I J C T A, 10(8), 2017, pp. 697-703 ISSN: 0974-5572

Proposed Model for Detecting Frauds in ATM Transaction Using Statistical Assumption Theory

Nilesh R. Pardeshi* and Dr. K.V.D. Kiran**

ABSTRACT

Frauds in ATM transaction are causing billions of dollar losses in banking industry. In Today's scenario payment through ATM card is one of easily accepted mode of payment for regular purchasing and online as well, therefore fraud related to ATM transactions are also increasing. To avoid such frauds during transactions, we proposed an Advanced Security Model (ASM) for ATM payment using location based statistical assumption theory, which detects the fraud by learning cardholder's spending patterns. Initially advanced security model will focus on learning of cardholder's normal spending behavior and after getting perfection in the Advanced Security Model (ASM) we are applying few advanced securities like Amount, Time Location and transactional sequence. If learned model of Security found any misconduct in behavior of transaction, then that transaction is blocked permanently until the user enters High Security Alert Password (HSAP). This paper provides an ATM overview, ATM card statistics and solution of ATM frauds. The main outcome of our paper is to find the fraudulent transaction before it happens.

Index Terms: HSAP, HMM, ATM Fraud, FDS, Transaction, Skimming, Location

1. INTRODUCTION

Now a day banking industry is facing so much of challenges to provide good & secured facility for offline as well as online transaction. For a transaction purpose our bank provides us one smart chip which we called ATM card. This ATM card is a magnetic chip with fully loaded with your account details on it. As we see in today's life use of ATM card is so much increased and due to which fraudulent activity with respect to transaction is also increased. ATM card is most accepted payment method in banking services. There is no security system to detects the fraudulent transaction before is happens [5]. So we proposed an advanced fraudulent detection system, which is based on multiple parameters. Which detects the frauds in transaction before it happens.

2. RELATED STUDY

Mike Bond et. al. [1] proposed the how to avoid the cloning. They explain the EMV protocol into this paper; also they developed a methodology in which the ATM system is generating a nonce, called the unpredictable number [1], to ensure an every transaction is new one. Getting with the conclusion that the EMV cards are can't be cloned. Mohamed Musallam Khasib AI Rawahi and Smitha Sunil Kumaran Nair [2] propose a technique which detects the skimming devices which are attached to the ATM. Detection of skimming devices is done using the image processing. They have explained how the skimmer works and cloning of card is achieved. The risk of card cloning is reduced with the image processing. Ayhan Demiriz and Betul Ekizoglu [3] they explored the rule based prevention and fraud detection system for retail banking using the location data. They have implemented this system in turkey.

* Research Scholar, K. L. University, Vaddeswaram, Guntur Dt, Andhra Pradesh, India, *Email: n.r.pardeshi@gmail.com*

** Associate Professor, K. L. University, Vaddeswaram, Guntur Dt, Andhra Pradesh, India, *Email: kiran_cse@kluniversity.in*

Prof. V. V. Jog and Nilesh R. Pardeshi [4] proposed a model which detects the frauds in ATM transaction using the Hidden Markov Model. The limitation with this paper is the trained model is not that much adequate to detect the advanced frauds due to less transactions are taken in the learning phase. Abhinav Shrivastava et. al. [5] proposed "Credit Card Fraud Detection Using Hidden Markov Model", they explains the fraud detection methodology for credit card using hidden markov model. In which only one customer's spending habit is considered to train the fraud detection model. Limitation with the paper is new kinds of frauds are not to be detected with the help of existing method.

Advantage of HMM based approach [5] is reducing the False Positive transactions (FP) caught by the fraud detection system as a fraudulent transaction but although it is genuine transaction. To avail the real transactions data is one of the biggest challenge. The objective of proposed model is the number of False Positive transactions (FP) are low as possible.

3. TYPES OF FRAUDS IN ATM TRANSACTION

3.1. Stolen or Lost Card

Such types of frauds are one of the oldest fraud method used by fraudster or criminal. When card is obtained by the criminal by the method of lost or stolen that can be used by the victim to purchases goods or used in online transaction. Online purchasing is the most common method which is used by the criminals in this category [8].

3.2. CNP

CNP is nothing but Card-not-present transaction (CNP). In this type of fraud payment card is not physically present at the time of transaction. In CNP fraudster don't need card physically to do transaction [8]. In Card-not-present transactions there is no chance to check card physically to identify its authenticity or identity of the cardholder, so therefore there is always risk of payments where you disclose your identity.

3.3. Skimming Attack

Skimming is the method used to stealing the money. In today's era skimming is used in the cloning of your ATM as well as credit card. Basically two hardware's are used in skimming activity in Automated Teller

Figure 1: ATM Keypad Skimmer [2]

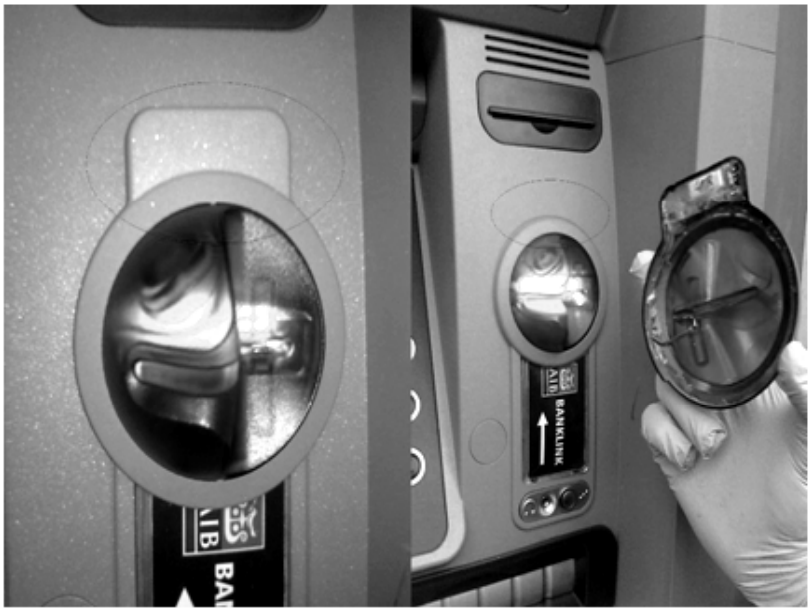


Figure 2: ATM Card Skimmer [2]

Machine [2]: a micro or mini camera which directly captures your PIN (Personal Identification Number) when cardholder enters the PIN or sometimes fraudsters may use duplicate keypad for capturing of PIN shown in fig.1 and the card reader shown in fig.2 which reads the magnetic strip of your card and this captured data is used in cloning of your card. After cloning this duplicate card is used immediately in worldwide. The cardholder will get to know after the transaction is happened. Such type of frauds is very dangerous and which makes you to face major financial loss.

To avoid such drawbacks we proposed a model which detects the fraudulent transaction in ATM in easy way.

4. WORKING CHARACTERISTICS

4.1. Transactional Security

The main objective of this proposed system is to provide security against the fraudsters. Primarily this system is focused on privacy in customer's personal transaction data. The data while performing the transaction is analyzed by the proposed model and which helps in detecting the upcoming fraudulent transaction.

4.2. Authentication & Authorization

Now a day's authentication of transaction is done by only PIN. But if the fraudsters have this PIN and data on magnetic chip they can do the transaction from any location. So authentication and authorization is very important aspect in our proposed model. We proposed multilayer authentication system which aware to the customer before fraud happens.

4.3. Blocking of Transaction

Blocking of transaction is done in the second phase of proposed model. Initially in the first phase the model is able to learn the previous sufficient transaction to prepare perfect customers spending behavior and by observing this if the model found any deviations in the upcoming transaction then the system is going to block the transaction and send the HSAP [4] (High Security Alert Password) on customer's registered mobile number.

4.4. Transaction Unblocking

We have proposed the many challenges to unblock the blocked transaction.

1. Enter the valid HSAP within stipulated time.
2. Enter the Current Latitude and Longitude details (Mobile device location details).
3. Questions related to personal data for authentication of genuine customer

Customer has to give the reply to the above any one or multiple challenges which are thrown by ATM to unblock the transaction.

5. PROPOSED MODEL

The proposed model is worked in two sections,

1. Transaction Section/ Learning Section
2. Prevention and Detection

Every second phase is totally depends on the result of first phase. The proposed model is designed with the help of CCFD model [5]. Steps involved in each phase are shown in the fig. 3.

6. ADVANCED FEATURES IN ATM SECURITY MODEL

There are four input parameters in proposed advanced security model.

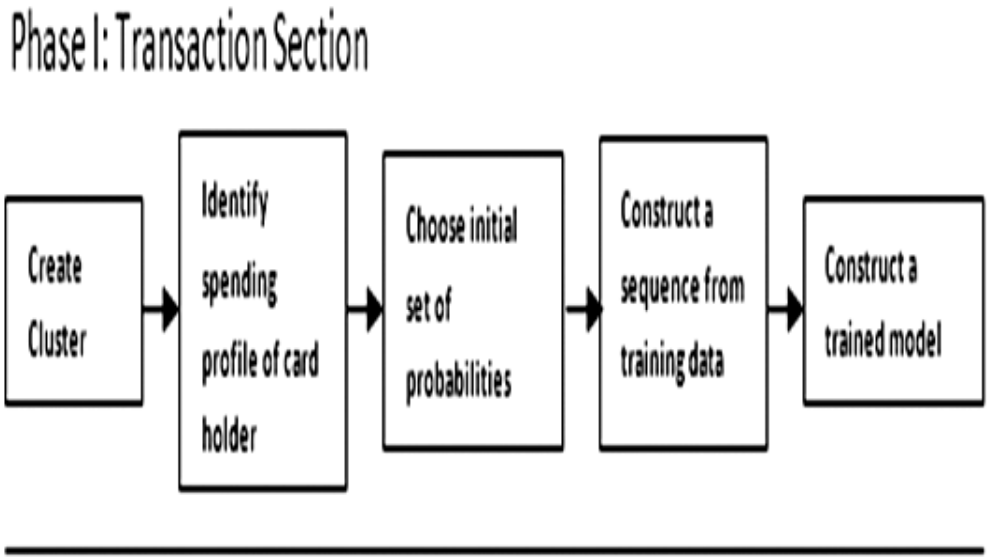
6.1. Location of Transaction

This advanced feature is checked at the time when cardholder enters the card into the machine. To calculate the location we have to follow the following steps,

Step1: Record the Latitude and Longitude of all previous transactions.

Step 2: Calculate the upcoming transactions location using its Latitude and Longitude.

Step 3: Compare this upcoming transactions latitude and longitude with the previous transactions latitude and longitude and generate the distance between these two locations in Km. Compare this distance value with the time threshold value. If any deviation appears then system will block the transaction and send the HSAP on user's personal mobile number.



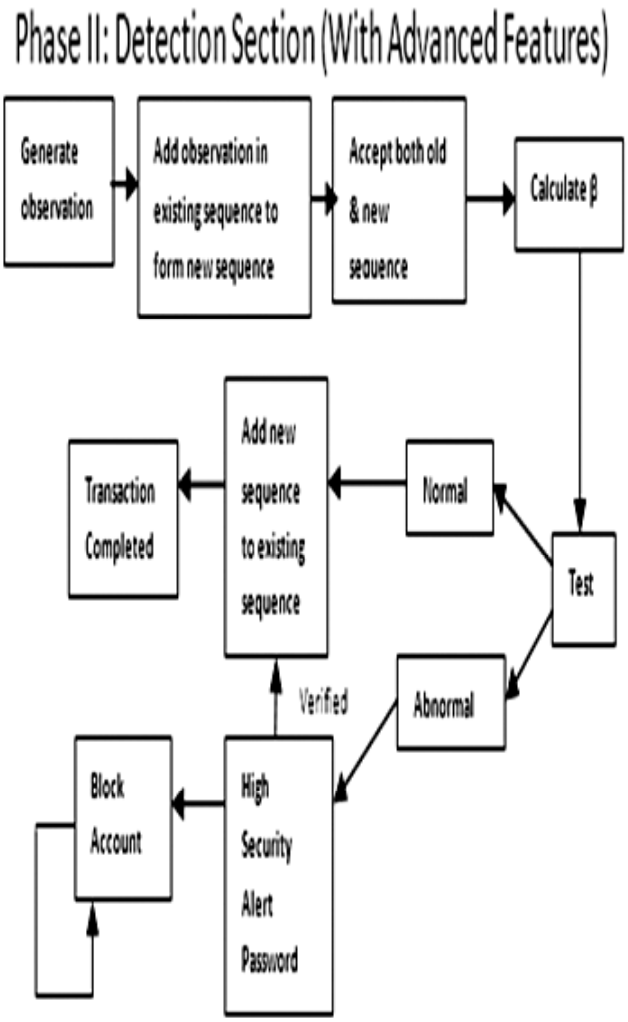


Figure 3: Proposed Model [5]

6.2. Sequence of Transaction

Every cardholder has the different habits to withdraw the money from ATM.

Scenario 1: Check the balance and withdraw the money

Scenario 2: Withdraw the money.

Scenario 3: Withdraw the money and generate the mini statement.

Like that every cardholder has their different habits of doing transaction. Such habits initially learned by proposed model in phase 1. We are considering such previous 50 transactions for training purpose.

6.3. Time Taken for Transaction

Time taken by cardholder to perform the transaction is calculated in this feature and compares this time with the previous transactions spending time. Mean of the time is calculated using the k-means clustering algorithm. This parameter is one of the major in inputs to the fraud detection system.

6.4. Amount of Transaction

In this feature the amount of previous 50 transactions is considered to train the fraud detection system in phase 1. Following are the steps to detect fraudulent activity by using the amount as a parameter as [4],

Step 1: Set of previous 50 transactions amounts will be considered.

Step 2: Do the Clustering of these transactions into 10, 15, 25 groups and find the mean of each cluster.

Step 3: Subtract mean value of each cluster from each amount of every transaction.

Step 4: pvalue will be calculated for all 50 transactions. We will get the get the set of pvalues after this step. There are three pvalues

1. pvalue[i] = 0; for low value transactions
2. Pvalue[i] = 1; for mid value transactions
3. Pvalue[i] = 2; for high value transactions

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

Step 6: Do the multiplication of each probability values which is calculated in above step, which will give us the value of *Alpha* ($\alpha 1$)

Step 7: Here the upcoming new transaction is considered. We replace this new amount with the previous amount from the set and calculate the probability values by the same mean. Repeat step 3 to 6, at the end this step will provide us the value of *Alpha* ($\alpha 2$)

Step 8: Calculation of *Beta* (β) is done into this step,

$$Beta\ (\beta) = Alpha\ (\alpha 1) - Alpha\ (\alpha 2)$$

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

The system flow of proposed advanced security model is shown in fig. 4.

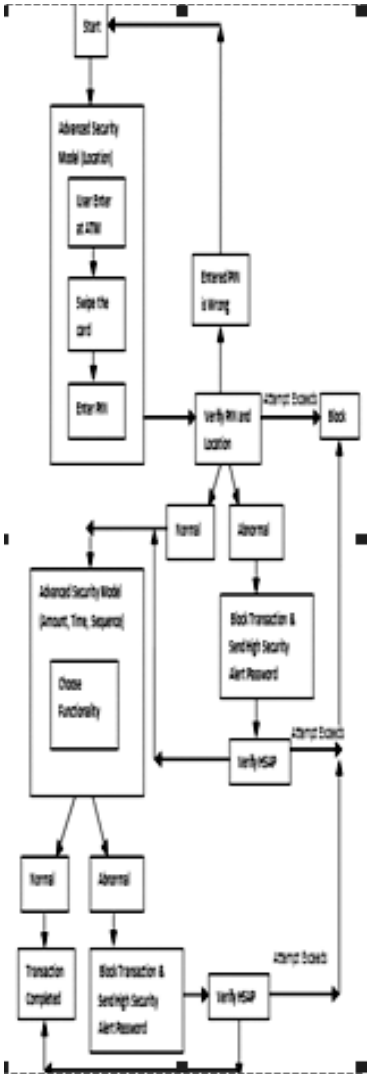


Figure 4: System Flow

7. CONCLUSION

We have reviewed various papers on ATM frauds and proposed an advanced security model which totally depends on customers spending patterns. This model includes four new input parameters which gives strong methodology for detecting the frauds in ATM transaction. The objective of this paper is to propose the methodology to detect the frauds in ATM transaction without hampering the existing system. In this it is less chances that genuine user will be treated as fraudulent, that is FP (false positive) transactions will be decreased. So this will be the major advantage of the proposed work. The proposed model is able to combines the features of detection and the prevention mechanism simultaneously. This will be more beneficial for banking industry. The paper would conclude with the advanced methodology and looking with the any new state of proposed work if any.

8. ACKNOWLEDGMENT

It's my pleasure to express sincere gratitude towards Prof. Dr. K. V. D. Kiran for guiding me throughout this research paper and providing me required resources to make this paper possible.

REFERENCES

[1] Mike Bond, Omar Choudary, Steven J. Murdoch, Sergei Skorobogatov, Ross Anderson: Chip and Skim: Cloning EMV cards with pre-play attack. IEEE Symposium on security and privacy, (2014).

[2] Mohamed Musallam Khasib AI Rawahi, Smitha Sunil Kumaran Nair: Detecting Skimming Devices in ATM through image processing. IEEE, 978-1-5090-0478-2/15, (2015).

[3] Ayhan Demiriz, Betul Ekizoglu: Using Location Aware Business Rules for Preventing Retail Banking Frauds. IEEE, 978-1-4799-7620-1/15, (2015).

[4] Prof. Vivek V. Jog, Mr. Nilesh R. Pardeshi: Advanced Security Model for Detecting Frauds in ATM Transaction. International Journal of Computer Applications (0975 –8887) Volume 95–No. 15, (2014).

[5] Abhinav Shrivastava, Amlan Kundu, Shamik Sural, Senior Member, IEEE, and Arun K. Majumdar, Senior Member: "Credit Card Fraud Detection Using Hidden Markov Model", IEEE TRANSACTION ON DEPENDABLE AND SECURE COMPUTING, VOL 5, No. 1, (2008).

[6] Divya Iyer, Arti Mohanpurkar, Sneha Janardhan et. al: "Credit Card Fraud Detection Using Hidden Markov Model", Information and Communication Technologies (WICT), 2011 World Congress on, 978-1-4673-0126-8, (2011).

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

[8] Rina Sakharova and Latifur Khan: Payment Card Fraud: Challenges and Solutions, Technical Report UTDCS3411, The University of Texas at Dallas, (2011).

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

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