial estimation of the model parameters.

In our proposed model, we have found out more than 88% transactions are genuine and very low false alarm which is about 8 % of total number of transactions.

The relative studies and our results sure that the correctness and effectiveness of the proposed system is secure to 82 percent over a broad deviation in the input data.

7. References

[1] Internet usage world statistics, (http://www.internetworldstats.com/stats.htm) (2011).

[2] Trends in online shopping, a Global Nelson Consumer Report, (2008).

[3] European payment cards fraud report, Payments, Cards and Mobiles LLP & Author, (2010).

[4] Statistics for General and On-Line Card Fraud, (2007).

[5] Ghosh, Sushmito & Reilly, Douglas L., (1994) “Credit Card Fraud Detection with a Neural-Network”, *Proc. of 27th Hawaii Int’l Conf. on System Science: Information systems: Decision Support and Knowledge-Based Systems,* Vol.3, pp. 621-630.

[6] Maes, Sam, Tuyls Karl, Vanschoenwinkel Bram & Manderick, Bernard, (2002) “Credit Card Fraud Detection Using Bayesian and Neural Networks”, *Proc. of 1st NAISO Congress on Neuro Fuzzy Technologies. Hawana.*

[7] Bentley, Peter J., Kim, Jungwon, Jung, Gil-Ho and Choi, Jong-Uk, (2000) “Fuzzy Darwinian Detection of Credit Card Fraud”, *Proc. of 14th Annual Fall Symposium of the Korean Information Processing Society.*

[8] Kokkinaki, A. I., (1997) "On Atypical Database Transactions: Identification of Probable Frauds Using Machine Learning for User Profiling", *IEEE Knowledge and Data Engineering Exchange*

Workshop, kdex, pp.107.

[9] Bolton, Richard J. & Hand, David J., (2002) "Statistical Fraud Detection: A Review", *Statistical Science*, Vol.10, No. 3, pp. 235-255.

[10] Chan, Philip K., Fan, Wei, Prodromidis, Andreas L. & Stolfo, Salvatore J., (1999) "Distributed Data Mining in Credit Card Fraud Detection", *IEEE Intelligent Systems*, Vol. 14, No. 6, pp. 67-74.

[11] Rabiner, Lawrence R., (1989) "A Tutorial on Hidden Markov Models and Selected Applications in Speech Recognition", *Proc. of IEEE,* Vol. 77, No. 2, pp. 257-286.

[12] Fonzo, Valeria De, Aluffi-Pentini, Filippo and Parisi, Valerio, (2007) "Hidden Markov Models in Bioinformatics", *Current Bioinformatics*, Vol. 2, pp. 49-61.

[13] Srivastava, Abhinav, Kundu, Amlan, Sural, Shamik and Majumdar, Arun K., (2008) "Credit Card Fraud Detection Using Hidden Markov Model", *IEEE Transactions on Dependable and Secure Computing*, Vol. 5, No. 1, pp. 37-48.

Author

Vrunda Bhusari received B. E. degree in computer technology from Kavikulguru Institute of Technology and Science, Nagpur in 2007 and currently perusing M Tech in computer science from Bharati VidyaPeeth, Pune. Her research interests include data mining, network security and database security.