IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 17, Issue 2, Ver. 1 (Mar – Apr. 2015), PP 61-64
www.iosrjournals.org

Analysis of Spending Pattern on Credit Card Fraud Detection

Capt. Dr. S Santhosh Baboo[1], N Preetha [2]
[1] *Associate Professor,* [2] *Research Scholar*
[1,2]*Department of Computer Science and Applications*
[1] *D.G.Vaishnav College, Arumbakkam, Chennai,*
[2]*PhD Research Scholar SCSVMV University, Enathur, Kancheepuram*

Abstract: *Credit card is one of the convenient way of payment in online shopping. In this on line shopping, payment is made by giving information like card no, security code , expiration date of the Credit card etc . To rectify the risk factors of using the credit card, every card holder's spending method is modeled by using HMM. By using this authenticated security check the information of transaction is fraudulent or genuine. It is highly secured from unauthorized anomalous user using credit card and avoids fraud usage of card through online transactions.*

Keywords: *HMM, FDS, TP, FP*

I. Introduction

Now a days, credit card frauds have been rampantly increased, while making e-payments made for the purchased goods or service provided on internet. These frauds are happening in two types of purchase using the credit cards. 1) Physical card 2) Virtual card. In this first type of physical card purchase, the purchaser has to provide the card to a merchant and make payment. In this type , the credit card fraudulent is happened by stealing the credit card. If the card holder is unaware of this, the credit card company has to face the financial loss and in the second type of virtual card purchase, the card holder, has to provide the secret details of the card (like security code, card no, expiration date etc.) either thru internet or over phone . Without knowing the consequences, the genuine card holder is providing the information to the fraudsters. The result is that they loss their money also. To detect this type of criminal activity , the spending patterns of the card holder is analyzed .

To discover & prevent this type fraudulent activities, some intelligent & effective methods has been provided by the data mining, machine learning & statistics areas. In these data mining, the cyber credit card fraud has been detected by using artificial intelligence and algorithms techniques, which analyses the usage of unusual patterns derived from the data given. In this method, it is detected whether the transaction is legitimate or illegitimate.

II. Related Work

Ghosh and Reilly [1] have proposed credit card fraud detection with a neural network. They have built detection system, which is trained on a large sample of labeled 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 (NRI) fraud. Stolfo et al [2] suggest a credit card fraud detection system (FDS) using meta-learning techniques to learn models of fraudulent credit card transactions. Meta learning is a general strategy that provides a means for combining and integrating a number of separately built classifiers or models. The same group has also worked on a cost-based model for fraud and intrusion detection [3]. They use Java agents for Meta-learning (JAM), which is a distributed data mining system for credit card fraud detection. A number of important performance metrics like TP-FP (True Positive – False Positive) spread and accuracy have been defined by them.

Aleskerov et al. [4] present CARDWATCH, database mining system used for credit card fraud detection. The system, based on a neural learning module, provides an interface to a variety of commercial databases. Fan et al. [5] suggest the application of distributed data mining in credit card fraud detection. Braise et al. Stolfo use an agent-based approach with distributed learning for detecting frauds in credit card transactions. It is based on artificial intelligence and combines inductive learning algorithms and metal earning methods for achieving higher accuracy.

Phua et al. [6] suggest the use of met classifier similar to in fraud detection problems. Recognizing this problem, the switching-service provider decided to provide a capability to the issuing banks to flag in real-time those transactions that appeared to be suspicious, and possibly fraudulent. In this way, at the bank's option, suspicious or fraudulent transactions were identified and rejected much earlier and faster than previously possible.

III. Proposed Work

This work focusing on an application which is used to detect the fraudulent credit card activities on internet transaction. In this peculiar type, the pattern of current fraudulent usage of the credit card has been analyzed with the previous transactions, by using the neural networks in algorithm of data mining.

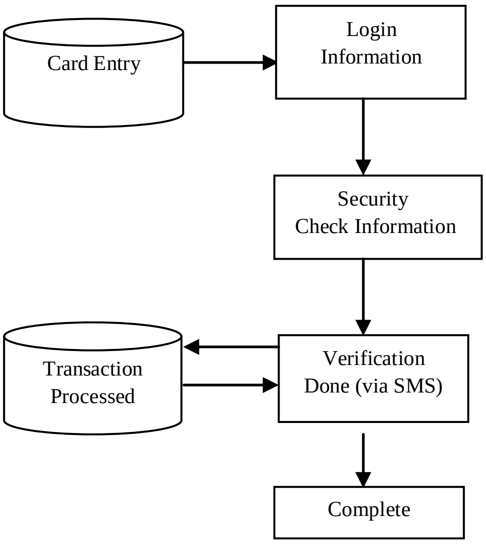

Figure.1 Proposed Architecture for investigation of credit card.

A. Credit card Fraud Detection using HMM.

To find out the fraudulent transactions, Hidden Markov model is used by detecting and analyzing the spending profile of the credit card user. generally the profile is being divided into three types a) lower profile b) middle profile c) higher profile . as every card holder has a different method of spending profile, This can easily find out fraudulent one by keeping the in consistent record of the usage of the card. Even though this cannot find out the number of purchased items & its categories, This identifies the fraudulent transaction easily by analyzing the spending patterns of the card user. in this the last twenty transactions of card holder can be easily studied & can identify which one is a fraudulent one (i.e.) the amount, the time of transaction etc. It can be easily noted via the shadow based replication engine.

The ultimate goal of this analysis is to give a note about the fraudulent transaction, to the issuing bank and also to the merchant and to take appropriate action by the issuing bank. A critical problem faced by the issuing banks is that of fraudulent transactions. This problem has, of course, exploded with the high speed nature of electronic submission of credit and debit transactions. An ATM or POS transaction may be fraudulent, for instance, if the credit card is stolen. Online purchases may be fraudulent if the credit card number, expiration date, and CID number are copied from the card. This copying can easily be done, for example, by a waiter taking a customer's credit card to pay for a meal or when a phone order is placed and paid for with a credit card. Identifying fraudulent transactions typically takes hours or days, and many such transactions may slip through before a hold can be put on the card. Worse, because the information can be quickly shared with thieves in multiple countries, they can rapidly attack via multiple avenues by submitting many different types of transactions simultaneously, anticipating that the lesser (slower, etc) infrastructure that some of them may take will allow at least some of them to get through successfully.

The fraud detection system flags a suspicious transaction with a severity flag and writes this information to another log. Periodically, the log is sent to the bank's authorization system, which takes appropriate action on the card. A credit hold might be placed on the card so that all further transactions will be rejected until the issue is researched or until the problem is resolved. Alternatively, upon the next attempted transaction, the merchant might be informed to ask the customer to call the bank in order to authorize the transaction.

This method is still generally the primary fraud detection procedure in use today. The problem with this method is that it typically takes hours or even days to flag a card that is perhaps being used fraudulently. During this time, the bank can experience significant losses as additional fraudulent transactions are made. In general, the bank is responsible for such transactions and purchases made by the customers based on the price ranges that can be determined dynamically by applying a clustering algorithm on the values of each cardholder's transactions, as shown in Table 1

B. Investigation made on Customer Transaction.

Cust_ID	Frequency of Card Usage	Average Amount
R0T 8K7	5	3000
W7X 2P8	3	45000
Y9T 8Q6	1	2000
Q6V 6Z2	5	1000
O1M 8P3	4	250
Y1A 4K1	2	6500

Table 1. Customer Monthly Transaction

Consider three price ranges namely, low (l), medium (m), and high (h)]. Our set of observation symbols for example, let l= (0, 10000), m = (10000, 50000), and h= (50000 to credit card limit). If a cardholder performs a transaction of ₹15000, then the corresponding observation symbol is m.

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, 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. The authentication code will be send to the registered mobile number of the user, every time the user tries to purchase. 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. A card transaction is captured by such devices as a point-of-sale (POS) terminal in a store, a customer's browser communicating with a website, or an ATM. The information concerning the request must be rapidly gathered from the servicing network to which the devices are connected, sent to the issuing bank for authorization/approval, and the response rapidly returned in order for the system to complete the transaction. Highly Secured from unauthorized anomalous user using credit card and avoids fraud usage of card through online transactions.

IV. Results And Discussion

The transaction-switching service provider realized that there was an opportunity to provide a unique and important service to the issuing banks. If it could detect suspicious or fraudulent activity in real-time, it could stop fraudulent transactions at the retail counter or at the ATM much sooner, or in some cases, even before they were authorized. This service would be a value-added service that would distinguish it from other ATM/POS switching networks. To implement this system, the switching provider installed multiple high-performance servers that could quickly analyze transactions on-the-fly to determine if they were suspicious. The selected servers were large Sun Solaris servers running Oracle databases. Each server comprised eight quad-core CPUs. Each data centre is provided with its own fraud detection complex; comprising multiple Sun Solaris/Oracle servers (the cards/accounts are assigned to particular Sun Solaris/Oracle servers at a site in order to partition the work load). The fraud detection complex is easily scalable to handle additional load by adding additional servers and reassigning the accounts/cards accordingly. Fraud detection will be checked on last 20 transactions and also calculate percentage of each spending profile (low, medium and high) based on total number of transactions. In Table 2, list of all transactions are shown.

Cust_ID	No. of Transaction	Transaction Amount
R0T 8K7	5	$15x10^3$
W7X 2P8	3	$135x10^3$
Y9T 8Q6	1	$2x10^3$
Q6V 6Z2	5	$5x10^3$
O1M 8P3	4	$1x10^3$
Y1A 4K1	2	$13x10^3$

Table2. List of transactions.

The most recent transaction is placed at the first position. The pattern of spending profile of the card holder is shown in (Figure 2) based on all transactions done. In this new approach, when a transaction is received by a switch node, it is sent not only to the issuing bank for authorization, but it is also replicated in real-time to a fraud detection server via a Shadow base replication engine. Shadow base engine routes the transaction to the particular fraud detection server that is monitoring that card or account. Transaction distribution by card number or account is accomplished via routing rules configured into the Shadow base replication engine.

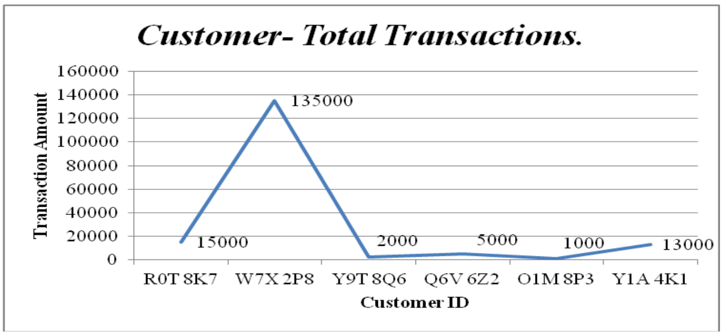

Figure 2: Spending pattern for customer transactions.

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 Figure 3

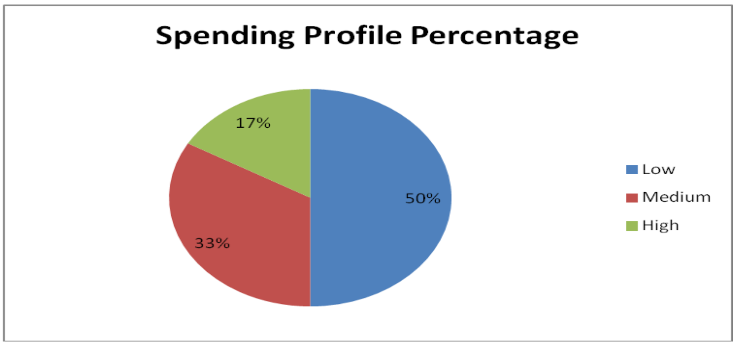

Figure 3: Percentage of Spending Profile 1

It has been noticed that low spending profile has maximum percentage of 50, followed by medium profile 33% and then 17% of high spending profile as per details of transactions in Table 2.

V. Conclusion And Future Work

The proposed solution for credit card fraud detection using HMM has different steps in credit card transaction processing are represented as the under-lying a statistical process involving a number of random variables depending on a variable parameter of an HMM and it secure the transaction using OTP via sms. It Detect the anomalous transaction when cardholder lost the card. 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. It has also been explained how the HMM can detect whether an incoming transaction is fraudulent or not. Experimental results show the performance and effectiveness of the spending profile of the cardholders. The system is also scalable for handling large volumes of transactions. In Future thumb impression or face recognition can also be implemented while using credit card in purchases.

References

[1]. Ghosh, S., and Reilly, D.L., 1994. Credit Card Fraud Detection with a Neural-Network, 27th Hawaii International l Conference on Information Systems, vol. 3 (2003), pp. 621- 630.

[2]. Stolfo, S. J., Fan, D. W., Lee, W., Prodromidis, A., and Chan, P. K., 2000.Cost-Based Modeling for Fraud and Intrusion Detection: Results from the JAM Project, Proceedings of DARPA Information Survivability Conference and Exposition, vol. 2 (2000), pp. 130-144

[3]. R. Brause, T. Langsdorf, and M. Hepp, "Neural Data Mining for CreditCard Fraud Detection," roc. IEEE Int'l Conf. Tools with ArtificialIntelligence, pp. 103-106, 1999.

[4]. Aleskerov, E., Freisleben, B., and Rao, B., 1997. CARDWATCH: ANeural Network Based Database Mining System for Credit Card FraudDetection, Proceedings of IEEE/IAFE: Computational Intelligence forFinancial Eng. (1997), pp. 220-226.

[5]. W. Fan, A.L. Prodromidis, and S.J. Stolfo, "Distributed Data Mining inCredit Card Fraud Detection," IEEE Intelligent Systems, vol. 14, no. 6,pp. 67-74, 1999.

[6]. C. Phua, D. Alahakoon, and V. Lee, "Minority Report in FraudDetection: Classification of Skewed Data," ACM SIGKDD ExplorationsNewsletter, vol. 6, no. 1, pp. 50-59, 2004.