



IJIRCCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 11, Issue 3, March 2023

ISSN INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

Impact Factor: 8.379



9940 572 462



6381 907 438



ijircce@gmail.com



www.ijircce.com

Credit Card Fraud Detection

Mrs. Hemlata Bhandare¹, Snehal Labture², Ruksana Ansari², Shital Pawar², Sanika Kshirsagar²

Lecturer, Department of Computer Engineering, JSPM's Rajarshi Shahu College of Engineering, Polytechnic,
Tathawade, India¹

Student, Department of Computer Engineering, JSPM's Rajarshi Shahu College of Engineering, Polytechnic,
Tathawade, India²

ABSTRACT: - The usage of credit cards for online and regular purchases is exponentially increasing and so is the fraud related with it. A large number of fraud transactions are made every day. Various modern techniques like artificial neural network Different machine learning algorithms are compared, including Logistic Regression, Decision Trees, Random Forest, Artificial Neural Networks, Logistic Regression, K-Nearest Neighbors, and K-means clustering etc. are used in detecting fraudulent transactions. This paper uses genetic algorithm, and neural network which comprises of techniques for finding optimal solution for the problem and implicitly generating the result of the fraudelIntransaction.The main goal is to develop methods to detectfraudulent transactions and generate test data. This algorithm is a heuristic approach used to solve highly complex computational problems. Implementing an effective fraud detection system is essential for all credit card companies and their customers to minimize losses.

KEYWORDS: logistic regression, decision trees, random forests, artificial neural networks, logistic regression, K-nearest neighbors

I. INTRODUCTION

Today, card information is read by ATMs, store readers, banks, and is also used in online banking systems. They have a unique card number which is most important. Security depends on the physical security of the plastic card and the confidentiality of the credit card number. The dramatic increase in the number of credit card transactions has led to a significant increase in fraudulent activity. Credit card fraud is a broad term for theft and fraud perpetrated by using a credit card as a source of fraudulent funds in certain transactions.In general, most credit card fraud detection systems are based on artificial intelligence, meta-learning, and pattern matching

II. LITERATURE SURVEY

Samidha Khatri et al. (2020) A person's credit card information can be fraudulently obtained and used for fraudulent transactions. To address this problem, specific machine learning algorithms can be used to collect data.This study compares three well-known supervised learning methods to discriminate between legitimate and fraudulent transactions. Provides precision and sensitivity.

S. P. Maniraj et al. (2019) focused on the application of various anomaly detection methods, such as evaluation and preprocessing of datasets, local outlier factors, and isolated forest algorithms, for credit card transaction data converted to PCA.

b.Sellam et al. (2021) To deal with highly imbalanced datasets, this study proposes various machine learning-based classification methods such as logistic regression, random forest, and naive Bayes. Finally, accuracy, precision, recall, f1 score, confusion matrix, and Roc-AUC score are evaluated in this study. Anuruddha Tennakun et al. (2019) In this article, the authors use real-time data and predictive analytics performed by ML models and API modules to determine whether a transaction is fraudulent or not. We'll also look at a new way to deal with uneven data distribution. Under a Confidential Information Agreement, the data used in this study were provided by financial institutions. Ruttala Saylyusha et al. (2020) This study focused on the Random Forest Algorithm, and the Adaboost algorithm was used. Compare the results using precision, accuracy, recall, and F1 score of thetwo algorithms.

C. The confusion matrix is used to plot the ROC curve. Dejan Varmeja et al. (2019) This study used the credit card fraud detection dataset. Because the data set was highly imbalanced, it was resampled using the SMOTE method. The data set is divided into two parts: training data and test data.

In this study, the authors used logistic regression, random forest, naive Bayes algorithm, and multi-layer perceptron. Results show that each algorithm can accurately detect credit card fraud.

D. Tanuz et al. (2021) Create and analyze graphs, commonly referred to as plots. Then, three machine learning algorithms are used: lightweight GBM, Adaboost, and random forest classifier to determine model recall, accuracy, and accuracy. There is also a function to calculate the time required to run various algorithms. Finally, the values generated by these three algorithms are compared to determine which one gives the best results.

Saurabh Arora et al. (2021) They evaluate the dataset in this study, then select features and apply various machine learning techniques.

Hassan I. and Rizvi S. (2022) In this paper, the authors review several artificial intelligence and machine learning techniques to reduce fraud detection. They analyze and provide advantages for several methods for research work

III. OBJECTIVE

The goal of this project is to implement a machine learning algorithm to detect credit card fraud in terms of transaction time and amount. The core task of any credit card fraud detection system is to identify suspicious events and report them to analysts. Useful for both banks and cardholders.

IV. METHODOLOGY

We propose a machine learning model for detecting credit card fraud in online financial transactions. Due to the huge amount of data and its complexity, manual analysis of fake transactions is impossible. However, machine learning can be used to do this, given the informational capabilities properly. This hypothesis is investigated in the project. Classify fraudulent and legitimate credit card transactions using supervised learning algorithms such as random forests. To help you get information about scams without losing money.

V. PACKAGES

Used for data mining, specialized processing, and random forest usage:

- NumPy: for simple arrays.
- Pandas: Reading files.
- SciKit: Learn - for preprocessing.
- Matplotlib or Seaborn: for plotting and representing confusion matrix color formats.
- Tensorflow: for matrix format.

VI. SYSTEM ARCHITECTURE

Step 1: Read the dataset.

Step 2: Random Sampling is done on the data set to make it balanced.

Step 3: Divide the dataset into two parts i.e., Train dataset and Test dataset.

Step 4: Feature selection are applied for the proposed models.

Step 5: Accuracy and performance metrics has been calculated to know the efficiency for different algorithms.

Step 6: Then retrieve the best algorithm based on efficiency for the given dataset.

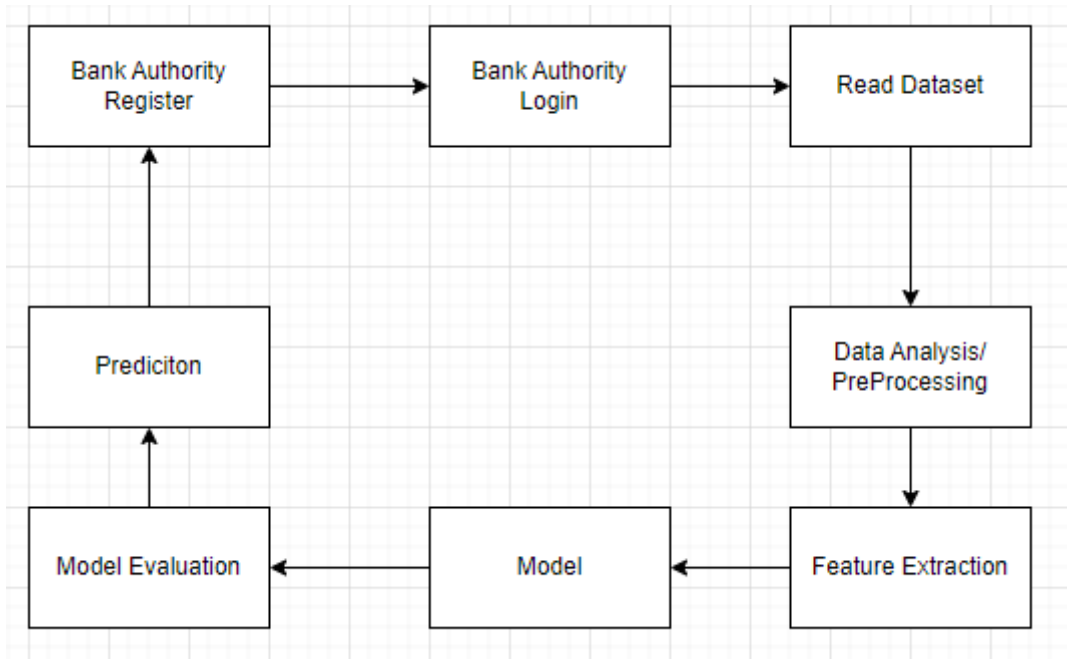


Fig 1. Architecture Diagram

VI. CONCLUSION & FUTURE SCOPE

In the future enhancement of this project, We will give a solution after the prediction of fraud transaction classifies what can we do further. We also go with real-time data or make real-time fraud detection systems as well. We can also use the deep learning method for better results. We can build an app as well as a website also who detects fraud transactions in real-time. From the literature, they used an imbalanced dataset to check the accuracy, precision and recall of different machine learning algorithms to predict the fraudulent transaction. But we will use sampling techniques to the balanced dataset. For an imbalanced dataset we can't rely on the accuracy, we have to see precision, recall, F1-score, and roc-AUC curve, etc. From this evaluation, we can easily see which model works best on the imbalanced dataset as well as a balanced dataset.

REFERENCES

- 1] K. Sim, V. Gopalkrishnan, A. Zimek, and G. Cong - "A survey on enhanced subspace clustering," Data Mining Knowledge Discovery, vol. 26, no. 2, pp. 332–397, 2019.
- 2] S. Mckimming- "Trade-based money laundering: Responding to an emerging threat," Deakin Law Rev, vol. 15, no. 1, 2020.
- 3] Nitu Kumari, S. Kannan and A. Muthukumaravel - "Credit Card Fraud Detection Using Genetic-A Survey" published by MiddleEast Journal of Scientific Research , IDOSI Publications, 2014
- 4] Satvik Vats, Surya Kant Dubey, Naveen Kumar Pandey - "A Tool for Effective Detection of Fraud in Credit Card System", published in International Journal of Communication Network Security ISSN: 2231 – 1882, Volume-2
- 5] S.H. Projects and W. Lovo , —JMU Scholarly Commons Detecting credit card fraud : An analysis of fraud detection techniques, | 2020. [2] S. G and J. R. R, —A Study on Credit Card Fraud Detection using Data Mining Techniques, | Int. J. Data Min. Tech. Appl., vol. 7, no. 1, pp. 21–24, 2018, doi: 10.20894/ijdmta.102.007.001.004
- 6] V. N. Dornadula and S. Geetha —Credit Card Fraud Detection using Machine Learning Algorithms, Procedia Comput. Sci., vol. 165, pp. 631–641, 2019, doi: 10.1016/j.procs.2020.01.057.
- 7] A. H. Alhazmi and N. Aljehane - A Survey of Credit Card Fraud Detection Use Machine Learning, 2020 Int. Conf. Computes. Inf. Technol. ICCIT 2020, pp. 10–15, 2020, doi: 10.1109/ICCIT-144147971.2020.9213809
- 8] M. Kanchana, V. Chadda , and H. Jain - Credit card fraud detection, | Int. J. Adv. Sci. Technol., vol. 29, no. 6, pp. 2201–2215, 2020, doi: 10.17148/ijarccce.2016.5109.



INNO  SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.165

 **doi**[®]
cross **ref**

ISSN INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

 9940 572 462  6381 907 438  ijircce@gmail.com



www.ijircce.com

Scan to save the contact details