A Novel Approach for Credit Card Fraud Detection Targeting the Indian Market

Jaba Suman Mishra[1], Soumyashree Panda[2], Ashis Kumar Mishra [3]

[1] Department Of Computer Science & Engineering , College Of Engineering & Technology(BPUT), Bhubaneswar, Pin-751003 , Odisha, India

[2] Department Of Computer Science & Engineering , College Of Engineering & Technology(BPUT), Bhubaneswar, Pin-751003 , Odisha, India

[3] Department Of Computer Science & Engineering , College Of Engineering & Technology(BPUT), Bhubaneswar , Pin-751003, Orissa, India

Abstract

Due to a rapid advancement in the electronic commerce technology, the use of credit cards has dramatically increased. So, the rate of fraudulent practices is also increasing every year. In this paper we present the necessary theory to detect fraud in credit card transaction processing using a Hidden Markov Model. If an incoming credit card transaction is not accepted by the Hidden Markov Model with sufficiently high probability, it is considered to be fraudulent. At the same time, we try to ensure that genuine transactions are not rejected. We show how HMM helps to obtain high fraud coverage combined with a low false alarm rate. The existing models detect that a fraud has occurred only after the fraudulent transaction is completed but in our proposed model, we have shown how it can be reported instantly while the fraudulent transaction is on process.

Keywords: *Electronic commerce, Credit card, Fraud detection system, Hidden Markov Model, False alarm.*

1. Introduction

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].

In online payment mode, attackers need only little information for doing fraudulent transaction (secure code, card number, expiration date etc.). In this purchase method, mainly transactions will be done through Internet or telephone. To commit fraud in these types of purchases, a fraudster simply needs to know the card details. Most of the time, the genuine cardholder is not aware that someone else has seen or stolen his card information. 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 behavioristic 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. Deviation from such patterns is a potential threat to the system.

Several techniques for the detection of credit card fraud have been proposed in the last few years. We briefly review some of them in the Literature Survey.

In this paper, we model the sequence of operations in credit 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 credit card transaction is not accepted by the trained HMM with

sufficiently high probability, it is considered to be fraudulent. 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.

The first section gives a brief idea of the different research works done on credit card fraud detection which helps us to decide the most efficient method for it. The next section deals with the necessity for credit card fraud detection also giving an overview of HMM model as a solution to it. Finally we conclude with the result based on various analysis done.

2. LITERATURE REVIEW

Credit card fraud detection has drawn a lot of research interest and a number of techniques, with special emphasis on neural networks, data mining and distributed data mining have been suggested. Ghosh and Reilly [8] have proposed credit card fraud detection with a neural network. They have built a detection system, which is trained on a large sample of labeled credit card account transactions. These transactions contain example fraud cases due to lost cards, stolen cards, application fraud, counterfeit fraud, mail-order fraud, and non received issue (NRI) fraud. Recently, Syeda et al. [9] have used parallel granular neural networks (PGNNs) for improving the speed of data mining and knowledge discovery process in credit card fraud detection. A complete system has been implemented for this purpose. Stolfo et al. [10] suggest a credit card fraud detection system (FDS) using meta-learning techniques to learn models of fraudulent credit card transactions. Meta-learning is a general strategy that provides a means for combining and integrating a number of separately built classifiers or models. A meta-classifier is thus trained on the correlation of the predictions of the base classifiers. The same group has also worked on a cost-based model for fraud and intrusion detection. They use Java agents for Meta-learning (JAM), which is a distributed data mining system for credit card fraud detection. A number of important performance metrics like True Positive—False Positive (TP-FP) spread and accuracy have been defined by them. Aleskerov et al. [11] present CARDWATCH, a database mining system used for credit card fraud detection. The system, based on a neural learning module, provides an interface to a variety of commercial databases. Kim and Kim [12] have identified skewed distribution of data and mix of legitimate and fraudulent transactions as the two main reasons for the complexity of credit card fraud detection. Based on this observation, they use fraud density of real transaction data as a confidence value and generate the weighted fraud score to reduce the number of misdetections. Fan et al. [13] suggest the application of distributed data mining in credit card fraud detection. Brause et al. [14] have developed an approach that involves advanced data mining techniques and neural network algorithms to obtain high fraud coverage. Chiu and Tsai [15] have proposed Web services and data mining techniques to establish a collaborative scheme for fraud detection in the banking industry. With this scheme, participating banks share knowledge about the fraud patterns in a heterogeneous and distributed environment. To establish a smooth channel of data exchange, Web services techniques such as XML, SOAP, and WSDL are used. Phua et al. [16] have done an extensive survey of existing data-mining-based FDSs and published a comprehensive report. Prodromidis and Stolfo [17] use an agent-based approach with distributed learning for detecting frauds in credit card transactions. It is based on artificial intelligence and combines inductive learning algorithms and metal earning methods for achieving higher accuracy. Phua et al. [18] suggest the use of meta-classifier similar to in fraud detection problems. They consider naïve Bayesian, and Back Propagation neural networks as the base classifiers. A meta-classifier is used to determine which classifier should be considered based on skewness of data. Although they do not directly use credit card fraud detection as the target application, their approach is quite generic. Vatsa et al. [19] have recently proposed a game-theoretic approach to credit card fraud detection. They model the interaction between an attacker and an FDS as a multi stage game between two players, each trying to maximize his payoff. HMM-based applications are common in various areas such as speech recognition, bioinformatics, and genomics. In recent years, Joshi and Phoba [20] have investigated the capabilities of HMM in anomaly detection. They classify TCP network traffic as an attack or normal using HMM. Cho and Park [21] suggest an HMM-based intrusion detection system that improves the modeling time and performance by considering only the privilege transition flows based on the domain knowledge of attacks. Ourston et al. [22] have proposed the application of HMM in detecting multistage network attacks. Hoang et al. [23] present a new method to process sequences of system calls for anomaly detection using HMM. The key idea is to build a multilayer model of program behaviors based on both HMMs and enumerating methods for anomaly detection. Lane [24] has used HMM to model human behavior. Once human behavior is correctly modeled, any detected deviation is a cause for concern since an attacker is not expected to have a behavior similar to the genuine user. Hence, an alarm is raised in case of any deviation.

3. PROPOSED MODEL

3.1 HMM Background

It is a double embedded stochastic process with two hierarchy levels. A Hidden Markov Model is a finite set of states; each state is linked with a probability distribution. Transitions among these states are governed by a set of probabilities called transition probabilities. In a particular state a possible outcome or observation can be generated which is associated symbol of observation of probability distribution. It is only the outcome, not the state that is visible to an external observer and therefore states are "hidden" to the outside; hence the name Hidden Markov Model.

An HMM can be characterized by the following:
1. N is the number of states in the model. We can denote the set of state as $S = \{S_1, S_2 \ldots S_N\}$. The state at time instant t is denoted by q_t.
2. M is the number of distinct observation symbols per state. The observation symbols correspond to the physical output of the system being modeled.
3. The state transition probability matrix $A = [A_{ij}]$.
4. The observation symbol probability matrix $B = [B_{jk}]$.
5. The observation sequence $O = O_1, O_2 \ldots O_N$.
It is evident that a complete specification of an HMM requires the estimation of two model parameters, N and M, and three probability distributions A, B, and π. We use the notation (A, B, π) to indicate the complete set of parameters of model, where A, B implicitly include N & M
6. N is the number of hidden states. [4]

3.2 Advantages of using HMM in the proposed model:

1. Hidden Markov Model is a perfect solution for addressing detection of fraud transaction through credit card.

2. 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.

There are 3 canonical problems to solve with HMMs as described in [5]:
1. Given the model parameters, compute the probability of a particular output sequence. This problem is solved by the Forward and Backward algorithms.
2. Given the model parameters, find the most likely sequence of (hidden) states which could have generated a given output sequence. Solved by the Viterbi algorithm and Posterior decoding.
3. Given an output sequence, find the most likely set of state transition and output probabilities. Then solve by the Baum-Welch algorithm.

- But according to [6], if we go through the above stated steps then there is a greater probability of High False Alarms, thereby degrading the Performance of the Fraud Detection System. So, our aim is to propose a Hidden Markov Model that aims at reducing High False Positives or High False Alarms and thereby improving the Performance of the System…

3.3 A Proposed Model

3.3.1 Credit Card Fraud Detection Using HMM

In this section, it is shown that system of credit card fraud detection based on Hidden Markov Model, which does not require fraud signatures and still it is capable to detect frauds just by bearing in mind a cardholder's spending habit. The particulars of purchased items in single transactions are generally unknown to any Credit card Fraud Detection System running either at the bank that issues credit cards to the cardholders or at the merchant site where goods is going to be purchased. As business processing of credit card fraud detection system runs on a credit card issuing bank site or merchant site. Each arriving transaction is submitted to the fraud detection system for verification purpose. The fraud detection system accept the card details such as credit card number, cvv number, card type, expiry date and the amount of items purchase to validate, whether the transaction is genuine or not. The implementation techniques of Hidden Markov Model in order to detect fraud transaction through credit cards, it create clusters of training set and identify the spending profile of cardholder. The number of items purchased, types of items that are bought in a particular transaction are not known to the Fraud Detection system, but it only concentrates on the amount of item purchased and use for further processing. It stores data of different amount of transactions in form of clusters depending on transaction amount which will be either in low, medium or high value ranges. It tries to find out any variance in the transaction based on the spending behavioral profile of the cardholder, shipping address, and billing address and so on. The probabilities of initial set have chosen based on the spending behavioral profile of card holder and construct a sequence for further processing. If the fraud detection system makes sure that the transaction to be of fraudulent, it raises an alarm, and the issuing bank declines the transaction. For the security purpose, the Security information module will get the information features and its store's in database. If the card lost then the Security information module form arises to accept the security information. The security form has a number of security questions like account number, date of birth, mother name, other personal question and their answer, etc. where the user has to answer it correctly to move to the transaction section. All these information

must be known by the card holder only. It has informational privacy and informational self determination that are addressed evenly by the innovation affording people and entities a trusted means to user, secure, search, process, and exchange personal and/or confidential information. The system and tools for pre-authorizing business provided that a connections tool to a retailer and a credit card-owner. The cardholder initiates a credit card transaction processing by communicating to a credit card number, card type with expiry date and storing it into database, a distinctive piece of information that characterizes a particular transaction to be made by an authoritative user of the credit card at a later time. The details are received as network data in the database only if an accurate individual recognition code is used with the communication. The cardholder or other authoritative user can then only make that particular transaction with the credit card. Since the transaction is Pre-authorized, the vendor does not need to see or transmit an accurate individual recognition code.

3.3.2 Fraud Detection System (FDS)

An FDS runs at a credit card issuing bank. Each incoming transaction is submitted to the FDS for verification. FDS receives the card details and the value of purchase to verify whether the transaction is genuine or not. The types of goods that are bought in that transaction are not known to the FDS. It tries to find any anomaly in the transaction based on the spending profile of the cardholder, shipping address, and billing address, etc. If the FDS confirms the transaction to be malicious, it raises an alarm, and the issuing bank declines the transaction. The concerned cardholder may then be contacted and alerted about the possibility that the card is compromised. In this section, we explain how HMM can be used for credit card fraud detection.

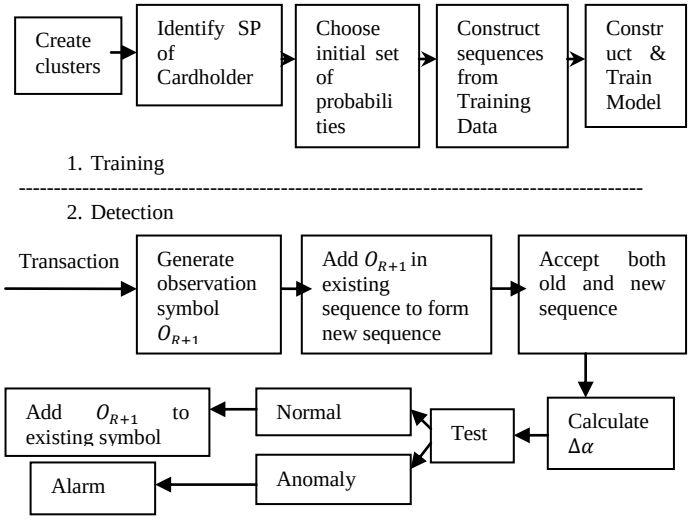

Fig. 1 Proposed Process Flow Diagram of FDS.

This system works in two phases:

1. Training phase.
2. Detection phase.

3.3.2.1 Training Phase

This is the important phase of the fraud detection system. In this phase the HMM is trained. 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.

So, the steps followed in the Training Phase are:

3.3.2.1.1 Dynamic Generation of Observation Symbols

To map the credit card transaction processing operation in terms of an HMM, we start by first deciding the observation symbols in our model. We quantize the purchase values x into M price ranges V_1, $V_2 \ldots V_M$. Forming the observation symbols at the issuing bank. The actual price range for each symbol is configurable based on the spending habit of individual cardholders. These price ranges can be determined dynamically by applying a clustering algorithm on the values of each cardholder's transactions. We use V_k, k=1, 2,…..M to represent both the observation symbol, as well as the corresponding price range. In this work, we consider only three price ranges, namely, low (l), medium (m), high (h). Our set of observations is therefore = {l, m, h} making M=3. If cardholder performs a transaction as Rupees 7000 and the cardholders profile groups are l = (0, 5000]; m = (5000, 25000]; h = (25000, up to Credit Card limit], then transaction which card holder want to do will come in medium profile group. So, the corresponding observation symbol is 'm'. Although various clustering techniques could be used, we use K-means clustering algorithm determine the clusters. K-means is an unsupervised learning algorithm for grouping a given set of data based on the similarity in their attribute (often called feature) values. [David A. Montague, 2010, Fraud Prevention Techniques for Credit Card Fraud.]

The **K-Means Clustering Algorithm** consists of basic steps. In this algorithm we initially determine the number of clusters present, assume it to be K and we also assume the center or centroid of these clusters. Now we can consider a random object as the initial centroids or we can also consider the sequence of first K objects as the centroids. Later the K-Means algorithm will carry

out the iteration of below stated 3 steps till the convergence.

Step1: Determine the centroid coordinate

Step2. Determine the distance of each object to the centroids.

Step 3.Group the object based on minimum distance (find the closest centroid).

In our work, K is the same as the number of observation symbols M. Let c_1, c_2….c_m be the centroids of the generated clusters. These centroids or mean values are used to decide the observation symbols when a new transaction comes in. Let x be the amount spent by the Cardholder u in transaction T. FDS generates the observation symbol for x (denoted by O_x) as follows:

$$O_x = V_{\arg\min_i |x-c_i|}. \quad (1)$$

As mentioned before, the number of symbols is 3 in our system. Considering M=3, if we execute K-means algorithm on the example transactions in Table 1, we get the clusters, as shown in Table 2, with c_l, c_m, c_h as the respective centroids. Since the model proposed here is for the Indian market, so we have taken all the transaction amounts in rupees.

Table 1: List of all Transactions happened till date.

Number of transactions	Amount(in rupees)	Number of transactions	Amount(in rupees)
1	7000	11	16500
2	6250	12	27500
3	750	13	40000
4	250	14	5500
5	500	15	1750
6	6250	16	5900
7	750	17	1000
8	6000	18	7400
9	500	19	7050
10	14000	20	300

In this section, it is shown that fraud detection will be checked on last 10 transactions and also calculate percentage of each spending profile (low, medium and high) based on total number of transactions. In Table 1, list of all transactions are shown. The most recent transaction is placed at the first position and correspondingly first transaction is placed at the last position in the table.

3.3.2.1.2 Finding Spending Profile (SP) of the Cardholders

The pattern of spending profile of the card holder is shown in Figure 2 based on all transactions done.

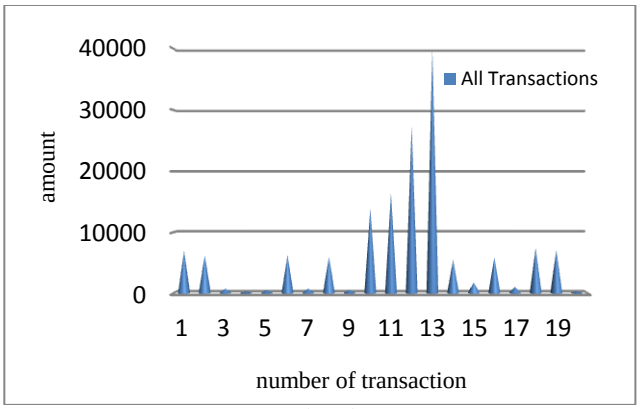

Fig. 2 Spending Profile of all Transactions.

Now we plot the output of the K-means Clustering Algorithm in Table 2.

Table 2: Output of K-means Clustering Algorithm.

Cluster mean/ centroid Name	c_l	c_m	c_h
Observation Symbol	V_1=l	V_2=m	V_3=h
Mean Value/Centroid	725	7585	33750
Percentage of total transaction	40%	50%	10%

The percentage calculation of each spending profile (low, medium and high) of the card holder based on price distribution range as mentioned earlier is shown in Fig. 3.

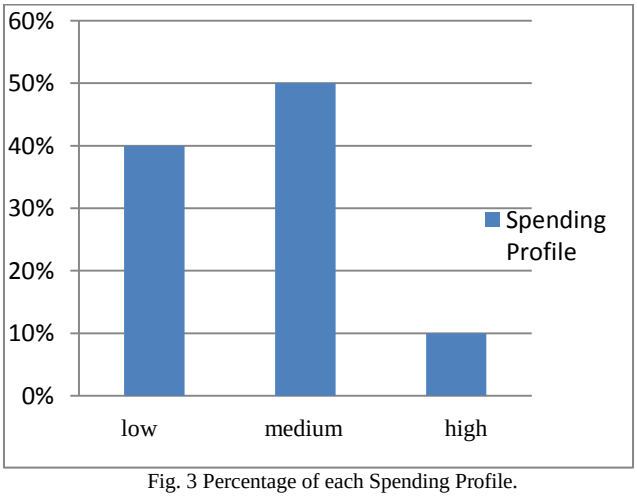

Fig. 3 Percentage of each Spending Profile.

3.3.2.1.3 Selection of the Best State Sequence

We select the best State sequence from the found observation sequence by using the Viterbi Algorithm. The **Viterbi algorithm** chooses the best state sequence that maximizes the likelihood of the state sequence for the given observation sequence.

Let $\delta_{t(i)}$ be the maximal probability of state sequences of length t that end in state i and produce the t first observations for the given model.

$\delta_t(i) = \max \{p(q(1),q(2),\ldots..,q(t-1); o(1),o(2),\ldots.o(t)|q(t)=q_i\}$ (1)

The Viterbi algorithm is a dynamic programming algorithm that uses the same schema as the Forward algorithm except for two differences:

1. It uses maximization in place of summation at the recursion and termination steps.
2. It keeps track of the arguments that maximize $\delta_t(i)$ for each t and i, storing them in the N by T matrix φ. This matrix is used to retrieve the optimal state sequence at the backtracking step.

3.3.2.1.4 Evaluation of HMM Parameters & Training the HMM model

We use Baum-Welch algorithm to estimate the HMM parameters for each cardholder. The algorithm starts with an initial estimate of HMM parameters A, B, and π and converges to the nearest local maximum of the likelihood function. Initial state probability distribution is considered to be uniform, that is, if there are N states, then the initial probability of each state is 1/N. Initial guess of transition and observation probability distributions can also be considered to be uniform. However, to make the initial guess of observation symbol probabilities more accurate, spending profile of the cardholder, as determined in the earlier section. Based on the cardholder's spending profile, we choose the corresponding set of initial observation probabilities. The initial estimate of symbol generation probabilities using this method leads to accurate learning of the model. Since there is no a priori knowledge about the state transition probabilities, we consider the initial guesses to be uniform.

Let us define $\varepsilon_t(i,j)$ the joint probability of being in state q_i at time t and state q_j at time (t+1), given the model and the observed sequence:

$\varepsilon_t(i,j)=P(q(t))=q_i,q(t+1)=q_j(O|A)$ (2)

Therefore we get,

$$\varepsilon_t(i,j) = \frac{\alpha_i(i)a_{ij}b_j\left(o(t+1)\right)\beta_{t+1}(j)}{P(O|A)} \quad (3)$$

The probability of output sequence can be expressed as

$P(O|A) = \sum_{i=1}^{N}\sum_{j=1}^{N}\alpha_t(i)\,a_{ij}b_j\left(o(t+1)\right)\beta_{i+1}(j) = \sum_{i=1}^{N}\alpha_t(i)\beta_t(i)$ (4)

The probability of being in state q_i at time t:

$\gamma_t(i) = \sum_{j=1}^{N}\varepsilon_t(i,j) = \frac{\alpha_t(i)\beta_t(i)}{P(O|A)}$ (5)

Estimates:

Initial probabilities

$\bar{p}_i = \gamma_1(i)$ (6)

Transition probabilities

$$\bar{\alpha}_{i,j} = \frac{\sum_{i=1}^{T-1}\varepsilon_t(i,j)}{\sum_{t=1}^{T-1}\gamma_t(i)} \quad (7)$$

Emission probabilities

$$\bar{b}_{jk} = \frac{\sum_{1}^{*}\gamma_t(j)}{\sum_{t=1}^{T}\gamma_t(j)} \quad (8)$$

In the above equation Σ^* denotes the sum over t such that $o(t) = o_k$. [7]

3.3.2.2 Detection Phase

Training phase is performed offline, whereas detection is an online 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 O_1, $O_2,\ldots$, O_R be one such sequence of length R. This recorded sequence is 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 α_1 which can be written as follows: $\alpha_1 = P(O_1, O_2 \ldots O_R | \lambda)$.

Let $O_{(R+1)}$ be the symbol generated by a new transaction at time t+1. To form another sequence of length R, we drop O_1 and append $O_{(R+1)}$ 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 α_2.

$\alpha_2 = P(O_1, O_2 \ldots O_R | \lambda)$ (9)

$\Delta\alpha = \alpha_1 - \alpha_2$ (10)

If $\Delta\alpha > 0$, it means that the new sequence is accepted by the HMM with low probability, and it could be a fraud. The newly added transaction is determined to be fraudulent if the percentage change in the probability is above a threshold, that is,

$\Delta\alpha / \alpha_1 \geq$ Threshold (11)

The threshold value can be learned empirically.

If $O_{(R+1)}$ is malicious, the issuing bank does not approve the transaction, and the FDS discards the symbol. Otherwise, $O_{(R+1)}$ is malicious, the issuing bank does not approve the transaction, and the FDS discards the symbol. Otherwise, $O_{(R+1)}$ is added in the sequence permanently, and the new sequence is used as the base sequence for determining the validity of the next transaction. The reason for including new non-malicious symbols in the sequence is to capture the changing spending behavior of a cardholder.

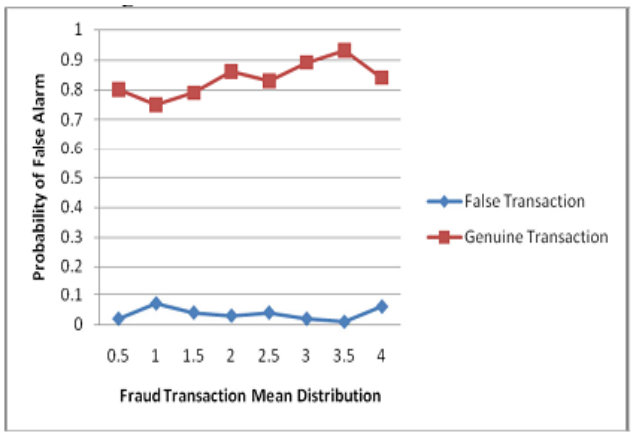

Fig. 4 Probability of False Alarm compared with Fraud Transaction Mean Distribution.

Fraud detection mean distribution is shown in Figure 4, where probability of false transaction compared with that of genuine transaction. In Fig. 4, it is noted that when probability of genuine transaction is going down correspondingly probability of false transaction is going to increase and vice-versa. It helps to find out the false alarm for the detection of fraud transaction. Hence, when the probability of false alarm will be more than threshold probability, then it will generate an alarm for fraudulent and also decline the transaction.

3.3.2.2.1 Alerting User Regarding Fraud Transaction

In the recent years, Short Message Service (SMS) has emerged as one of the very popular means of communications. Using SMS Gateway Interface system utilized the existing GSM SMS service. Sending SMS messages from a Fraud Detection System to a mobile phone via an SMPP gateway server on the Internet. There are so many 3rd party companies to let you use their gateways for sending SMS which helps to alert the credit card holder at the time of fraud transaction. Whenever the Fraud Detection System suspects a transaction as fraud, it blocks the transaction and alerts the credit card holder regarding the transaction by means of SMS, which helps the card holders regarding fraud transaction.

4. Conclusions

In this paper, we have proposed an application of HMM in credit card fraud detection keeping in view the current Indian Market. We have used different ranges of transaction amount as the observation symbols whereas the types of items have been considered to be states of the HMM. We have suggested a method for finding the Spending Profile of the Cardholders as well as application of this knowledge in deciding the observation symbols. Then we have selected the best state sequence and finally determined the parameters of HMM. It has also been explained how the HMM can detect whether an incoming transaction is fraudulent or not and if it is found to be fraudulent then how the user is notified instantly regarding the fraud. In our proposed model, we have found that more than 85% transactions are genuine and very low false alarms which is about 8% of the total number of transactions. Comparative studies reveal that accuracy of the system is close to 82% over a wide range of input data. The proposed Fraud Detection System is also scalable for handling large volume of transactions.

Acknowledgments

We would like to thank our teacher for his great efforts of supervising and leading us, to accomplish this fine work. To our friends and families, they were a great source of support and encouragement. We thank every person who gave us something to light our pathway; we thank them for believing in us.

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] International Journal of Emerging Technology and Advanced Engineering Website: www.ijetae.com (ISSN 2250-2459, Volume 2, Issue 7, July 2012)511 Credit Card Fraud Detection Using Hidden Markov Model ; Vaibhav Gade, Sonal Chaudhari; All Saint College of Technology, Bhopal (M.P.), India.
[5] 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.
[6] CREDIT CARD FRAUD DETECTION USING HIDDEN MARKOV MODEL by Divya.Iyer,Arti Mohanpurkar, Sneha Janardhan, Dhanashree Rathod, Amruta Sardeshmukh ; Department of Computer engineering and Information Technology , MMIT, Pune ,India.
[7] Credit Card Fraud Detection Using Hidden Markov Model by Abhinav Srivastava, Amlan Kundu, Shamik Sural,Senior Member, IEEE, and Arun K. Majumdar,Senior Member, IEEE
[8] Ghosh, S., and Reilly, D.L., 1994. Credit Card Fraud Detection with a Neural-Network, 27th Hawaii International Conference on Information Systems, vol. 3 (2003), pp. 621-630.
[9] Syeda, M., Zhang, Y. Q., and Pan, Y., 2002 Parallel Granular Networks for Fast Credit Card Fraud Detection, Proceedings of IEEE International Conference on Fuzzy Systems, pp. 572-577 (2002).
[10] Stolfo, S. J., Fan, D. W., Lee, W., Prodromidis, A., and Chan, P. K., 2000. Cost-Based Modeling for Fraud and Intrusion Detection: Results from the JAM Project, Proceedings of

DARPA Information Survivability Conference and Exposition, vol. 2 (2000), pp. 130-144.
[11] Aleskerov, E., Freisleben, B., and Rao, B., 1997. CARDWATCH: A Neural Network Based Database Mining System for Credit Card Fraud Detection, Proceedings of IEEE/IAFE: Computational Intelligence for Financial Eng. (1997), pp. 220-226.
[12] M.J. Kim and T.S. Kim, "A Neural Classifier with Fraud Density Map for Effective Credit Card Fraud Detection," Proc.Int'l Conf. Intelligent Data Eng. and Automated Learning, pp. 378-383, 2002.
[13] W. Fan, A.L. Prodromidis, and S.J. Stolfo, "Distributed Data Mining in Credit Card Fraud Detection," IEEE Intelligent Systems, vol. 14, no. 6, pp. 67-74, 1999.
[14] R. Brause, T. Langsdorf, and M. Hepp, "Neural Data Mining for Credit Card Fraud Detection," Proc. IEEE Int'l Conf. Tools with Artificial Intelligence, pp. 103-106, 1999.
[15]C. Chiu and C. Tsai, "A Web Services-Based Collaborative Scheme for Credit Card Fraud Detection," Proc. IEEE Int'l Conf. e-Technology, e-Commerce and e Service, pp. 177-181, 2004.
[16] 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.
[17] S. Stolfo and A.L. Prodromidis, "Agent-Based Distributed Learning Applied to Fraud Detection," Technical Report CUCS-014-99, Columbia Univ. , 1999.
[18] C. Phua, D. Alahakoon, and V. Lee, "Minority Report in Fraud Detection: Classification of Skewed Data," ACM SIGKDD Explorations Newsletter, vol. 6, no. 1, pp. 50-59, 2004.
[19] V. Vatsa, S. Sural, and A.K. Majumdar, "A Game-theoretic Approach to Credit Card Fraud Detection," Proc. First Int'l Conf. Information Systems Security, pp. 263-276, 2005
[20] S.S. Joshi and V.V. Phoha, "Investigating Hidden Markov Models Capabilities in Anomaly Detection," Proc. 43rd ACM Ann. Southeast Regional Conf., vol. 1, pp. 98-103, 2005.
[21] S.B. Cho and H.J. Park, "Efficient Anomaly Detection by Modeling Privilege Flows Using Hidden Markov Model," Computer and Security, vol. 22, no. 1, pp. 45-55, 2003.
[22] D. Ourston, S. Matzner, W. Stump, and B. Hopkins, "Applications of Hidden Markov Models to Detecting Multi-Stage Network Attacks," Proc. 36th Ann. Hawaii Int'l Conf. System Sciences, vol. 9, pp. 334-344, 2003.
[24] X.D. Hoang, J. Hu, and P. Bertok, "A Multi-Layer Model for Anomaly Intrusion Detection Using Program Sequences of System Calls," Proc. 11th IEEE Int'l Conf. Networks, pp. 531-536, 2003.
[25] T. Lane, "Hidden Markov Models for Human/Computer Interface Modeling," Proc. Int'l Joint Conf. Artificial Intelligence, Workshop Learning about Users, pp. 35-44, 1999.

First Author Jaba Suman Mishra is currently pursuing bachelor's degree program (2009-2013) in computer science and engineering in College of Engineering and Technology (BPUT), Odisha, India. Her current Field of research being Machine Learning and Data Mining.

Second Author Soumyashree Panda is currently pursuing bachelor's degree program (2009-2013) in computer science and engineering in College of Engineering and Technology (BPUT), Odisha, India. Her current Field of research being Machine Learning and Data Mining.

Third Author Ashis Kumar Mishra has completed his post graduate from KIIT University(2011) and under graduate from Biju Pattnaik University of Technology (2007). He is currently a faculty member in Department of CSE in College of Engineering and Technology, Bhubaneswar, Odisha, India. He has published 10 numbers of International Journals and a National Conference in fields of Cryptography, Real Time Systems, Evolutionary algorithm, Cloud Computing and machine learning.