International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Online Frauds Detection

Vivek Sehrawat[1], Mahesh Kumar Malkhani[2]

[1]PG Student, Cyber Forensics and Information Security, GITAM Jhajjar, India
[2]HOD, CSE Dept. Ganga Institute of Technology and Management, Jhajjar

ABSTRACT

Online credit/debit card transactions appear to be a factor in the expansion of the internet and e-commerce. Fraud is on the rise as a result of more people using credit and debit cards. The frauds can be found using a variety of methods, but each has its own limitations in terms of accuracy. The behavior-based approach to categorization is employed in this study to increase accuracy using Support Vector Machines. The frauds are anticipated and taken for further action if there are any changes in the transaction's conduct. The proposed solution solves the problem of credit/debit card fraud detection caused by the vast volume of data.

Keywords: Online Fraud Detection, Data Flow Diagram, Credit Card Transaction

I. INTRODUCTION

Due to the explosive rise of e-commerce, online transactions and purchasing are now increasing daily. People all around the world use Credit Card payments as their method of receiving in vast numbers. The number of people using credit cards is rising daily. According to research, about 430 million people in Europe use cards for payment, especially credit and debit cards. As more people use these cards, there are also more fraudulent users. The two main categories of credit cards are.

1. A real card.
2. A digital card.

When making a purchase with a real card, the user must display the card. If a fraudulent user of this type needs to access a user card, he has to steal that card only. The customer who wants to use a virtual card fraudulently has to know the specifics of the credit card, including the CVV number, security code, and digit of the credit card. The payment gateway (secured) is therefore required to match the exact data to confirm whether the cardholder is a legitimate person or sniffer. Behavior and Location Analysis is the most effective and appropriate method for detecting fraud.

II. TECHNOLOGY

The issue will be resolved through the employment of a variety of security elements, the majority of which are designed to enhance user identification and authorization requirements. The next generation of credit cards, known as smart cards, include computer chips in place of holograms because they are inefficient at preventing fraud. Each card has a magnetic stripe with stored data and a microprocessor memory chip. To receive authorization, the cardholder must enter the personal identification number (PIN) printed on the microchip. The market anticipates a time when bank customers will have access to a single card that can be used to handle all of their financial needs. French banks have been using this technology since the late 1980s, and reports indicate that the amount of fraud they experience has greatly decreased. Over 2S million smart cards, or roughly 50% of all smart cards, are currently in use worldwide.

III. FRAUDDETECTION SYSTEM

The identification of credit card fraud is a pattern recognition issue. Each cardholder has a shopping pattern that creates a profile for them. The Fraud Detection System may not be aware of new patterns of behavior because patterns of conduct vary over time as a result of individual demands or seasonal factors (FDS).

A 'strange' transaction is frequently genuine. It is noteworthy that this thesis consistently uses the terms legitimate and non-fraud interchangeably. FDS currently classifies a high number of valid accounts as fraudulent, leading to a lot of false positives (FPs). The variety of transactions is huge since every cardholder has a ton of opportunities to establish new behavioral patterns. As a result, it is very hard to find stable and consistent patterns for every transaction. In actuality, there are an exponential number of possible behavioral variants for each individual, making it difficult to list all possible combinations of anonymous situations. The Fis now has a significant number of FPs (about 90% of flagged accounts) that need to be investigated due to the ever-changing pattern of activity and the mix of legitimate and fraudulent cases.

To solve these issues, this research was motivated. The aim is to, in essence, post-process the FDS data and separate the genuine transactions (True Negatives, TN) from the stream of flagged transactions. The system we create must be able to extract the True Negatives (TNs) from the pool of data without overlooking fraudulent transactions because this identification is a classification task. The bank personnel might not need to call these genuine consumers for transaction verification if this goal could be accomplished.

IV. CHALLENGES

Payment methods based on plastic cards are extremely popular and are increasingly employed by businesses and people. It goes without saying that sectors with this rate of expansion are open to fraudsters' attacks. A group of 14 credit card criminals admitted to using over LOO different credit card fraud schemes in a 1993 study that was performed in the United States (U.S.).The majority of fraud incidents involve lost or stolen cards. Cards that have been lost or stolen account for 55% of Visa losses and 49% of MasterCard losses. The typical loss from this type of fraud is $700. The chance for fraud opens up when a card is lost or stolen. The main sites where cards are stolen include workplaces, car glove boxes, and athletic venues. A friend or family member using the card without the cardholder's consent frequently results in these losses. Cardholders occasionally sell their cards to criminals, report the cards as stolen or lost, or they shop, deny the transaction, and report the cards as stolen or lost.

V. SOLUTION

The present fraud solution approaches are introduced in this chapter, along with a quick overview of the current fraud detection systems (FDS). It briefly discusses neural network technology's use in detecting credit card fraud as well as its benefits and drawbacks. It goes into more detail about the challenges involved with fraud investigation.

VI. REPORT AND TESTING

This study is a summary of the complete procedure meant to respond to several queries, such as: What is the issue? Exists a workable solution to the stated issue? As soon as the issue is known, a viability study is done. A viable study is required to evaluate the technical, operational, and economic aspects of the proposed system in order to determine its viability. A thorough feasibility assessment will give management a clear understanding of the suggested system. Since the project is so huge, testing is always necessary to ensure its success. The success of a project is determined by how well each component functions overall and how well it produces the expected results for every input given. A test should be taken to check the success of the project, which is the conclusion.

Here, system testing was carried out to see whether the user requirements were met. Python was used exclusively to create the new system's code, with Django serving as the front-end design interface. The new system has undergone thorough user testing, and each application has been examined from every angle by a user.

VII. FUTURE SCOPE

Although the trained system's potential to distinguish between genuine and fraudulent transactions that are reported by FDS is promising, its forecast accuracy must be improved. The following list includes some of the most significant recommendations for further research that can examine the potential for improving the prototype and its possible application in card fraud detection:

- Learning systems make the most use of the resources available to them. For the same learning approach, it is entirely plausible that revisions or the addition of new features could result in significantly improved performance (WEIS91 J. All learning systems are built on sufficient and representative data, and this study has shown that incorporating all characteristics led to classifiers that performed better. Therefore, require sufficient data to create the trained system further. In this regard, a larger fraud dataset and FDS scores are two important prerequisites for further study.
- To create datasets with higher minority instances of fraud/non-fraud cases (i.e., 60:40, 70:30, etc.) in order to investigate the impact of class distribution on the performance of the classifiers and, based on this evaluation, to select the highest predictive classifier for deployment.
- The same sample data can be used to apply a variety of learning approaches. Some learning systems may perform better than others for a particular application. In general, there is no assurance that any of these techniques will be effective or that one technique in particular is necessarily the best. One well-known learning programme (SeeS) was used in this study. It is also important to look at the other two well-known programmes, CART [BREl84] and RIPPER [COHE9!]. These programmes have demonstrated amazing results when used to solve real-world issues like detecting credit card fraud. The performance can be measured using a variety of approaches, and the algorithm that produces the best performance can then be chosen.

As was previously mentioned, the environment for fraud is dynamic, hence the system being created needs to be adaptable to shifting fraud environments.

VIII. RESULT

The experimental outcomes of processing several data sets with diverse training class distributions are shown in this section. Unfortunately, there was no information on the expenses related to fraud offices investigations, therefore it was unable to determine any potential savings from the technique employed in this study.

- The system keeps track of each user's previous transactional patterns.
- It determines the user's attributes based on their spending capacity and even their nation.
- The use of OTP (One Time Password) increases the security of the system.
- Every transaction includes IP address tracking.
- Security questions for exceeding the payment cap.
- If a user's transaction (history of purchases and country of operation) deviates by more than 20 to 30 percent, the system deems the attempt invalid and takes appropriate action.

References

[1]. "A Survey of Credit Card Fraud Detection Techniques", Data and Technique Oriented Perspective, Nov 2016. - SamanehSoroumejad, Zahra Zojaji, Reza EbrahimiAtani and Amir Hassan Monadjemi

[2]. Bank Fraud Detection Using Support Vector Machines, 2018. - Nana Kwame Gyamfi and Jamal-DeenAbdulai

[3]. A Comparative Analysis of Various Credit Card Fraud Detection Techniques, vol. 7, no. 5S2, January 2019, ISSN 2277-3878. - Yashvi Jain, Namrata Tiwari, Shripriya Dubey and Sarika Jain

[4]. "Fraud Detection in Online Credit Card Payment", International Research Journal of Engineering and Technology, vol. 05, no. 03, Mar 2018, ISSN 2395-0056. - AishwaryaKaneri, Anugrah S, Isha Bharti, SamruddhiJadhav and MitaliKadu

[5]. Credit card fraud and detection techniques, vol. 4, no. 2, 2009. - Linda Delamaire, Hussein Abdou and John Pointon