HMM Based Enhanced Security System for ATM Payment

[AICTE RPS sanctioned grant project , Affiliated to University of Pune , SKNCOE, Pune]

Vivek V. Jog [1],
Affiliated to University of Pune,
Smt.Kashibai Navale College of Engineering,
Pune,India

Aaradhana A. Deshmukh[2],
Affiliated to University of Pune,
Smt.Kashibai Navale College of Engineering,
Pune,India

Sonal S.Dhamak[3]
Affiliated to University of Pune,
Smt.Kashibai Navale College of Engineering,
Pune,India

Purvaja P. Khatod[4],
Affiliated to University of Pune,
Smt.Kashibai Navale College of Engineering,
Pune,India

Vikalpa B. Landge[5],
Affiliated to University of Pune,
Smt.Kashibai Navale College of Engineering,
Pune,India

Sneha C. Kamble[6]
Affiliated to University of Pune,
Smt.Kashibai Navale College of Engineering,
Pune,India

Abstract

A **hidden Markov model** (**HMM**) is a statistical model using a Markov process with observed state thus is clearly a dynamic Bayesian network of statistical assumption technique. Mobile device induced distributed security environment is proposed for meeting pass code challenge to complicate security by making the ATM payment frauds impossible. If an incoming ATM card transaction is not accepted by the trained HMM with sufficiently high probability, it is considered to be fraudulent, Assuring that genuine transactions are not rejected. "*Hidden"* state is not directly visible, but output dependent on the state is visible.

Evaluation: generating sequence of observations? The forward algorithm solves this problem.
Decoding: predicting most probably sequence of observations? The Viterbi algorithm solves this problem.
Learning: Is accomplished by using the forward-backward algorithm. Thus attempt is to use this proven technology (in fields like weather forecasting) in e-commerce to secure the ongoing fraud of ATM payment.

Keyword:HMM,FDS,TP,FP

1. INTRODUCTION

An ATM credit or debit card which is issued by a bank,credit union or building society is used for deposits, withdrawals, account information, and other types of transactions.With increase in use of ATM card,cases of fraud associated with it are also increasing.Thus a method should be devised inorder to avoid such frauds.r

Our idea is to find patterns which appear and reappear over a space of time. Pattern detection can be used in many areas; thepattern of commands someone uses in instructing a computer, sequence of words in sentences, sequence of phonemes in spoken words. In the same way it is also possible to project or forecast the possible behavior or habits of user in case of ATM transaction and to detect cases that deviate from normal transaction pattern of user.These computations will provide additional security on the ATM system.

HMM model is used to recognize and understand various transactions patterns of the user. It helps in maintaining and updating a database that describes the operational behavior of the specified user in the form of the pattern. With every transaction of user,behavioural pattern of user will be checked with previous patterns.If there is slight deviation then the transaction will be blocked.Inorder to unblock the transaction,user will be offered a challenge.After receiving correct response unblocking of transaction will be done. Thus the whole system tends to increase

the complexity to next level thereby making ATM payment frauds almost impossible.

2. HMM BACKGROUND

An HMM is a double embedded stochastic process having two hierarchy levels. It can be used to model much more complicated stochastic processes. An HMM has a finite set of states which are governed by a set of transition probabilities. An outcome or observation for particular state can be generated according to an associated probability distribution. It is only the outcome and this state is not visible to an externalobserver.Speech recognition, bioinformatics and genomics are some of the common HMM based applications. In recent years, Joshi and Phoba have investigated the probabilities of HMM in anomaly detection and they classified TCP network traffic as an attack or normal using HMM. Cho and Park suggested an HMM based instruction detection system which improves the modeling time and performance by considering only the privilege transition flows based on the domain knowledge of attacks. Ourston et al have proposed the application of HMM for detecting multistage network attacks. Lane used HMM to model human behavior.

HMM can be characterized by following[1]:Let N be the number of states in the model. We denote the set of states S={S1,S2,…….S_N}, Where S_i ,i= 1,2,…..N is an individual state. The state at time instant t is denoted by q_t.M be the number of distinct observation symbols corrected to the physical outcome of the system being modeled. We denote the set of symbols V={V1, V2, ….V_M}, where V_i, i=1,2,….M is an individual symbol.

1. The state transition probability matrix A=[I,j], where a_{ij} =P(q_{t+1} =S_j |q_t=S_i), 1≤ i ≤ N, 1≤ j ≤ N;t=1,2….(1)

2. For the general case where any state j can be reached from any other state I in a single step, we have a_{ij} > 0 for all i,j. Also, $\sum_{j=1}^{N} a_{ij}$ = 1, 1≤ i≤ N.

3. The observation symbol probability matrix B=[b_j (k)], where

   b_j (k)= P(V_k |S_j), 1≤ j≤ N, 1≤ k≤ M and

   $\sum_{k=1}^{M} b_j$ (k) =1, 1≤ j≤ N.(2)

4. The initial state probability vector π = [π_i], whereπ_i = P(q_1 = S_i), 1≤ i≤ N , such that

   $\sum_{i=1}^{N} \pi_i$ =1. (3)

5. The observation sequence

6. O = $O_1, O_2, O_3, \ldots O_R$, where each observation O_t is one of the symbols from V , and R is the number of observations in the sequence.

Notation	Meaning
M	Number of observation symbols
N	Number of hidden states
V_k k=1….M	Observation symbols
l, m, h	Price ranges – low , medium and high
a_{x-y}	Probability of transition from the hidden Markov Model state x to state y
K	Number of clusters
C_i	Centroid of cluster i

Table 1 : Notation Table

Table 2 : Acronym Table

Acronym	Expanded Form
FDS	Fraud Detection System
HMM	Hidden Markov Model
SP	Spending Profile
hs, ms, ls	High spending, Medium spending, Low spending group
TP, FP	True Positive, False Positive

3. USE OF HMM FOR ATM CARD FRAUD DETECTION

In our system , each transaction is submitted to the system for verification. System checks whether transaction is genuine or not depending upon the behavior of the cardholder,i.e, transaction delay , sequence of operation and spending pattern. And depending upon these parameters , computational decision is taken. If system finds the transaction malicious it blocks cardholders account and transaction gets failed.

But there may be possibility that the user is the sameuser,in this case he is able to unblock his account through his mobile by challenge response procedure.

4. PROPOSED SYSTEM

4.1 PROPOSED MODEL

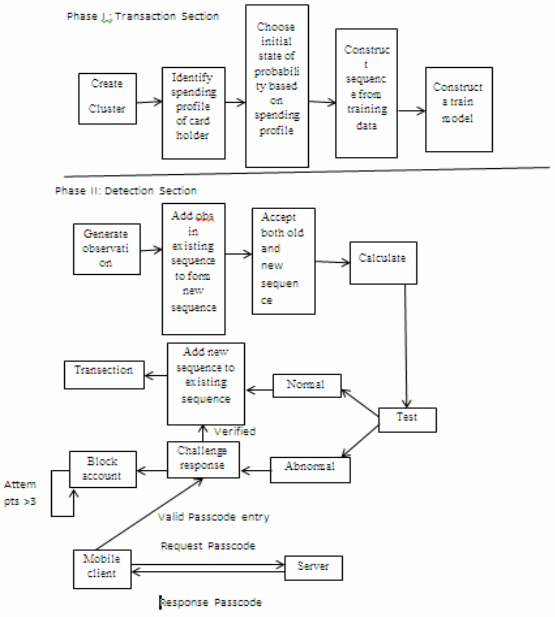

Figure1: Proposed Model

4.2 PROPOSED OPERATIONAL PROCEDURE

1) Starting Bank Server

2) Starting HMM server

3) Initiate Client for transaction (ATM)

4) HMM start observing comparing the operation

5) HMM traps the transaction if identified fraud and is blocked

6) User reply with password on mobile using Bluetooth if same bank ATM else using SMS

7) Password is verified for authentication and transaction is allowed

8) Transaction is totally blocked after three failed attempts

4.3 SYSTEM FLOW

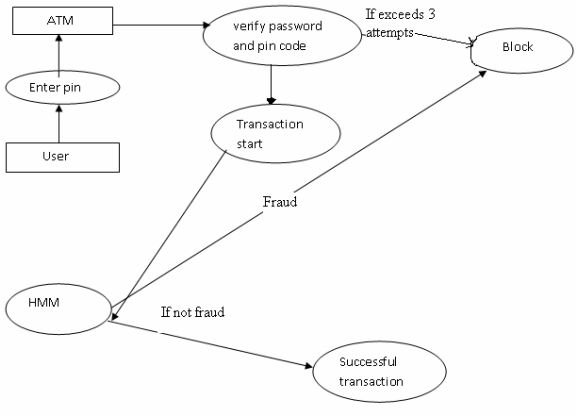

Figure 2 : System flow

4.4 WORKING CHARACTERISTICS

4.4.1 Secure transaction

The main aim of the system is to provide secure transaction of the ATM and privacy of customer's account. The data access is based on the behavior of customer and sequence of operation performed during the transaction.

4.4.2 Authorization

Usually authorization is done with the help of only pincode, but it is not sufficient way to detect the fraud case. Hence we are using Hidden Markov Model for authentication.

4.4.3 Block transaction

If system detects any fraud case using HMM, then it will block the further operations.

4.4.4 Unblock transaction

If customer's transaction getting blocked because of any reason even though he is a valid customer then he is able to unblock the transaction at that time by just giving reply to the challenge thrown by ATM.

4.5 ALGORITHMS USED

4.5.1 Viterbi Algorithm

The viterbi algorithm is dynamic programming algorithm used for finding the probable sequence of hidden states which is called as viterbi path that results in a sequence of observed events; especially in the context of Markov Information source and generally Hidden Markov Model. It belongs to the area of probability theory.

Assumption for Viterbi algorithm

1. Both observed events and hidden events must be in a sequence, the sequence is in time order of occurrence.

2. These two sequences should be aligned: an instance of an observed event should correspond to exactly one instance of a hidden event.

3. For computing the most likely hidden sequence (For a particular state) up to certain point t must depend only on the observed event at t, and the most likely sequence which leads to that state at point t-

These all assumptions are satisfied in a first-order hidden Markov model.Viterbi algorithm works on state machine assumption. System operates on finite number of states.

4.5.2BAUM-WELCH ALGORITHM

Initial guess for BAUM-WELCH Algorithm

Below given are the parameters that ideally suits to for fraud detection task in practice. Any given transaction will be scanned in the chronological order given below

1) Call Given for Building HMM

2) Call to generate new object for newly building HMM

3) Initial Parameters set for HMM deductions

4) For estimating a transaction being 80 % o or 20% fraud

5) For estimating a transaction that has slips from 80-20 probability barrier

Estimate to be made for 10% OK and 90% Fraud transactions.

4.6 GENERATE SEVERAL OBSERVATION SEQUENCES USING A HMM

Using HMM generate several observations.

Comparisons will be made with closely resembled 100 observations to compute result

Add the new sequences to the observation sequences.

Probabilistic derivatives considered during generations of sequence from history
Settings digraph G are

0 -> 0 [label=0.95];

0 -> 1 [label=0.05];

1 -> 0 [label=0.1];

1 -> 1 [label=0.9];

Above mentioned parameters can be read as

For - 0

Pi= 0.92 –[Discrete distribution - OK 0.95, FRAUD 0.05]"];

For - 1

Pi= 0.08 - [Discrete distribution --- OK 0.194, FRAUD 0.806]"];

Double safety Algorithm:

We are providing centroid calculation at 2 levels. Firstly centroid is calculated for each parameter parallely . Then those three centroids are taken as input for next stage centroid calculation. Now we are having final cenroid. Depending on this final centroid, We take compound decision about fraud detection. If centroid is above threshold value then transaction is not fraudulent. And when it is below threshold value then fraud is detected, so that transaction is considered as fraudulent transaction.

4.7 PARAMETERSETTINGS FOR HMM

The algorithm has two steps:

Calculating the forward probability and the backward probability for each HMM state.On the basis of this, determining the frequency of the transition-emission pair values and dividing it by the probability of the entire string. This amounts to calculating the expected count of the particular transition-emission pair. Each time a particular transition is found, the value of the quotient of the transition divided by the probability of the entire string goes up, and this value can then be made the new value of the transition.

Due to this HMM that will be using this algorithm need to know the exact permissible limit other than what standard deductions allow as a part of practical variations

4.8TIME VERIFICATION TOLERANCE LIMIT SETTINGS

Variations in withdrawal time for last 10 successful transactions for User 1 are as follows
Consider the set of sample space
1) 42, 2) 35, 3) 38, 4) 36, 5) 47, 6) 28, 7) 39, 8) 43, 9) 60, 10) 53
Set 1, it requires 42 sec for the transaction, we have given 10 sets with their transaction times.
Then we will calculate the centroid of these values for detecting that whether it is fraudulent or not.
If the value is above centroid then it is considered as fraudulent otherwise not fraudulent.

4.9 SEQUENCE OF OPERATIONS

Consider the 6 different transaction types A,B,C,D,E,F : k-p-1=5
P: probability of getting fraud=1/2
Q: probability of getting not fraud =1/2

Suppose user has done transaction 210 times
Frequency of getting A,B,C,D,E,F are the groups of successive sequences of operations and are mapped w.r.t terms of binomial expansion:

$$210\ (p+q)^5$$

$$=210[p^5+5p^4q+10p^3q^2+10p^2q^3+5p^1q^4+q^5]$$
$$=210[1/32+5/32+10/32+5/32+1/32]$$
$$=7+33+66+66+33+7$$

Theroticaltransaction are
7,33,66,66,33,7

$$X_5^2=\frac{(2-7)^2}{7}+\frac{(5-33)^2}{33}+\frac{(20-66)^2}{66}+\frac{(60-66)^2}{66}+\frac{(100-33)^2}{33}+\frac{(37-7)^2}{7}$$

$$X_5^2=3.57143+23.7576+32.06061+0.5455+136.0303+82.285$$
$$X_5^2=278.2511$$
$$X_5^{2,0.05}=11.070$$

Since the calculated value of x^2 is much grater than X_5^2,0.05,the hypothesis that the data follow the binomial distribution is rejected and the transaction is markesfradulant, where 0.05 is significance level at which x^2 value is used.

5. RESULT

5.1 PRACTICAL FRAUD EVALUATION PROCESS FOR AMOUNT

(Delta alpha calculations)
A systematic approach towards detection of fraudulent transaction comprises of two phases Phase - I & Phase – II

5.1.1 *Phase I*

1. Take two arrays (Size 10 for this example)

   Two arrays are used to read the transactions from history to compute

   a. Amounts[i]

   b. M_amounts[i]

2. Select 10 transactions from database and order all them date wise descending. Hence, the transaction amount are as,

Amounts[i]={200,400,500,2000,200,6000,5000,500, 1800,7000}

M_amounts[i]={200,400,500,2000,200,6000,5000,50 00,1800,7000}

3. Sort the M_amounts[i] array. Hence, amounts in array are as follows

   M_amounts[i]={200,200,500,500,1 800,2000,5000,6000,7000}

4. Compute centroids:[C for Centroid]

C1=200+200+500=900/3=300
C2=500+1800+2000+5000+5000 =14300/5=2860
C3=6000+7000=13000/2=6500

5. Now take the array amounts[i] and subtract each centroid value from each value in amounts[i]. Here you will get 3 values (say probabilities values) for each transaction. Take one profiling values array i.e. pvalue[i]. Note: In this example take size of pvalue 10.

   Ex. For transaction 1 in amounts[i] i.e. first value in array.

   T1=200

   P1 =200-300=|-100|=100

   P2=200-2860=|-2660|=2660

   P3=200-6500=|-6300|=6300

   If any negative value, take a modulus of a value. Check above calculation carefully.

   Now we are going to do profiling for transaction using pvalue[i] array, as

   If (P1> P2 && P1> P3) then

   Accommodate pvalue[i] with 0 // Zero for lower profile

   Else if (P2 <= PP1 && P2 < P3) then

   Accommodate pvalue[i] with 1 // One for medium profile

   Else

   Accommodate pvalue[i] with 2 // Two for higher profile

6. Get 3 probability values for each transaction values in amounts[i] and correspondingly profile the positions in pvalue[i].

7. Note after all the above calculations the pvalue[i] is as follows:

   pvalue[i] ={0,0,2,1,0,2,2,0,1,2}

8. Count the total number of 0,1,2 in pvalue[i].

   In Our Example,

count_l=4
count_m=2
count_h=4
Find probability for lower, mid and high asfollows

PL=count_l/10=0.4
PM=count_m/10=0.2
PH=count_h/10=0.4

9. Calculate alpha1

$$\text{alpha1} = PL*PM*PH = 0.4*0.2*0.4 = 0.032$$

5.1.2 *Phase II*

1. Replace last transaction value in amounts[i] array by current amount i.e. amounts[g] = amount // let amount=500

2. Use some centrioids as in phase 1. Do some calculations next in this phase as in phase 1 i.e. repeat steps (5) to (10) as in phase 1 and compute pvalue[], alpha2

After computations the pvalue[i] array will look like…

Pvalue[i] = {0,0,2,1,0,2,2,0,1,0}

In this case

Alpha2 = 0.03

3. Compute ΔAlpha as

ΔAlpha = alpha1 – alpha2

= 0.032 -0.03

=0.00200

4. If Dalpha> 0 then

Fraud = False // Transaction is not Fraudulent in behavior

Fraud = True // Transaction is Fraudulent in behavior.

5.1.3. Final Result

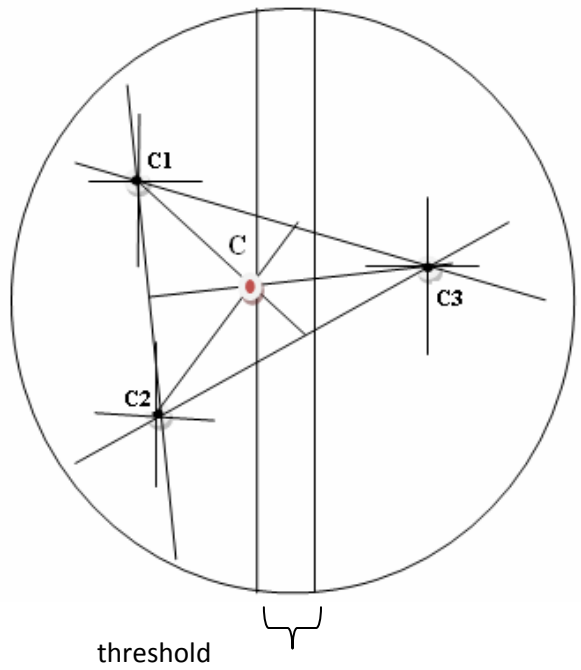

Fig. 5.1 Calculating final cenroid from C1, C2 and C3.

C1 : Centroid of parameter 1(Transaction delay)

C2 : Centroid of parameter 2(Spending pattern)

C3 : Centroid of parameter 3(Sequence of operation)

We are taking final decision by calculating final centroid C from these three values C1, C2, C3.

which is shown in fig. 5.1

If C < threshold then transaction is fraudulent.

Else transaction is not fraudulent.

After setting the parameters and taking random values for the parameters we got the graph which is shown

below:

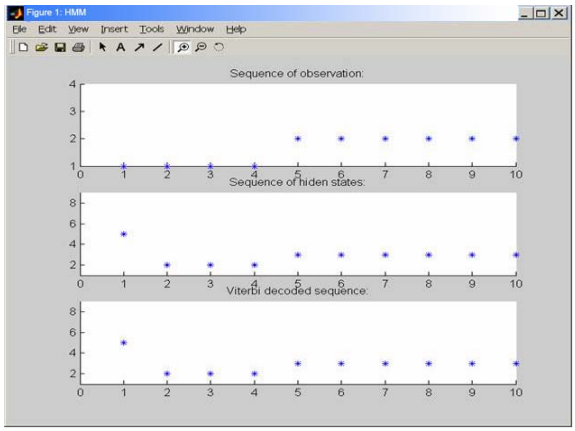

Figure 9.1: Graph constructed in matlab by given appropriate values.

Sequence of observation is given as input, depending on it as well as sequence of hidden state stored in database, we got viterbi decoded sequence by using viterbi algorithm.

6. CONCLUSION

HMMs have proved to be of great value in analyzing real systems; their usual drawback is the over-simplification associated with the Markov assumption - that a state is dependent only on predecessors, and that this dependence is time independent. With its utter closeness to the realistic predictions it thus helps in preventing as well as controlling many system behaviors.

In this paper, it has been discussed that how Hidden Markov Model will facilitate to stop fraudulent transaction through ATM card. The Fraud Detection System is also scalable for handling vast volumes of transactions processing. This system will provide better security as two level of encryption is done. Also authentication mechanism will help to achieve better security through mobile. The Hidden Markov Model makes the processing of detection very easy.At the initial state HMM checks the upcoming transaction is fraudulent or not and it allows to accept or reject the whole transaction based on the probability result. A technique for finding the spending behavioural habit of cardholders, also the application of this knowledge in deciding the value of observation symbols and initial estimation of the model parameters are recommended in this paper. The relative studies and our results ensure that the correctness and effectiveness of the proposed system is secure to 80 percent over a broad deviation in the input data.

7. ACKNOWLEDGEMENT

The authors would like to be anonymous reviewers for their constructive and useful comments.This work is supported by research grant from AICTE RPS sanctioned grant project, Affiliated to University of Pune , SKNCOE, Pune

8. REFERENCES

[1] Credit Card Fraud Detection Using Hidden Markov Model AbhinavSrivastava, AmlanKundu, ShamikSural, Senior Member, IEEE, and Arun K. Majumdar, Senior Member, IEEE.

[2] 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.

[3] S.S. Joshi and V.V. Phoha, "Investigating Hidden Markov Models Capabilities in Anomaly Detection," Proc. 43rd ACM Ann. South-east Regional Conf., vol. 1, pp. 98-103, 2005.

[4] L. Kaufman and P.J. Rousseeuw, Finding Groups in Data: An introduction to Cluster Analysis, Wiley Series in Probability and Math. Statistics, 1990.Math.Statistics, 1990.

[5] DEPENDABLE AND SECURE COMPUTING, VOL. 5, NO. ,JAN-MAR 2008 Credit Card Fraud Detection Using Hidden Markov Model BY :- AbhinavSrivastava, AmlanKundu, ShamikSural, Senior Member, IEEE, and Arun K. Majumdar, Senior Member, IEEE.

[6] "Statistics for General and On-Line Card Fraud" available as guidance paper at site http://www.paynews.com/statistics/fraud.html, Mar. 2007

[7] 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," Proc. AAAI Workshop AI Methods in Fraud and Risk Management, pp. 83-90, 1997