iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** IV **Month of publication:** April 2023

DOI: https://doi.org/10.22214/ijraset.2023.51243

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue IV Apr 2023- Available at www.ijraset.com

Counterfeit Diagnosis Using Artificial Neural Network

Karnaram Patel[1], Rutul Waradkar[2], Amaan Shaikh[3], Nirmal Nemade[4], Ms. Smita Bansod[5]
[1, 2, 3, 4]*B.E. Student, Department of Information Technology, Shah & Anchor Engineering College, Mumbai, Maharashtra, India*
[5]*Asst. Professor, Department of Information Technology, Shah & Anchor Kutcchi Engineering College, Mumbai, Maharashtra, India*

Abstract: ***One of the best payment methods that clients may use to conduct transactions effortlessly and boost their purchasing power is a credit card. In addition, it is incredibly simple to use and provides a number of benefits, like cashback and reward points. However, the primary issue is credit card fraud, which is fast rising every day. The most common type of identity theft worldwide is still credit card fraud. The use of credit cards has grown too dangerous in recent years. In reality, there are many other kinds of credit card fraud, including phishing and vishing, keystroke logging, POS fraud, application fraud, loss of card or theft, and POS fraud and vishing. However, the person should take safety steps and safeguards to protect his or her money. The vast bulk of this fraud is being committed by organized crime rings, whose operations have been industrialized and computerized. So how may these frauds be found? Utilizing machine learning algorithms is the solution. Conventional fraud detection is another method, however, machine learning algorithms are much more accurate and exact. The basic objective is to create a model that can foretell whether a Transaction will be fraudulent or not. In this project, predictive models utilized in this research include Artificial Neural Networks, Random Forests, Support Vector Machines, KNN, Decision Trees, Gaussian Naive Bayes, and Logistic Regression. The results from each of these models are evaluated for accuracy, and the best model is selected.***
Keywords: Feature Extraction, Fraud Detection, Online Payment, Credit Card, Deep Learning, Artificial Neural Network (ANN), Machine Learning, Support Vector Machine (SVM).

I. INTRODUCTION

In recent years, as there are so many advancements in technology, most of them are because of the usage of credit cards for buying their wishes so the fraud associated with it is also rising progressively. nearly all firms from small to big industries use credit cards as a mode of payment. credit card fraud is occurring in all agencies together including home equipment enterprises, vehicle enterprises, banks, and so on. several methods like information mining and device getting-to-know algorithmic methods are implemented to identify fraud within credit card transactions however did not get a considerable result. consequently, there is a need for powerful and efficient algorithms to be evolved that work efficiently. we try to avoid the fraudster the usage of our credit card before the transaction gets accepted through the use of synthetic neural network algorithms and in comparison, with a few different gadgets gaining knowledge of algorithms. Credit Card Fraud Detection is critical and vital for any credit card corporation. Extortion in charge card exchanges is characterized because the unapproved and undesirable usage of a file with the aid of somebody who isn't the record's owner. credit score Card includes addresses, social insurance numbers, phone variety, credit card numbers, and many extra personal sensitive data. these statistics may be muddled through hackers, so all people have to be cautious. they will call us and ask us about the discount of interest charge on the credit score card for a charge. They sound like they call from a financial institution or credit card agency, but they're not anything but scams that must not be believed. if you need to store cash while paying off your debt. however, those agents may not lessen your interest price. And it's not all approximately that one-time rate. What they're after is your identification and it's far known as a Low hobby scam. turns out banks or credit card groups usually do credit score tests with one credit bureau but now not both and correct good fortune

A. Classifications Of CreditCard Frauds

1) *Utility Fraud:* Whilst a fraudster acquires the manage over the account, steals the credentials of the account, and makes a fraud account after which the transactions take place.
2) *Digital or Guide Card Imprints:* In this type of fraud, the fraudster skims the data from the magnetic strip that's present on the cardboard and then uses the credentials and fraud transactions are done

3) *Counterfeit Card Fraud:* The fraud kind wherein the fraudster will copies all the data from a magnetic strip and the real card looks like an authentic card and works as the original card most effectively. This card was used for fraud.
4) *Card identity Theft:* The sort of fraud in which the identification of the cardholder is stolen and fraud takes region.
5) *Account Takeover:* The fraudster takes complete control of the account holder to make fraud.
6) *Lost/Stolen Card:* This type of fraud is due to loss of the card by means of the cardholder or by using stealing the card from the cardholder.

.

II. LITERATURE SURVEY

To forecast better identification of credit card fraud, specific algorithms will also be created and applied based on Artificial and Neural Intelligence Networks. The data sets that are utilised to spot fraud are dispersed and unbalanced. Several detection algorithms examined for fraud recognition had a variety of problems, according to research experts. Scientists are working to develop a system that can identify and stop theft since fraudulent behaviour results in significant losses. There have already been a lot of suggestions that have only been reviewed.

in paper [1] The dataset needs to be divided up to identify the information example as part of the pre- processing of the information. This includes examining how information is delivered to different classes. Then double-check the type of information in each section. Depending on the case, the decision will be made to exclude some sections. Without additional planning, the segments that have higher faults will be dropped immediately.

The paper [2] addressed widely used supervised techniques and a detailed review of supervised learning techniques has been presented. It have also shown that all algorithms change depending on the field of problem.

The paper [4][5][7] are based on deep learning algorithms and as compared to other machine learning algorithms the deep learning algorithms are much more accurate.in all these 3 papers deep learning topologies that have been suggested for detecting fraud in online financial transactions. This method is derived from an artificial neural network with built-in time and memory components, including long-term and short-term memory, among other factors. Considering how well these elements work in detecting fraud, about 80 million Online credit card transactions have been flagged as both legitimate and fraudulent. They made use of a distributed, high-performance cloud computing environment. The research team's paper serves as a useful manual for sensitivity analysis of the suggested factors in relation to fraud detection performance. The researchers also suggested a methodology for deep learning topologies' parameter adjustment for fraud detection. As a result, the financial institution might lower the prediction on the class data was predicted by our algorithm

III. METHODOLOGY

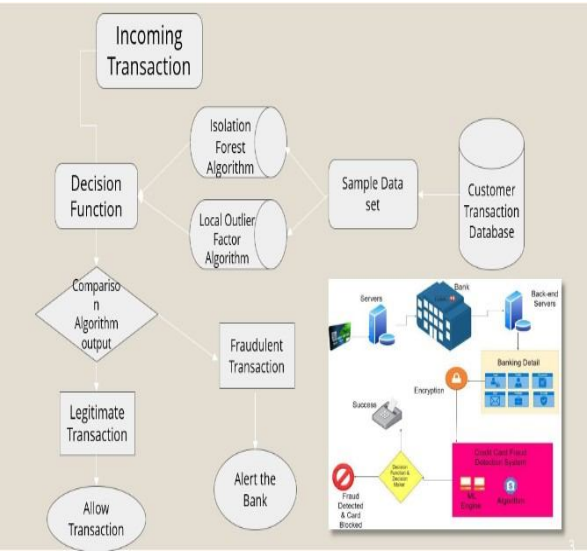


Figure 3.1: Architecture

A. Dataset

The dataset includes credit card transactions performed by European cardholders in September 2013.We have 492 frauds out of 284,807 transactions in our dataset of transactions that took place over the course of two days. The dataset is very skewed, with frauds making up 0.172% of all transactions in the positive class. It only has numeric input variables that have undergone PCA transformation. Unfortunately, we are unable to offer the original characteristics and additional context for the data due to confidentiality concerns. The major components obtained with PCA are features V1, V2,..., V28. The only features that have not been changed with PCA are "Time" and "Amount." The seconds that passed between each transaction and the dataset's first transaction arelisted in the feature "Time."

B. Data Processing & Pre-processing

The implementation of the algorithm utilised for the suggested system is explained in this section. The implementation in this paper begins with data collecting (Data collecting). Then comes data cleaning, which fills in any missing numbers in the transaction using mean, median, and standard deviation approaches, as well as data normalisation. The data set is divided into train and test data sets, and the model is trained and evaluated to gauge its accuracy. Finally, the system forecasts whether the transaction involves fraud or not. Splitting of the data is carried out in pre-processing part and the data is send for training

C. Training & Testing the Model

Dataset was spilt in the manner that 80% of the data goes into the training and the rest of the data is used for the testing part and the data was analyzed on the class data that is presented in the dataframe and the prediction on the class data was predicted by our algorithm

D. Backend Functioning

Artificial Neural Networks work in a way similar to that of their biological inspiration. It consists of an input layer, multiple hidden layers, and an output layer. ANN is biologically stimulated by means of human mind. The neurons are interconnected inside the human mind just like the same nodes are interconnected in artificial neural network. Fig. 1 depicts the structure of ANN with input, output and hidden layers. Inputs are x1, x2…Xn and output is y. w1…wn are the weights associated with inputs x1…xn respectively. There are 15 hidden layers used in this neural community. The activation feature utilized in our credit score card fraud detection version is sigmoid which is better at predicting the predictions than Relu.

1) *Input Layer:* Input Layer accepts inputs in several different formats provided by the programmer.
2) *Hidden Layer:* Hidden Layer performs all the calculations to find hidden features and patterns.
3) *Output Layer:* The input goes through a series of transformations using the hidden layer, which finally results in output that is conveyed using this layer. The data is predicted on the class column of the data frame and the predictions ,accuracy, classification report are analysed.

IV. EXPERIMENT AND RESULTS

Result of the different matrix on which the model isevaluate are shown in fig 4.1

Results include precision , recall , f-1 score and support for class 0 (normal) & 1(fraud). In the result given below model have predicted that the precision for the normal class is 0.92. This means that the data contains small percentage of fraud data. Further the model have predicted the recall as 1 this means that the model have all the data inputs correctly and f-1 score as 0.96 and support as 106

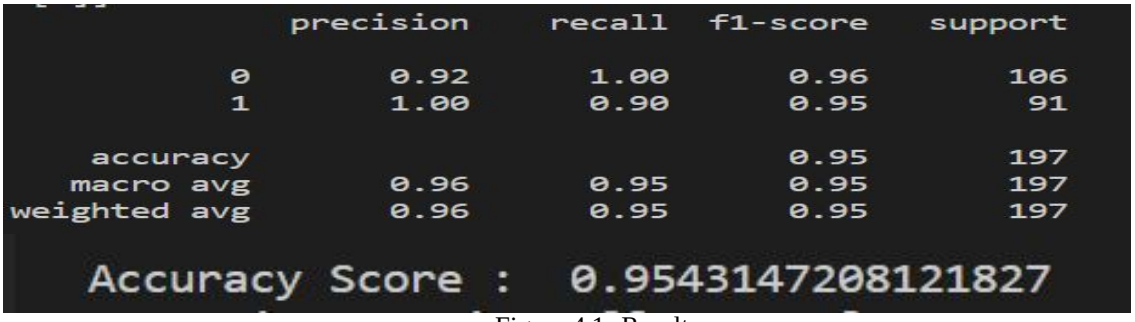


Figure 4.1- Results

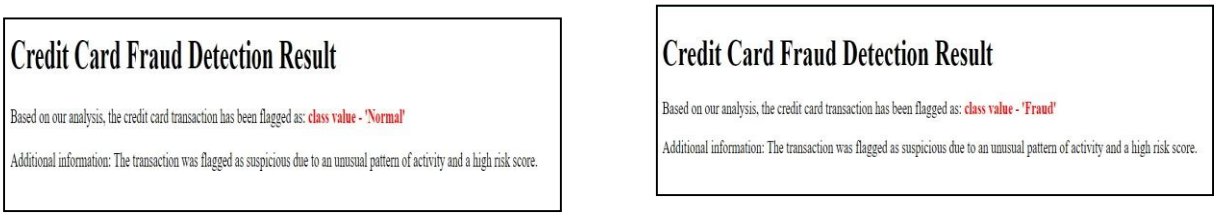


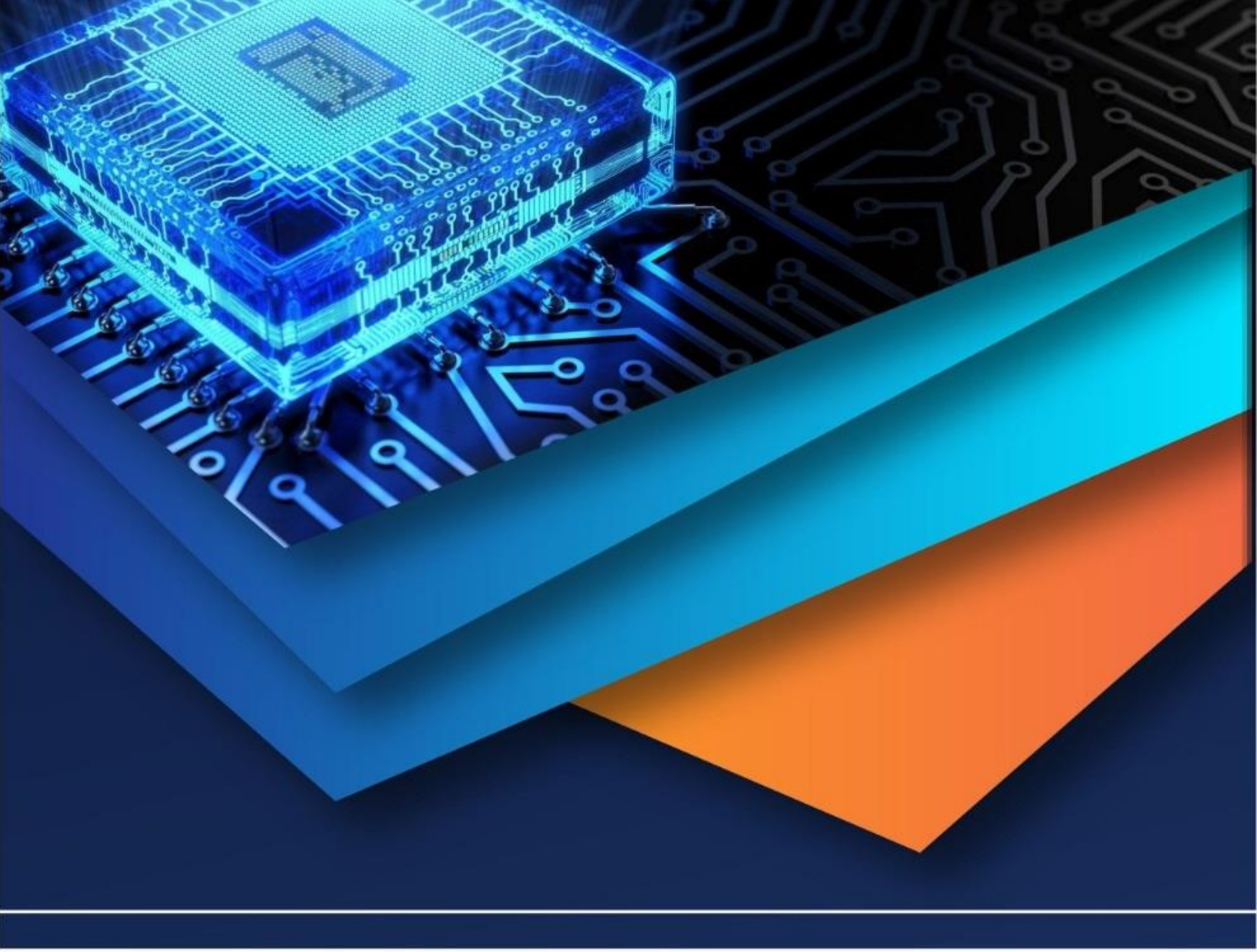
Figure 4.2- Front End Predicted results

V. CONCLUSION

As usage of credit cards or online payment become more and more common in every field of the daily life. So we need security for any transaction from fraudulent user. In these proposed systems we analysed and detect the fraud in online credit-card transactions in real time. Firstly, Principal Component Analysis was employed to create balanced data sheet. More room for improvement can be found in the dataset. The precision of the algorithms increases when the size of dataset is increased. Hence, more data will surely make the model more accurate in detecting frauds. However, this requires official support from the banks themselves.

REFERENCES

[1] P. Singh, V. Chauhan, S. Singh, P. Agarwal and S. Agrawal, "Model for Credit Card Fraud Detection using Machine Learning Algorithm," 2021 International Conference on Technological Advancements and Innovations (ICTAI), Tashkent, Uzbekistan, 2021, pp. 15-19, doi: 10.1109/ICTAI53825.2021.9673381..
[2] S. K. Saddam Hussain, E. Sai Charan Reddy, K. G. Akshay and T. Akanksha, "Fraud Detection in Credit Card Transactions Using SVM and Random Forest Algorithms," 2021 Fifth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I- SMAC), Palladam, India, 2021, pp. 1013- 1017, doi: 10.1109/I- SMAC52330.2021.9640631.
[3] K. I. Alkhatib, A. I. Al-Aiad, M. H. Almahmoud and O. N. Elayan, "Credit Card Fraud Detection Based on Deep Neural Network Approach," 2021 12th International Conference on Information and Communication Systems (ICICS), Valencia, Spain, 2021, pp. 153-156, doi: 10.1109/ICICS52457.2021.9464555.
[4] A. A. El Naby, E. El-Din Hemdan and A. El-Sayed, "Deep Learning Approach for Credit Card Fraud Detection," 2021 International Conference on Electronic Engineering (ICEEM), Menouf, Egypt, 2021,pp.1-5,doi: 10.1109/ICEEM52022.2021.9480639.
[5] A. Shah and A. Mehta, "ComparativeStudy of Machine Learning Based Classification Techniques for Credit Card Fraud Detection," 2021 International Conference on Data Analytics for Business and Industry (ICDABI), 2021, pp. 53-59, doi: 10.1109/ICDABI53623.2021.9655848
[6] A. P. Lopes, S. Parshionikar, A. Kale, N. Sharma and A. A. Varghese, "Comparative Analysis of Deep Learning Techniques For Credit Card Fraud Detection," 2021 International Conference on Advances in Computing, Communication, and Control (ICAC3), 2021, pp. 1-5 doi: 10.1109/ICAC353642.2021.9697205.
[7] E. Esenogho, I. D. Mienye, T. G. Swart, K. Aruleba and G. Obaido, "A Neural Network Ensemble With Feature Engineering for Improved Credit Card Fraud Detection," in IEEE Access, vol. 10, pp. 16400-16407, 2022, doi: 10.1109/ACCESS.2022.3148298.
[8] G. M. Suhas Jain, N. Rakesh, K. Pranavi and L. Bale, "A Novel Approach in Credit Card Fraud Detection System Using Machine Learning Techniques," 2021 International Conference on Forensics, Analytics, Big Data, Security (FABS), 2021,pp. 1-5, doi: 10.1109/FABS52071.2021.9702672..
[9] R. Sailusha, V. Gnaneswar, R. Ramesh and G. R. Rao, "Credit Card Fraud Detection Using Machine Learning," 2020 4th International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, India, 2020, pp. 1264- 1270.
[10] C. H. Sumanth, P. P. Kalyan, B. Ravi andS. Balasubramani., "Analysis of Credit Card Fraud Detection using Machine Learning Techniques," 2022 7th International Conference on Communication and Electronics Systems (ICCES), 2022, pp. 1140-1144, doi: 10.1109/ICCES54183.2022.9835751.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY