Online Credit Card Transaction Fraud Detection Using Hidden Markov Model

Miss. Reema S. Rachh[1]; Miss. Usha D. Tikale[2] & Mr. Ansar I. Sheikh[3]

[1]Miss.Reema S. Rachh: Computer Science & Engineering.
[2]Miss. Usha D. Tikale: Computer Science & Engineering.
[3]Mr. Ansar I. Sheikh: Assistant Professor, Dept. of Computers Science & Engineering.

Abstract:

Online transactions through Online cards has more increased. As Online card becomes the most popular mode of payment for both online and offline, cases of fraud associated with it are also rising. In this paper, we model the sequence of operations in Online card transaction processing using a Hidden Markov Model (HMM) and show how it can be used to the detection of frauds. An HMM is initially trained with the normal behavior of a cardholder. If an incoming Online card transaction is not accepted by the trained HMM with sufficiently high probability, it is considered to be fraudulent. At the same time, we will attempt to guarantee that fraud transactions are rejected. We will present detail experimental results to show of our approach and will compare it with other techniques available in the literature

Keywords: Internet; online shopping; credit card; e-commerce security fraud detection; Hidden Markov Model.

1. Introduction:

Online-card-based purchases can be categorized into two types: 1) physical card and 2) virtual card. In a physical-card, the cardholder can purchase of any item through offline . To carry out fraudulent transactions in this kind of purchase, an attacker has to steal the card. If the cardholder does not realize the loss of card, it can lead to a substantial financial loss to the Issuing card company. In the second kind of purchase, only some important information about a card is required to make the payment. Some item the can buy through internet or telephone. To commit fraud in these types of buy, a fraudster simply needs to know the card details. Most of the time, the actual user is not aware that someone else has seen his card information. The only way to detect this kind of fraud is to analyze the spending habit on every card and to figure out any inconsistency with respect to the “common” spending patterns. Fraud detection based on the analysis of existing purchase data of user is a promising way to reduce the rate of successful Online card frauds. Since humans tend to exhibit specific behavior profiles, every user can be represented by a set of patterns containing information about the typical purchase category, the time since the last buy, the amount of money spent, etc. Deviation from such patterns is a potential threat to the system.

2. Literature Survey:

Credit card fraud detection has drawn a group of analysis interest and a number of methods, with special importance on neural networks, data mining and distributed data mining have been suggested. Ghosh and Reilly [1] have proposed credit card fraud detection with a neural network. They have built a detection system, which is trained on a large test 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 nonreceived issue (NRI) fraud. Recently, Syeda et al. [2] have used parallel granular neural networks (PGNNs) for improving the speed of data mining and knowledge discovery method in credit card fraud detection. A complete system has been implemented for this purpose. Stolfo et al. [3] advise a credit card fraud detection system (FDS) using metalearning method to learn models of fraudulent credit card transactions. Metalearning is a general strategy that get a means for combining and integrating a number of separately built classifiers or models. A metaclassifier is thus trained on the correlation of the predictions of the base classifiers. The similar group has also worked on a cost-based display for fraud and intrusion detection. They use Java agents for Metalearning (JAM), which is a distributed data mining system for credit card fraud detection. A number of important act as metrics like True Positive—False Positive (TP-FP) spread and accuracy have been defined by them. Aleskerov et al. [4] present CARDWATCH, a database mining system used for credit card fraud detection.

The system, based on a neural learning module, put an interface to a variety of commercial databases. Kim and Ki [5] have identified skewed distribution of data and mix of legitimate and fraudulent transactions as the two main reasons for the complexity of credit card fraud detection. Based on this investigation, they use fraud density of real transaction data as a confidence value and create the weighted fraud score to decrease the number of misdetections. Fan et al. [6] suggest the application of divided data mining in credit card fraud detection. Brause et al. [7] have developed an approach that involves advanced data mining methods and neural network algorithms to obtain high fraud coverage. Chiu and Tsai [8] have proposed Web services and data mining method to create a collaborative scheme for fraud detection in the banking industry. With this scheme, participating banks share knowledge about the fraud patterns in a heterogeneous and distributed environment. To create a smooth channel of data exchange, Web services techniques such as XML, SOAP, and WSDL are used. Phua et al. [9] have complete an extensive survey of existing data-mining-based FDSs and published a comprehensive report. Prodromidis and Stolfo transaction with the credit card. Since the transaction is pre-authorized, the vendor does not need to see or transmit an accurate individual recognition code.

3. Problem Definition:

- Offline payment does require physical card.
- Anyone who knows the detail card can make fraud detection.
- Currently user comes to know only after the fraud transaction is carried out.
- No mechanism to track the fraud transaction.

4. Existing System:

In existing system the fraud is detected after the fraud has been done that is, the fraud is detected after the complaint of the user. And so the user faced a lot of trouble before the investigation finish. And also the log which is maintained, we need to maintain a huge amount of data. And also now a days lot of online purchase are made so we don't know the user how is using the card online, we just capture the IP address for verification purpose. So there need a help from the online crime to investigate the fraud. To avoid the entire above disadvantage we propose the system to detect the fraud in a best and easy way.

5. Proposed System:

In this proposed system, we present a Hidden Markov Model (HMM).Which does not require fraud signatures and still is able to detect frauds by considering a user's spending habit. The details of items purchased in Individual transactions are normally not known to any Fraud Detection System(FDS) running at the bank that issues Credit cards to the cardholder. Hence, we feel that HMM is an perfect select for addressing this problem. Another important advantage of the HMM-based approach is a totally reduction in the number of False Positive transactions identified as malicious by an FDS although they are actually genuine. An FDS runs at a card issuing bank. Each incoming transaction is submitted to the FDS for verification. FDS is collect the card details and the value of buy to verify, whether the transaction is actual or not. The types of items that are purchase in that transaction are not known to the FDS. It tries to find any anomaly in the transaction based on the spending habit of the cardholder, shipping address, and billing address, etc. If the FDS confirms the transaction to be of fraud, it boosts an alarm, and the issuing bank reject the transaction.

6. Module Description:

New card:

When registration of new card user has to provide their details . The information is all about their contact details. If user have to generate their own user id and password for their future use of the credit card.

Login:

User fills their own username and password in the login module. If the user enters a valid username and password they will be permit to access another module.

Security information:

In Security information module it will provide the questions and its save's in database. If the card lost then the Security questions is arise. It has a set of question where the cardholder has to answer the correctly to move to the transaction section. It have security question and informational self-determination are addressed squarely by the invention affording users and entities a trusted means to cardholder, protected, investigate, process, and exchange private/secret information.

Transaction:

The technique and gadget for pre-authorizing transactions includes get a communications gadget to a vendor and a Online cardholder . The Online card owner initiates a Online card transaction by communicating to a Online card number, and storing therein, a different piece of information that characterizes a particular transaction to be made by an actual cardholder of the Online card at a later time. The information is accepted as "network data" in the database only if a correct private recognization code (PRC) is used with the communication. The "network data" will serve to later actual that particular transaction. The Online card owner or other authorized user can then only make that specific transaction with the Online card. Because the transaction is pre-authorized, the vendor does not need to see or transmit a PRC.

Verification:

Verification information is get with respect to a transaction between an starting party and a verification-seeking party, the authentication details being given by a third, verifying party, based on secret information in the control of the starting party. In verification the process will search card number and if the card number is correct the next process will be executed. If the card number is wrong, mail will be sent, card has been block and that user can't do the further transaction.

7. Module Diagram:

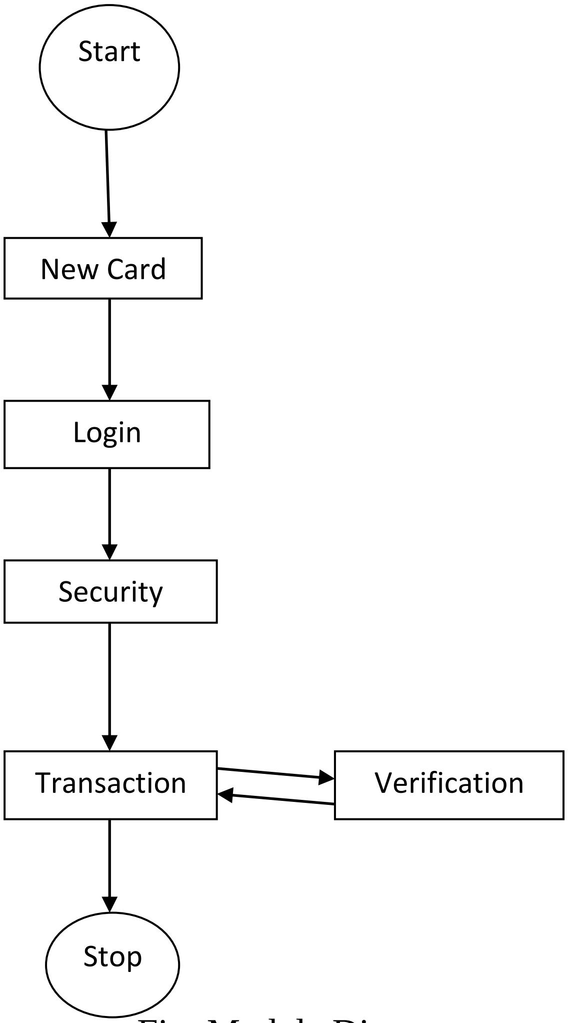

Fig: Module Diagram

8. Techniques and Algorithm is used:

To keep details the credit card transaction dispensation process in conditions of a Hidden Markov Model (HMM), it creates through unique deciding the inspection sign in our representation. We quantity the purchase items of values x into M cost ranges V1, V2 . . . VM, form the study sign by the side of the issuing bank. The actual cost variety for each sign is configurable based on the expenditure routine of personal cardholders. HMM determine these cost range change by using clustering algorithms (like K clustering algorithm) on the cost values of every cardholder transactions. It uses bulk Vk for clustering algorithm as k ¼ 1, 2. . . . M, which can be represented both observations on price value symbols as well as on cost value range.

In prediction process it considers mainly three cost value ranges such as low(l), Medium(m), and High(h). So set of this design prediction sign is V{ l, m, h}, so V ¼ f as l(low), m(medium), h(high) which makes M ¼ 3. E.g. If cardholder execute a transaction as $ 250 and card holders profile groups as low(l) = (0, $ 100), medium (me) = ($ 200, $ 500), and high (h) = ($ 500, up to credit card limit), then transaction which cardholder want to do will come in medium profile group. So the corresponding profile group or symbol is M and V (2) will be used.

9. Conclusion:

1. We will have proposed an application of HMM in credit card fraud detection.
2. The different steps in credit card transaction method are represented as the underlying stochastic process of an HMM.
3. We will have used the ranges of transaction amount as the observation sign, whereas the types of item have been considered to be states of the HMM.
4. We will have suggested a process for finding the spending profile of cardholders, as well as application of this knowledge in deciding the value of observation sign and initial estimate of the model parameters.
5. It has also been explained how the HMM can find whether an incoming transaction is fraudulent or not.

10. Reference:

[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] Syeda, M., Zhang, Y. Q., and Pan, Y., 2002 Parallel Granular Networks for Fast Credit Card Fraud Detection, Proceedings of IEEE International Conference on Fuzzy Systems, pp. 572-577 (2002).

[3] 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.

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

[5] M.J. Kim and T.S. Kim, “A Neural Classifier with Fraud Density Map for Effective Credit Card Fraud Detection,” Proc. Int’l Conf.

Intelligent Data Eng. and Automated Learning, pp. 378-383, 2002.

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

[7] R. Brause, T. Langsdorf, and M. Hepp, "Neural Data Mining for Credit Card Fraud Detection," Proc. IEEE Int'l Conf. Tools with Artificial Intelligence, pp. 103-106, 1999.

[8] C. Chiu and C. Tsai, "A Web Services-Based Collaborative Scheme for Credit Card Fraud Detection," Proc. IEEE Int'l Conf. e-Technology, e-Commerce and e Service, pp. 177-181, 2004.

[9] C. Phua, V. Lee, K. Smith, and R. Gayler, "A Comprehensive Survey of Data Mining-Based Fraud Detection Research, Mar. 2007.