ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

Multi Stage Credit Card Fraud Detection System

Shilpa Khurana, Ritika

M.Tech Scholar, Department of Computer Science and Engineering, T.I.T &S Bhiwani, India

Assistant Professor, Dept. of Computer Science, Govt. College Hansi (Hisar), India

ABSTRACT: Intoday's scenario, Credit card is used for online transaction and security of these is also abig issue. Here, the fraud detection is completed in two Steps. First is training or learning of transactions and second is detection of fraud in transaction. In first Step, sequences of transactions are added in to the system.In second step, multiple stages are used to detect fraud. In first stage, HMM (Hidden Markov Model) is used with thespending behavior of card holdersand categorized them:low, medium and high spending behavior. These categories depend on amount of transaction. If an incoming transaction is notnormal, various tests are performed at multiple stages. These are: matching with last transaction amount, checking fraud history and raising security questions**.**

KEYWORDS*:* Fraud Detection; HMM; FDS**.**

I. INTRODUCTION

In everyday life, credit cards are used not only in shops, malls or others places but also in online shopping because it provides the cashless mode of payment to the user. There is an expeditious increment in the number of card transactions, but there is disadvantage of credit cards also which has increased fraudulent activities. Credit Card fraud is an illegal activity done by unauthorized person and it can affect all consumers, merchants and issuing banks. Hence, it is exigent to design a system for identifying frauds to support safe credit card services. There are bunches of techniques but still fraudulent activities taking place. So, a proposed model of detection of fraud is explained to identify fraud transactions with multiple stages. In first stage of detection, HMM is used and calculates the $\Delta\alpha$ value. This value represents the unusual spending behavior of user and its value may be positive or negative. If value is Positive then transaction is normal in behavior otherwise it might be fraud. In second stage, transaction matched with last transaction. If transaction is greater than last transaction amount with in ten minutes then asked security question from user otherwise checked with the fraud history database. In third stage, If Answers are matched then transaction is normal otherwise it is fraud and add into the fraud history. In forth stage, check transaction with fraud history, if it is already present then it is fraud transaction otherwise normal transaction.

A. NEED OF CREDIT CARDS FRAUD DETECTION

Only the credit card authorized users have the permission to do transaction by using Information related to credit card details (card number, CVV number, Expiry month and year of card etc.).In this case, fraudster have to steal the card's information and done the transaction. So, authorization technique for secure transaction is not sufficient. Hence, further test is required to detect the frauds. These labels of frauds can be pinpointed by ruminating the user's spending behavior. The parameters related to spending behavior of a human such as type of item, time and amount of purchases which are ascendancy by income[1]. Spending behavior categorize in three types that will be Low, Medium and High spending behavior and Fraud transaction can be identified either by checking changes in user spending behavior or by building fraud detection system (FDS) to classify individual transactions[2],[3]. Two types of credit card fraud are there first is done by physical card and second is virtual card. In physical cards, frauds are done with lost, stolen or fake cards and with virtual card, need the card details to do transaction. Hence, a FDS is essential for security purpose.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

II. RELATED WORK

Now a day, detection of fraud is a much ventilate topic in industry of credit cards.Abhinavsrivastavaet al [3] has proposed a HMM for fraud detection.Vivek[5] has proposed an HMM based system of security of ATM payments.S.J Stolfo [6] has suggested fraud detection of credit cards. Jaba Suman Mishra [7] has proposed an HMM based application of credit cards fraud detection keeping in view the current Indian Market.Here, a proposed model of FDSis given where HMM is used as first stage of detection.

III. HIDDEN MARKOV MODEL

HMM is an idealistic solution for detecting fraud transactions. Here, HMM work as training the transactions. HMM initially process the transactions by first decoding the consideration symbols.So,the transaction amounttoconsideration symbols are V_1,V_2, . . . $V_{m.}$ Thespending behavior of user profile depends on transaction amounts.Vk is stand for both price range and consideration symbol, k =1, 2, . . .m.

Mathematically an HMM can be defined as below [4]:

1. S={S_1, S_2, S_3……...,Sn}, where n is number of states.
2. V={V_1,V_2,V_3.....,Vm*}*, where m is consideration symbols.
3. The matrix of statetransition X= [a_{ij}], Where [a_{ij}] is transition probability of I to j state.
$$a_{ij} = P(q_{t+1} = S_j | q_t = S_i)$$
4. The matrix of consideration symbolY= [b_j (k)], Where b_j (k) is probability of consideration symbolkat state *j*.
$$b_j = P(V_k | S_j)$$
5. The incipientstate of distribution π= [πi], Where π_i =P (q1= S_i).
6. O is the consideration sequence= O_1, O_2…. O_U, where U is consideration number.

It is observable that anaccomplished detail of HMM depends on the two parameters, m and n, and X, Y, πisthree probability distribution factors. A complete parameter set of the model used the notation λ= (*X*, *Y*, and π) where X, Y implicitly include n and m.

IV. PROPOSED MODEL

In Proposed Model, FDS work in two steps:

1. Training
2. Detection of Fraud

Training Step:

In first step, sequences of credit cards transaction are added in to the system. This step is just for training the sequence of transactions.

Detection Step:

This is done in various stages.

Stage 1: In first stage,HMM convert the cardholder's transaction amount into consideration symbols. HMM uses spending behavior cardholder's to identify fraud.Here, spending behaviors are categorizedin three categories.Credit Card holders profile groups as ls (low spending behavior) = (0, 5000), ms (medium spending behavior) = (5000, 20000), and hs (highspending behavior) (20000, up to credit card limit), and transaction amount is in Indian currency that is rupees. If card holder performs a transaction as 3000 rupees then transaction will come in low profile group. So the corresponding profile group and symbol is "ls" and "V_1" will be used.

Let C_1, C_2, . . . C_M be the mean or centroids. These are used toselect the consideration symbol. $C_{ls,}$ $C_{hs,}$ $C_{hs}$are the Respective centroids.

Now, HMM work is started. Accept the symbols from incipientsequence andfrom card holder's training data. Let U is length of consideration sequence O_1,O_2,…,O_U. This is the recorded sequence of the cardholder's transactions. HMM takes this sequence as input and calculates the probability. Let the probability be α_{old} as follows:

$$\alpha_{old} = P\_ls \times P\_ms \times P\_hs$$

- P_ls=Probability of Low spending profile. If low spending profile transaction is 3 from total 10 transactions in sequence then p_ls=3÷10=0.3.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

P_ms, P_hsare also calculated as P_ls.

- P_ms= Probability of Medium spending profile
- P_hs= Probability of High spending profile

Let O_{U+1} be the next symbol originatedfrom a new next transaction. To form another sequence of length U, ignore O_1 and append O_{U+1} in that sequence, generating O_2, O_3,. . .O_U, O_{U+1} as the new sequence. Now,this new sequence is given to HMM as input and calculates the probability. Let the new probability be α_{new} as follows:

$$\alpha_{new} = P\_ls \times P\_ms \times P\_hs$$

Let $\Delta\alpha = \alpha_{old} - \alpha_{new}$. Now checkthe value of $\Delta\alpha$ that it is positive or negative. If $\Delta\alpha$ value is positive then transaction is normal otherwise transaction is might be fraud in behavior and for further checking goes to stage 2.

Stage 2: when $\Delta\alpha$ value is negative, Match with Last transaction and test Transaction is greater than Last Transaction with in ten minutes then asked security question from user otherwise check with fraud history in 4^{th} stage.

Stage 3: If answers are matched then transaction is normal otherwise it is fraud.

Stage 4: Fraud History- when transaction is already present in fraud history then called it fraud otherwise normal transaction and save it in the sequence.

The above described model works on the current two monthof transaction.

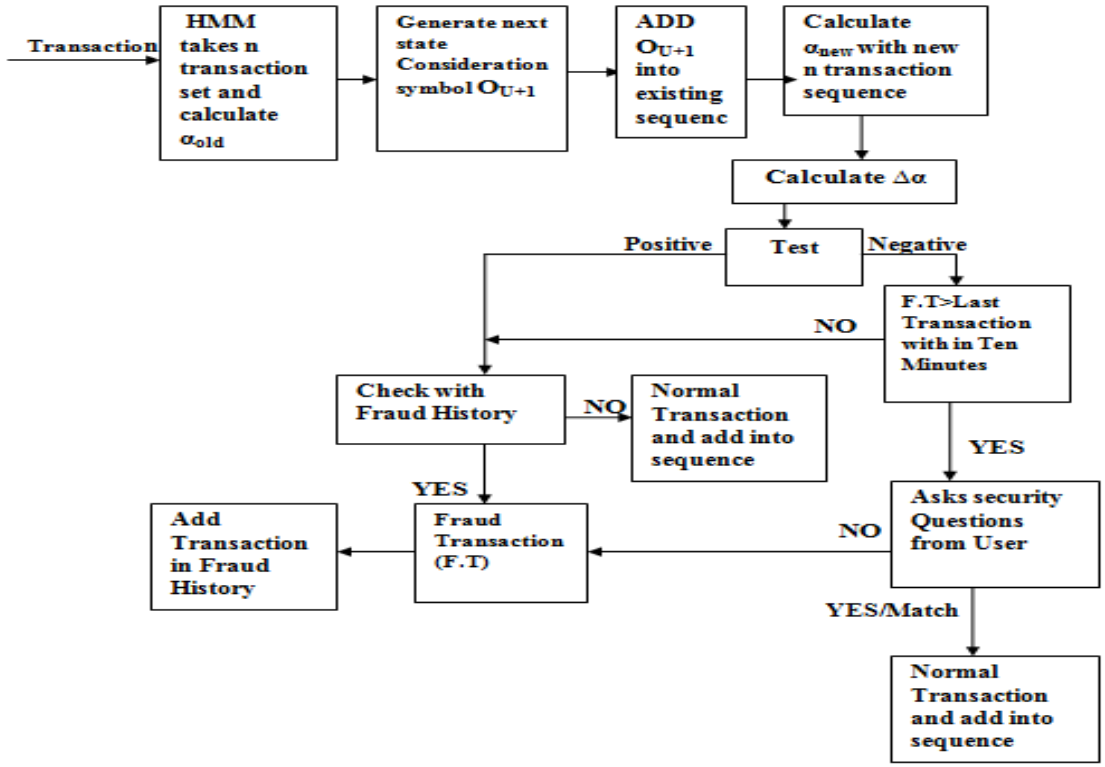

Fig 1. Block Diagram -Proposed Model of FDS.

A. COMPARISONS OF TRANSACTION AT DIFFERENT LEVEL.

In this, transactions comparisons are given with their mean of spending behaviors in example 4.1 with 3 steps, with the corresponding figure 2, figure 3 and figure 4.

Example 4.1: Fraud transaction will be checked on 10 transactions set every time and also calculates the percentage of each spending profile that is based on number of transactions. Mean values calculated by these values.ls (low

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

spending behavior) = (0, 5000), ms (medium spending behavior) = (5000, 20000), and hs (high spending behavior) = (20000, up to credit card limit) and transaction amount is in Indian currency that is rupees.

Step 1: In Table I, list of 10 transaction amounts are shown.
In Table II calculate the output of spending behavior Means based on transaction amount in table I.
V_1= ls=1000+2000+3000=6000÷3=2000
V_2=ms=12000+7000+15000+9000+7000=50000÷5=10000
V_3=hs=35000+25000=60000÷2=30000

TABLE I: List of Transactions.

Transaction Number	Transaction Amount	Transaction Number	Transaction Amount
1	35000	6	15000
2	12000	7	9000
3	7000	8	7000
4	1000	9	3000
5	2000	10	25000

TABLE II: Output of Spending Behavior Means

Mean/Centroid Name	C_{ls}	C_{ms}	C_{hs}
Consideration symbol	V_1 = ls	V_2= ms	V_3= hs
Mean Value(Centroids)	2000	10000	30000
Percentage of total transactions(p)	30	50	20

Figure 2 shows the percentage calculation of spending profile for step 1, where transaction number range is 1st to 10th.

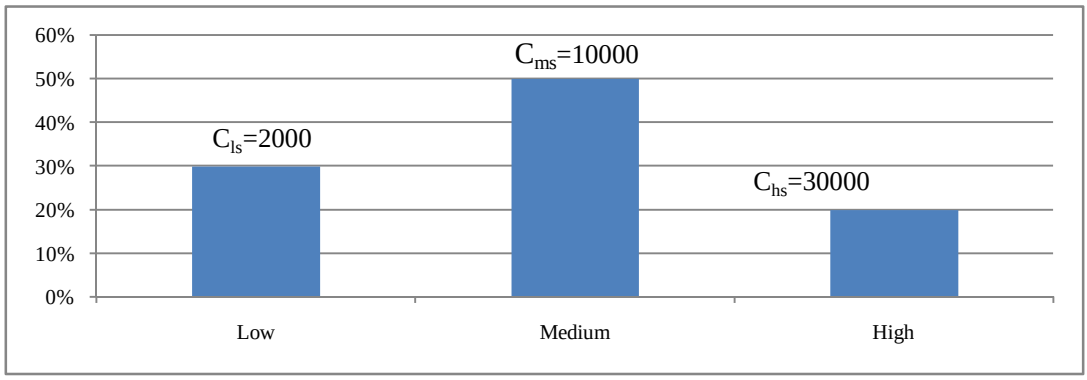

Fig 2. Percentage of Each Spending Profile for Step 1.

To calculate α1: Probability values for each spending profile i.e. P_ls=0.3, P_ms=0.5, P_hs=0.2
α1= P_ls × P_ms × P_hs=0.3×0.5×0.2=0.030

Step2:Ignore first five transactionscalculate the mean of 6th to 15th transaction as shown in Table III.

TABLE III: List of Transactions.

Transaction Number	Transaction Amount	Transaction Number	Transaction Amount
6	15000	11	2400
7	9000	12	2000
8	7000	13	1000
9	3000	14	1200
10	25000	15	1500

In Table IV calculate the output of spending behavior Means based on transaction amount in table III.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

TABLE IV: Output of Spending Behavior Means.

Mean/Centroid Name	C_{ls}	C_{ms}	C_{hs}
Considerationsymbol	V_1 = ls	V_2= ms	V_3= hs
Mean Value(Centroids)	2200	9500	25000
Percentage of total transactions(p)	60	30	10

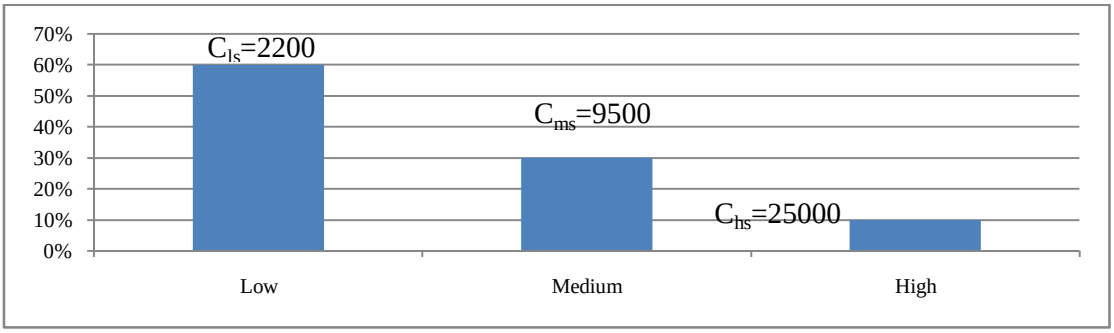

Fig 3.Percentage of Each Spending Profile for Step 2.

Figure 3 shows the percentage calculation of spending profile for step 2, where transaction number range is 6^{th} to 15^{th}.

Step3: Ignore first ten transactions and calculate the mean of 11^{th} to 20^{th}transaction as shown in Table V and In Table VI calculate the output of spending behavior Means based on transaction amount in table V.

TABLE V: List of Transactions.

Transaction Number	Transaction Amount	Transaction Number	Transaction Amount
11	2400	16	4000
12	2000	17	5000
13	1000	18	6000
14	1200	19	1200
15	1500	20	1400

TABLE VI: Output of Spending Behavior Means

Mean/Centroid Name	C_{ls}	C_{ms}	C_{hs}
Considerationsymbol	V_1 = ls	V_2= ms	V_3= hs
Mean Value(Centroids)	2337.50	6500	0
Percentage of total transactions(p)	80	20	0

Figure 4 shows the percentage calculation of spending profile for step 2, where transaction number range is 11^{th} to 20^{th}.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

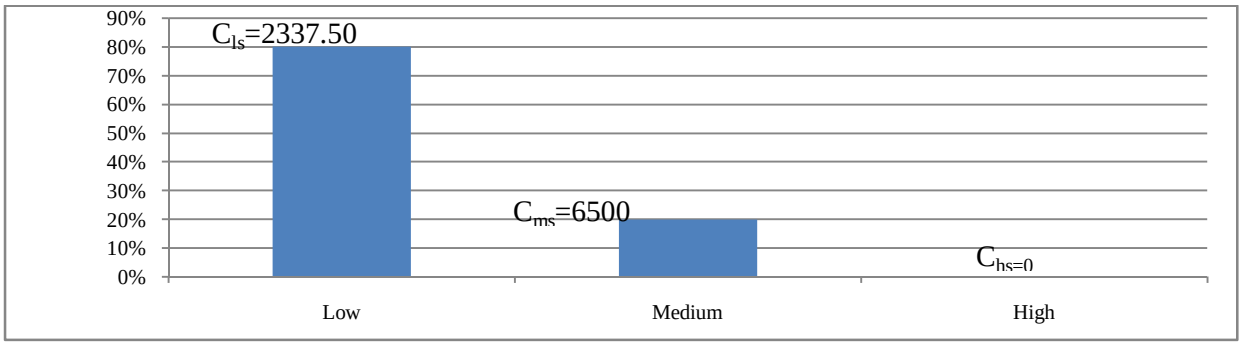

Fig 4.Percentage of Each Spending Profile for Step 3.

B. PROPOSED ALGORITHM OF DETECTION PHASE:

This algorithm is worked when transaction having value $\Delta\alpha$ is negative. For $\Delta\alpha$ value is Positive, Proposed Model done the transaction as normal and adds in to sequence of the transaction.

Algorithm:

1. Take a set of transactions in queue of n elements and pass to the HMM.
2. HMM, calculates α_{old} value. After adding new element in queue of n, again check α_{new}.
3. Calculate $\Delta\alpha = \alpha_{old} - \alpha_{new}$ and check $\Delta\alpha$.
4. If value of $\Delta\alpha$ is negative then transaction might be fraud then
5. And if Transaction is greater than last transaction with in ten minutes then asked security questions from user
6. If Answers are matched then transaction is normal and adds in the sequence.
7. Otherwise, Transaction adds in fraud history and called it fraud transaction.
8. Else If Transaction already in fraud history then called it fraud transaction.
9. Otherwise, Transaction is normal and adds into sequence.

V. CONCLUSION AND FUTURE SCOPE

AFDS is proposed consisting of two steps: Training and Detection of Fraud in the paper. In training, sequence of credit card transactions is added in to the system. In second step, detection is done with multiple stages. These are: matching with last transaction amount, checking fraud history and raising security questions. The proposed detection system performed the best and accurate result. As transactions are checked and passed through multiple tests, the algorithm become more robust. These tests are applied inmultiple stages. Only after passing the all stages, user is required to ask the security questions.

Here, this whole process is done by an example and also given the comparison of transactionsat different level with the mean of spending behaviors. In Future, extend this system to a more secure level.

REFERNCES

1. AmlanKundu, SuvasiniPanigrahi, ShamikSural, "BLAST-SSAHA hybridization for credit card fraud detection", IEEE Trans. dependable and secure computing, vol. 6, no. 4, October - December 2009.
2. S. Ghosh, D.L. Reilly, "Credit card fraud detection with a Neural- Network", Proceedings of the International Conference on System Science, pp. 621- 630, 1994.
3. AbhinavSrivastava, AmlanKundu, ShamikSural, Arun K. Majumdar, "Credit card fraud detection using Hidden Markov Model", IEEE Trans. dependable and secure computing, Vol. 5, No. 1, January-March 2008.
4. L.R. Rabiner, (1989)."A Tutorial on Hidden Markov Models and Selected Applications in Speech Recognition," Proc. IEEE, vol. 77, no. 2, pp. 257-286, 1989.
5. Vivek V. Jog, Aaradhana A. Deshmukh (2012, April). "HMM Based Enhanced Security System forATM Payment", IRACST – Engineering Science and Technology: An International Journal (ESTIJ), ISSN: 2250-3498, Vol.2, No. 2, April 2012.
6. S.J Stolfo, D.W Fan, W.Lee, A.L Prodromidis and P.K.Chan, "Credit Card Fraud Detection Using Meta- Learning: Issues and Initial Results", Proceedings of AAAI Workshop AI Methods in Fraud and RiskManagement, pp. 83-90, 1997.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

7. Jaba Suman Mishra, Soumyashree Panda, Ashish Kumar Mishra (2013, May). "A Novel Approach for Credit Card Fraud Detection Targeting the Indian Market", IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 3, No 2, May 2013.
8. Divya Singh, "Credit Card Fraud Detection Using Hidden Markov Model," International Journal of Scientific & Engineering Research, Volume 6, Issue 1, January-2015 SSN 2229-5518.
9. V. Bhusari, S. Patil, Study of Hidden Markov Model in Credit Card Fraudulent Detection, International Journal of Computer Applications (0975 – 8887) Volume 20– No.5, April 2011.
10. MohdAveshZubairKha, Jabir DaudPathan, Ali HaiderEkbal Ahmed,Credit Card Fraud Detection System Using Hidden Markov Model and K-Clustering, International Journal of Advanced Research in Computer and Communication Engineering, Vol. 3, Issue 2, February 2014.

BIOGRAPHY

Shilpa is an M.Tech Scholar in the Computer Science Department, The Technology of Textile Institute of Sciences (TIT & S) Bhiwani. She will be received her Master of Technology in Computer Science degree in 2016 from MDU, Rohtak, India. Her research interests are in Multimedia Technologies and Data Mining.

Ritika is a Lecturer in the Computer Science Department, Govt. College Hansi (Hisar) Kurukshetra University. She Received Master Of Computer Application (MCA) Degree in 2012 from DCSA, MDU, Rohtak, India. Her research interests are in Multimedia Technologies and Data Mining.