Synopsis

B. Tech (VII Semester) Project

Work-1

Credit Card Fraud Detection Website

A Synopsis

for

Project Work-1

BACHELOR OF TECHNOLOGY in COMPUTER SCIENCE & ENGINEERING

BY

Aaditya Anand	**Abhay Singh Chauhan**	**Advait Patidar**
EN19CS301004	**EN19CS301011**	**EN19CS301027**

Under the Guidance of

Dr. Harsh Singh Rajpoot

Department of Computer Science & Engineering
Faculty of Engineering
MEDI-CAPS UNIVERSITY, INDORE- 453331

NOVEMBER 2022

Introduction

As the payment method is simplified by the combination of the financial industry and IT technology, the payment method of the consumers is changing from cash payment to electronic payment using a credit card, mobile micropayment, and app card. As a result, the number of cases in which anomalous transactions are attempted by abusing e-banking has increased and financial companies started establishing a Fraud Detection System (FDS) to protect consumers from abnormal transactions. The abnormal transaction detection system aims to identify abnormal transactions with high accuracy by analyzing user information and payment information in real-time. Although FDS has shown good results in reducing fraud, most cases being flagged by this system are False Positives that result in substantial investigation costs and cardholder inconvenience. The possibilities of enhancing the current operation constitute the objective of this research. Based on variations and combinations of testing and training class distributions, experiments were performed to explore the influence of these parameters. In this project, we will investigate the trend of abnormal transaction detection using payment log analysis and data mining and summarize the data mining algorithm used for abnormal credit card transaction detection. We will use python programming with Apache spark for advanced processing of data and high accuracy.

Literature Review

Millions and billions of people use credit cards for payment in both online and offline transactions, due to the existence of a widespread point of sale (POS). countless transactions occurred per minute everywhere on the planet. The reason behind fraud is the negligence of the user. When a third person steals the most important information about credit cards and user details easily fraud can be achieved. To detect what type of fraud occurs during a transaction, we need to face several challenges. Fetching that among all the transactions is occurred and which one is real could be a task.

Amongst the standard and very common ways of making payment globally and especially in North America, because of the presence of a far-reaching point of sale. A huge number of individuals around the globe use charge cards to buy products and services by getting credit for a time of half a month. Any helpful framework could be mishandled, and a charge card is no exemption from this. Alongside the ascent of charge card use, extortion is on the ascent. Monetary Institutions (FIs) endure refined fake exercises and bear many dollar misfortunes every year. Considering statistics [2] frauds account for more than $1 billion every year for Visa and MasterCard around the world.

Credit card companies and their part banks attempt to discover better approaches to forestall scams. A portion of the precautionary measures on the cards is magnetic stripes, 3D monograms, and CVC. Credit card companies are likewise taking steps to have an alternative for credit cards such as Smart Cards, be that as it may, given assessments this substitution will be over the top expensive because of the broad POS network in the USA and the gigantic no. of cards available for use in those places. FIS additionally utilizes an assortment of computing mechanisms, such as Neural Networks (NNs), to follow and distinguish dubious exchanges and ban them for additional examination.

Nagi et al. presented intrusion detection frauds using data mining techniques for financial fraud detection. The papers from 49 journals were published in 2018. This paper allows the analysis and classified into four fraud categories and six data mining techniques [5].

Sanjeev et al. Is a paper that analyzes and classifies fraud type classification and fraudulent transaction frequency and the amount by country through actual credit card fraud transaction data and visually expresses the distribution using a box plot [6].

Michael et al. presented signature-based research on fraud detection and a fraud detection model [7] to provide a comprehensive survey of existing research related to fraud detection and to conduct fraudulent transactions in real-time [7].

In the case of real-time detection, it is necessary to make accurate judgments in an instant and consider the characteristics of the data mining algorithm. TS Quah et al. Implemented real-time detection by separating detection mechanisms into the initial authentication layer, inspection layer, core layer for risk score evaluation and behavior analysis, and additional review layer using the SOM algorithm [8][9][10].

Problem Definition

Not al1 doubtful transactions consider fraudulent. It is commonly called a false positive (FP) which means that the case was not a fraud although it was flagged as being a potential scam. This process of affirming each transaction those outliers from the cardholder's normal routine brings doubt about possible client disappointment. Additionally, the expenses related to exploring an enormous no. of false positives are high.

As of now, a considerable amount of time is given to examining countless genuine cases (FPs). On the off chance that the quantity of examination on FPs could be dropped down, scam analysts can invest more energy and time in genuine fraud transactions that restrict the losses to the FIs.

Objectives

There is a substantial rise in some technologies like “machine learning, artificial intelligence, deep learning” and other relevant fields of information technology. These technologies help us automate the credit card fraud classification process. Automation saved a huge amount of time and work in detecting the fraudulent transactions present in the dataset.

The key objective of the Credit card Fraud Detection Website is to improvise the procedure of personal follow-up on many suspicious transactions and to discover a path to preprocess the flagged records to recognize the probable genuine entries from the list of genuine/falsified entries. Here, the volume of needless analysis is decreased leading to significant savings for the financial institutions. Moreover, the current FDS threshold can also be lowered and several fraudulent cases, being missed under this level, can be detected. As a result, the fraud is discovered earlier, and the overall losses may be reduced. For addressing these challenges, outlier detection, and GBT Classifier is used, i.e., among the very commonly used applications of Machine Learning for addressing pattern recognition and classification problems.

The system will overcome the low accuracy forecast problems, utilize the latest AI methods, reduce false alerts, recognize fraudulent transactions, and attain fast and reliable solutions.

Methodology

The performance of fraud detection in credit card transactions is greatly affected by the sampling approach on the dataset, selection of variables, and detection technique(s) used. The Credit Card Fraud Detection Problem includes modeling past credit card transactions with the knowledge of the ones that turned out to be a fraud. Hence, we are using the technique of machine learning for fraud detection. In this, we take the real bank dataset and split the dataset into a training set and testing set, and then apply the Logistic Regression method.

Reading the dataset from the file “creditcard.csv” which has 2,84,807 transactions. To get all variables in an equivalent range, we subtract the mean and divide it by the standard deviation such that the distribution of the values is normalized.

Then we perform normalization. To get all variables in an equivalent range, we will subtract the mean and divide it by the standard deviation such that the distribution of the values is normalized.

The plotting of the dataset is done. We will first define some models like the “Logistic Regression, Gaussian Naïve-Bayes, and Decision Tree Classifier”, and then loop through a training and testing set. First, we will train the model with the training set and then validate the results with the testing set.

References

[1] Donald V. Macdougall, Richard G. Mosley, Garioch J. l. Saunders; Credit card crime in Canada: Investigation - Prosecution; The Canadian Association of Crown Counsel; page 1-56; January 1985.

[2] Isabelle Sender; Detecting and combating fraud; Chain Store Age; New York; Vol. 74; Issue 7; Page 162; July 1998. International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056 Volume: 07 Issue: 08 | Aug 2020 www.irjet.net p-ISSN: 2395-0072 © 2020, IRJET | Impact Factor value: 7.529 | ISO 9001:2008 Certified Journal | Page 1645

[3] Elford Dean, Raj Thomas, Lorry; Visa security center; Personal meetings; January 7 and February 11, 1999.

[4] Gyusoo Kim and Seulgi Lee, "2014 Payment Research", Bank of Korea, Vol. 2015, No. 1, Jan. 2015.

[5] EWT Nagi, Yong Hu, HY Wong, Yijun Chen, Xin Sun, "The Application of Data Mining Techniques in Financial Fraud Detection: A Classification Framework and an Academic Review of Literature," Decision Support Systems, Vol. 50, No. 3, Feb. 2011.

[6] Jha, Sanjeev, J. Christopher Westland, "A Descriptive Study of Credit Card Fraud Pattern," Global Business Review, Vol. 14, No. 3, pp. 373-384, 2015.

[7] Edge, Michael Edward, Pedro R. Falcone Sampaio, "A Survey of Signature-based Methods for Financial Fraud Detection," Computers & Security, Vol. 28 No. 6, pp. 381- 394. 2009.

[8] Aihua Shen, Rencheng Tong, Yaochen Deng, "Application of Classification Models on Credit Card Fraud Detection," Service Systems and Service Management of the 2007 IEEE International Conference, pp. 1-4, Jun.2007.

[9] Chengwei Liu, Yixiang Chan, Syed Hasnain Alam Kazmi, Hao Fu, "Financial Fraud Detection Model: Based on Random Forest," International Journal of Economics and Finance, Vol. 7, No. 7, pp. 178-188, 2015.

[10] Ganesh Kumar.None and P.Vasanth Sena, "Novel Artificial Neural Networks and Logistic Approach for Detecting Credit Card Deceit," International Journal of Computer Science and Network Security, Vol. 15, No. 9, Sep. 2015.

****