Credit Card Fraud Detection Analysis

J. Keziya Rani[#1] , S. Prem Kumar[*2], U. Ram Mohan[#3], C. Uma Shankar[*4]

[#1]*Asst.Professor, Dept.of.CST, S.K. University, Anantapur.*

[#3]*Supdt.Of.Police, Cyber Crime, Hyderabad.*

[*2]*HOD, Dept.Of.CS, G.Pullaiah Engineering College, Kurnool*

[*4]*Professor, Dept. Of OR& SQC, Rayalaseema University, Kurnool*

ABSTRACT : Computer security and certain aspects of cyber crime is beeing increasing day by day. The detailed study of the present day most commonly encountered cyber crime like Credit card fraud analysis is presented in this paper . The model reported in this paper is based on Hidden Markov Model(HMM), is a markov chain for which the state is only partially observable. In HMM model , We quantize the purchase values x into M price ranges V1; V2; . . . VM, forming the observation symbols at the issuing bank. The actual price range for each symbol is configurable based on the spending habit of individual cardholders. These price ranges can be determined dynamically by applying a clustering algorithm on the values of each cardholder's transactions, In this work, we consider only three price ranges, namely, low (l), medium (m), and high(h). Our set of observation symbols is, therefore, V ¼ fl; m; hg making M ¼ 3.

Keywords: Computer Security, Cyber Crime, Credit Card, HMM model.

INTRODUCTION

Credit-card-based purchases can be categorized into two types:

1) Physical card 2) 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 the second kind of purchase, only some important information about a card (card number, expiration date, secure code) is required to make the payment. Such purchases are normally done on the Internet or over the 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. The only way to detect this kind of fraud is to analyze the spending patterns on every card and to figure out any inconsistency with respect to the ―usual spending patterns. 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. Since humans tends to exhibit specific behaviourist profiles, every cardholder can be represented by a set of patterns containing information about the typical purchase category, the time since the last purchase, the amount of money spent, etc. Deviation from such patterns is a potential threat to the system.

The "Credit Card Fraud Detection" is an application that allows the software to enrol the details of an individual user who applied for credit card. The user details are done by the admin. He plays a major role in an organization. This helps the credit card users to buy their shares using online through payment gateway by which we can observe the spending patterns of each and every individual. By observing the spending patterns of each and every individual we can overcome the fraud transactions. To detect and block from fraud transactions using a credit card, and to built a detection system, which is trained on a large sample of labelled credit card account transactions. These transactions contain example fraud cases due to lost cards, stolen cards, application fraud, counterfeit fraud, mail-order fraud, and non received issue fraud. The model reported in this section is based on Hidden Markov model is a Markov chain for which the state is only partially observable. In other words, observations are related to the state of the system, but they are typically insufficient to precisely determine the state. Using the concept the analysis part is carried out in subsequent section of the paper.

A credit cardholder makes different kinds of purchases of different amounts over a period of time. One possibility is to consider the sequence of transaction amounts and look for deviations in them. However, the sequence of types of purchase is more stable compared to the sequence of transaction amounts. The reason is that, a cardholder makes purchases depending on his need for procuring different types of items over a period of time. This, in turn, generates a sequence of transaction amounts. Each individual transaction amount usually depends on the corresponding type of purchase. Hence, we consider the transition in the type of purchase as state transition in our model. The type of each purchase is linked to the line of business of the corresponding merchant. This information about the merchant's line of business is not known to the issuing bank running the FDS. Thus, the type of purchase of the cardholder is hidden from the FDS. The set of all possible types of purchase and, equivalently, the set of all possible lines of business of merchants forms the set of hidden states of the HMM. It should be noted at this stage that the line of business of the merchant is

known to the acquiring bank, since this information is furnished at the time of registration of a merchant. Also, some merchants may be dealing in various types of commodities (For example, Wal-Mart, K-Mart, or Target sells tens of thousands of different items). Such types of line of business are considered as Miscellaneous, and we do not attempt to determine the actual types of items purchased in these transactions. Any assumption about availability of this information with the issuing bank and, hence, with the FDS, is not practical and, therefore, would not have been valid.

REQIREMENT ANALYSIS:

The main aim at this stage is to assess what kind of a system would be suitable for a problem and how to build it. The requirements of this system can be defined by going through the existing system and its problems. They discussing (speak) about the new system to be built and their expectations from it.

PROBLEM RECOGNITION:

The main problem here is the storing of information and the data of a customer who purchased the items. A comprehensive solution has to be developed which will facilities to storing and retrieving the data in a faster and more efficient way.

EVALUATION AND SYNTHESIS:

The system has to be designed only after complete evaluation of the existing one. In the proposed system the information several aspects and storing the recruitments data is very effective and convenient. So this has to be used such that there is no waste of time.

SPECIFICATION:

The specifications from the user had to be taken. The appearance of forms, and their field names, the different screens he desired, the stages of this database etc., were all given. The system has been built following all the specifications.

EXISTING SYSTEM AND ITS PROBLEMS:

In case of the existing system the fraud is detected after the fraud is done i.e., the fraud is detected after the complaint of the card holder. And so the card holder faced a lot of trouble before the investigation finish. And also as all the transaction is maintained in a log, we need to maintain a huge data. And also now a-days lot of online purchase are made so we don't know the person how is using the card online, we just capture the IP address for verification purpose. So there need a help from the cyber crime to investigate the fraud. To avoid the entire above problems we propose the system to detect the fraud in a best and easy way.

MODULE DESCRIPTION:

To develop the proposed model the following modules is designed,

A. NEW CARD: In this module, the customer gives the information to enrol a new card. The information is all about their contact details. They can create their own login and password for their future use of the card.

B. LOGIN: In Login Form module presents site visitors with a form with username and password fields. If the user enters a valid username/password combination they will be granted access to additional resources on website. Which additional resources they will have access to can be configured separately.

C. SECURITY INFORMATION: In Security information module it will get the information detail and its store's in database. If the card lost then the Security information module form arise. It has a set of question where the user has to answer the correctly to move to the transaction section. It contain informational privacy and informational self-determination are addressed squarely by the invention affording persons and entities a trusted means to user, secure, search, process, and exchange personal and/or confidential information.

D. TRANSACTION: The method and apparatus for pre-authorizing transactions includes providing a communications device to a vendor and a credit card owner. The credit card owner initiates a credit card transaction by communicating to a credit card number, and storing therein, a distinguishing piece of information that characterizes a specific transaction to be made by an authorized user of the credit card at a later time. The information is accepted as "network data" in the data base only if a correct personal identification code (PIC) is used with the communication. The "network data" will serve to later authorize that specific transaction. The credit card owner or other authorized user can then only make that specific transaction with the credit card. Because the transaction is pre-authorized, the vendor does not need to see or transmit a PIC.

E. VERIFICATION: Verification information is provided with respect to a transaction between an initiating party and a verification-seeking party, the verification information being given by a third, verifying party, based on confidential information in the possession of the initiating Party. In verification the process will seek card number and if the card number is correct the relevant process will be executed. If the number is wrong, mail will be sent to the user saying the no card has been blocked and he can't do the further transaction.

To build or modify database , the design structure of the sample work tables herein presented.

TABLES:

ACCOUNT:

NAME	DATATYPE	SIZE
CardNo	NOTNULL VARCHAR	16
Holder Name	NOTNULL VARCHAR	50
Holder Address	NOTNULL VARCHAR	100
ACNO	NOTNULL VARCHAR	25
Bank Name	NOTNULL VARCHAR	50
PlaceofTransaction	NOTNULL VARCHAR	50
PlaceID	NOTNULL int	
Amount*	NOTNULL int	
DateTime	NOTNULL VARCHAR	50

CARD:

NAME	DATATYPE	SIZE
Card No	PK,NOTNULL VARCHAR	16
Credit Limit	NULL int	
Holder Name	NULL VARCHAR	50
Holder Address	NULL VARCHAR	100
Bank Name	NULL VARCHAR	50
ACNO	NULL VARCHAR	25

Fraud:

NAME	DATATYPE	SIZE
Card No	NULL VARCHAR	16
Holder Name	NULL VARCHAR	50
Holder Address	NULL VARCHAR	100
AC NO	NULL VARCHAR	25
Bank Name	NULL VARCHAR	50
PlaceofTransaction	NOTNULL VARCHAR	50
PlaceID	NOTNULL int	
Amount	NOTNULL int	
DateTime	NOTNULL VARCHAR	50

LOGIN:

NAME	DATATYPE	SIZE
Uname	PK,NOTNULL VARCHAR	25
pwd	NOTNULL VARCHAR	25
Roll	NULL VARCHAR	5
Uid	NULL int	

PRODUCT INFO:

NAME	DATATYPE	SIZE
pName	NULL VARCHAR	100
pRate	NULL FLOAT	

PRODUCT LIST:

NAME	DATATYPE	SIZE
ProId	NULL int	
pName	NULL VARCHAR	100
pRate	NULL FLOAT	
pQty	NULL int	
pTotal	NULL FLOAT	

SECURITY:

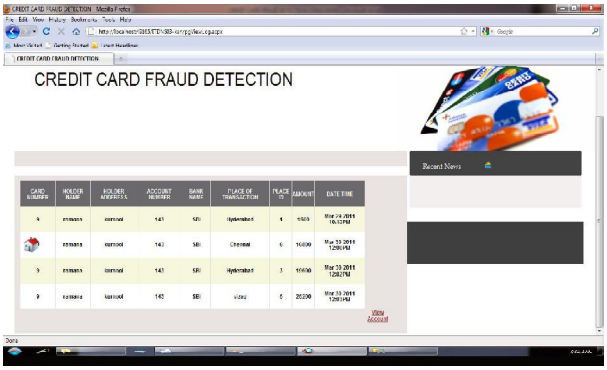
NAME	DATATYPE	SIZE
Uid	NULL int	
SecQues1	NULL VARCHAR	50
SecAnswer1	NULL VARCHAR	50
SecQues2	NULL VARCHAR	50
SecAnswer2	NULL VARCHAR	50
SecQues3	NULL VARCHAR	50
SecAnswer3	NULL VARCHAR	50
SecQues4	NULL VARCHAR	50
SecAnswer4	NULL VARCHAR	50
SecQues5	NULL VARCHAR	50
SecAnswer5	NULL VARCHAR	50
Email	NULL VARCHAR	25
DOB	NULL VARCHAR	50
Gender	NULL VARCHAR	6

USERINFO:

NAME	DATATYPE	SIZE
FirstName	NULL VARCHAR	25
LastName	NULL VARCHAR	25
Uid	PK NOTNULL int	
UName	NOTNULL VARCHAR	25
pwd	NOTNULL VARCHAR	25
Email	NULL VARCHAR	25
DOB	NULL VARCHAR	50
Gender	NULL VARCHAR	6
Address1	NULL VARCHAR	50
Address2	NULL VARCHAR	50
City	NULL VARCHAR	25
State	NULL VARCHAR	25
Country	NULL VARCHAR	
pincode	NULL int	

Phone	NULL VARCHAR	50
CardNo	NULL VARCHAR	16

View Log



CONCLUSION:

By using credit card fraud detection system, the users who have their own credit cards can perform their transactions securely and safely without a chance of fraud. The different steps in credit card transaction processing are represented as the underlying stochastic process of an HMM. we have used the ranges of transaction amount as the observation symbols, whereas the types of item have been considered to be states of the HMM.

We have suggested a method for finding the spending profile of cardholders, as well as application of this knowledge in deciding the value of observation symbols and initial estimate of the model parameters. It has also been explained how the HMM can detect whether an incoming transaction is fraudulent or not.

The maintenance of the user details is made efficient, as all the records are stored in the database, through which data can be retrieved easily. The navigation control is provided in all the forms to navigate through the large amount of records. The editing is also made simpler. Each and every individual can perform their updates and modifications to his/her own profile.

REFERENCES:

Association rules applied to credit card fraud detection Original Research Article Expert Systems with Applications, Volume 36, Issue 2, Part 2, March 2009, Pages 3630-3640

Ekrem Duman, M. Hamdi Ozcelik Detecting credit card fraud by genetic algorithm and scatter search Original Research Article Expert Systems with Applications, Volume 38, Issue 10, 15 September 2011, Pages 13057-13063

Subagging for credit scoring models Original Research Article European Journal of Operational Research, Volume 201, Issue 2, 1 March 2010, Pages 490-499Giuseppe Paleologo, André Elisseeff, Gianluca Antonini

The comparisons of data mining techniques for the predictive accuracy of probability of default of credit card clients Original Research Article Expert Systems with Applications, Volume 36, Issue 2, Part 1, March 2009, Pages 2473-2480 I-Cheng Yeh

Fraud Detection Handbook of Statistical Analysis and Data Mining Applications, 2009, Pages 347-361
Robert Nisbet, John Elder, Gary Miner