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 5, May 2016

ATM Card Fraud Detection Using Hidden Markov Model

Sonawne V.D, Prashant Gupta, Afsari Raut , Farhan Saudagar

Assistant Professor, Dept. of Computer, Al-Ameen College of Engineering, Pune University, Maharashtra, India

B.E Student, Dept. of Computer, Al-Ameen College of Engineering, Pune University, Maharashtra, India

B.E Student, Dept. of Computer, Al-Ameen College of Engineering, Pune University, Maharashtra, India

B.E Student, Dept. of Computer, Al-Ameen College of Engineering, Pune University, Maharashtra, India

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 ATM 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 behaviour. This Security Model is primarily focusing on the normal spending behaviour of a cardholder and some advanced securities such as Location, Amount, Time and Sequence of transactions. If the trained Security model identifies any misbehaviour 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.

KEYWORDS: HSAP, HMM, FDS, Patterns, Transaction, Location, Fraud.

I. INTRODUCTION

1.1OVERVIEW:

Technology is all about making life more and more flexible, simple and affordable. It is all about devising a method to bridge a gap that lies between predictions to practical implementation of the ideas. In the world of computer engineering, one of the most effective methods that hold a key of success for implementations of such innovations is the algorithmic approach. This is the reason that the seed idea of this research based application has been incorporated from one such algorithm.

The model proposed in these applications is all about recognizing and understanding various transactions patterns of the user. It helps in maintaining and updating a database that will describe the operational behavior of the specified user in the form of a pattern. This model totally depends on the pattern evaluating and recognizing Forward-Backward algorithm. This research based application totally rely on the decision drawn by the computational model suggested by the algorithm there by helping to knock out the ongoing issues related to ATM transaction fraud.

Integration of the distributed security environment with such a type of application throws in additional challenge to the hackers and crackers. Thus the whole system intends to increase the complexity to next levels there by making the ATM payment frauds almost impossible.

1.2BACKGROUNDS

Existing method of ATM transaction is proving day by day vulnerable for various attacks like given below Major frauds are happening due to our very Nears and Dears …..This a growing trend in most of the cases due to sharing of secret PIN and not keeping the Debit/Credit card in safe custody.

The above statement clearly puts in a thought on the use, utility and efficacy of the ATM mode of banking. Listing cases on ATM frauds leads to huge set of existent state of affairs. Times News Network one of the biggest in

DOI: 10.15680/IJIRCCE.2016. 0405132

this nation puts a question to Developers of the technology for ATM transaction on how secure actually this network is. Some of its recent reports on frauds are:-
1) Need to check ATM frauds: High Court suggest Government [Allahabad]
Times of India,Oct 7, 2010 | by Pandey, R N
ALLAHABAD: The Allahabad High Court has observed that there is a great need to check ATM frauds as the issue is assuming alarming proportions and is constantly in news. Innocent persons are deprived of hard earned bank deposits by fraudsters who are operating in gangs and a large number of cards have even been recovered from some of those who have been arrested, remarked a division bench while dismissing a writ petition filed by an alleged accused in ATM fraud case.
2) Woman forgets ATM card in machine, loses Rs. 20,000 since she leaves the ATM house without collection her ATM card as well as without completing the transaction Kannada Daily, Mar 26, 2010.
According to the news printed in the above daily addition, Rs 20,000 cash was stolen from the account of Tarannum Desai, a resident of Makarba, Juhapura on Wednesday. The incident took place owing to Desai's negligence, said police officials. An application of complaint has been registered with Satellite police station. According to police, Desai had been to HDFC Bank ATM at FunRepublic on Wednesday. After completing her transaction, she forgot to take her ATM card and left.

"After a while, she got a message on her mobile phone that Rs 20,000 was withdrawn from her account. Shocked, she realized that she had forgotten the ATM card inside the machine while finishing the transaction in a hurry," said a police official. Investigating officials have sought CCTV footage of the ATM booth to identify the accused. "We believe it might not be a pre-planned theft. An opportunist may have used the card to withdraw money from an already-inserted card," said a senior official.

This is enough to state that existing system need some additional safety measures that will help us to bring in some check on such frauds.

An exhaustive study made in this direction revealed some facts that some applications like speech recognition system, DNA analysis are already being used effectively which uses the concepts related to pattern generation and recognition. These applications use strongly build Hidden Markov Model that intern is totally based Compound decision making theory from probability and statistics. Thus all such applications use the algorithms that adhere to concepts that finally help in making the decision based on multiple factors. HMM uses many of such like Baulm-Welch, FW-BW, Vierbi, K-Means etc.

A **hidden Markov model** (**HMM**) is a statistical model in which the system being modeled is assumed to be a Markov process with unobserved state. An HMM can be considered as the simplest dynamic Bayesian network.
In a regular Markov model, the state is directly visible to the observer, and therefore the state transition probabilities are the only parameters. In a *hidden* Markov model, the state is not directly visible, but output dependent on the state is visible. Each state has a probability distribution over the possible output tokens. Therefore the sequence of tokens generated by a HMM gives some information about the sequence of states. Note that the adjective 'hidden' refers to the state sequence through which the model passes, not to the parameters of the model; even if the model parameters are known exactly, the model is still 'hidden'. Hidden Markov models are especially known for their application in temporal pattern recognition such as speech, handwriting, gesture recognition, part-of-speech tagging, musical score following, partial discharges and bioinformatics

This study reveals that if it is possible to make compound decisions in critical domains like DNA analyses as well as speech recognition system making, then it must be still very easy to device a technique that will help us to study users spending patterns, users daily transaction habits, users normal transactions delays, which we will finally use to observe abnormal transactions. Such abnormalities can be easily traced and blocked before the transaction is committed.

II. RESEARCH METHODOLOGY TO BE EMPLOYED

- To introduce a set algorithms like Baum-Welch learning with scaling that help in generating long observation sequences
- To implement mobile based communication with integration and transmission of data in encrypted form using Bluetooth.
- To implement a code for Multivariate Gaussian distribution for observation distribution.
- To device a method for Pseudo-Random number generation and implement it.
- To device methods for implementation of algorithms like Forward-Reverse algorithm, Sequence Generator algorithm etc.
- It supports mobile comm. Over Bluetooth technology
- It support identification and authentication for mobile hardware based on Unique H/W number so called IME number .

III. LITERATURE SURVEY

In [1] AbhinavShrivastava and team proposed, “Credit Card Fraud Detection Using Hidden Markov Model”1 March 2008. They explains in that the problem with most of the previous approaches is that they require labelled 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 labelled data is not available.

In [2]AshishGupta,JagdishRaikwal, “ Fraud Detection in credit Card Transaction Using Hybrid Model” 1 Jan, 2014.They proposed survey number of technique for credit card fraud detection and basis on that we will propose a strong literature of Hybrid Markov Modelwhich is a combination of Bayesian Classifier and Hidden Markov Model, based system which will consist of the process of all the surveyed technique and result in better fraud detection than all previous proposed system of fraud detection.

In [3] Fabio Cuzzolin and Michael Spanienza , “Learning Pullback HMM Distances ”IEEE Trans, August 2013.They proposed general framework for learning distances function of generative dynamical model, given a training set of labelled videos. The optimal distances function is selected among of family of pullback ones, induced by a parameterised automorphism of the space model. They focus here on HMM models and their models spaces and design. It improves the action recognition performances with respect to base distances.

IV. PROBLEM STATEMENT

In our system, each transaction is submitted to the system for verification. Systems check whether transaction is genuine or not depending upon a behavior of the cardholder, i.e. is transaction delay, sequence of operation and spending pattern. And depending upon these parameters, computational decisions are
taken .If system find the transaction malicious it block cardholders account and transaction get failed.

V. ARCHITECTURE

In proposed system, we present a Hidden Markov Model (HMM).Which does not require fraud signatures and yet is able to detect frauds by considering a cardholder’s spending habit. Card transaction processing sequence by the stochastic process of an HMM. The details of items purchased in Individual transactions are usually not known to any Fraud Detection System(FDS) running at the bank that issues credit cards to the cardholders. Hence, we feel that HMM is an ideal choice for addressing this problem. Another important advantage of the HMM-based approach is a drastic reduction in the number of False Positives transactions identified as malicious by an FDS although they are actually genuine. An FDS runs at a credit card issuing bank. Each incoming transaction is submitted to the FDS for verification. FDS receives the card details and the value of purchase to verify, whether the transaction is genuine or not. The types of goods that are bought in that transaction are not known to the FDS. It tries to find any anomaly in the

DOI: 10.15680/IJIRCCE.2016. 0405132

transaction based on the spending profile of the cardholder, shipping address, and billing address, etc. If the FDS confirms the transaction to be of fraud, it raises an alarm, and the issuing bank declines the transaction.

In the 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 same user, in this case he is able to unblock his account through his mobile by challenge response procedure.

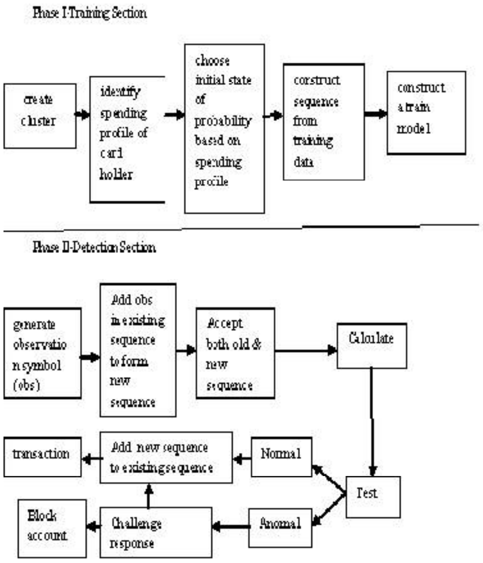

Phase I-Training Section
create cluster
identify spending profile of card holder
choose initial state of probability based on spending profile
construct sequence from training data
construct a train model
Phase II-Detection Section
generate observation symbol (obs)
Add obs in existing sequence to form new sequence
Accept both old & new sequence
Calculate
Test
Normal
Anomal
Add new sequence to existing sequence
transaction
Challenge response
Block account

Fig1.Architecture of HMM model

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

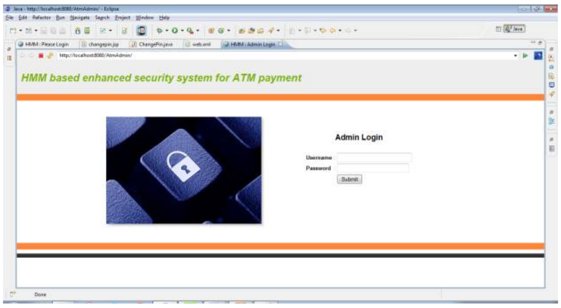
5.1.PROPOSEDOPERATIONAL PROCEDURE

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.

VI. RESULT AND DISCUSSION

1.Admin login

Admin login is performed by admin only. Admin performed function such as add user, update , block or ublock etc.


Java - http://localhost:8080/AtmAdmin/ - Eclipse
File Edit Refactor Run Navigate Search Project Window Help
Java
HMM : Please Login
changepin.jsp
ChangePin.java
web.xml
HMM : Admin Login
http://localhost:8080/AtmAdmin/
Submit
Done

HMM based enhanced security system for ATM payment

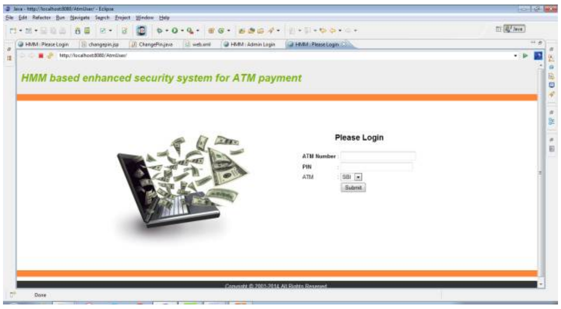
Admin Login

Username
Password

Fig2.Admin Login

2.User Login

User login is performed by only user. User performed function such as deposit and withdraw money, check balance etc.


Java - http://localhost:8080/AtmUser/ - Eclipse
File Edit Refactor Run Navigate Search Project Window Help
Java
HMM : Please Login
changepin.jsp
ChangePin.java
web.xml
HMM : Admin Login
HMM : Please Login
http://localhost:8080/AtmUser/
Submit
Done

HMM based enhanced security system for ATM payment

Please Login

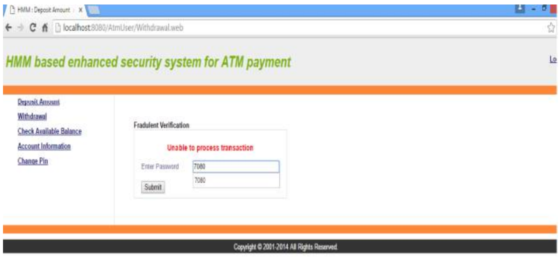
ATM Number :
PIN :
ATM : SBI

Copyright © 2001-2014 All Rights Reserved

Fig3.User login

3.Unable to transaction

When user do transaction its transaction depen upon the parameter such as location ,amount,time,pattern etc. For example if user have a limitation or hav a habbit of withdrawing monetupto 1000.If



HMM based enhanced security system for ATM payment

Fradulent Verification

Unable to process transaction

Enter Password 7080

7080

Copyright © 2001-2014 All Rights Reserved.

Fig4.Unable Transaction

suddenly or urgently he wants to withdraw money up to 20000 at that time 10 last transaction will be compare with current transaction If current transaction and last 10 transaction have a different then the otp is send to original registered mobile number.If actual is there the by entering the otp transaction become successfully otherwise unsuccessfull.

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 5, May 2016

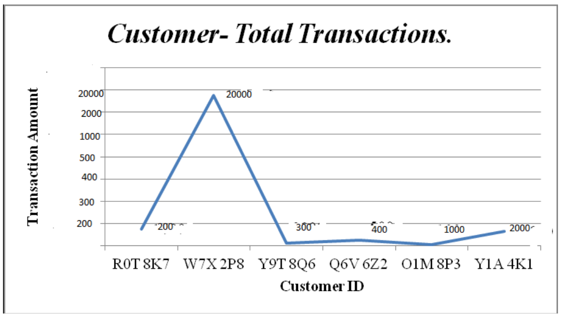


Fig5. Spending pattern for customer transactions

4. Result

The action taken by the switch node for a suspicious transaction can be configured to correspond to the desires of the issuing bank and the merchant. In still other situations, the issuing bank may want to allow the transaction but leave a voice or e-mail message or sms for the customer notifying him of a potentially suspicious transaction. It secures the transaction using OTP via sms and Detect the anomalous transaction when cardholder lost the card. The percentage calculation of each spending pattern (low, medium and high) of the card holder based on price distribution range as mentioned earlier is shown in Fig4 The ranges of transaction amount has been used as the observation symbols, whereas the types of item have been considered to be states of the HMM.

VII. ADVANTAGE

1. Avoids fraud usage of card through online transactions.
2. Detect if card used by others if card lost.

VIII. CONCLUSIONS

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 research work the project framework will provide better security as two level of encryption is done. Also authentication mechanism will help to achieve better security. Dynamic generation of the keys and dynamic rekeying will help to optimize performance. Decentralization of security with the help of inclusion of third party devices like mobile will help in making it more difficult to crack.

REFERENCES

[1]AbhinavShrivastava , “Credit Card Fraud Detection Using Hidden Markov Model”, IEEE Transaction, VOL 5 No.1, March 2008.
[2]AshishGupta,JagdishRaikwal, “Fraud Detection in credit Card Transaction Using Hybrid Model” ,International Journal of engineering and computer science ISSN-2319-7242 volume 3 issue,1 Jan, 2014.
[3]Fabio Cuzzolin and Michael Spanienza, “Learning Pullback HMM Distances”, IEEE Trans, August 2013.
[4].KhyatiChaudhary, JyotiYadavBhawnaMallick, “A review of Fraud Detection Techniques: Credit Card”, International Journal of Computer Applications, May 2012.
[5].Lean Yu Shouyang Wang, “Kin Keung Lai “Credit risk assessment with a multistage neural network ensemble learning approach”, Expert Systems with Applications, Elsevier-Feb 1, 2008.
[6]. MubeenaSyeda, Yan-Qing Zhang and Yi Pan, “Parallel Granular Neural Networks Detection for Fast Credit Card Fraud Detection”, IEEE, 2002.
[7].Purvalkharat, Ankushbhat, Rohitwattal, Yogeshkamble.“Securing Financial Transactions Using Hmm And Location Based Service”13-Apr-2015.
[8].Renu and Suman, “Analysis on Credit Card Fraud Detection Methods”, International Journal of Computer Trends and Technology, 1 Feb 2014.
[9]SamruddhiBelan, Sujata Mane, Tejas, “Fraud Detection in Online Banking Using Hidden Markov MODEL” 1 February 2014.
[10]. 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.