Card Fraud Detection using Approach of Machine Learning

Mir Auqib Yaqoob[1], Talwinder Kaur[2]
[1]M.Tech (CSE), Indo Global College, Abhipur Mohali, Punjab, India
[2]Department of Computer Science Engineering, Indo Global College, Abhipur Mohali, Punjab, India

Abstract: The usage of internet banking and credit cards is growing at an exponential rate. As more people use credit cards, online banking, and debit cards, the probability of becoming a victim of fraud of various kinds also increases. In recent times, there have been a number of instances in which users of credit card companies have, as a result of a lack of understanding, given their card information, personal information, and one-time password to an unidentified fraudulent caller. As a direct consequence of this, fraudulent activity will occur on the account. Fraud is a problem for the same reason that it is tough to track down a con artist who used a phone identity sim or made the call that utilized an internet provider: it is difficult to find them. Therefore, in order to detect fraudulent activity, this research makes use of supervised methodologies and algorithms, and the results are quite accurate. Customers lose trust in an organization when it engages in activities that are fraudulent or illegal, which in turn has a huge negative impact on the organization. Additionally, it has an effect on the total income and turnover of the company. The isolation forest technique is used in this study to classify data sets acquired from professional survey firms in order to detect fraud activities.
Index Terms: Credit Card, Fraud Detection, Decision Tree, Random Forest and Hybrid Approach, Data Set, Machine learning.

I. INTRODUCTION

Since the beginning of the digital process, there were always individuals who are looking for new methods to get unauthorized access to the financial information of another person. Due to the fact that all purchases can now be readily performed online by just inputting the credit card details, this has developed into a significant concern in the current day.

Technology that is capable of learning is a very crucial component in the process of determining whether or not credit card transactions include fraudulent behavior. Different techniques to machine learning have been used, historical data has also been accumulated, and new features have been introduced to increase the accuracy of predictions in order for banks to be able to anticipate these types of transactions.

When it comes to detecting fraudulent activity in credit card transactions, the effectiveness of the anti-fraud measures can be significantly influenced by a number of factors, including the sampling strategy that was applied to the data set, the variables that were selected, and the detection methods that were put into action. Theft and fraudulent activity done using or utilizing a credit card at the moment of payment are both examples of credit card fraud

Credit Card Fraud Detection with Machine Learning is an approach that takes the data investigation by a team of Data Scientists as well as model development, which will give the best outcomes in preventing revealing and fraudulent transactions. This process can be thought of as a hybrid between traditional data analysis and artificial intelligence.

II. LITERATURE WORK

A variety of strategies and algorithms have previously been devised to aid in the detection of such scams. Using machine learning is also a part of this investigation.

To conduct research on the data, trained ANN algorithms are used to obtain datasets from various overseas survey organizations. Algorithms like SVM and decision trees are used to detect and prevent fraudulent activity.

Misuse identification and information discovery are the two principle access utilized for credit card misrepresentation location. The accentuation on abuse location access is more often than not after applying order strategies the exchange level.

All extra security frameworks are commonly found on cardholder confirmation yet overlook the trader check which makes the exchange framework defenseless against vendor related and Internet-related cheats, for example, website cloning, dealer conspiracy, triangulation and so on.

III. PROBLEM FORMULATION

The most significant problem with credit card databases is that they are exceedingly uneven and biased. Actual transactions take precedence over fraudulent transactions. Fraudulent events do not occur frequently. If this is kept in mind, it may be difficult to detect the fraudulent transaction, as the criminal will be driven to attempt invalid transactions, resulting in the loss of cardholder data. The more datasets there are, the higher the dimensionality of the data. Dealing with a large amount of data in an effective manner is not an easy task. A scalable device learning gadget is needed to analyze the enormous volume of data. By using hybrid approach, we will increase the accuracy for detecting rates of fraud cases for machine learning algorithms in credit cards.

IV. OBJECTIVES

1) To study the various credit card fraud detection techniques for recognizing their advantages as well as shortcomings.
2) To design an improved credit card fraud detection scheme utilizing the machine learning classification.
3) To compare the results of the proposed research problem with the existing techniques of credit card fraud detection.

V. WORK DONE

The process flow is follow,
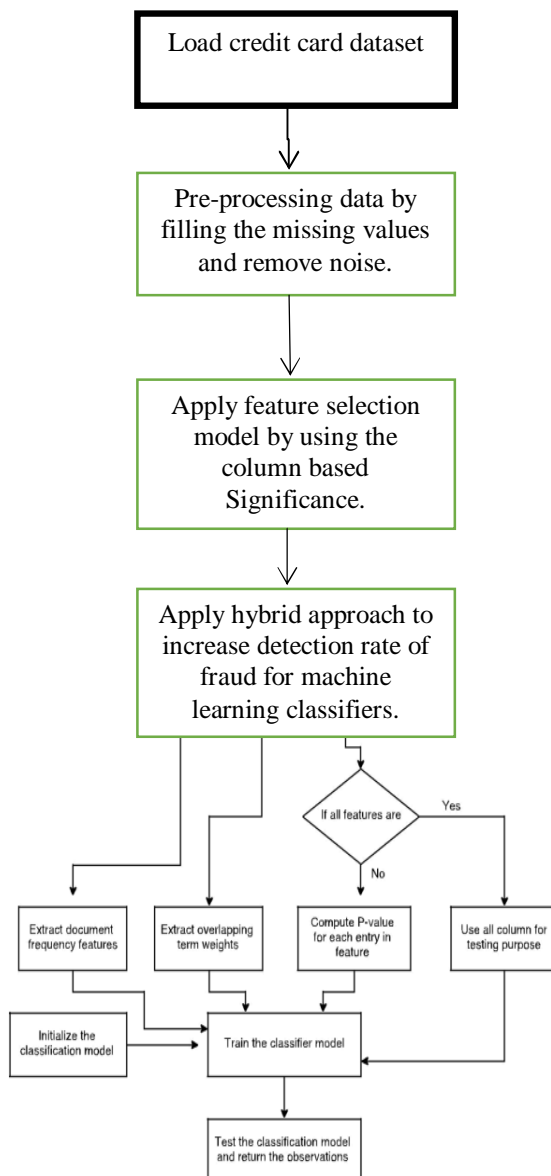
1) Gathering Historical data.
2) Data Formatting.
3) Define Parameters
4) Training Process and Trained Model
5) Forecasting Process
6) Image Transformation
7) Extract functions functionality

VI. CONCLUSION

The statistical models for credit card fraud detection have grown in popularity during the last decade. Such models are utilized in order to improve the pattern recognition process, that, in comparison to other methods, requires much less time and is capable of managing a significant number of transactions on a daily basis. Hybrid approaches, RF (Random Forests), DF (Decision trees), and other statistical models based on binary classification may increase the accuracy of credit card fraudulent pattern identification.

REFERENCES

[1] Chavan, J., 2013. Internet banking-benefits and challenges in anemerging economy. International Journal of Research in Business Management 1(1), pp.19-26.
[2] Al Hasib, A., 2009. Threats of online social networks. IJCSNS International Journal of Computer Science and NetworkSecurity,9(11), pp.288-93.
[3] Resnick, P. and Zeckhauser, R., 2002. Trust among strangers inInternet transactions: Empirical analysis of eBay's reputationsystem. InThe Economics of the Internet and E-commerce (pp.127-157). Emerald Group Publishing Limited.
[4] Franklin, J., Perrig, A., Paxson, V. and Savage, S., 2007,October. An inquiry into the nature and causes of the wealth ofinternet miscreants.In ACM conference on Computer andcommunications security (pp. 375-388).
[5] Özkan, S., Bindusara, G. and Hackney, R., 2010. Facilitating theadoption of e-payment systems: theoretical constructs andempirical analysis. Journal of enterprise informationmanagement,23(3), pp.305-325 International Journal of Computer Sciences and Engineering Vol.7(14), May2019, E-ISSN:2347-2693
[6] Minelli, M., Chambers, M. and Dhiraj, A., 2012. Big data, biganalytics: emerging business intelligence and analytic trends fortoday'sbusinesses.John Wiley & Sons.
[7] Davenport, T. and Harris, J., 2017.Competing on Analytics:Updated, with a New Introduction: The New Science of Winning.Harvard Business Press.
[8] Bhattacharyya, S., Jha, S., Tharakunnel, K., and Westland, J. C.(2011). Data burrowing for Mastercard deception: A close report.Decision Support Systems, 50(3), 602613. Elsevier B.V.
[9] Rahul Johari and shalinigupta" A New Framework for Credit CardTransactions including Mutual Authentication among CardholderandMerchan 978-0-7695-4437-3/11 $26.00 © 2011 IEEE DOI10.1109/CSNT.2011.12
[10] Mahmoud Reza Hashemi and Leila Seyedhossein" MiningInformation from Credit Card Time Series for Timelier FraudDetection" 978-1-4244-8185-9/10/$26.00 ©2010 IEEE

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089   (24*7 Support on Whatsapp)