Artificial & Computational Intelligence / Published Online : June 2020
https://acors.org/ijacoi/VOL1_ISSUE3_03.pdf

Artificial & Computational Intelligence

Credit Card Fraud Detection System Using Data Mining

T Archana Das[1], Komal C Lagade[2], Minakshi P Girase[3], Ramesh Patole[4]
Department of Information Technology
das_archana.ghrcemit@raisoni.net[1], komalclagade@gmail.com[2], rajputminakshi07@gmail.com[3], ramesh.patole@raisoni.net[4]
G.H.Raisoni College of Engineering and Management,Pune

Abstract

This paper deals with the implementation of Hidden Markov Model to detect credit card related fraud by considering a card-holder's spending habit. Card transaction is processed sequentially by the stochastic process of an HMM. This observes histogram data as every cardholder possess a unique pattern. A spending profile of the cardholder is made. Each incoming transaction is submitted to the fraud detection system. Then several modules of the system are matched to verify and recognize patterns. When some deviation is observed then the system generates an alarm to the issuing bank as well as the user. Finally implement a fraud detection system which prevents fraud from happening rather than detecting one after its done.

Keywords: Purchases, Fraudulent Transactions, Spending Patterns, Behaviorist Profile, Payment, Cardholder.

1. Introduction

Credit-card-based purchases can be categorized into two types:
1) physical card and 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 of such type of purchase, an attacker will have to steal the credit card. If the cardholder doesn't realize the loss of card, it can cause a considerable 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 for making the payment. Such purchases are normally done on the web or over the telephone. To commit fraud in these kinds of purchases, a fraudster simply needs to know the card details. Most of the time, the real cardholder isn't aware that somebody else has seen or stolen his card information. The only way to detect this type of fraud is to figure out the spending patterns on every card and to work out any inconsistency with respect to the “usual” spending

patterns. Fraud detection On the basis of analysis of already present purchase data of cardholder is a promising method to reduce the scale of successful credit card frauds. Since humans tend to exhibit specific behaviorist profiles, every cardholder can be represented by a set of patterns containing information about the usual purchase type, since the last purchase, the amount of money spent, etc. Deviation from such patterns is a potential threat to thesystem.

2. Literature Review

In March 2019, research paper published in International Journal of Engineering Sciences & Research Technology, by Kaithekuzhical Leena Kurien and Dr. Ajeet Chikkamannur of VTU Research Center, Bangalore, India, describes probability of fraudulent transactions in prevalence and context of credit card usage. A conscious effort being put to bring about a conceptual distinction between fraud detection and predicting probable fraudulent opportunities on the digital space of financial transactions. This emerges a new dimension of financial fraud as a

complex phenomenon that can take very different forms, depending on the market segments and the actorsinvolved.

In July 2019, research paper published in International Journal of Recent Technology and Engineering by Devika S P, Nisarga K S, Gagana P Rao, Chandini S B, Rajkumar N, discusses various methods of detecting and controlling the fraudulent activities using the HMM. Thus, discussing about phishing and Trojan horse virus attacks in fraudulent activities.

In October 2019, research paper of the topic "Electronic Credit Card Fraud Detection System by Collaboration of Machine Learning Models" in International Journal of Innovative Technology and Exploring Engineering by Shiv Shankar Singh, discusses about fraud activities that cannot be detected manually by carrying out research and examine the results of logistic regression, decision tree and support vector machine. A dataset of electronic payment card is taken from European electronic cardholders, the machine learning techniques are applied on the unstructured and process-freedata.

3. Motivation

In case of the present system the fraud is detected after the fraud has already taken place which means, the fraud is detected after the complaint of the card holder. And so the card holder faced a great deal of trouble before the investigation finish. And also as all the transaction is maintained in the form of a log, which requires to keep up with a huge data. And also in recent times a lot of online purchases are made so we don't know the person how is using the credit-card online, we just get the IP address for verification. So there is requirement of help from the cybercrime to investigate the fraud. To avoid the entire above disadvantage, we propose the system to detect the fraud in a way which is best and in a simpleway.

4. Project Scope

It presents Hidden Markov Model (HMM).Which is able to detect frauds by considering a card-holder's spending habit. Card transaction processing sequence by the stochastic process of an HMM. The details of items purchased in Single person transactions generally can't be known to any Fraud Detection System; running at the bank that issues credit cards to the cardholders. Hence, we feel HMM is an ideal choice for addressing this problem. Another important advantage of the HMM-based approach is a drastic reduction in the number of False Positives transactions marked as malicious by an fraud-detection system although they are actually genuine. An FDS runs at credit card issuing bank. Every transaction that comes in is submitted to the fraud- detection system for verification. FDS receives the card details and also the value of purchase to verify, whether transaction is genuine or not. The types of products that are bought in the mentioned transaction aren't known to the FDS. It tries to find any anomaly in the Pattern of transaction of the spending profile of the cardholder, address etc. If the fraud-detection system confirms the transaction to be of fraud, it raises an alarm, and therefore the issuing bank declines thetransaction.

Software Quality Attributes

Usability:

The system should be user friendly and self-explanatory. Proposed system is **Flexible**, **Robust,** and easily **Testable**.

Accuracy:

The level of accuracy in the proposed system will be higher.

Openness:

The system should be extensible to guarantee that it is useful for community system.

Usability:

The proposed system will helpful in detecting credit card fraud, more precisely any unauthorized activity before happening.

System Architecture

User enters their login details to access their account. Then account details for making any transactions. In order for the transaction to take place, a verification is done. Only then the action is complete.

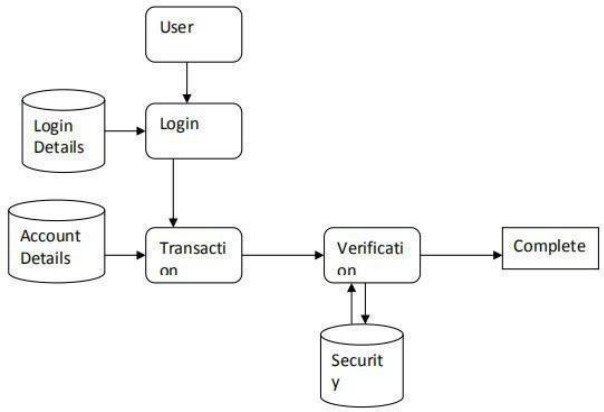

Figure 1 shows the system architecture

Activity Diagram

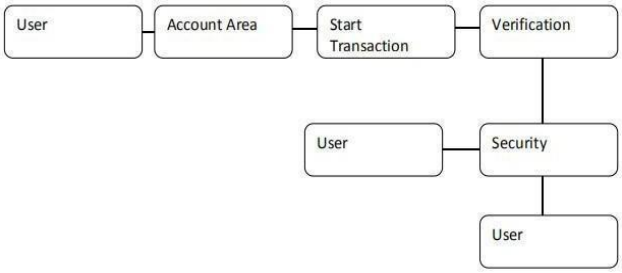

Figure 2 shows the activity diagram

5. Conclusion

In this paper, we've proposed an application of HMM in credit card fraud detection. 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 are considered to be states of the HMM. We have suggested a technique for analyzing the spending profile of cardholders, as well as application of this information in deciding the value of observation symbols and initial estimate of the model parameters. It has also been explained The way the HMM can detect if an transaction which is being received is fraudulent or not. Experimental results show the performance and effectiveness of our system and demonstrate the usefulness of learning the spending profile of the cardholders. Comparative studies reveal that the Accuracy of the system is somewhat 80 percent over a good amount of variation.

References

[1] Abbott, D., Matkovsky, P. & Elder, J. (1998). An Evaluation of High-End Data Mining Tools for Fraud Detection. Proc. of IEEE SMC98. Aleskerov, E., Freisleben, B. & Rao, B. (1997).

[2] CARDWATCH: A Neural Network-Based Database Mining System for Credit 11 Card Fraud Detection. Proc. of the IEEE/IAFE on Computational Intelligence for Financial Engineering, 220-226.

[3] Artis, M., Ayuso M. & Guillen M. (1999). Modelling Different Types of Automobile Insurance Fraud Behaviour in the Spanish Market. Insurance Mathematics and Economics 24: 67-81.

[4] Barse, E., Kvarnstrom, H. & Jonsson, E. (2003). Synthesizing Test Data for Fraud Detection Systems. Proc. of the 19th Annual Computer Security Applications Conference, 384-395.

[5] Belhadji, E., Dionne, G. & Tarkhani, F. (2000). A Model for the Detection of Insurance Fraud. The Geneva Papers on Risk and Insurance 25(4): 517-538.

[6] Bell, T. & Carcello, J. (2000). A Decision Aid for Assessing the Likelihood of Fraudulent Financial Reporting. Auditing: A Journal of Practice and Theory 10(1): 271-309.

[7] Beneish, M. (1997). Detecting GAAP Violation: Implications for Assessing Earnings Management Among Firms with Extreme Financial Performance. Journal of Accounting and Public Policy 16: 271-309.

[8] Bentley, P. (2000). Evolutionary, my dearWatson: Investigating Committee-based Evolution of Fuzzy Rules for the Detection of Suspicious Insurance Claims. Proc. of GECCO2000.

[9] Bentley, P., Kim, J., Jung., G. & Choi, J. (2000). Fuzzy Darwinian Detection of Credit Card Fraud. Proc. of 14th Annual Fall Symposium of the Korean Information Processing Society.

[10] Bhargava, B., Zhong, Y., & Lu, Y. (2003). Fraud Formalisation and Detection. Proc. of DaWaK2003, 330-339.

[11] Bolton, R. & Hand, D. (2002). Statistical Fraud Detection: A Review (With Discussion). Statistical Science 17(3): 235-255.

[12] Bolton, R. & Hand, D. (2001). UnsupervisedProfiling Methods for Fraud Detection. Credit Scoring and Credit Control VII.

[13] Bonchi, F., Giannotti, F., Mainetto, G., Pedreschi, D. (1999). A Classification-based Methodology for Planning

Auditing Strategies in Fraud Detection. Proc. of SIGKDD99, 175-184.

[14] Brause, R., Langsdorf, T. & Hepp, M. (1999). Neural Data Mining for Credit Card Fraud Detection. Proc. of 11th IEEE International Conference on Tools with Artificial Intelligence.

[15] Brockett, P., Derrig, R., Golden, L., Levine, A. & Alpert, M. (2002). Fraud Classification using Principal Component Analysis of RIDITs. Journal of Risk and Insurance 69(3): 341-371.

[16] Brockett, P., Xia, X. & Derrig, R. (1998). Using Kohonen's Self Organising Feature Map to Uncover Automobile Bodily Injury Claims Fraud. Journal of Risk and Insurance 65(2): 245-274.

[17] Burge, P. & Shawe-Taylor, J. (2001). An Unsupervised Neural Network Approach to Profiling the Behaviour of Mobile Phone Users for Use in Fraud Detection. Journal of Parallel and Distributed Computing 61: 915-925.

[18] Cahill, M., Chen, F., Lambert, D., Pinheiro, J. & Sun, D. (2002). Detecting Fraud in the Real World. Handbook of Massive Datasets 911-930.

[19] Caruana, R. & Niculescu-Mizil, A. (2004). Data Mining in Metric Space: An Empirical Analysis of Supervised Learning Performance Criteria. Proc. of SIGKDD04, 69-78.