Modeling Credit Card Transaction Sequences to Detect and Prevent Fraudulent Activities

N.Balasubramanian[1], M.Mohamed Rafi[2], K.Dhineshkumar[3]
[1,2,3]*Department of MCA, Mohamed Sathak Engineering College, Kilakarai, India*

Abstract: Now a day the usage of credit cards has dramatically increased. As credit card becomes the most popular mode of payment for both online as well as regular purchase, cases of fraud associated with it are also rising. In this paper, we model the sequence of operations in credit card transaction processing can be used for the detection of frauds. An FDS is initially trained with the normal behavior of a cardholder. If an incoming credit card transaction is not accepted by the trained FDS with sufficiently high probability, it is considered to be fraudulent. At the same time, we try to ensure that genuine transactions are not rejected. We present detailed experimental results to show the effectiveness of our approach and compare it with other techniques available in the literature.

This project is developing used to detect and block from fraud transactions using a credit card. 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 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.

Keywords: Genuine Transactions, FDS (Fraud Detection System), Physical Card Purchases, Spending Patterns Analysis.

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 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.

2 RELATED WORKS

Sumit kumar Jha, Raghvendra Kumar, and Pushpendra Kumar Pateriya (2016) This survey paper provides an overview of various techniques used in credit card fraud detection, including statistical methods, machine learning algorithms, and hybrid approaches. It discusses the strengths and weaknesses of different approaches and highlights current trends in fraud detection research.

Vishal Vyas, Himanshu Gupta, and Shashank Gupta (2019) This paper reviews recent advances in credit card fraud detection techniques, focusing on data analytics approaches. It covers topics such as anomaly detection,pattern recognition, and machine learning algorithms applied to fraud detection. The paper also discusses challenges and future directions in the field.

K. Ravi Kumar,P. Ravi Kumar, and G. Lavanya (2018) This survey paper presents an extensive review of credit card fraud detection techniques, including rule-based systems, data mining approaches, and neural networks. It discusses the effectiveness of different methods and compares their performance based on various criteria such as accuracy, scalability, and interpretability.

3. PURPOSE OF WORK

The purpose of this work is to develop a robust fraud detection system (FDS) aimed at identifying and preventing fraudulent credit card transactions. With

the increasing use of credit cards for both online and offline purchases, the incidence of fraud has also risen. This project models the sequence of operations in credit card transaction processing to detect fraudulent activities. By training the FDS with the normal behavior patterns of cardholders, it can flag transactions that deviate from these patterns as potentially fraudulent. The system aims to ensure the accurate detection of fraud while minimizing the rejection of genuine transactions. Additionally, the project seeks to analyze and compare the effectiveness of this approach with other existing techniques, ultimately contributing to reducing the rate of successful credit card frauds and protecting both cardholders and financial institutions from substantial financial losses.

3.1 System Architecture

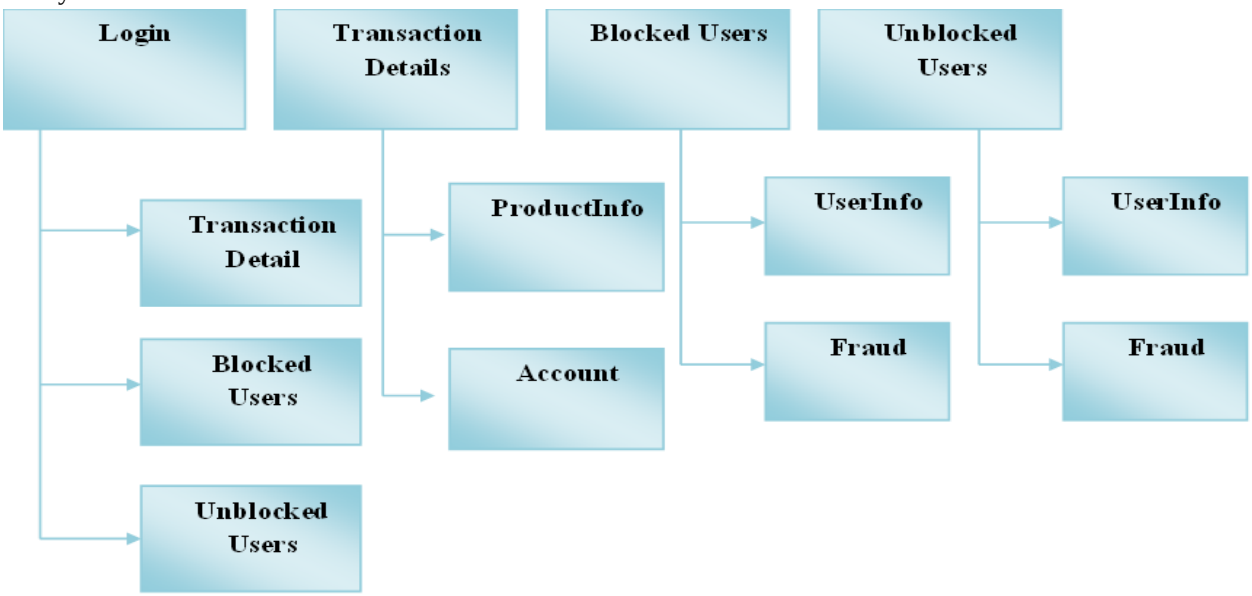


Fig 1.System Architecture

Admin view transactions, view blocked and unblocked users. User login to the application, do the transaction. If credentials are wrong user details blocked; otherwise transactions executed.

3.2 ALGORTIHM

AdaBoost Algorithm

It is a supervised learning algorithm that is used to classify data by combining multiple weak or base learners (e.g., decision trees) into a strong learner. AdaBoost works by weighting the instances in the training dataset based on the accuracy of previous classifications. AdaBoost is a flexible algorithm that can be applied to a variety of machine-learning problems, including classification and regression. 2. It can handle datasets with missing values and outliers well.

Data Preprocessing: The dataset containing credit card transactions is preprocessed to handle missing values, outliers, and imbalance issues between normal and fraudulent transactions.

Feature Engineering: Relevant features such as transaction amount, time, merchant information, and others are selected or engineered to provide meaningful information for fraud detection.

Initialization: Each training example (transaction) is assigned an equal weight initially.

Train Weak Learner: A weak learner, often a decision tree with limited depth (a decision stump), is trained on the dataset. The weak learner aims to classify transactions as either normal or fraudulent, based on the selected features.

Evaluate Performance: The performance of the weak learner is evaluated by calculating its error rate on the training set. The error rate is typically computed as the weighted sum of misclassified examples.

Output: The combined model serves as a fraud detection system where transactions are classified as normal or fraudulent based on the ensemble of weak learners.

4. PROPOSED SYSTEM

In proposed system, we present a Hidden Markov Model (HMM).Which does not require fraud signatures and yet is able to detect frauds by considering a cardholder's spending habit. Card transaction processing sequence by the stochastic process of an HMM. The details of items purchased in Individual transactions are usually not known to any Fraud Detection System (FDS) running at the bank that issues credit cards to the cardholders. Hence, we feel that 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 identified as malicious by an FDS although they are actually genuine. An FDS runs at a credit card issuing bank.

Each incoming transaction is submitted to the FDS for verification. FDS receives the card details and the value of purchase to verify, whether the transaction is genuine or not. The types of goods that are bought in that transaction are not known to the FDS. It tries to find any anomaly in the transaction based on the spending profile of the cardholder, shipping address, and billing address, etc. If the FDS confirms the transaction to be of fraud, it raises an alarm, and the issuing bank declines the transaction.

The detection of the fraud use of the card is found much faster that the existing system. In case of the existing system even the original card holder is also checked for fraud detection. But in this system no need to check the original user as we maintain a log. The log which is maintained will also be a proof for the bank for the transaction made. We can find the most accurate detection using this technique. This reduces the tedious work of an employee in the bank.

5. TESTING AND IMPLEMENTATIOM

5.1 TESTING

A. New card

In this module, the customer gives there information to enroll 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

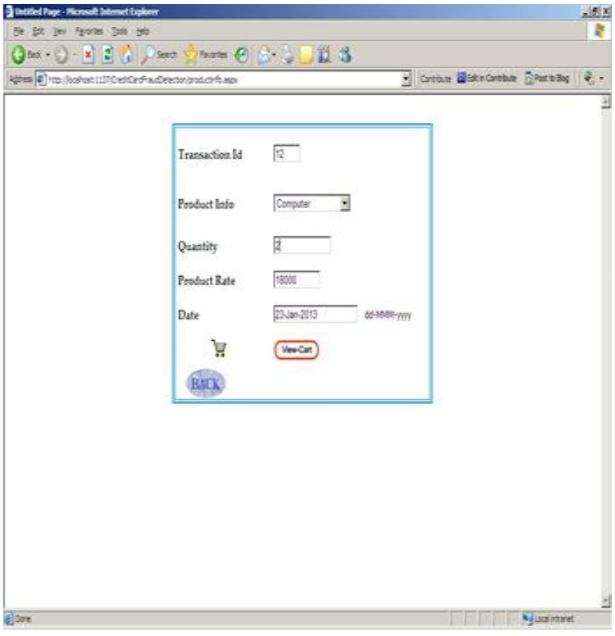
The method and apparatus for pre-authorizing transactions includes providing a communications device to a vendor and a credit card owner. The credit card owner initiates a credit card transaction by communicating to a credit card number, and storing therein, a distinguishing piece of information that 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 seeks 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 card no has been block and he can't do the further transaction.

5. 2 IMPLEMENTATION



6.CONCLUSIONS AND FUTURE ENHANCEMENT

Since humans tend to exhibit specific behaviorist 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 to detect and block from fraud transactions using a credit card. Here, I kindly convey that special feature of this software is the geniality and it can be worded on the personal computer, since the web page gives a variety option and the message gives clear understanding of the next page it is easy to follow and use.

We are sure that this software will be useful for all company. this software, there is no need of knowledge of the computer operating method because, to enter into the menu just enter into windows and type the particular directory, in which the project is stored.

6.1 FUTURE ENHANCEMENT

In future this project will be using the following methods; With PCI [Payment Card Industry] compliance, vendors are required to harden their code and make access to personal information more secure. For instance, in order for our ecommerce engine to maintain its PCI certification, we are scanned by a third-party every night, and then we are tested to ensure we're not exposed. If we are, we're notified and we have between 24 and 72 hours to seal the leak, so-to-speak. If we miss the deadline, we lose our certification until we've completely sealed off the vulnerability.

7.REFERENCE

[1] Credit Card Fraud Detection and Prevention" by Adam Coates

[2] "Machine Learning for Credit Card Fraud Detection: Practical Real-Time Applications" by Edouard Tissot.

[3] Bolton, R. J., & Hand, D. J. (2002). "Statistical Fraud Detection: A Review". Statistical Science, 17(3), 235249.

[4] Bhattacharyya, S., Jha, S., Tharakunnel, K., & Westland, J. C. (2011). "Data Mining for Credit Card Fraud: A Comparative Study". Decision Support Systems, 50(3), 602-613.

[5] Delamaire, L., Abdou, H., & Pointon, J. (2009). "Credit Card Fraud and Detection Techniques: A Review". Banks and Bank Systems, 4(2), 57-68.

[6] Srivastava, A., Kundu, A., Sural, S., & Majumdar, A. (2008). "Credit Card Fraud Detection Using Hidden Markov Model". IEEE Transactions on Dependable and Secure Computing, 5(1), 37-48

[7] Phua, C., Lee, V., Smith, K., & Gayler, R. (2010). "A Comprehensive Survey of Data Mining-Based Fraud Detection Research". arXiv preprint arXiv:1009.6119.

[8] Juszczak, P., Adams, N. M., Hand, D. J., Whitrow, C., & Weston, D. (2008). "Off-Line Identity Fraud Detection Using Statistical and Machine Learning Methods". In Advances in Intelligent Data Analysis VIII (pp. 129-139). Springer.

[9] Bhattacharyya, S., Jha, S., Tharakunnel, K., & Westland, J. C. (2011). "Data Mining for Credit Card Fraud: A Comparative Study". Decision Support Systems, 50(3), 602-613.

[10] Dorronsoro, J. R., Ginel, F., Sánchez, C., & Cruz, C. S. (1997). "Neural Fraud Detection in Credit Card Operations". IEEE Transactions on Neural Networks, 8(4), 827-834.