International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 3 Issue 10, October- 2014

Overview of Credit Card Fruad Detection using Hidden Markov Model

Avghad Sangita D
M.E, CSE
Jawaharlal Nehru Engineering College
Dr.B.A.M.University,Aurangabad,Maharashtra

Dr Joshi Madhuri S
Professor,Department of CSE
Jawaharlal Nehru Engineering College
Dr.B.A.M.University, Aurangabad, Maharashtra

***Abstract*— by just clicking a mouse or touching a screen, shoppers can buy nearly any product online -from groceries to cars, from insurance policies to home loans. The world of electronic commerce, also known as e-commerce, enables consumers to shop at thousands of online stores and pay for their purchases without leaving the comfort of home. However Credit Card Fraud is one of the biggest threats to business establishments today. In this paper, we are aim to develop Fraud detection system using HMM., we model the sequence of operations in credit card transaction processing using a Hidden Markov Model (HMM) and show how it can be used for the detection of frauds. Initially we trained HMM with the normal behavior of a cardholder. If an incoming credit card transaction is not accepted by the trained HMM with sufficiently high probability, we generate one time password, if cardholder does not get OTP within time limit ,then we ask some security Question to cardholder. Depending on answer we detect the frauds**

Keywords*— hidden markov model (HMM),one time password (otp),Fruad detection system(FDS),personal Identification Number (PIN)

I. INTRODUCTION

With the introduction of internet, shopping online has become popular. Shopping online allows access to merchandise sold worldwide. It is a growing part of retail. Online shopping is time saving and convenient. There is often no cost for traveling when ordering items online. While performing online transaction using a credit card issued by bank, the transaction may be either Online Purchase or transfer .The online purchase can be done using the credit or debit card issued by the bank. Often card based purchase can be categorized into two types Physical Card and Virtual Card.

In a physical-card based purchase, the cardholder presents his card physically to a merchant for making a payment. To carry out fraudulent transactions in this kind of purchase, an attacker has to steal the credit card. If the cardholder does not realize the loss of card, it can lead to a substantial financial loss to the credit card company. In online payment mode, attackers need only little information for doing fraudulent transaction (secure code, card number, expiration date etc.). In this purchase method, mainly transactions will be done through Internet or telephone. To commit fraud in these types of purchases, a fraudster simply needs to know the card details. Most of the time, the genuine cardholder is not aware that someone else has seen or stolen his card information

To detect fraud in this type of purchase method is to analyze cardholder's behavior and location scanning to check for unusual patterns. These patterns include user characteristics such as user spending patterns as well as usual user geographic locations to verify his identity. If any unusual pattern is detected, the system analyses user credit card data for various characteristics.

These characteristics include user country, usual spending procedures. Based upon previous data of that user the system recognizes unusual patterns in the payment procedure. Fraud detection based on the analysis of existing purchase data of cardholder is a promising way to reduce the rate of successful credit card frauds

In both the cases if the card or card details are stolen the fraudster can easily carry out fraud transactions which will result in substantial loss to card holder or bank. Hence we aim to Develop System which will capture purchasing behavior of Card holder using Hidden Markov Model.

II. RELETED WORK

In paper [1] they proposed algorithm for credit card fraud detection named as BLAH. It Comprise of BLAST and SSAHA Algorithm. These algorithms are pretty much proficient sequence aligning algorithm in detecting credit card frauds. The system named as BLAHFDS identifies fraudulent transactions using a Profile Analyzer and a Deviation Analyzer. These two analyzers use BLAH as a sequence alignment tool to detect fraud. They proposed stochastic model for the generation of synthetic transactions to analyze the performance of BLAHFDS. Performance of this system in detecting fraud is good and its accuracy is high .also processing speed is Fast but it cannot detect the duplicate transaction or clone credit card frauds. BLAST-SSAHA hybridization approach can be effectively used to counter fraud in other domains such as telecommunication

In "Credit card fraud detection: A fusion approach using Dempster–Shafer theory and Bayesian learning," Paper [2], they proposed FDS Which Merges the result obtained from present and precedent behavior. The fraud detection system (FDS) consists of four Element: rule-based filter, Dempster–Shafer adder, transaction history database and Bayesian learner. Rule-based Filter extract the doubt level of each transaction based on variation from normal form of spending patterns. , Dempster–Shafer adder, in this component ,all the transaction that are doubtful obtained by rule based filter are combine to form primary belief. in third component transaction history database ,here all values

formed as primary belief are combined to form on the whole belief. And transaction is categorized as normal, abnormal or suspicious depending on this whole Belief. If transaction is found to be suspicious; belief is r strengthened or weakened according to its similarity with fraudulent or genuine transaction history using Bayesian learning. they used stochastic models to generate synthetic transactions for analyzing the performance of the system and The simulation yielded up to 98% True Positive and less than 10% False Positive

In Paper [3] "Fuzzy Darwinian Detection of Credit Card Fraud ", They proposed the detection method for fraud Detection which uses Genetic Programming, Search Algorithm and fuzzy expert System.FDS Uses GP in order to develop some fuzzy logic rule that can be helpful in determining some fuzzy logic rules which is helpful in finding the suspicious and non suspicious classes of transaction. System using Classifier to determine transaction as either safe or suspicious, when information about transaction is provided to System. Three sets of experiments were performed and the four different setups of fuzzy rule evolver were run for each experiment. 1. Standard fuzzy logic with non-overlapping membership functions 2. Standard fuzzy logic with overlapping membership functions 3. Membership-preserving fuzzy logic with overlapping membership functions 4. Membership-preserving fuzzy logic with smooth membership functions. The best accuracy overall is achieved by standard fuzzy logic with overlapping membership functions. Detecting 100% of the "suspicious" claims for both on the training and the test set, while showing that 5.79% of false negative error, which is relatively low

In "CARDWATCH: A Neural Network Based Database Mining System for Credit Card Fraud Detection" Paper[4] ,They have Proposed "CARD WATCH" by Using Neural network Techniques : conjugate gradient, back propagation, and batch back propagation .this is useful Product For Banking system because of ease of implementation with Commercial Database. Drawback of Card Watch is the need of building a separate neural network or each card holder Account that demand a very large network and large amounts of resources.

III.SYSTEM ARCHITECURE

Overall system For Credit card Fraud Detection consists of Following Module/Phases:

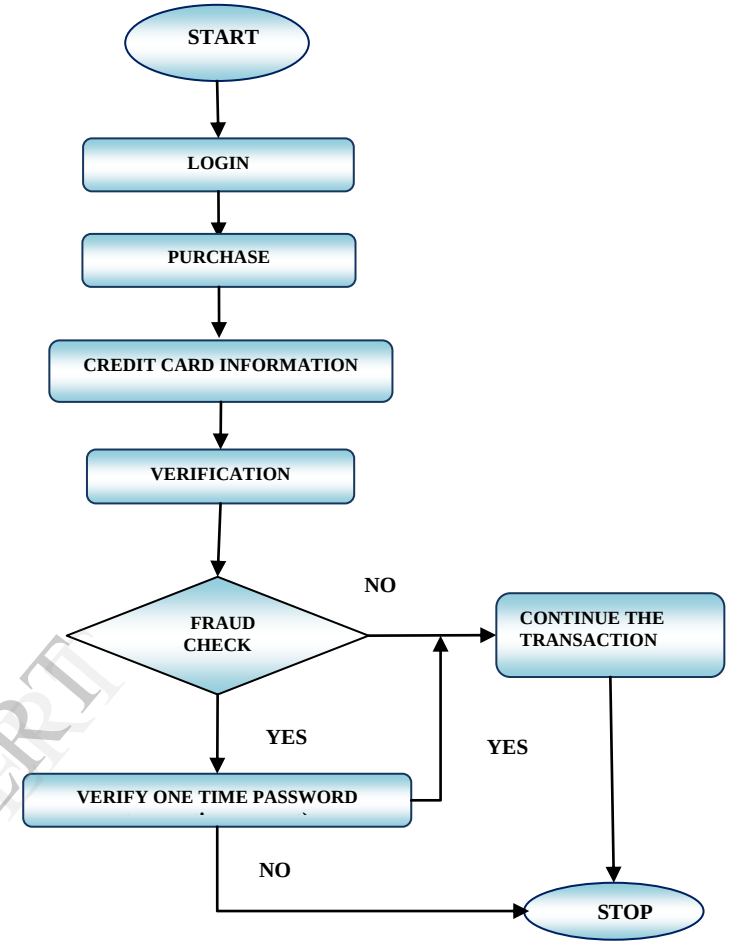
1. Online Purchase
2. Cluster Formation
3. Fraud detection
4. Send one time Password (OTP)

Module Description :

Phase1: Online Purchase

The Online Shopping system will enables vendors to set up online shops, customers to browse through the shops. It will consists of product details, security system, status and exits

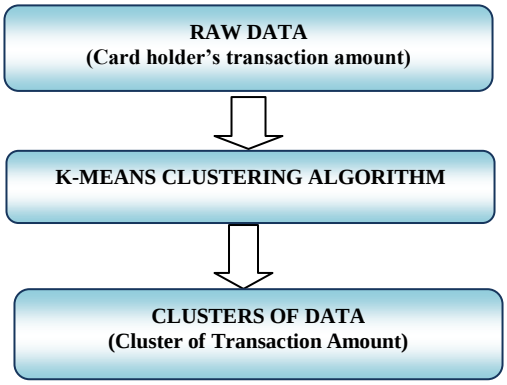
The administrator can enter the name and password and generate the report and can perform operations like Add, search, delete the products in the database. The database will maintain the product details information. Customer can view their product details. She/he can view her/his product details and buy their product. When he/she buy product, he/she will be directed to bank web site page. Here he/she authenticate fraud detection system by providing username and password. if information provided by he/she is correct then FDS system will come in action



.

Phase2: Cluster Formation

Credit Card Transaction Processing Operation will be map into HMM, by converting Transaction Amount into observation symbols. These observation symbols are configuring into three type of cluster high, low and medium. In this way we will get card holder profile based on purchasing behavior of card holder.



Phase 3: Fraud detection using Hidden Markov Model

Hidden Markov Models (HMM) are stochastic methods to model temporal and sequence data. Hidden Markov Models can be seem as finite state machines where for each sequence unit observation there is a state transition and, for each state, there is a output symbol emission .

HMM can be characterized by 5 Parameters.

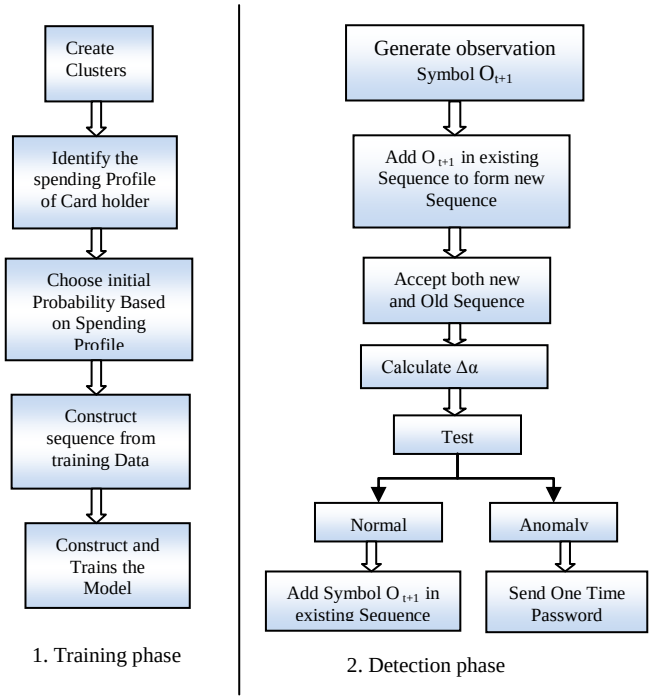
$$\lambda = (N, M, A, B, \pi)$$

1. N is the number of states in the model. We denote the set of states S = {S1; S2;..; SN} Where S_i ,i = 1,2,…N is individual state. The state at time instant I is denoted by q_t
2. M is the number of distinct observation symbols per state. The observation symbols correspond to the physical output of the system being modeled. We denote the set of symbols V = { V1 ;V2 ;...VM }, where Vi,I =1;2;...;M is an individual symbol .
3. The state transition probability matrix $A=[a_{ij}]$ where $a_{ij} = P(q_{t+1} = S \mid q_t = S_i), 1 \le i \le N, 1 \le j \le N; t=1,2,\ldots$
4. The Observation Symbol Probability matrix $B = [b_j(k)]$. Where bj (k) is the probability distribution of observation symbol k at state j.

$b_j(k) = P(V_k \mid Sj), 1 \le j \le N, 1 \le K \le M$

5. Initial state distribution $\pi = [\pi_i]$ where $\pi_1 = P(q_1 = S_j), 1 \le i \le N$.
6. The observation sequence $O = O_1, O_2, O_3, \ldots O_R$,where each observation sequence O_t one of the observation symbols from V and R is the number of observation in the sequence.

Complete specification of HMM requires the estimation of two model parameters, N and M and three Probability Distribution A, B and π. Notation $\lambda = (A,B,\pi)$ is used to indicate the Complete set of Parameter of the Model ,where A,B implicitly include N and M.



1. Training phase

2. Detection phase

Fraud Detection using Hidden Markov Model comprises Two Phases: First Training Phase and Second Detection Phase. In Training phase, we will train the Model to Cardholders Normal Behavior. And in detection phase, we try to find deviation from normal behavior of card holder. If FDS find Deviation in expected and Actual behavior then we assume as Suspicious Transaction and one time Password is send to Card holders mobile

Phase 4: One time password Generation

Passwords are the most basic forms of authentication, but they are easily guessed, frequently forgotten and expensive to maintain. Typically Static Passwords have long lifespan and are often reused for multiple applications. They are vulnerable to phishing attacks because the user can potentially be duped into entering a password into a fraudulent web site or application. A phisher can then collect the information and use it later for fraud and theft.

One time password provide Two-factor authentication and provides improved protection, since users enter something they know—a Personal Identification Number (PIN)—and something they have—the changing code on an authenticator the size of a keychain. Strong, two-factor authentication is a proven solution for security within the enterprise, but it is designed for authenticating the user to the application.

IV. CONCLUSION

In our Dissertation, we aim to develop Credit card fraud Detection System by using Hidden Markov Model. We Train the Hidden Markov Model based on overall purchasing behavior of the Cardholder. Fraud detection is a useful tool in reducing unauthorized transactions. As Model track buying habits of cardholders, it become familiar with where the cardholder shops, and how much Card holder spends on average at each merchant. In our Base Paper, they detect the

Fraud using by cluster, clustering Card holder Profile into three classes low, medium and high and then train the Hidden Markov Model normal behavior of card holder .we aim to extend this work, by sending one time password if trained model find deviation between expected and actual behavior.

ACKNOWLEDGMENT

We are thankful to all anonymous Researchers for providing their Finding, opinions and their constructive and useful comments and also thankful to all those People who contributed to Credit Card Fraud Detection and whose ideas help us for writing this Paper.

REFERENCES

1. Amlan Kundu, Suvasini Panigrahi, Shamik Sural, Senior Member, IEEE,and Arun K. Majumdar, Senior Member,IEEE "BLAST-SSAHA Hybridization for Credit Card Fraud Detection", IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 6, NO. 4, OCTOBER-DECEMBER 2009
2. Amlan Kundu, Suvasini Panigrahi, Shamik Sural and Arun K. Majumdar, "Credit card fraud detection: A fusion approach using Dempster–Shafer theory and Bayesian learning," Special Issue on Information Fusion in Computer Security, Vol. 10, Issue no 4, pp.354- 363, October 2009.
3. Peter J. Bentley, Jungwon Kim, Gil-Ho Jung and Jong-Uk Choi "Fuzzy Darwinian Detection of Credit Card Fraud". In the 14th Annual Fall Symposium of the Korean Information Processing Society; (2000). (1-4).
4. Aleskerov E., Freisleben B., and Rao B., "CARDWATCH: A Neural Network Based Database Mining System for Credit Card Fraud Detection", Proc. IEEE/IAFE: Computational Intelligence for Financial Eng., pp.:220-226, 1997.
5. Abhinav Srivastava, Amlan Kundu, Shamik Sural, Senior Member, IEEE, and Arun K. Majumdar, Senior Member, IEEE" Credit Card Fraud Detection Using Hidden Markov Model ",IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 5, NO. 1, JANUARY-MARCH 2008
6. Twinkle Patel1, Ms. Ompriya Kale2" Survey on Credit Card Fraud Detection Using Different Data Mining Techniques" *IJSRD - International Journal for Scientific Research & Development| Vol. 1, Issue 7, 2013 | ISSN (online): 2321-0613*
7. Vaibhav Gade, Sonal Chaudhari *All Saint College of Technology, Bhopal (M.P.), India."Credit Card Fruad Detection using Hidden Markov Model"* International Journal of Emerging Technology and Advanced Engineering Website: www.ijetae.com (ISSN 2250-2459, Volume 2, Issue 7, July 2012)
8. SHAILESH S. DHOK" Credit Card Fraud Detection Using Hidden Markov Model" International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-1, March 2012
9. F.N Ogwueleka "FRAUD DETECTION IN MOBILE COMMUNICATIONS NETWORKS USING USER PROFILING AND CLASSIFICATION TECHNIQUES", © 2009 Kwame Nkrumah 31 University of Science and Technology (KNUST) Journal of Science and Technology, Vol. 29, No. 3 (2009), pp 31-42
10. Alese B. K., Adewale O. S., Aderounmu G. A., Ismaila W.O., Omidiora E. O. "Investigating the Effects of Threshold in Credit CardFraud Detection System"International Journal of Engineering and Technology Volume 2 No. 7, July, 2012
11. Masoumeh Zareapoor,Seeja.K.R,M.Afshar.Alam."Analysis on Credit Card Fraud Detection Techniques: based on Certain Design Criteria",International Journal of Computer Applications (0975 – 8887) Volume 52– No.3, August 2012