Advanced Security Model for Detecting Frauds in ATM Transaction

Vivek V. Jog
Assistant Professor
Dept. of Comp. Engg.
SKNCOE, Pune

Nilesh R. Pardeshi
PG Student
University of Pune
SKNCOE, Pune

ABSTRACT
ATM card fraud is causing billions of dollars in losses for the card payment industry. In today's world the most accepted payment mode is Debit card for both online and also for regular purchasing; hence frauds related with it are also growing. To find the fraudulent transaction, we implement an Advanced Security Model for ATM payment using Hidden Markov Model (HMM), which detects the fraud by using customers spending behavior. This Security Model is primarily focusing on the normal spending behavior of a cardholder and some advanced securities such as Location, Amount, Time and Sequence of transactions. If the trained Security model identifies any misbehavior in upcoming transaction, then that transaction is permanently blocked until the user enter High Security Alert Password (HSAP). This paper provides an overview of frauds and begins with ATM card statistics and the definition of ATM card fraud. The main outcome of the paper is to find the fraudulent transaction and avoids the fraud before it happens.

General Terms
Hidden Markov Model, Advanced Fraud Detection System.

Keywords
HSAP, HMM, FDS, Patterns, Transaction, Location, Fraud.

1. INTRODUCTION
It is the need of era and many challenges faced by banking system to provide good and secured facilities of E-transaction. For that our banks provide us a Magnetic Chip, we called it is as ATM card. As today's daily routine we see that use of ATM cards has significantly increased. Now a day the most accepted payment mode is using ATM cards. As the use of ATM card is increased, the frauds related with it have also increased.
The paper present a ATM fraud detection system which is based on Hidden Markov Model (HMM), which detects fraud just by learning the cardholder's spending habit/pattern.

2. BACKGROUND
In the existing fraud detection system [1], fraud is detected after fraudulent transaction is processed. Due to which the card holder faces a lot of problems before the investigation finish. The existing system [1] does not consider the spending behavior of cardholder as the key element to detect the fraudulent transaction. Hence the crime plays an important role to investigate the fraud. Due to such a long investigation process, the existing fraud detection system is time consuming process. Hence it affects the business processing of fraud detection system. So in this business processing we prefer to the Hidden Markov Model. Now a day's many of transactions are made with ATM/debit card so we don't know the person who is using the card, we just capture the image or record the video for authentication purpose.

3. MAJOR FRAUDS IN ATM

3.1 Lost or Stolen Card
This is one of oldest and common fraud technique which is used by fraudsters. In this fraud technique fraudsters stole the actual information of customer. This information they can use for making the anonymous transaction. To avoid such kind of transaction customers multiple patterns should be recorded somewhere in the database. [13].

3.2 Card Not Present
In this fraud, the transaction will be done without using actual card. Here the fraudster does not need a physical card to make a transaction. Because of this disadvantage, Card Not Present (CNP) is becoming more popular than other frauds. To secure such kind of transaction this paper proposes a location based fraud detection system considering multiple attributes of customer. [13].

To avoid such drawbacks our advanced ATM fraud detection system is very useful to detect the fraudulent transaction in a best and easy way.

4. LITERATURE SURVEY
Abhinav Shrivastava and team [1] proposed "Credit Card Fraud Detection Using Hidden Markov Model" They explains in that the problem with most of the previous approaches is that they require labeled data for both genuine, as well as fraudulent transactions, to train the classifiers. Getting real-world fraud data is one of the biggest problems associated with credit card fraud detection. Also, these approaches cannot detect new kinds of frauds for which labeled data is not available.
They model a credit card transaction processing sequence by the stochastic process of an HMM. The details of items purchased in individual transactions are usually not known to FDS running at the bank that issue cards to the cardholders. This can be represented as the underlying finite Markov chain, which is not observable.
An important advantage of the HMM-based approach [2] is a drastic reduction in the number of False Positives (FPs) transactions identified as malicious by an FDS although they are actually genuine. Since the number of genuine transactions is a few orders of magnitude higher than the number of malicious transactions, an FDS should be designed in such a way that the number of FPs is as low as possible.

5. WORKING CHARACTERISTICS

5.1 Secure Transaction

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

5.2 Authorization

Usually authorization is done with the help of only pin code, but it is not sufficient way to detect the fraud case. Hence we are using advanced security model for fraud detection and authorization.

5.3 Block Transaction

If system detects any fraud in transaction then the advanced security model will block that transaction immediately and send a High Security Alert Password on user's contact number.

5.4 Unblock Transaction

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

6. PROPOSED SYSTEM

This system consists of two different sections,
1. Transaction Section/ Learning Section
2. Detection Section

Scope of the work of each section is depends on each other. The model defines the restricted domain in which the scope lies. Thus we proposed new model (fig.1) with the help of CCFD model [1]

7. ADVANCED SECURITY MODEL

In our advanced security model there are four input parameters.

7.1 Location

This input parameter will be checked at the time of user login. To calculate this parameter we have to go through following steps,

Step1: First we calculate the Latitude and Longitude of previous transaction.

Step 2: Then we calculate the upcoming transaction's Latitude and Longitude.

Step 3: We calculate one threshold value of location parameter from last 20 transactions, we compare this threshold value with the difference of step1 and step 2 values. If that difference is greater than our threshold then the upcoming transaction may fraud.

This input parameter will start the checking from the beginning when user enters an ATM pin. If our advanced security model founds fraud then he will block the transaction and send a HSAP on user's registered mobile number.

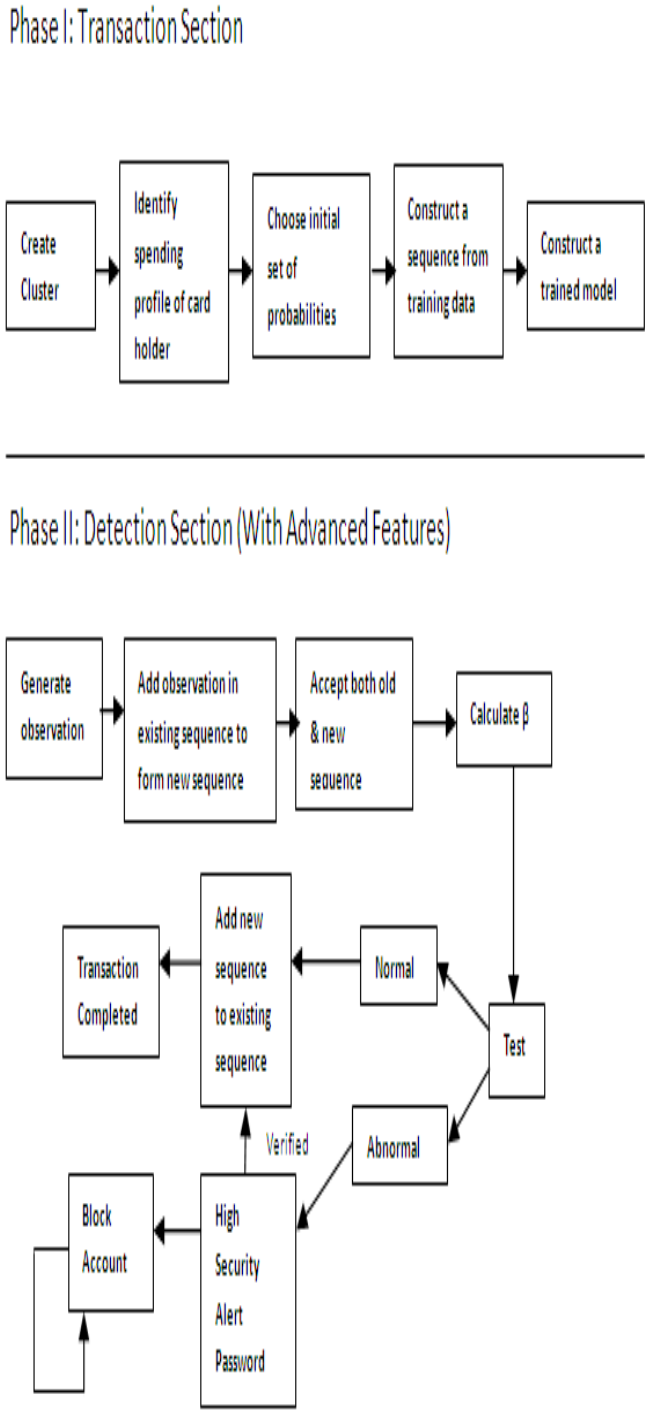

Fig 1: Proposed Model

7.2 Sequence of Transaction

This input parameter is depending on user's behavior, how he withdraws the money. For example, consider one user who having the habit like first he checks the account balance and then he withdraw the money and vice versa. Like this every user have their different patterns of doing transaction.

We consider such previous 20 transactions patterns, and that patterns are forwarded to our FDS system as an input parameter.

7.3 Time Taken for Transaction

Here we consider the time taken for doing the transaction right from the moment a user enters a password to user enter an amount and presses the confirmation button of withdraw money. Here the major role of our FDS system is to calculate the current transaction spending time and compare this time with the previous 20 transactions before giving out the money. If current time deviates with our previous record then we block the transaction.

7.4 Amount

The amount is most important factor for our fraud detection system. Here we consider previous 20 transactions amounts for finding the fraud. The steps to detect fraud using the amount parameter as,

Step 1: Consider previous 20 unique transactions amounts.

Amounts= {20 Transactions Amount} // Unsorted

M_Amounts= {20 Transactions Amount} // Sorted

Step 2: Cluster these transaction into 4,6,10 and find the mean of each.

C [0] = Mean 1

C [1] = Mean 2

C [2] = Mean 3

Step 3: Subtract each mean value from each amount.

V [0] = M_Amount[i] – C[0]

V [0] = M_Amount[i] – C[0]

V [0] = M_Amount[i] – C[0]

Step 4: Calculate pvalue for all 20 transactions.

If (V [0] < V [1] && V [0] < V [2])

Then pvalue[i] = 0;

Else if (V [1] <= V [0] && V [1] < V [2])

Pvalue[i] = 1;

Else Pvalue[i] = 2;

And finally we get the set of pvalue.

Step 5: Find the probability values of low, medium, high value from pvalue set.

Step 6: Then find the Alpha (α1) as,

Alpha (α1) = P (low) * P (medium) * P (high)

Step 7: Now consider the upcoming new transaction, calculate the Alpha (α2) by replacing last amount from amount set and calculate pvalues using same mean values we used to calculate alpha1 & then repeat the steps 3 to 6. Then we get the value of Alpha (α2).

Step 8: Calculate the final result using Beta (β),

Beta (β) = alpha (α1) – alpha (α2)

If Beta (β) >0 then this transaction is fraud else not.

The system flow for our advanced security model is shown in fig. 2.

8. HIGH SECURITY ALERT PASSWORD

This facility will get enabled when our fraud detection system got any fraudulent transaction. So as it occurs system will send a High Security Alert Password (HSAP) on user's registered mobile number. As user got this password, user has to enter this password on screen of HSAP to continue the transaction. The time limit to enter the High Security Alert Password is 2 minutes. After 2 minutes the password will get expired. You have to regenerate the new HSAP.

If the current user is fraudulent one then the transaction would remain unblocked and the original user get a High Security Alert Password through SMS service and realize that the someone unauthorized user has accessed his/her account so he/she need to block his ATM card as soon as possible.

9. OBSERVATION & RESULT

It is very difficult task to test debit card fraud detection system using real data set. Bank do not shares their data with the researchers. There is also no possibility of avail such data set for experimentation. Therefore, numbers of transactions were performed to test the efficiency of the system. A simulator is used to generate a mix of genuine and fraudulent transactions. The genuine transactions are generated according to the cardholder's profiles. The cardholders are classifieds into three categories i.e. low, medium, high price transactions respectively [1]. The effects of spending group and the percentage of transactions that belong to the low, medium, and high price range cluster. Then set of experiments were carried out to determine the correct combination of HMM design parameters namely, amount of transaction, time of transaction and the sequence of transaction.

10. CONCLUSION

This paper proposes a model which is combination of various input model based on spending profile of user. This model impose much security to the cardholder as it has taken four things under consideration ATM Location, spending habits such as amount, time and sequence of transaction. In this there are less chances that legitimate user will be treated as fraud, means genuine transaction will be decreased. We can extend this approach for different other ATM frauds and their explicit detection techniques. This type of detection model which combines complete detection and prevention mechanism will be more productive to electronic commerce. 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. The paper should conclude the work and state proposed work if any.

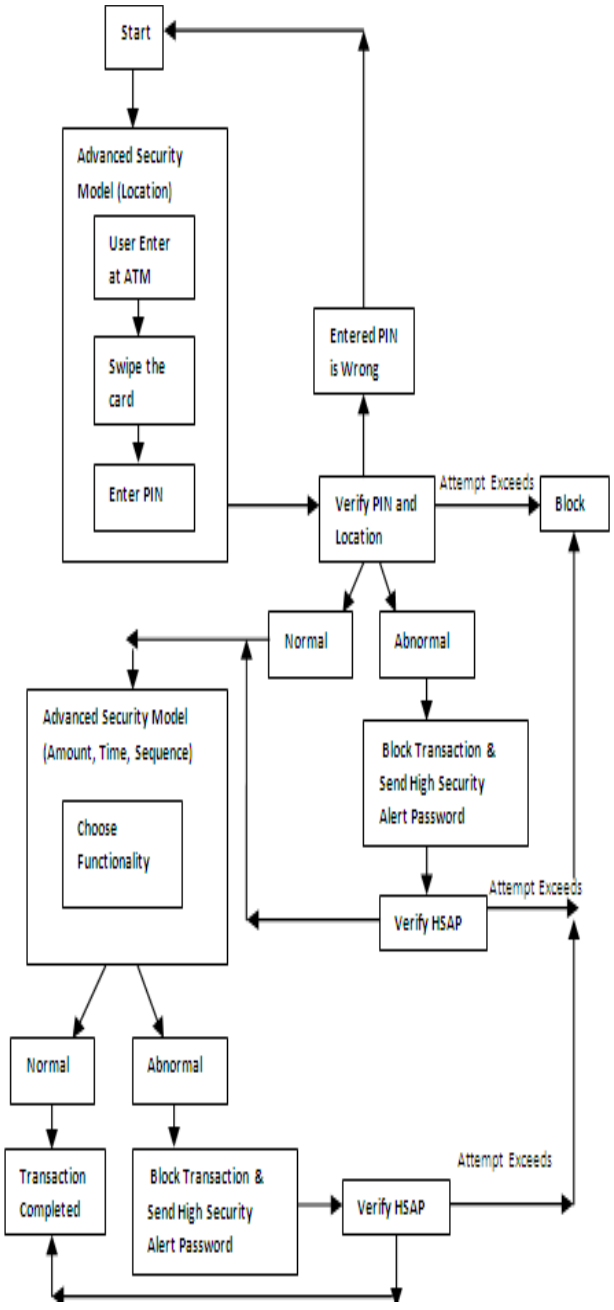

Fig 2: System Flow

11. ACKNOWLEDGMENTS

For proposing advanced model we referred the IEEE Transaction paper under the title "Credit Card Fraud Detection Using Hidden Markov Model" published in IEEE TRANSACTIONS, VOL. 5, NO. 1, Jan-Mar 2008. This paper mentions fraud detection system for credit card which is also helpful in proposed system.

I would like to express my sincere gratitude towards Prof. V. V. Jog for guiding me throughout this paper research and providing me eclectically the resources needed for me to make this paper possible.

12. REFERENCES

[1] "Credit Card Fraud Detection Using Hidden Markov Model" Abhinav Shrivastava, Amlan Kundu, Shamik Sural, Senior Member, IEEE, and Arun K. Majumdar, Senior Member, IEEE Transactions, VOL 5, No. 1, Jan-Mar 2008.

[2] "Credit Card Fraud Detection Using Hidden Markov Model" by Divya Iyer, IEEE Conference. 2011

[3] "Distributed Data Mining in Credit Card Fraud Detection" by Phili K. Chan, IEEE Intelligent Systems, Nov-Dec 1999.

[4] S. Ghosh and D.L. Reilly, "Credit Card Fraud Detection with a Neural-Network," Proc. 27th Hawaii Int'l Conf. System Sciences:Information Systems: Decision Support and Knowledge-Based Systems,vol. 3, pp. 621-630, 1994.

[5] "Theft Prevention ATM Model using Dormant Monitoring for Transactions" by Prof. V. V. Jog, IEEE Conference. 2012.

[6] "HMM Based Enhanced Security System for ATM Payment" by Prof.V.V.Jog and Prof.A.A.Deshmukh, IRACST, ISSN No. 2250-3498, Vol 2 No 2, April 2012

[7] 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.

[8] "Statistics for General and On-Line Card Fraud," http://www. epaynews.com/statistics/fraud.html

[9] "Online Banking Fraud Detection Based on Local and Global Behavior" by Stephan Kovache and Wilson Vicente Ruggiero, The Fifth International Conference on Digital Society, 2011.

[10] "Plastic card fraud goes back up". BBC. March 12, 2008. http://news.bbc.co.uk/2/hi/business/7289856.stm. Retrieved January 2, 2010.

[11] 2010 Identity Fraud Survey Report: Consumer Version :https://www.javelinstrategy.com/uploads/files/1004.R_2010IdentityFraudSurveyConsumer.pdf

[12] "Understanding Credit Card Frauds" By Tej Paul Bhatla, Tata Consultancy Services,June 2003

[13] Technical Report UTDCS3411, The University of Texas at Dallas, Payment Card Fraud: Challenges and Solutions by Irina Sakharova and Latifur Khan, Nov 2011