WWW.IJRPR.COM

International Journal of Research Publication and Reviews

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

Credit Card Fraud Detection Using Machine Learning

Chaitra P C[1], N Sriniketh Sagar[2], V Sai Ganesh[2], Shahbaz Ali Mir[2]

[1]*Assistant professor, Computer Science Engineering, Dayanand Sagar Academy of Technology and Management, Bangalore, India*

[2]*UG student (VIIIth semester) Computer Science Engineering, Dayanand Sagar Academy of Technology and Management Bangalore, India*

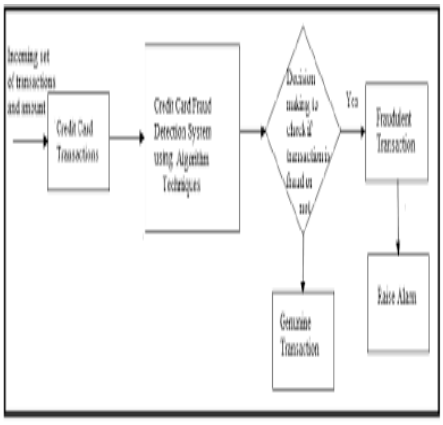
A B S T R A C T

Machine learning has been extensively used for fraud detection in recent years and has seen promising results. According to the Financial Industries, recent statistical methodologies are being used to solve the credit card fraud crisis. Our research offers a detailed guide to sensitivity analysis of current criteria in terms of credit card fraud detection results.. Unfortunately, due to privacy concerns, we may not be able to include the original functionality, but we will provide more context material. as well as to classify the most relevant variables that may contribute to increased accuracy in credit card fraud detection. We may also analyse and address the performance of various machine learning algorithms on the bank credit dataset, as well as describe the uncertainty matrix and scalar metrics, using the evaluation classification framework from Principal component analysis.

Keywords:. Credit Card Fraud; Data Mining; Naïve Bayes; Decision Tree; Logistic Regression, Comparative Analysis

1 INTRODUCTION

Since the beginning of my data science trip, I've been dreaming about how to use data science for good while still extracting value. As a result, when I came across this credit card fraud identification data collection on Kaggle, I was instantly hooked. There are 31 features in the data collection, 28 of which have been anonymized and numbered V1 to V28. The time and duration of the transaction, as well as whether or not the transaction was illegal, are the remaining three attributes. The anonymized variables had been updated in the form of a PCA before being submitted to Kaggle (Principal Component Analysis). Furthermore, the data collection had no missing values. Let's get started with some exploratory data processing now that we have this simple overview of the data.



1. Fig1. block diagram

2 SYSTEM DESIGN

Existing system:

The use of credit cards has risen steadily in the last decade, thanks to the growth in e-commerce. In 2011, there were around 320 million credit card purchases in Malaysia, which rose to around 360 million in 2015. The number of credit card fraud cases has steadily risen in tandem with the growth of credit card use. Despite the fact that various authorizing techniques have been implemented, credit card theft cases have not been successfully thwarted. Fraudsters use the internet because it conceals their identification and location. Credit card fraud is on the rise, and it's having a huge impact on the banking industry. In 2015, global credit card fraud totaled a whopping USD $21.84 billion. Merchants incur all risks associated with credit card theft, including card issuer fees, fines, and operating costs. Since retailers must take the loss, certain products are priced higher, and discounts and offers are limited. As a result, reducing the loss is critical, and having an efficient fraud prevention mechanism in place to minimise or remove fraud cases is critical. Several reports on credit card fraud prevention have been conducted. These techniques may be used on their own or in conjunction with others to create hybrid versions.

Proposed System:

Methods for detecting fraud in the credit card system that are easy. Different machine learning algorithms can be used in it, such as logistic regression, decision trees, and random forest, to make comparisons. Fraud detection methods have greatly advanced in recent years, and we have applied a number of machine learning algorithm techniques to speed up the fraud detection process. The fraud identification mechanism should be carried out mostly in the banking industry. We've enhanced some security features in this phase to reduce the time it takes to detect fraud. Finally, it displays "0" for fraudulent transactions and "1" for non-fraudulent transactions. As a result, we use machine learning algorithms to determine if the transaction operation is secure or not.

The method proposed in this paper employs the most up-to-date machine learning algorithms to identify anomalous behaviours known as outliers. The following is a representation of the basic rough architecture diagram

:

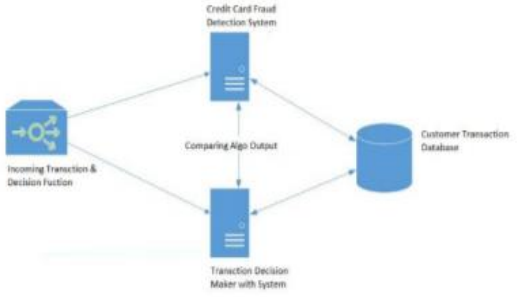


Fig.2 architecture diagram

The entire architecture diagram can be interpreted as follows when seen on a larger scale with real-life elements:

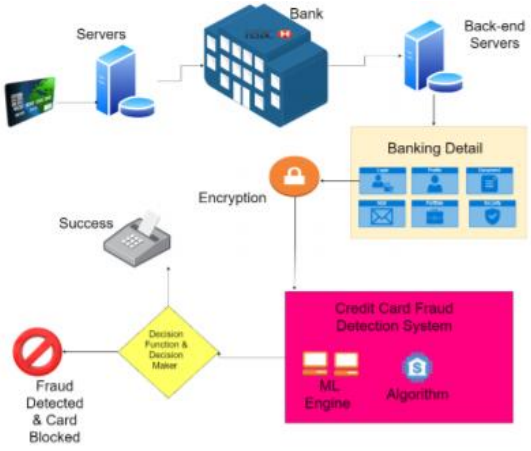


Fig.3

First and foremost, we got our data from Kaggle, a data discovery platform that offers datasets. There are 31 columns in this dataset, with 28 of them labelled v1-v28 to shield confidential information. Time, Number, and Class are represented by the other columns. The time difference between the first and subsequent transactions is seen in this graph. The amount of money exchanged is referred to as the amount.

3 RESULTS

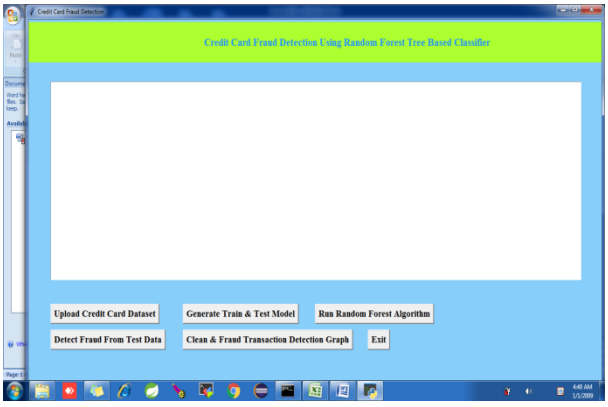


Fig 3 Loading data set

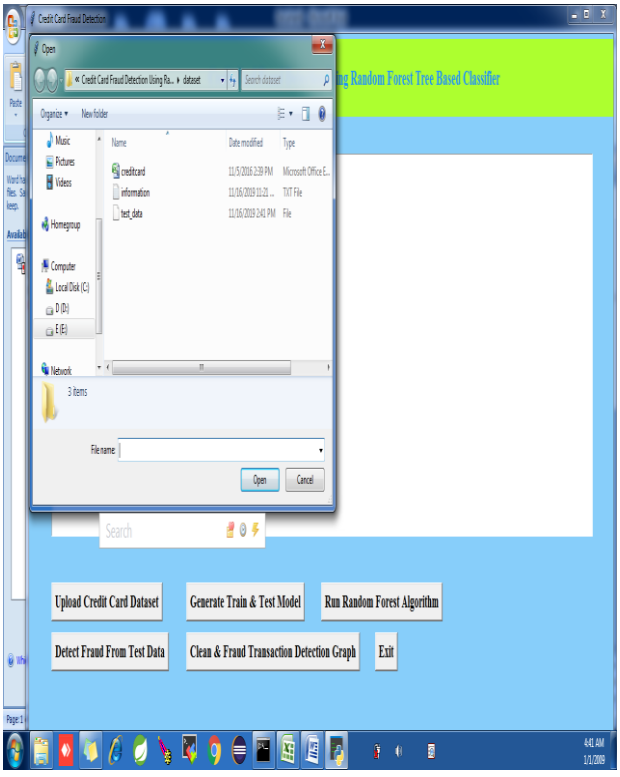


Fig 4. Selecting data set

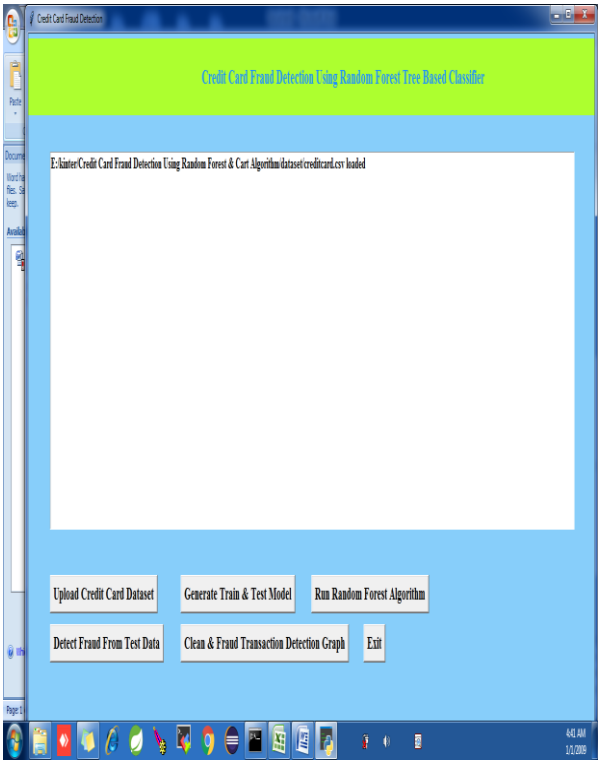


Fig 5. Data set loaded

Fig 6. Splitting data set into testing and training

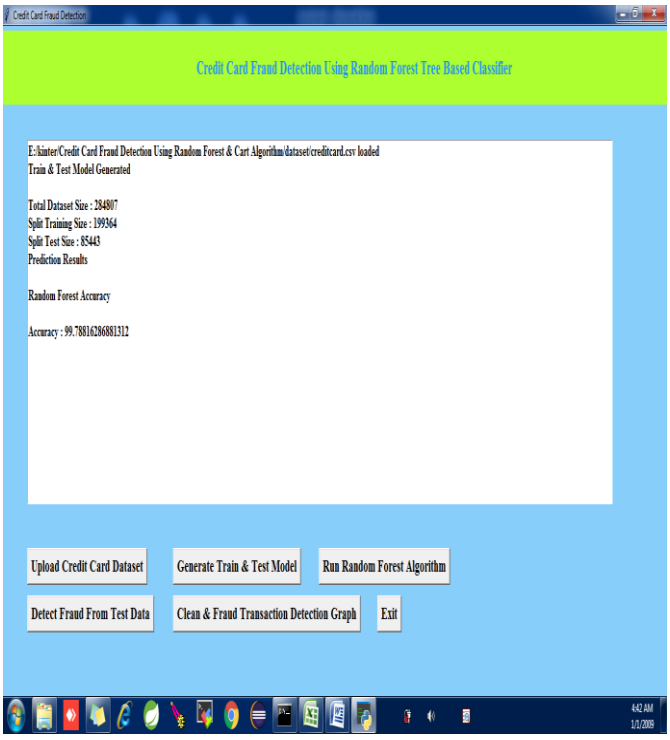


Fig 7. Random forest algorithm accuracy

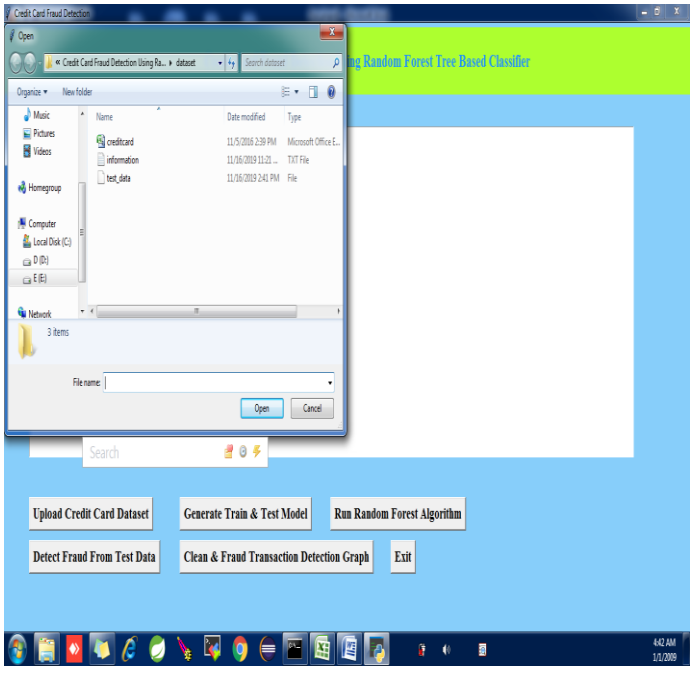


Fig.8 Loading test data

Fig 9. Results

Fig 10. results

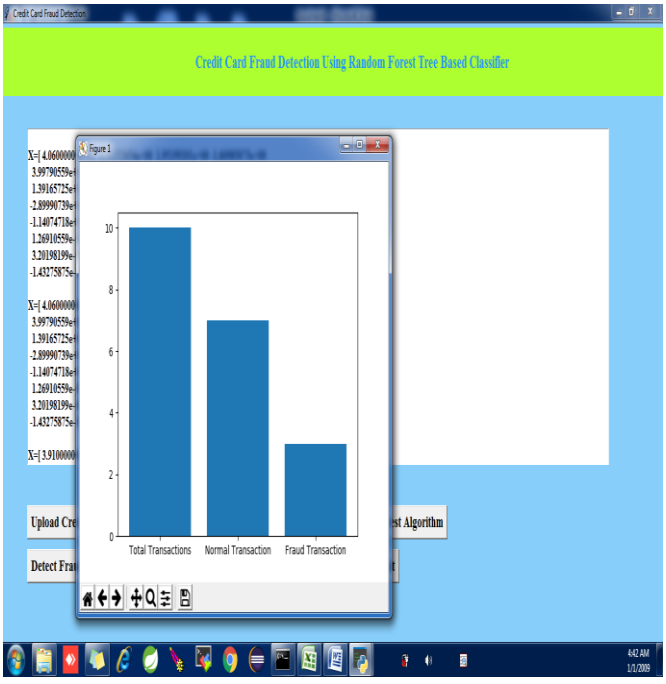


Fig 11. Total transactions, fraud, un fraud graph

4 CONCLUSION

Fraud detection methods have greatly advanced in recent years, and we have applied a number of machine learning algorithm techniques to speed up the fraud detection process. The fraud identification mechanism should be carried out mostly in the banking industry. We've enhanced some security features in this phase to reduce the time it takes to detect fraud. Finally, it displays "0" for fraudulent transactions and "1" for non-fraudulent transactions. As a result, we use machine learning algorithms to determine if the transaction operation is secure or not.

REFERENCES

[1] .CLIFTON PHUA1, VINCENT LEE1, KATE SMITH1 & ROSS GAYLER2 “Comprehensive Study of Data Fraud Detection Research” Published by School of Business Systems,

[2]College of Information Technology, Monash University, Wellington Road, Clayton State Road. Victoria 3800. Australia

[3] “Investigation Document of Sunan Credit Card Fraud” by GJUS & T Hisar HCE, Sonepat, published by International Journal of Advanced Research in Computer Engineering and Technology (IJH), Part 3, March 2014

[4] "Study on a Model for Detecting Credit Card Fraud Based on the Distance from Wen-Feng You and Nao Nao", published by the 2009 Joint International Conference on Artificial Intelligence.

[5] "Discovering Credit Card Fraud by Parenclitic Network Analysis - By Massimiliano Zanin, Love Miguel, Regino Criado and Santiago Moral" Published by Hihihi Complex Complex 2018 ID Article 5764370 Page 9

[6] "Credit Card Fraud Detection: Demonstration and New Learning Strategies" published by IEEE TRANSACTIONS on Nettle and Learning System. 29, no. August 8, 2018

[7] "Credit Card Fraud Detection - By Ishu Trivedi, Monica, Mrigya, Mridushi," published by the International Journal of Advanced Research in Computer Engineering and Numerical Communications. 5, Issue 1, January 2016

[8] David J. Wetson, David J., D.M., Ed Witt, and Petho Yuschak, “Detecting Plastic Card Fraud Using Group Analysis,” Spring 2008