

Plagiarism Scan Report

Report Generated on: Jun 11,2023

<div><div>0%</div><div>Plagiarised</div></div>	<div><div>100%</div><div>Unique</div></div>	<div><div>Total Words:941</div><div>Total Characters:8074</div><div>Plagiarized Sentences:0</div><div>Unique Sentences:44 (100%)</div></div>
--	---	--

Content Checked for Plagiarism

Credit Card Fraud Detection Using

Machine Learning & Python

AUTHORS :

Mr. Samprit Ghosh & Mr. Koushik Nath

TECHNO INTERNATIONAL NEWTOWN, ELECTRONICS & COMMUNICATION ENGINEERING , WEST .
BENGAL, INDIA .

ABSTRACT

In recent years, credit cards have taken on important roles in people's lives. The danger of fraud has increased as a result of the unexpected boom in e-commerce and the widespread usage of credit cards for online purchases. Instead than carrying around a lot of cash, it is easier to keep credit cards on hand. But that's also dangerous now. A serious problem that is now on the increase dramatically is credit card fraud.

Keywords: Automated fraud detection, isolation forest method, local outlier factor, applications of machine learning, and data science.

I. INTRODUCTION

As we can see, there has been a substantial rise in online payments over the past several years, and for the majority of them, credit cards are the preferred payment option. For marketing companies, credit card fraud is a serious barrier. A range of actions, such as paying taxes on another account, applying for loans using false information, and more, can be used to perpetrate fraudulent fraud. Therefore, we require an efficient fraudulent detection model in order to decrease fraudulent behaviour and their losses.

Methods for detecting fraud are always being improved to prevent criminals from altering their fraudulent tactics. These scams are categorised as:

- * Online and offline
- * credit card fraud
- * Card theft
- * account bankruptcy
- * device intrusion app fraud
- * counterfeit cards and telecom fraud are only a few examples of fraud.

Some of the methods currently employed to identify such fraud include:

- * Support Vector Machines
- * Bayesian Networks
- * Hidden Markov Model

- * Genetic Algorithm
- * Fuzzy Logic
- * Logistic Regression
- * Decision Tree
- * Artificial Neural Network
- * K-Nearest Neighbour

II. LITERATURE REVIEW

Fraud is defined as an illegal or criminal deception meant to produce a monetary or personal profit. It is an intentional action that violates a rule, legislation, or policy with the intention of obtaining overlooked pecuniary benefit. A lot of publicly available information has previously been published in this sector on the subject of anomaly or fraud detection.

III. METHODOLOGY

The method this study suggests makes advantage of the most recent machine learning techniques to identify outliers, or unusual activities. The following image can be used to illustrate the fundamental rough architecture diagram:

Data is processed by a collection of modules' algorithms. The module diagram below depicts how these algorithms interact with one another: Once the data has been fitted into a model, the following outlier identification modules are applied to the data:

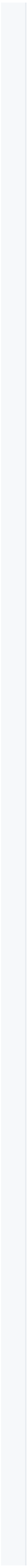
Isolation Forest Algorithm with Local Outlier Factor.

IV. WORKING OF OUR MODEL

It is difficult to put this idea into effect since it requires the cooperation of banks, which are wary of sharing information owing to market competitiveness, legal reasons, and the protection of their users' data. We looked for several reference works that employed similar methods in order to gather information. One of these reference papers states: According to one of these reference publications, a sizable application data set provided by a German bank in 2006 was exposed to this method.

V. RESULTS AND DISCUSSION

The code displays the results after comparing the true numbers to the amount of false positives it discovered. This is used to evaluate the algorithms' precision and accuracy. 10% of the entire dataset was made up of the dataset component we selected for quicker testing .The subset of the dataset we utilised for expedited testing was 10% of the overall dataset. At the end, which also takes use of the complete dataset, both outcomes are presented. Class 0 indicates that the transaction was determined to be genuine, while class 1 indicates that the transaction was determined to be fraudulent in the output shown below. These results are also provided together with the categorization report for each technique. This result was compared to the class values in order to exclude any potential false positives. As a result of using 10% of the data, we find:



VI. CONCLUSION

It goes without saying that using a credit card fraudulently is a crime. This page lists the most common fraud schemes and describes how to recognise them. It also highlights current academic work in the field. Along with the strategy, this study has provided a thorough description of how machine learning may be applied to improve fraud detection. Even though the method is over 99.6% accurate, its precision is still just 28% when only a tenth of the data set is taken into account. When the system is fed the entire dataset, the accuracy rises to 33%. Given the enormous difference in the quantity of legitimate, it is reasonable to expect such a high accuracy rate.

VII. FUTURE ENHANCEMENTS

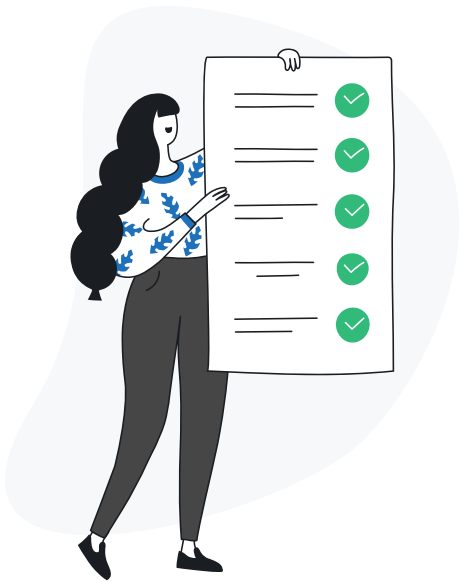
While we were unable to achieve our original aim of 100% accuracy in fraud detection, we did manage to develop a system that can, given enough time and data, come very near to it. As with any attempt of this kind, there is room for improvement here. The project's structure makes it feasible to integrate several algorithms as modules and combine their outputs to increase the accuracy of the final result.

REFERENCES

[2] KATE SMITH¹, VINCENT LEE¹, CLIFTON PHUA¹, and ROSS GAYLER² School of Business Systems, Faculty's "A Comprehensive Survey of Data Mining-based Fraud Detection Research"

Monash University, Wellington Road, Clayton, Victoria 3800, Australia, Department of Information Technology

[3] Researcher, GJUS&T Hisar HCE, Sonepat published "Survey Paper on Credit Card Fraud Detection by Suman" in International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), Volume 3 Issue 3, March 2014.



No Plagiarism Found