iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** V **Month of publication:** May 2024

DOI: https://doi.org/10.22214/ijraset.2024.61553

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 12 Issue V May 2024- Available at www.ijraset.com

Deep Learning based Credit Card Fraudulency Detection System

Kavyasri.G[1], Keerthana. D[2], Keerthi Reddy. B[3], Keerthi.K[4], KesavaAditya.J[5], Prof.S.Ramesh kumar[6]
Department of AI-ML Malla Reddy University, Maisammaguda, Hyd.

Abstract: ***Huge increase in the internet usage has been observed since last decade. It led to the emergence of services like e-commerce, tap and pay systems, online bill payment systems, etc. have proliferated and become more widely used. Due to various online payment options introduced by e- commerce and other numerous websites, the possibility of online fraud has risen drastically. Thus, due to an increase in fraud rates, research on analyzing and detecting fraud in online transactions has begun utilizing various machine learning techniques. The Deep Learning techniques viz., Convolutional***
Neural Network Architecture is used to detect credit card frauds in the proposed model. The Principal Component Analysis transformation gives a set of numerical input variables as output which are taken as the features to be considered. Due to confidentiality concerns, some of the original characteristics and background information about the data are not entirely disclosed. Features of credit card frauds must be chosen carefully as they play important role when deep learning techniques are used for credit card fraud detection. The TensorFlow and Keras are used for the development of the current proposed model. The proposed model aims to predict credit card frauds with 91.9% accuracy.
Keywords: Credit card, Fraudulent, Deep learning, Principal Component Analysis, TensorFlow, Keras

I. INTRODUCTION

The advancement in technology led to the emergence of services like e- commerce, tap and pay systems, online bill payment systems, etc. have proliferated and become more widely used. Due to various online payment options introduced by e-commerce and other numerous websites, the possibility of online fraud has risen drastically. This opened the doors to the research on analysing and detecting fraud in online transactions by applying various techniques. The current project focusses on detecting credit card fraudulency using deep learning techniques and aims to
predict credit card frauds with at-most accuracy.
To detect credit card frauds and to come up with a deep learning model which will accurately predict whether the credit card transaction is fraudulent or not is the aim the project. The scope of the proposed project is to develop an application that,

1) Enables to classify credit card transactions into fraudulent and non- fraudulent.
2) Based on the dataset containing the features and attributes related to credit card
3) Determines accuracy in detecting frauds.

Because of the time constraint, limited parameters are considered for the study and only selected DL techniques are being used to cross check the accuracy given by our model.

II. LITERATURE SURVEY

Dejan Varmedja [1] studied numerous machine learning algorithms and analysed them relating to credit card fraud detection systems. Multilayer perceptron is used (Artificial neural network) whichconsist of 4 hidden layers and relu activation functioned is used that is to avoid negative values andoptimizer used is Adam for its best performance. It is observed that random forest yields the finestresult in case of credit card fraud detection. Changjun Jiang [2] suggested a method for fraud detection clustering the homogeneous historical transaction data ended up in aggregating transactions using sliding window strategy. Sahil Dhankhad [3] has applied supervised machine learning algorithms on the real-world data set- a Novel Approach Using Aggregation Strategy and Feedback Mechanism. Algorithms to implement a super classifier using ensemble learning are developed and are compared with the performance of supervised algorithms implementing super classifier. Out of ten machine learning algorithms implemented, Logistic Regression evolved as better option for predicting fraud transactions. Rishikeshan O V, Sakala Sai Kiran et.al., [5] proposed an improved algorithm for credit card frau detection. That is named as Naïve Bayes improved K-nearest Neighbour method (NBKNN). They have used a dataset on which they had applied the algorithms to identify the fraudulent transactionin the taken dataset.

Mohamad Zamini [6] purposed an unsupervised fraud detection method using autoencoder based clustering. The autoencoder is an auto associator neural network, used to lower the dimensionality, extract the useful features, and increase the efficiency of learning in a neural network. European dataset with 2,84,807 transactions is considered for experimentation which resulted in 0.024 as training loss, 0.027 as validation loss and the mean non-fraudulent data is 75% less than the mean of reconstructive error.

III. PROBLEM STATEMENT

Huge increase in the internet usage can be observed since the last decade. A surge in financial fraud cases, such as credit card fraud, has been caused by recent developments in e-commerce and e-payment systems. Thus, it is essential to create systems that can recognize credit card fraudulency which is a threat to the financial system as a whole. The proposed project focusses on detecting credit card fraudulency using deep learning techniques and aims to predict credit card frauds with at- most accuracy.

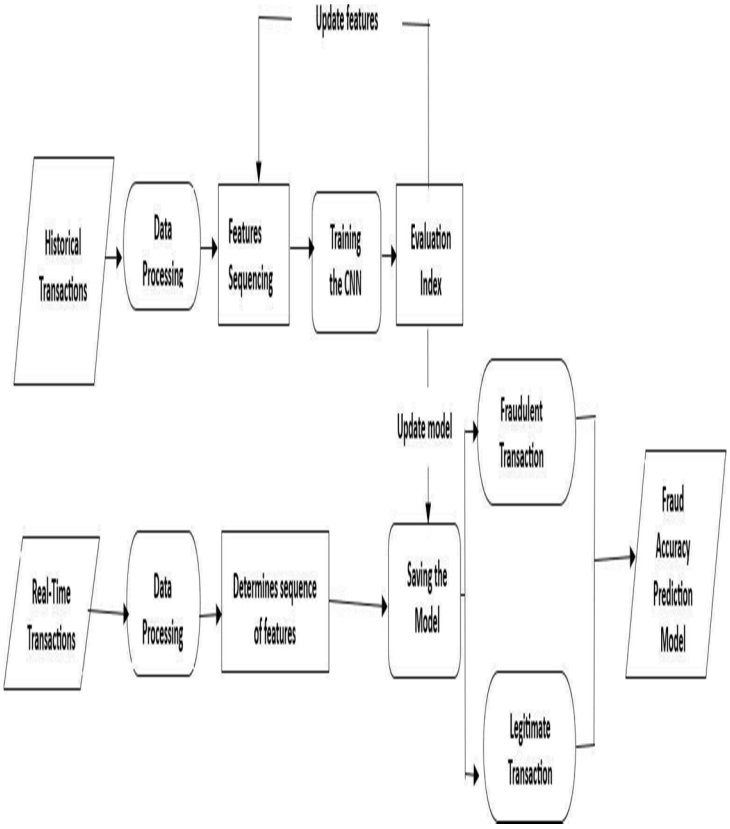
IV. EXISTING METHODOLOGY

Credit card fraud detection has been an active research area for several years, and with the advent of deep learning techniques, it has become possible to develop more accurate and efficient fraud detection systems. Most of the existing credit card fraudulent detection systems are based on the machine learning techniques. Some of the recent studies on credit card fraud detection using deep learning: "Credit Card Fraud Detection using Recurrent Neural Networks" by Bhattacharya et al. (2019) "Credit Card Fraud Detection using Deep Learning and Random Forests" by Amorim et al. (2020) though there are very few traces of DL model, still effort is on to come out with more efficient system.

V. PROPOSED METHODOLOGY

The proposed system is a Deep Learning based credit card fraud detection system. It uses a library called TensorFlow which is used for deep learning models. The proposed model uses a simple CNN architecture and evaluates the performance of the model using metrics such as accuracy, precision, recall, and F1-score. It reports high values for these metrics, indicating that the model is effective in detecting credit card fraud.

VI. ARCHITECTURE DIAGRAM:



VII. DATASET DESCRIPTION

For any model to understand how to perform various actions, training datasets must first be fed into the machine learning algorithm, followed by validation datasets (or testing datasets) which ensures that the interpretation of the model data is accurate. Credit card fraud datasets are highly imbalanced, with a small fraction of transactions being fraudulent. Handling imbalanced data is a crucial challenge in fraud detection. Techniques like oversampling, under sampling, and costsensitive learning have been employed to address this issue. The proposed project is carried over on the existing dataset. Credit card fraud detection datasets typically include a wide range of features that can help identify fraudulent transactions, while the specific features may vary depending on the dataset. The dataset consists of multiple features like Transaction amount, Transaction type, Time of transaction, Merchant ID, Merchant country, Merchant state, Number of previous transactions, Average transaction amount, Number of transactions within a time window, Card usage patterns, Device information, Account age, Card expiration date and Card issuing bank so on. Each attribute has its own importance. The dataset used is relatively small as it contains only 30,000 transactions.

VIII. DATA PRE-PROCESSING TECHNIQUES

First step in deep learning workflow is pre-processing data which ensures that the data is in a format that the network can accept. Before preparing the data to be fed to the network the input dataset must be pre- processed. Sample data is obtained which further undergoes the cleaning step where the null, missing, and irrelevant data is handled. Then the data is split into respective testing, training, and validation sets. TensorFlow and Keras is used to create feedforward neural network. The model is evaluated using several metrics and most importantly the ROC AUC score and curve are obtained.

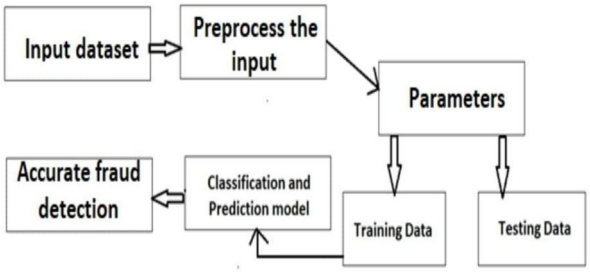


Fig. Data pre processing flow

IX. MODEL EVALUATION

The credit card fraud detection using Keras and TensorFlow with a convolutional neural network (CNN) architecture. The model on the testing set and prints the loss and accuracy scores. The model finally evaluates the following:

1) Basic investigation on the input dataset.
2) Number of fraudulent and non-fraudulent transactions.
3) Total number of records.
4) The accuracy of model to predict or detect credit card frauds after training.

X. MODULES

1) NumPy (np): Used for numerical operations and array manipulation.
2) Pandas (pd): Used for data manipulation and analysis, particularly for handling the dataset in tabular format.
3) Matplotlib (plt): Used for data visualization, particularly for creating plots and charts.
4) Seaborn (sns): Built on top of Matplotlib, used for statistical data visualization.
5) TensorFlow (tf): TensorFlow is an open-source machine learning framework developed by Google used for building and training deep learning models.

XI. ALGORITHMS

Convolutional Neural Network (CNN): A type of deep learning algorithm commonly used for image recognition. However, it can also be applied to sequential data such as time series or 1D signals, which is the case for this credit card fraud detection task. The CNN architecture consists of convolutional layers followed by max-pooling layers, a flattening layer, dense layers, and an output layer with a sigmoid activation function. Since your project involves deep learning, it's essential to leverage frameworks like TensorFlow or Keras to build and train neural network models, such as CNN to effectively detect credit card fraud.

XII. OUTPUT SCREENS

Fig. Fraudulent Transaction Screen

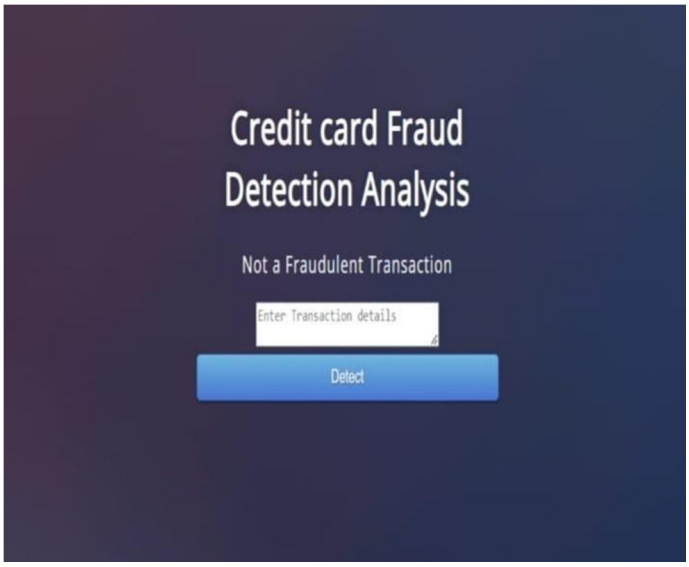


Fig. Not a Fraudulent Transaction Screen

XIII. FUTURE ENHANCEMENT

It's worth noting that research in credit card fraud detection is an ongoing process, and new techniques and advancements are continuously being explored. To reduce the fraud as much as possible and to find the fraud
as soon as possible. In the future, As the data we considered for training and validation is of one type and there are more kinds of frauds which need to be trained. Larger datasets is to be considered.

XIV. CONCLUSION

Fraud is a major problem for the whole credit card industry that grows bigger with the increasing popularity of electronic money transfers. To effectively prevent the criminal actions that lead to the leakage of bank account information leak, skimming, counterfeit credit cards, the theft of billions of dollars annually, and the loss of reputation and customer loyalty, credit card issuers should consider the implementation of advanced Credit Card Fraud Prevention and Fraud Detection methods. Deep Learning-based methods can continuously improve the accuracy of fraud prevention based on information about each cardholder's behaviour. It is very important to train the Fraud Detection model continuously whenever new data arrives, so new fraud schemas/patterns can be learned, and fraudulent data detected as early as possible.

REFERENCES

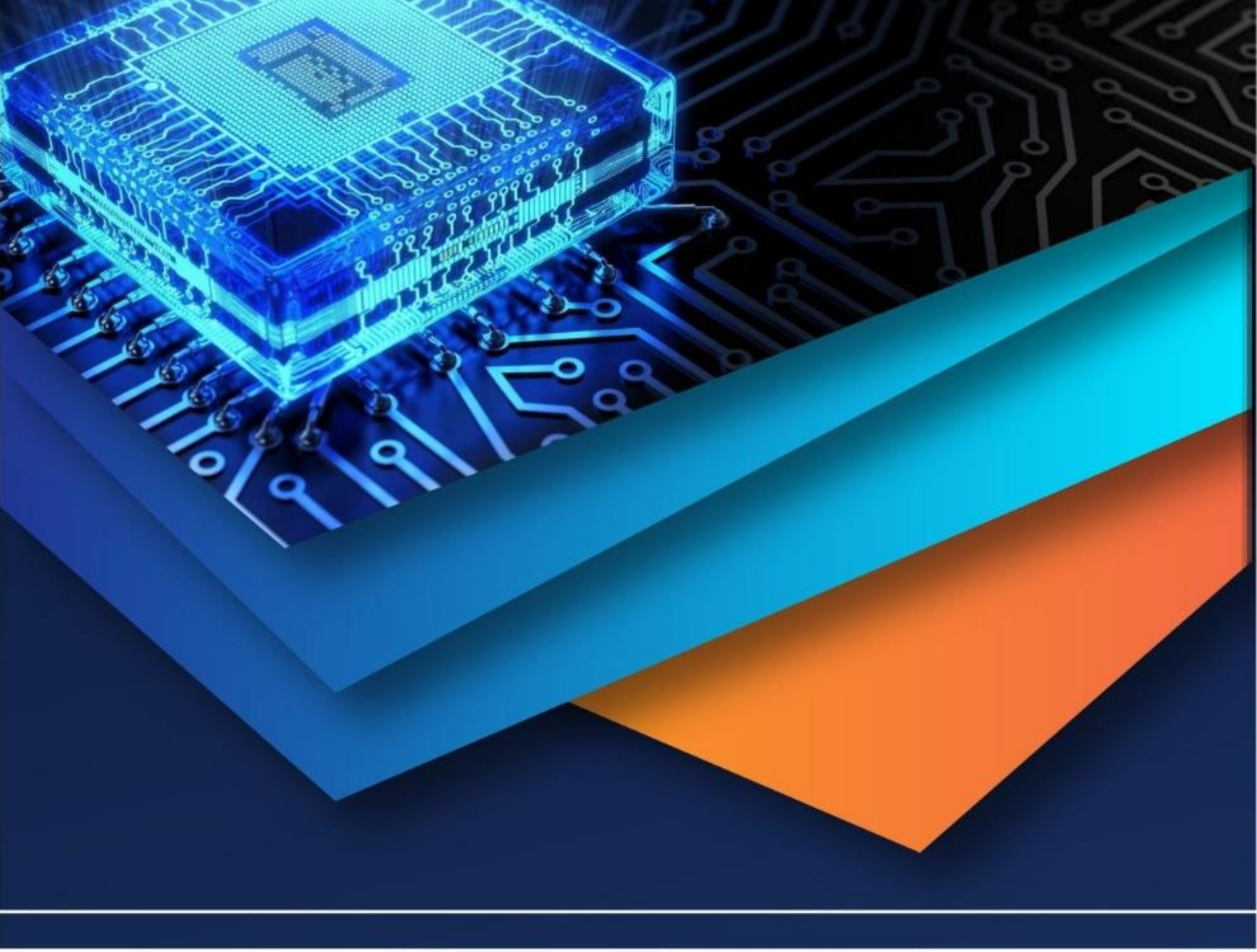
[1] D. Varmedja, M. Karanovic, S. Sladojevic, M. Arsenovic and A. Anderla, "Credit Card Fraud Detection - Machine Learning methods," 2019 18th International Symposium INFOTEH-JAHORINA (INFOTEH), East Sarajevo, Bosnia, and Herzegovina, 2019, pp. 1-5, doi: 10.1109/INFOTEH.2019.8717766.

[2] C. Jiang, J. Song, G. Liu, L. Zheng, and W. Luan, "Credit Card Fraud Detection: A Novel Approach Using Aggregation Strategy and Feedback Mechanism," in IEEE Internet of Things Journal, vol. 5, no. 5, pp. 3637-3647, Oct. 2018, doi: 10.1109/JIOT.2018.2816007.

[3] S. Dhankhad, E. Mohammed and B. Far, "Supervised Machine Learning Algorithms for Credit Card Fraudulent Transaction Detection: A Comparative Study," 2018 IEEE International Conference on Information Reuse and Integration (IRI), Salt Lake City, UT, USA, 2018, pp. 122-125, doi: 10.1109/IRI.2018.00025.

[4] K. Randhawa, C. K. Loo, M. Seera, C. P. Lim, and A. K. Nandi, "Credit Card Fraud Detection Using AdaBoost and Majority Voting," in IEEE Access, vol. 6, pp. 14277-14284, 2018, doi: 10.1109/ACCESS.2018.2806420.

[5] Rishikeshan O V, Sakala Sai Kiran, Prasath S, Anitha M, “Credit Card Fraud Detection Using Isolation Forest and Local Outlier Factor”, 2022, in International Journal of Scientific Research in Engineering and Management.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY