CREDIT CARD FRAUD DETECTION USING IMPLICIT PASSWORD AUTHENTICATION

[1]AMITA PATIL, [2]PRATIKSHA POHARE, [3]SOPAN PATIL, [4]PRASHANT SHELAR, [5]L.A.BEWOOR

Vishwakarma Institute Of Information Technology, Kondhwa, Pune, Maharashtra, India
Email:patilamita10@yahoo.in,pohare pratiksha@gmail.com,184sopan@gmail.com

Abstract- Due to rapid advancement in the e-commerce technology online shopping is becoming favourite trend among people. Credit card is the mostly preferred payment mode for online as well as regular purchase. Along with increased use of credit cards, frauds associated with it are also increasing day by day. Objective of this paper is to introduce a system which detects fraudulent transactions. It is possible with the use of Hidden Markov Model(HMM). HMM is initially trained with the behaviour of cardholder. If an incoming transaction is not accepted by the trained HMM with sufficient probability then it may be fraudulent. To ensure that transaction is fraudulent or not we are using Implicit Password Authentication (IPAS).This will also try to ensure that genuine transactions are not rejected by properly distinguishing between genuine and fraudulent transaction.

Keywords- GUI-Graphical User Interface, HMM-Hidden Markov Model, IPAS-Implicit Password Authentication System.

I. INTRODUCTION

Today, online shopping is becoming mostly followed trend by people. As per ACNielsen study conducted in 2005 one-tenth of the world's population is shopping online. Credit card is the most popular mode of payment in online shopping. To make a payment by credit card, the cardholder has to give important information about the card like card number, security code, expiration date etc. but there are some risks and threats associated with credit card. To commit fraud, fraudster simply needs to know the credit card details mentioned above. Such frauds cause financial loss of cardholder. It also affects the business processes. In proposed system, we are detecting fraud by analyzing the spending patterns of every card and figuring out any inconsistency with respect to the usual spending pattern of the cardholder. Every cardholder spending behaviour is modelled using HMM for this purpose. As fraud detection depends on probability in which transaction matches with spending profile or behaviour which is modelled .initially, we are using implicit password Authentication technique (IPAS) which considers password as piece of information known to server .Information is implicitly embedded in an image. It helps to confirm that transaction is fraudulent or genuine.

II. EXISTING SYSTEM

Existing systems use various authentication systems like textual password, graphical password, biometric authentication system etc. Each of this system are having certain drawbacks, due to which their reliability decreases. For example in banking system textual passwords are used which can be easily hacked. We are trying to overcome this using implicit authentication.

III. PROPOSED SYSTEM

Generally frauds are detected after they happen. The cardholder come to know about the fraud after his or her financial loss Proposed system will detect fraud before it happen rather it will prevent fraud. At the same time it will take care of the thing that genuine transaction should not be rejected.

IV. HIDDEN MARKOV MODEL (HMM)

A. Background

An HMM is double embedded stochastic process. It can be used to model complicated stochastic processes. It is having a finite states governed by a set of transition probabilities. In a particular state, observation or outcome is generated according to associated probability of distribution. In recent years, Joshi and Phoba have investigated the capabilities of HMM in anomaly detection.

B. Use of HMM in Credit Card Fraud Detection

When user personal Identity number matched and account balance of user's credit card is more than the purchase amount, this fraud detection module will be activated. The main algorithm or techniques used is Hidden Markov Model (HMM) for the fraud detection. This model is beneficial in identification of frauds. At the same it also take precautions that authorized transactions won't fall in to the category of fraudulent transactions.

C. Algorithm

HMM uses clustering algorithm which works as follow: Clustering Algorithm Input-Previous 10 transactions
Output: value of alpha
Step 1. Take latest 10 transactions from database
Amounts={100,333,600,200,1000,500,900,700, 1100,400};//unsorted

M_amount = {100,200,333,400,500,600,700, 900,1000,1100};//sorted
Step 2.Cluster as 3,5,2 and find mean of each
C[0] = 211;
C[1] = 620;
C[2] = 1050;
Step 3.Subtract each mean value from each amount
V[0] = M_amount[i] – C[0];
V[1] = M_amount[i] – C[1];
V[2] = M_amount[i] – C[2];
Step 4.Calculate pvalue as for all 10 transactions
if (v[0] < v[1] && v[0] < v[2])
pvalue[i] = 0;
else if (v[1] <= v[0] && v[1] < v[2])
pvalue[i] = 1;
else
pvalue[i] = 2;
v[0] = 0; v[1] = 0; v[2] = 0;
now we have pvalue as
pvalue={0,0,0,0,1,1,1,2,2,2}
Step 5.Find probability values of low, medium, high value as
Low=(count(0)/10;
Medium=(count(1)/10;
High=(count(2)/10;
Here,
Low=4/10=0.4
Medium=3/10=0.3
High=3/10=0.3;

Step 6.
alpha1=low*medium*high
=0.4*0.3*0.3=0.036
Step 7.
Let say current amount = 1200
Now, Calculate alpha2 just replacing last amount from amounts set to current amount and calculate probability values using same mean values calculated in alpha1
Repeat from step 3 to step 6 for alpha2
So,
alpha2=0.036
Step 8.Calculate alpha
alpha= alpha1- alpha2
=0.036-0.036=0
if alpha>0 then this transaction is considered as a fraud.

V. COMPARATIVE STUDY OF AUTHENTICATION TECHNIQUES

1. Textual Password
It is simple authentication technique and having some disadvantages. If it is shorter in length, then it is easy to hack hence less secure. If it is complex and larger in length then it becomes hard to remember.
2. Biometric Authentication
It includes finger prints retina scan etc. It required hardware hence it is costly.
3. Graphical Passwords
According to Weinshall and Kirkpatrick users can remember graphical password with 90% accuracy even after one or two months [5]. Human remember images better than text. It improves security level.

3.1 .Passpoint scheme
It is a special type of graphical password. In this method some hints are provided to user. Hints are in the form of click points or hotspots .User has to click on some of the points to register the password. help users to reproduce their passwords with high accuracy. Comparative study suggests that graphical passwords are more efficient as per as security is concerned. Therefore we are making use of IPAS which is explained in point 4.

VI. IMPLICIT PASSWORD AUTHENTICATION (IPAS)

IPAS is similar to the PassPoint scheme with some finer differences. It considers password as a piece of information known the server at the time of registration. Information is implicitly embedded in an image. IPAS is immune to shoulder surfing and screen-dump attacks. Also, the authentication information is presented to the user in an implicit form that can be understood and decoded only by the legitimate end user. Traditional password based authentication scheme and Pass Point are special cases of IPAS. The strength of IPAS depends greatly on how effectively the authentication information is embedded implicitly in an image.

VII. MODULE INFORMATION

1. Client GUI: This GUI shall allow the user to log in and transact online using internet banking enabled account.
2. Client Server Interaction: A module shall be built that will allow the client application to call Servlets.
3. Client Side Item / Service Browser: A module that will allow the client to browse through all available items/services available on internet. Client can select any of these items/services and opt to buy them online.
4. Client Transaction Module: A module that will allow clients to enter their credentials authentication information and proceed with a transaction. This module also presents the client with transaction report (success / failure / etc.).
5. Card Database: A database containing account information of all clients is maintained on credit database s. The details may include card number, credit balance, etc.
7. Transaction Database: A database containing history of client's online transactions will also be maintained on database. The databases shall be maintained using Object Serialization.
8. Fraud Detection Using HMM: A module implemented using Hidden Markov Model algorithm

that will try to find out if the transaction is fraudulent or not will be implemented on system side.
9. Check user is genuine or not: send the question to user and display image related to questions answer on display and check answer.
10. Block the account: If click points are wrong for certain number of try then blocks account.
11. Server Report Generation: A module that will allow administrator to view all blocked accounts, reactivate them and change user credentials will be designed for server end.

CONCLUSION

In this paper we have suggested a technique which uses HMM and implicit password authentication system to detect the transaction is fraudulent or not. In IPAS authentication information is implicitly presented to the user. If the user "clicks" the same grid-of-interest compared with the server, the user is implicitly authenticated. No password information is exchanged between the client and the server in IPAS. The strength of IPAS lies in creating a good authentication space with a sufficiently large collection of images to avoid short repeating cycles.

REFERENCES

[1] "Global Consumer Attitude Towards On-Line Shopping,"http://www2.acnielsen.com/reports/documents/2005_cc_online shopping.pdf, Mar. 2007.
[2] Credit Card Fraud Detection using Hidden Markov Model, IEEE Transactions on Dependable and Secure Computing, VOL. 5, NO. 1, January-March 2008. By Abhinav Srivastava, Amlan Kundu, Shamik Sural, Senior Member, IEEE, and Arun K. Majumdar, Senior Member, IEEE.
[3] S. Stolfo and A.L. Prodromidis, "Agent-Based Distributed Learning Applied to Fraud Detection," Technical Report CUCS-014-99,Columbia Univ., 1999
[4] Sadiq Almuairfi, Parakash Veeraraghavan and Naveen Chilamkurti IPAS: Implicit Password Authentication System, 2011 Workshops of International Conference on Advanced Information Networking and Applications.
[5] Haichang, G., L. Xiyang, et al. (2009). "Design and Analysis of a Graphical Password Scheme", Innovative Computing, Information and Control (ICICIC), 2009 Fourth International Conference on Graphical Passwords.
[6] 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.
[7] S.S. Joshi and V.V. Phoha, "Investigating Hidden Markov Models Capabilities in Anomaly Detection," Proc. 43rd ACM Ann. Southeast Regional Conf., vol. 1, pp. 98-103, 2005.
[8] S. Stolfo and A.L. Prodromidis, "Agent-Based Distributed Learning Applied to Fraud Detection," Technical Report CUCS-014-99, Columbia Univ., 1999.

★★★