International Journal of Thesis Projects and Dissertations (IJTPD)
Vol. 1, Issue 1, PP: (7-16), Month: October-December 2013, Available At: www.researchpublish.com

Credit Card Fraud Detection System through Observation Probability Using Hidden Markov Model

Ashphak P. Khan[1], Vinod S. Mahajan[2,]Shehzad H. Shaikh[3], Akash B. Koli[4]
North Maharashtra University- Jalgaon
D.N.Patel College of Engineering, Shahada, India

Abstract: **The internet becomes most popular mode of payment for online transaction. Banking system provides e-cash, e-commerce and e-services improving for online transaction. Credit card is one of the most conventional ways of online transaction. In case of risk of fraud transaction using credit card has also been increasing. Credit card fraud detection is one of the ethical issues in the credit card companies, mortgage companies, banks and financial institutes. The most used technique in this field is the Hidden Markov Models (HMMs) which is a statistical and extremely powerful method. HMM statistical tool used for modeling generative sequences characterized by a set of observable sequences. Observation probabilistic in an HMM Based system is initially studies spending profile of the cardholder and followed by checking an incoming transaction against spending behavior of the cardholder we can show clustering model is used to classify the legal and fraudulent transaction using data conglomeration of regions of parameter , HMM based credit card fraud detection during credit card transaction. We presented experimental result to show the effectiveness of our approach.**

Keyword: **Hidden Markov Model, online transaction, credit card, credit card fraud detection, E-commerce, clustering.**

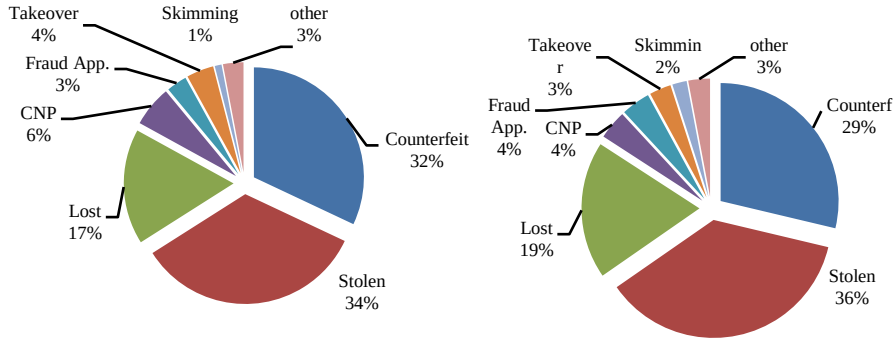
I. INTRODUCTION

The concept of credit card is not new; it has been in the market many years ago. Everybody is getting used to the credit card across the globe, because of its accessibility and simplicity to use it became more popular. The concept of paying for goods and services electronically is not a new one. Since late 1970 and early 1980, a range of Methods has been initiated to accept payment to be resulted across a computer network. After a period of rapid expansion, 1.5 billion populations have internet access globally as of 2008. The e-commerce began at the beginning of the year 1997, an enormous selection of diverse payment techniques developed by the researched some of these were instigated some of these were instigated on the market and unsuccessful to arrive at a critical mass. The e-commerce is a process of value exchange in electronic e-commerce; where the amount is transferred online on internet, other computer network [1] [2] .The e-commerce has progressed from conventional recompense methods, and subsequently the two modes of systems have much similarity. Electronic payment systems are much influential, in particular due to its simplicity and convenience. Credit card was launched decade's ago. These cards have been made with the magnetic strips with read-only data. In the year 1996, Master, and Visa card proclaimed the introduction of process of making payments by credit cards on internet. The online credit card payments are much trouble-free and expedient. However, certain amount of risk is involved in updating personal details such as person's name, contact numbers, credit card numbers and expiry dates of these cards online as it allows the fraudsters to misuse the same [2]. Of lately, prevention of credit card fraud has always been the main concern faced by major banks over recent years, as the level of online credit card fraud has gone up drastically. Detection and deterrence of e-commerce credit card fraud is very imperative outline of risk management in the history of credit card [1][2].

A. *CREDIT CARD FRAUD*

Application Fraud: When someone applies for a credit card with false information that is termed as application fraud. For detecting application fraud, two different situations have to be classified. When applications come from a same user with the same details, that is called duplicates, and when applications come from different individuals with similar details, that is termed as identity fraudsters [3]. **Theft Fraud /Counterfeit Fraud**: Theft fraud refers using a card that is not yours. As soon as the owner give some feedback and contact the bank, the bank will take measures to check the thief as

early as possible. Likewise, counterfeit fraud occurs when the credit card is used remotely; where only the credit card details are needed [3]. **Account Takeover**: This type of fraud occurs when a fraudster illegally obtains a valid customers' personal information. The fraudster takes control of (takeover) a legitimate account by either providing the customer's account number or the card number [3]. **Skimming** Most cases of counterfeit fraud involve skimming, a process where genuine data on a card's magnetic stripe is electronically copied onto another. Skimming is fast emerging as the most popular form of credit card fraud [3]. **Stolen and counterfeit** cards together contribute to more than 50% of fraud losses According to figures published by both MasterCard and Visa in figure 1 and figure 2.



Credit card we can use both purpose for online or offline transaction, mostly credit card is divide two brought categories, first physical credit card, now in physical credit card where card holder is present, which is relation between selling counter and card holder. Selling counter can use the EMV (Europay, MasterCard, and visa) machine. Transaction of amount is done in front of card holder. Virtual credit card is where card holder in not present, internet baking is part of virtual credit card. Online baking is challenging part of traditional baking system. The credit card is use of modern society day by day. Prevalent of credit card fraud is difficult task when using online transaction.

II. LITERATURE STUDY OF CREDIT CARD FRAUD

Ghosh and Reilly [4] used a neural network system which consists of a three-layered feed-forward network with only two training passes to achieve a reduction of 20% to 40% in total credit card fraud loses. This system also significantly reduced the investigation workload of the fraud analysts.

Aleskerov, Freisleben, and Rao [5] developed a fraud detection system called Card watch that is built upon the neural network learning algorithm. This system is aimed towards commercial implementation and therefore can handle large datasets, and parameters of an analysis can be easily adjusted within a graphical user interface. Card watch uses three main neural network learning techniques: conjugate gradient, back propagation, and batch back propagation. This system is a useful product for large financial institutions due to its ease of implementation with commercial databases. Unfortunately, the disadvantage of this system is the need to build a separate neural network for each customer. This results in a very large overall network that requires relatively higher amounts of resources to maintain.

Dorronsoro and others developed a neural network based fraud detection system called Minerva. This system's main focus is to imbed itself deep in credit card transaction servers to detect fraud in real-time. It uses a novel nonlinear discriminant analysis technique that 43 combine the multilayer perceptron architecture of a neural network with Fisher's discriminant analysis method. Minerva does not require a large set of historical data because it acts solely on immediate previous history, and is able to classify a transaction in 60ms. The disadvantage of this system is the difficulty in determining a meaningful set of detection variables and the difficulty in obtaining effective datasets to train with [6].

Kokkinaki suggested to create a user profile for each credit card account and to test incoming transactions against the corresponding user's profile. The attributes that were used to construct these profiles are: credit card numbers, transaction dates, type of business, place, amount spent, credit limit and expiration time. Kokkinaki proposed a Similarity Tree algorithm, a variation of Decision Trees, to capture a user's habits. The analyses found that the method has a very

small probability for false negative errors. However, in this approach the user profiles are not dynamically adaptive and therefore continual updates are needed when user habits and fraud patterns change [7].

Chan and Stolfo studied the class distribution of a training set and its effects on the performance of multi-classifiers on the credit card fraud domain. It was found that increasing the number of minority instances in the training process results in fewer losses due to fraudulent transactions. Furthermore, the fraud distribution for training was varied from 10% to 90% and it was found that maximum savings were achieved when the fraud percentage used in training was 50% [8].

Brause and others looked specifically at credit card payment fraud and identified fraud cases by combining a rule-based classification approach with a neural network algorithm. In this approach the rule-base classifier first checked to see if a transaction was fraudulent, and 44 then the transaction classification was verified by a neural network. This technique increases the probability for the diagnosis of "fraud" to be correct and therefore it is able to decrease the number of false alarms while increasing the confidence level [9].

Ehramikar showed that the most predictive Boosted Decision Tree classifier is one that is trained on a 50:50 class distribution of fraudulent and legitimate credit card transactions. It was also reported that training decision tree classifiers on datasets with a high distribution of legitimate transactions leads to high fraudulent cases classified as legitimate (a high false negative rate). This suggests that predictive model over fitting occurs when the training dataset has a majority of legitimate transactions [10].

Wheeler and Aitken developed a case-based reasoning system that consists of two parts, a retrieval component and a decision component, to reduce the number of fraud investigations in the credit approval process. The retrieval component uses a weighting matrix and nearest neighbor strategy to identify and extract appropriate cases to be used in the final diagnosis for fraud, while the decision component utilizes a multi-algorithm strategy to analyze the retrieved cases and attempts to reach a final diagnosis. The nearest-neighbour and Bayesian algorithms were used in the multi-algorithm strategy. Initial results of 80% non-fraud and 52% fraud recognition from Wheeler and Aitken suggest that their multi-algorithmic case-based reasoning system is capable of high accuracy rates [11].

Bolton and Hand proposed an unsupervised credit card detection method by observing abnormal spending behavior and frequency of transactions. The mean amount spent over a specified time window was used as the comparison statistic. Bolton and Hand proposed the Peer Group Analysis (PGA) and the Break Point Analysis (BPA) techniques as unsupervised 45 outlier detection tools. The report showed that the PGA technique is able to successfully detect local anomalies in the data, and the BPA technique is successful in determining fraudulent behavior by comparing transactions at the beginning and end of a time window [12].

Kim proposed a fraud density map technique to improve the learning efficiency of a neural network. There is an overemphasis of fraudulent transactions in training data sets, therefore, the fraud density map (FDM) tries to address the issue of the inconsistent distributions of legitimate and fraudulent transactions between the training data and real data. FDM adjusts the bias found in the training data by reflecting the distribution of the real data onto the training data through the changing of a weighted fraud score [13].

Maes applied artificial neural networks (ANN) and Bayesian belief networks (BBN) to a real world dataset provided by Europay International. The best prediction rate was obtained for the experiment in which the features were pre-processed. It was found that by performing a correlation analysis on the features and removing the feature that was strongly correlated with many of the other features clear improvements to the results were obtained. Furthermore, their experiments showed that BBNs yields better fraud detection results and their training period is shorter, however ANN was found to be able to compute fraud predictions faster in the testing stage. Chen and others (2004) presented a new method to address the credit card fraud problem. A questionnaire-responded transaction (QRT) data of users was developed by using an online questionnaire. The support vector machine algorithm was then applied to the data to develop the QRT models, which were then used to decide if new transactions were fraudulent or legitimate. 46 It was found that even with very little transaction data the QRT model has a high accuracy in detecting fraud [14].

Chiu and Tsai identified the problem of credit card transaction data having a natural skewness towards legitimate transactions. The ratio of fraud transactions to normal transactions is extremely low for an individual FI, and this makes it difficult for FIs to maintain updated fraud patterns. The authors of this thesis proposed web service techniques for FIs to share their individual fraud transactions to a centralized data centre and a rule-based data mining algorithm was then applied to the combined dataset to detect credit card fraud [15].

Foster and Stine attempted to predict personal bankruptcy using a fully automated stepwise regression model. Neural network models used in fraud detection modelling are often regarded as black-boxes, and it is difficult to follow the process from input to the output prediction. On the other hand, the benefit of a statistical model is the ability to easily understand the procedures in the prediction process. The results from this thesis indicate that standard statistical models are competitive with decision trees [16].

III. HIDDEN MARKOV MODEL

The elements of a discrete-time hidden markov model will now be summarized. These elements will be used throughout the thesis:

Number of states N. although the states are hidden, for many practical applications there is often some physical significance attached to the states or to sets of states of model [17]. For instance in the urn and ball model, the states corresponds to the urns. The labels for the individual states are {1, 2, 3… N}, and the states at time t denoted qt.

Model parameter M. if discrete observation densities are used, the parameter M is the number of class or cells that should be used, e.g. M equals the number of colors in the urn and bell example. If continuous observation densities are used, M is represented by the number of mixtures in every state.

$$\pi = \{\pi_i\}_{i=1}^{N}$$

Initial state distribution in which πi is defined as:

$$\pi_i = P(q_1 = i)$$

States transition probability distribution A = [αij] where :

$$a_{ij} = P(q_{t+1} = j \mid q_t = i), \qquad 1 \le i, j \le N$$

$$B = \{b_j(o_t)\}_{j=1}^{N},$$

Observation symbol probability distribution, in which the probability functions for each state, j, is:

$$b_j(o_t) = P(o_t \mid q_t = j)$$

The calculation of $b_j(o_t)$ can be found with discrete- or continuous observation densities. In this thesis, is the continuous observation densities used.

It should now be clear that a complete specification of an HMM requires two model parameters N and M, the specification of the three sets of probability measures π, A and B are also necessary. For convenience will these probability measures used the notation, λ:

$$\lambda = (A, B, \pi)$$

IV. PROPOSED METHODOLOGY

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

Initial Probability: $\pi = \{\Pi_i\}$

Transition Probability: $A = \{a_{ij}\}$

Observation Probability: $B = \{b_j(k)\}$

HMM is:

Testing $b_j(a_t) = \sum C_{jm}\ \lambda(\mu_{jm}, \sum_{jm}, a_t)$

Where, C_{jm} = weighting coefficients, μ_{jm} = mean vectors, $\sum_{jm}$ = Covariance matrices

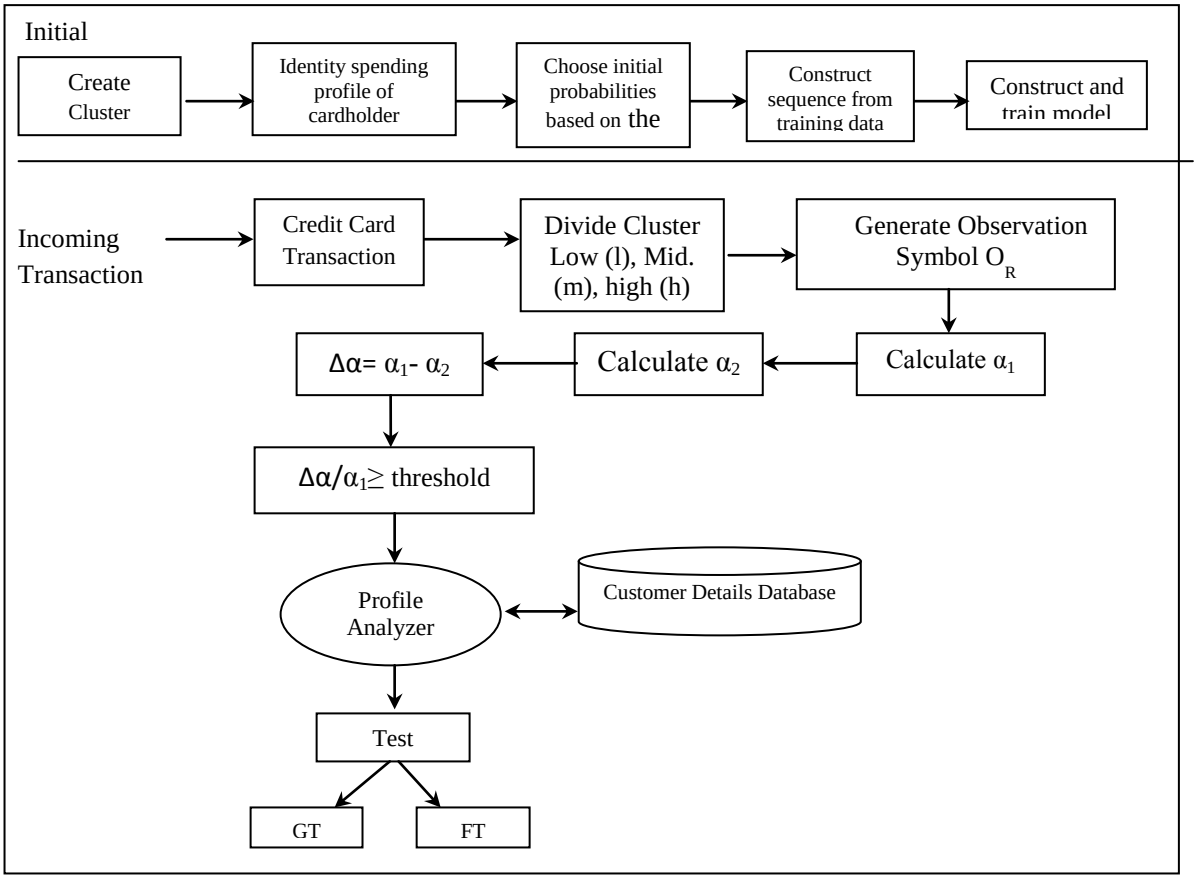


Figure 3: Proposed Fraud Detection System

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 ($101, $500] and high ($501, 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 [4]. 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.12 etc., are names given to the states to denote different purchase types such as bill payment, restaurant, electronics items etc. it has been shown that probability of transition from one state to another (for example from 1 to 2 and vice versa, represented as a1-2 and a2-1, respectively) and also probabilities of transition from a particular state (1, 2, or 3) to different spending habits h, m, or l (for example, b1-h, b1-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 O1, O2, OR 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 α1, which can be calculated as

$$\alpha_1 = P(O_1, O_2, O_3, ..., O_{R+1} | \lambda),$$

Let OR+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 O1 sequence and we will have R sequences from O2 to OR+1.

Let the probability of new R sequences be α_2

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

Hence, we will find (5.11) and (5.1

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

If Δα it means that HMM consider new sequence i.e. OR+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.

$$\Delta\alpha / \alpha_1 \geq 0 \text{ Threshold value},$$

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 OR+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.

IV. EXPERIMENTAL RESULT

All the information about credit card (Like Credit card number, credit card CVV number, credit card Expiry month and year, name on credit card etc.) will be checked with credit card database. If User entered database is correct then it will ask Personal Identity number (PIN). After matching of Personal Identity number (PIN) with database and account balance of user's credit card is more than the purchase amount, the fraud checking module will be activated. The verification of all data will be checked before the first page load of credit card fraud detection system. If user credit card has less than 10 transactions then it will directly ask to provide personal information to do the transaction. Once database of 10 transactions will be developed, then fraud detection system will start to work. By using this observation, determine users spending profile.

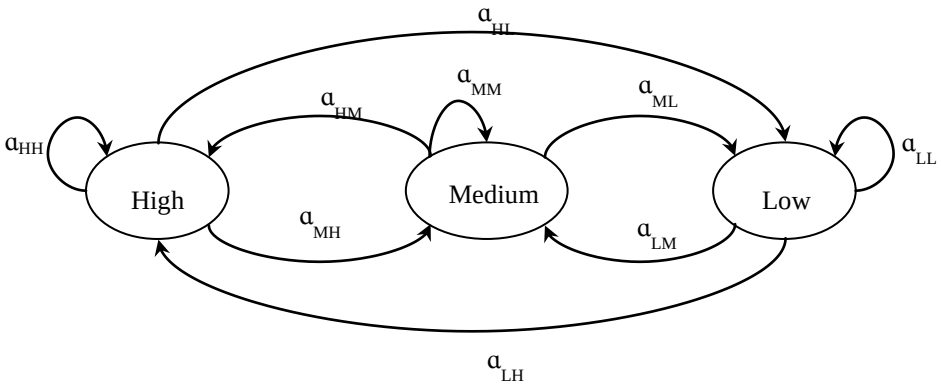


Figure 4: Different State of Credit Card Transition

he purchase amount will be checked with spending profile of user. By transition probabilistic calculation based on HMM, it concludes whether the transaction is real or fraud. If transaction may be concluded as fraudulent transaction then user

must enter security information. This information is related with credit card (like account number, security question and answer which are provided at the time of registration).If transaction will not be fraudulent then it will direct to give permission for transaction. If the detected transaction is fraudulent then the Security information form will arise. It has a set of question where the user has to answer them correctly to do the transaction. These forms have information such as personal, professional, address; dates of birth, etc. are available in the database. If user entered information will be matched with database information, then transaction will be done securely. And else user transaction will be terminated and transferred to online shopping website. The flowchart of proposed model in figure

It is very difficult to do simulation on real time data set that is not providing from any credit card bank on security reasons. In Table 2, 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 high, low, medium (h, l, and m) of every category (1, 2 and 3). Fraud detection of incoming transaction will be checked on last 20 transactions.

Table 1: List of Transaction Amount of different state

Transaction No.	Amount in `	Transaction No.	Amount in `	Transaction No.	Amount in `	Transaction No.	Amount in `
1st	102	6th	650	11th	740	16th	1580
2nd	1080	7th	2156	12th	450	17th	360
3rd	1730	8th	520	13th	560	18th	1360
4th	430	9th	380	14th	272	19th	680
5th	1420	10th	243	15th	930	20th	1250

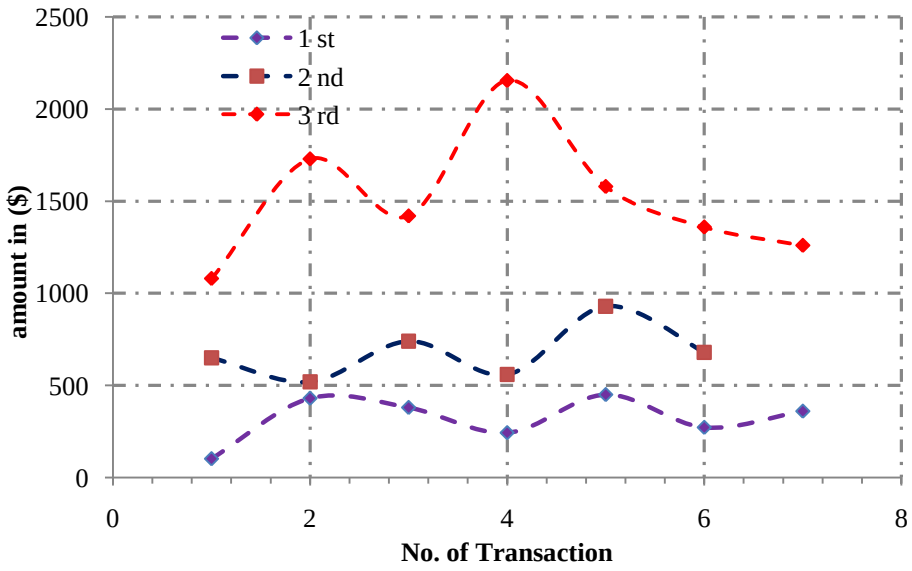


Figure 5: Different transactions amount in a category

In fig. 5.1 it is shown that the amount of purchased items or services in different categories such as 1st for bill pay online, 2nd for bill restaurant etc. and 3rd for online reservation, using internet technology or e-commerce techniques etc., with respect to their number of transactions.

We have simulated several large data sets; one is shown in Table 2, in our proposed fraud detection system and found out probability mean distribution of false and genuine transactions. In Fig. 6.3 it is noted that when probability of genuine transaction is going down, correspondingly probability of false transaction going up and vice 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.

Testing credit card FDSs using real data set is a difficult task. Banks do not, in general, agree to share their data with researchers. There is also no benchmark data set available for experimentation. We have, therefore, performed large-scale simulation studies to test the efficacy of the system. A simulator is used to generate a mix of genuine and fraudulent transactions. The number of fraudulent transactions in a given length of mixed transactions is normally distributed

With a user specified (mean) and (standard deviation), taking cardholder's spending behavior into account. Specifies the average number of fraudulent transactions in a given transaction mix. In a typical scenario, an issuing bank, and hence, its FDS receives a large number of genuine transactions sparingly intermixed with fraudulent transactions. The genuine transactions are generated according to the cardholders' profiles. The cardholders are classified into three categories as mentioned before-low, medium and high groups. We have studied the effects of spending group and the percentage of transactions that belong to the low, medium, and high-price-range clusters. We use standard metrics-True Positive (TP) and FP, as well as TP-FP spread and Accuracy metrics, as proposed in [40] to measure the effectiveness of the system.TP represents the fraction of fraudulent transactions correctly identified as fraudulent, whereas FP is the fraction of genuine transactions identified as fraudulent. Most of the design choices for FDS that result in higher values of TP also cause FP to increase. To meaningfully capture the performance of such a system, the difference between TP and FP, often called the TP-FP spread, is used as a metric

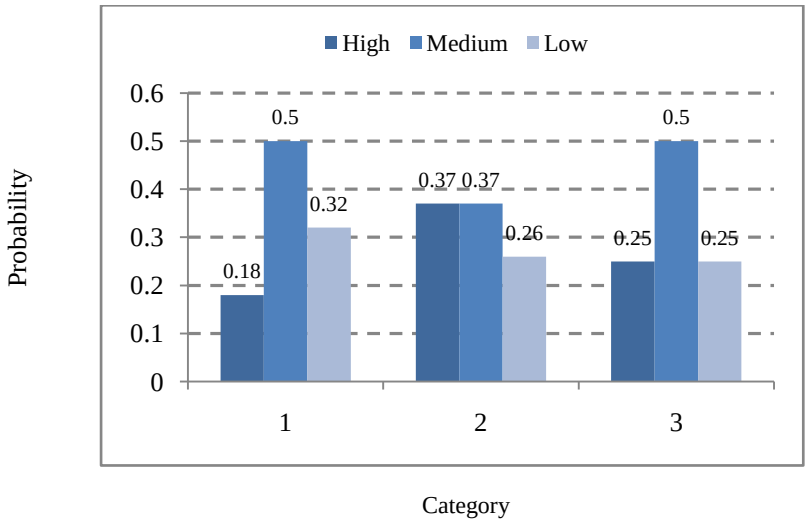


Figure 6: Probabilities of different spending profiles of eachcategory

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. In this Thesis, 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.

Table 5.2: Variation of GT and FT with different Sequence Length

. Threshold (%)	GT averaged over all the 6 state for different sequence length					FT averaged over all the 6 state for different sequence length				
	5	10	15	20	25	5	10	15	20	25
10	0.63	0.67	**0.72**	0.69	0.66	0.05	0.05	**0.05**	0.05	0.05
30	0.54	0.56	0.64	**0.68**	0.67	0.04	0.04	0.05	**0.03**	0.04
50	0.65	0.73	**0.82**	0.79	0.72	**0.04**	**0.04**	0.05	0.05	0.05

70	0.46	0.52	0.58	**0.64**	0.53	0.03	0.04	0.03	**0.02**	0.05

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.

To meaningfully capture the performance of such a system, the difference between TP and FP, often called the TP-FP spread, is used as a metric.

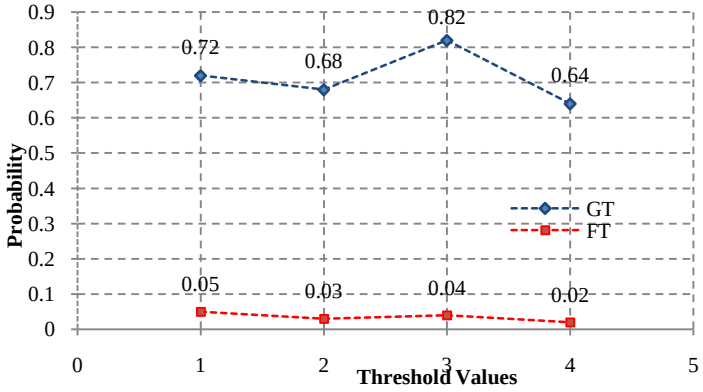


Figure 7: Variation of GT and FT with different Number of States

V. CONCLUSION

Efficient credit card fraud detection system is an utmost required for card issuing bank or all type of online transaction that through using credit card. In this report, we have implemented of hidden markov model in credit card fraud detection. The very easily detect and remove the complexity for using in this hidden markov model. It has also explained the hidden markov model how can detect whether an incoming transaction is fraudulent or not comparative studies reveal that the accuracy to the system is also 92 % over a wide variation in the input data. We are dividing the transaction amount in three categories that is grouping high, medium & low used on different ranges of transaction amount each group show the aberration symbols. In hidden markov model methods is very low compare techniques using fraud detection rate. The different steps in credit card transaction processing are represented as the underlying stochastic process of an HMM. i 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 also have been explained low the hidden markov model can detecting whether an incoming transaction is fraudulent or not. The system is also scalable for handling large volumes of transactions.

Future work

Future work of the findings obtained here may not be generalized to the global fraud detection problem. As future work, some effective algorithm which can perform well for the classification problem with variable miss classification costs could be developed. In future we can prepare an application with consistent Fraud Detection with new techniques and modules, develop a sophisticated module like calculating Fraud Timings, capturing the photo of the Fraud and many more modules can be developed

REFERENCES

[1] Nilsson M., Ejnursson M, "Speech Recognition using Hidden Markov Model performance evaluation I noisy environment", Department of Telecommunication and Digital Processing, 2010

[2] "Trends in online shopping, a global nelson consumer report", www.nileslen.com/us/en/ insights/reports-download/2012/global-trends-in-online-shopping-nielsen-consume-report.html, 2008.

[3] Bhatla, T.P., Prabhu V., and Dua A., "Understanding Credit Card Frauds", Tata Consultants Services, 2003.

[4] Ghosh S., Reilly D.L., "Credit Card Fraud Detection with a Neural- Network" Proceedings of the International Conference on System Science, pp.621-630, 1994.

[5] Aleskerov E., Freisleben B., and Rao B., "CARDWATCH: A Neural Network Based Database Mining System for Credit Card Fraud Detection", Proc. IEEE/IAFE: Computational Intelligence for Financial Eng., pp.:220-226, 1997.

[6] Dorronsoro J.R., Francisco G., Carmen S., and Carlos S.C., "Neural Fraud Detection in Credit Card Operation." IEEE Transaction on Neural Network, vol.-08, no.-04, pp.: 827-834, 1997.

[7] Kokkinaki, A., "On Atypical Database Transactions: Identification of Probable Frauds using Machine Learning for User Profiling." Knowledge and Data Engineering Exchange Workshop. IEEE, pp.:107-113, 1997.

[8] Stolfo S.J., Fan D.W., Lee W., Prodromidis A.L., and Chan P.K., "Credit Card FraudDetection Using Meta-Learning: Issues and Initial Results", Proc. AAAI Workshop AI Methods in Fraud and Risk Management, pp.:83-90, 1997.

[9] Brause R., Langsdorf T., and Hepp M., "Neural Data Mining for Credit Card Fraud Detection", Proc. IEEE Int'l Conf. Tools with Artificial Intelligence, pp.:103-106, 1999.

[10] Ehramikar S., "The Enhancement of Credit Card Fraud Detection Systems using Machine Learning Methodology", MASc Thesis, Department of Chemical Engineering, University of Toronto, 2000.

[11] Wheeler R., and Aitken S., "Multiple algorithms for fraud detection", Knowledge-Based Systems, no. 13 pp.: 93-99, 2000.

[12] Bolton R., and Hand D., "Unsupervised Profiling Methods for Fraud Detection", Credit Scoring and Credit Control VII, 2001.

[13] Kim, M, and Kim T., "A Neural Classifier with Fraud Density Map for Effective Credit Card Fraud Detection", Proceedings of IDEAL. pp.:378-383, 2002.

[14] Maes S., Karl T., Bram V., Bernard M., "Credit card fraud detection using Bayesian and neural networks", Interactive image-guided neurosurgery, pp.:261-270, 1993.

[15] Chiu A., Tsai C., "A Web Services-Based Collaborative Scheme for Credit Card Fraud Detection", Proceedings of the IEEE International Conference on e-Technology, e-Commerce and e-Service, pp.:177-181, 2004.

[16] Foster D., and Stine R., "Variable Selection in Data Mining: Building a Predictive Model for Bankruptcy", Journal of American Statistical Association, pp.: 303-313, 2004.

[17] Chen R., Chiu M., Huang Y., and Chen L., "Detecting Credit Card Fraud by Using Questionaire- Responded Transaction Model Based on Support Vector Machines", Proceedings of IDEAL. Pp.: 800-806, 2004.

[18] Srivastava A., Kundu, A., Sural S., and Majumdar A.K., "Credit Card Fraud Detection Using Hidden Markov Model", IEEE Transactions on Dependable and Secure Computing, Vol.5, No.1, pp.:37-48. 2008.

[19] Khan Ashphak, Singh Tejpal, Sinhal Amit, "Implement credit card fraudulent detection system using observation probabilistic in hidden Markov model" IEEE Explore 6479746 From 1 To 6, NUiCONE, 2012.

[20] Mr. Ashphak khan,Mr. Tejpal Singh, Mr. Amit Sinhal, "Observation probability in Hidden Markov Model for Credit Card Fraudulent Detection system Advances in Intelligent Systems and Computing" , Vol. 236 ISBN 978-81-322-1601-8 From 65 To 71, Springer – 2012.

[21] Mr. Ashphak khan,Prof. Tejpal Singh, Prof. Amit Sinhal, "A Survey of Fraud Detection System using Hidden Markov Model for Credit Card Application", International Journal of Artificial Intelligence and Mechatronics ISSN 2320. 5121 From 47 To 51.