International Journal of Scientific Research in Science, Engineering and Technology

Print ISSN - 2395-1990
Online ISSN : 2394-4099

OPEN ACCESS

Available Online at : www.ijsrset.com
doi : https://doi.org/10.32628/IJSRSET

Credit Card Fraud Detection Using Machine Learning

Prof. Sonali Dongare, Sakshi Salunke, Kishori Shinde, Sanika Thorat, Vaishnavi Shinde, Nitin Dhawas
Information Technology, Nutan Maharashtra Institute of Engineering and Technology Talegaon Dabhade, India

ARTICLEINFO

Article History :

Accepted: 10 Nov 2023
Published: 30 Nov 2023

Publication Issue :
Volume 10, Issue 6
November-December-2023
Page Number :
247-252

ABSTRACT

These days, credit card transactions and associated frauds are widespread occurrences. The most popular method of fraud is obtaining credit card information unlawfully and using it to make online purchases. It is extremely difficult for credit card companies and retailers to identify these fraudulent transactions amidst the many legitimate transactions. Device mastering methods could be used to solve this issue if sufficient data is acquired and made public. Popular supervised and unsupervised device learning techniques were used in this study to identify credit card fraud in a dataset that was incredibly unbalanced. Unsupervised machine learning algorithms were discovered to be capable of handling the skewness and give nice classification results.

Keywords :– credit card fraud, credit card detection, machine learning, supervised learning

I. INTRODUCTION

Ever since its inception, e-commerce has advanced significantly. For the majority of organizations, companies, and governmental bodies, it is now an essential tool for increasing the productivity of international trade. One of the main factors contributing to e-success is simple credit card transactions done online. The commercial We also need to take financial fraud into account when it comes to financial transactions. Financial fraud is a deliberate crime in which the offender benefits financially or by denying a victim's rights. Fraud has increased significantly as a result of credit card transactions becoming the most common form of payment in recent years. A significant issue facing businesses and government organizations is the substantial financial losses brought on by fraud. The massive yearly losses that card issuers suffer as the substantial yearly losses that credit card issuers suffer as a result of credit card fraud. In recent years, credit cards have become a widely used payment method for goods and services purchased online. Since then, in an effort to complete their own payment, scammers have tried to mimic normal user behavior. Most of the research on credit card fraud detection has focused on these problems because of them.

II. Literature Survey

[1] Credit Card Fraud Identification Using Machine Learning Approaches
Author: Pawan Kumar, Fahad Iqbal

Description: Online shopping has become an essential component of everyone's lives due to the internet's explosive expansion. When making online purchases, MasterCard is typically used as payment. People only need to search for your visual display unit or a smartphone to locate the thing they want. MasterCard will become the payment method of choice for many online transactions, however there are still some vulnerabilities in the system that allow for credit card fraud or online fraud. Consequently, in order to lower their losses, every MasterCard supply bank required fraud detection systems.

[2] A Deep Neural Network Algorithm for Detecting Credit Card Fraud
Author: Xiaohan Yu, Xianwei Li, Yiyang Dong, Ruizhe Zheng
Description: The credit card is easy to use for shopping and internet purchases. Conversely, credit card theft happens daily throughout the world and is challenging to identify by human means. Several organizations, including banks, information companies, and even the government, had to spend billions of dollars to create an automated fraud detection system. In this study, we suggest a deep network- based fraud detection method. Any problems with data skew in the dataset are addressed by the log transform. The network is trained using focus loss in order to handle difficult scenarios. The results show that our neural network model outperforms other industry standard models such as logistic regression and support vector machine.

[3] Comprehensive Analysis for Fraud Detection of Credit Card through Machine Learning
Author: Parth Roy, Prateek Rao, Jay Gajre, Yogesh Gajmal, Arvind Jagtap, Kanchan Katake
Description: Cashless transactions are possible with a credit card, which is still a commonly used payment method that may be used both online and offline. It's an easy, popular, and straightforward method of conducting business and making payments. These developments have led to an increase in credit card fraud. The cumulative effect of financial dishonesty is substantial in the worldwide statement enhancement. Billions have been lost as a result of these lies. These are performed with such elegance that they seem like real business dealings. Simple design methods and other less complex approaches will therefore become ineffectual. All banks now need to have a well-organized fraud detection mechanism in place in order to minimize turmoil and bring order back. [4] Credit Card Fraud Detection Using Machine Learning
Author: D. Tanouz, R Raja Subramanian, D. Eswar, G V Parameswara Reddy, A. Ranjith kumar, CH V N M praneeth
Description: In recent years, credit cards have become the most popular method of payment. As technology advances, the number of fraud instances grows, necessitating the development of a fraud detection algorithm capable of properly detecting and eliminating fraudulent actions. For managing the extremely imbalanced dataset, this research provides multiple machine learning-based classification techniques such as logistic regression, random forest, and Naive Bayes.

[5] Relative Analysis of ML Algorithm QDA, LR and SVM for Credit Card Fraud Detection Dataset
Author: P Naveen, Dr B Diwan
Description: The intention is to stop credit card companies from having to reimburse customers for purchases they did not make by identifying fraudulent online transactions. The accuracy of fraud detections varied depending on the data and model architecture, and a number of machine learning techniques were employed. This research evaluated and preprocessed data sources and may have developed many feature extraction algorithms, including Support Vector Machine (SVM), Logistic Regression (LR), and Quadratic Discriminant Analysis (QDA).

[6] An Intelligent Approach to Credit Card Fraud Detection Using an Optimized Light Gradient Boosting Machine

Author: Altyeb Altaher Taha, Sharaf Jameel Malebary
Decription: Due to recent developments in communication and electronic commerce systems, credit cards are now possibly the most widely used payment mechanism for both in-person and online purchases. As a result, there is a markedly higher risk of fraud in these types of transactions. Every year, fraudulent credit card transactions cause significant financial losses for both businesses and consumers, and con artists are always looking for new tools and ways to commit fraud. One major element influencing the increased use of electronic payments is the detection of fraudulent transactions. As a result, reliable and efficient methods for identifying fraud in credit card transactions are required. This research presents an intelligent method that makes use of an optimized light gradient boosting machine (OLightGBM) to detect fraud in credit card transactions. The suggested method uses a Bayesian-based [7]Fraud detectio in credit card transaction using machine learning techniques A light gradient boosting machine's (LightGBM) parameters are intelligently tuned by the integration of a hyperparameter optimization algorithm. Experiments were conducted utilizing two real-world public credit card transaction data sets, one of which included fraudulent transactions, in order to illustrate the efficacy of our proposed OLightGBM for identifying fraud in credit card transactions. The proposed approach outperformed the other approaches and achieved the highest performance in terms of accuracy (98.40%), precision (97.34%), area under the receiver operating characteristic curve (AUC) (92.88%), and F1-score (56.95%) based on a comparison with other approaches using the two data sets.

Author: Imane Sadgali, Nawal Sael, Fouzia Benabbou
Description: These days, credit card transactions are becoming more and more common. For the majority of cardholders, using your credit card for online purchases, as a mobile wallet, or just to make a small payment to a retailer has become second nature. The modern technology environment and virtual world have led to the digitization of banking transactions. Millions of online transactions are hence vulnerable to many kinds of fraud. Sophisticated fraudulent practices are invisible to conventional fraud detection methods. To be restricted to a study of the cardholder behavior's, or to static rules of risk management of the frauds, had never stopped the fraudulent to perform their crimes. However, as we can see from the literature [1], machine-learning algorithms have been able to address this need. In this work, We will compare a few machine learning methods that, when used on the identical set of data, produced the greatest outcomes, based on our state of the art [1]. Selecting the most effective credit card fraud detection methods to use in our next work is the goal of this study.

[8] Credit Card Fraud Detection Using Machine Learning Author: John Richard D. Kho Larry A. Vea
The old Magnetic stripe card technology caused a difficulty that was mostly remedied by the credit card industry's adoption of the EMV (Europay-MasterCard-VISA) chip card design. Nonetheless, a number of articles are beginning to challenge the EMV's conception and execution. In the event that the system fails, this study suggests having a detection model available to catch potentially abnormal transactions. During the model development process, a number of classifiers were investigated; however, only the Random Tree and J48 produced the highest accuracy values, 94.32% and 93.50%, respectively. A further examination of these two (2) classifiers reveals that the J48 is better suited to comprehend the data from the transaction logs.

Data Set and Data Preprocessing
We utilize two separate real-world data sets to design several experiments for assessing the proposed method and proving its generality.
284,807 credit card transactions conducted by credit card holders in Europe in September 2013 make up the first data set. 492 out of the 284,807 transactions in the data set were fraudulent; these fraudulent transactions, or the positive class, make up 0.172% of all transactions

[22]. There are 31 features in the data collection. main components analysis (PCA) yielded the main components, or the first 28 features (V1 to V28). Preserving data privacy is the major justification. The only two features that are not altered by PCA are "Time" and "Amount."

The second data set is an actual set of e-commerce transactions called the UCSD-FICO Data Mining Contest 2009 Dataset [39]. Finding unusual e-commerce transactions was the goal. 2,094 of the 94,683 transactions in the data set are fake. Over the course of 98 days, 73,729 credit cards provided the data set. The following fields have labels: amount, hour1, state1, zip1, custAttr1, field1, custAttr2, field2, hour2, flag1, total, field3, field4, indicator1, indicator2, flag2, flag3, flag4, flag5, and Class. There are 20 fields altogether, including class. The classification variable, which is 1 in the event of credit card fraud and 0 otherwise, is the Class feature in the two data sets. Table 1 provides a summary of the data The overall number of transactions, the number of authorised, the number of fraudulent, the number of features in the data set, and the download links for each data setdisplayed.sets.

Dataset	Total No. of transactions	No. of legitimate transactions	No. of fraudulent transactions	No. of Features	Ref.
Data set 1	284,807	284,315	492	31	[22]
Data set 2	94,683	92,589	2,094	20	[39]

• Existing System And Disadvantages

Credit card payments are becoming more and more common when making purchases online for products and services. Since then, scammers have attempted to deceitfully mimic typical user behavior in order to complete their own payment. The majority of studies on credit card fraud detection have concentrated on these issues. Modeling previous credit card transactions with the information of the one that turned out to be fraudulent is one aspect of the credit card fraud detection challenge. Then, a new transaction's likelihood of being fraudulent is determined using this model. Compared to a classification task, fraud detection systems are different because in the current system, human investigators only supply a small set of supervised samples and evaluate a small number of alarms. Additionally, labels are accessible for the majority of transactions. only a few days after clients reported fraudulent transactions.

Disadvantages:

False Positives: Overly sensitive fraud detection systems have the potential to produce false positives, which could cause legitimate cardholders' transactions to be mistakenly detected and so cause trouble.

Complexity and Cost: Sophisticated fraud detection system implementation and upkeep can be costly, requiring ongoing updates and investments in both technology and human resources.

Privacy Issues: Since sophisticated fraud detection techniques frequently entail intensive data monitoring, people may feel that their personal information is being examined unduly.

Adaptability Challenges: Since fraudsters are always changing their strategies, fraud detection systems may find it difficult to keep up, which can leave gaps in defense and make people more vulnerable.

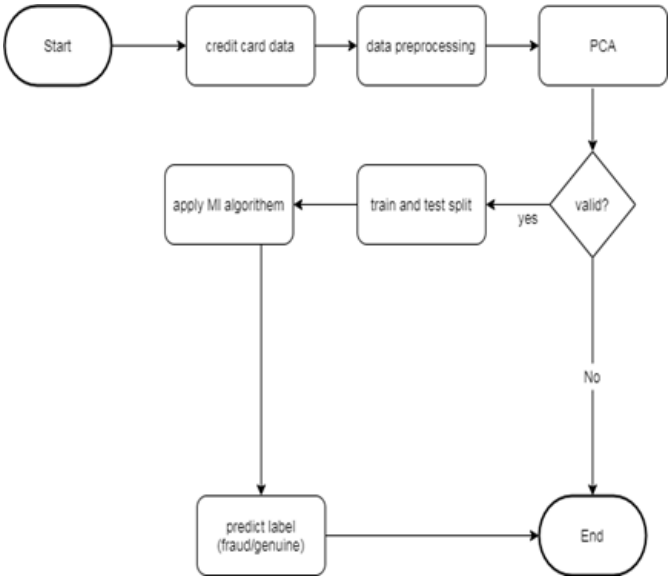

Fig: System Architecture

Demonstrates the credit card fraud detection system's system architecture. There are primarily five levels of

control in the fraud detection system shown in the above design. The terminal layer, which is the first layer, verifies the security of each transaction. Whenever a transaction is initialized, this layer is used. This layer performs security checks such as accurate PIN code, number of attempts, valid username, available balance, and credit card validity. The transaction will proceed if all valid checks are checked; if not, it will be rejected. The restrictions that are established for secure transactions are then known as transaction blocking rules. Instead of looking up past transactions or cardholder profiles, these regulations make use of the limited data that is available at the time the payment is requested. In the event that transactions made online lead to credit card fraud. The purpose of transaction blocking rules is to prevent the blockage of several legitimate transactions while ensuring real-time operations. As if-then statements, scoring rules are expert-driven models as well. If a transaction was completed less than an hour ago and on a separate continent, the fraud score would be 0.95. This is an example of a scoring rule. Because scoring rules can vary in design, they may be arbitrary. A classifier or similar statistical model is used by the Data Driven Model (DDM), which is solely data driven, to evaluate the likelihood that each vector is a fraud. It is anticipated that this layer would reveal false patterns. Just a small percentage of transactions were informed. activities and this task is performed by investigators. Using this system architecture, transaction is detected as fraud or normal. As the last line of defense, only a small percentage of detected transactions are reported to the investigators. Professionals with knowledge in credit card transaction analysis, investigators are in charge of the expert-driven layers of the fraud detection system. To stop more fraudulent activity, every card that is discovered to have been the victim of fraud is banned right away.

Advantages:

1). Allows cross platform compatibility.

2). Easy Implementation.

3). Distributed Architecture.

4). Increases performance rate.

5). Achieve optimized results.

III. Conclusion And Future Work

We formalize a practical FDS framework that satisfies practical requirements. When training an FDS, delayed samples should be handled individually because there is a strong alert-feedback connection that needs to be explicitly taken into account in real-world scenarios. In idea drifting situations, aggregating two different classifiers is a useful tactic that allows a promoter adaptability. The suggested learning technique relies heavily on feedbacks. It involves training a classifier on feedbacks independently from a classifier on delayed supervised samples, and then combining their posteriors to find alerts.

The results produced here might not apply to the worldwide fraud detection issue. Future research should focus on developing an efficient algorithm that can handle the classification problem with variable misclassification costs.

IV. REFERENCES

[1]. Jain R., Gour B., Dubey S., A hybrid approach for credit card fraud detection using rough set and decision tree technique, International Journal of Computer Applications 139(10) (2016).

[2]. Dermala N., Agrawal A.N., Credit card fraud detection using SVM and Reduction of false alarms, International Journal of Innovations in Engineering and Technology (IJIET) 7(2) (2016).

[3]. Phua C., Lee V., Smith, Gayler K.R., A comprehensive survey of data mining-based fraud detection research. arXiv preprint arXiv:1009.6119 (2010).

[4]. Bahnsen A.C., Stojanovic A., Aouada D., Ottersten B., Cost sensitive credit card fraud detection using Bayes minimum risk. 12th

International Conference on Machine Learning and Applications (ICMLA) (2013), 333-338.

[5]. Carneiro E.M., Dias L.A.V., Da Cunha A.M., Mialaret L.F.S., Cluster analysis and artificial neural networks: A case study in credit card fraud detection, 12th International Conference on Information Technology-New Generations (2015), 122-126.

[6]. Hafiz K.T., Aghili S., Zavarsky P., The use of predictive analytics technology to detect credit card fraud in Canada, 11th Iberian Conference on Information Systems and Technologies (CISTI) (2016), 1-6.

[7]. Sonepat H.C.E., Bansal M., Survey Paper on Credit Card Fraud Detection, International Journal of Advanced Research in Computer Engineering & Technology 3(3) (2014). VarrePerantalu K., BhargavKiran, Credit card Fraud Detection using Predictive Modelling (2014).

[8]. Kokane, Chandrakant D., and Sachin D. Babar. "Supervised word sense disambiguation with recurrent neural network model." Int. J. Eng. Adv. Technol.(IJEAT) 9.2 (2019).

[9]. Kokane, Chandrakant D., Sachin D. Babar, and Parikshit N. Mahalle. "Word Sense Disambiguation for Large Documents Using Neural Network Model." 2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT). IEEE, 2021.

[10]. Kokane, Chandrakant, et al. "Word Sense Disambiguation: A Supervised Semantic Similarity based Complex Network Approach." International Journal of Intelligent Systems and Applications in Engineering 10.1s (2022): 90-94.

[11]. Kokane, Chandrakant D., et al. "Machine Learning Approach for Intelligent Transport System in IOV-Based Vehicular Network Traffic for Smart Cities." International Journal of Intelligent Systems and Applications in Engineering 11.11s (2023): 06-16.

[12]. Kokane, Chandrakant D., et al. "Word Sense Disambiguation: Adaptive Word Embedding with Adaptive-Lexical Resource." International Conference on Data Analytics and Insights. Singapore: Springer Nature Singapore, 2023.

Cite this article as :

Prof. Sonali Dongare, Sakshi Salunke, Kishori Shinde, Sanika Thorat, Vaishnavi Shinde, Nitin Dhawas, "Credit Card Fraud Detection Using Machine Learning", International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Online ISSN : 2394-4099, Print ISSN : 2395-1990, Volume 10 Issue 6, pp. 247-252, November-December 2023.

Journal URL : https://ijsrset.com/IJSRSET2310620