IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

REAL TIME CREDIT CARD FRUAD DETECTION BASED ON LOGISTIC REGRESSION IN MACHINE LEARNING

[1]K.TULASI KRISHNA KUMAR, [2]POTNURI JOGIBABU,
[1]Assistant professor and placement officer, [2]MCA Final Semester
[1]Masters od Computer Application,
[1] Sanketika Vidya Parishad Engineering College, Visakhapatanam, India

Abstract: Credit card fraud detection is a critical task to ensure that customers are not charged for transactions they did not authorize. Leveraging the power of Data Science and Machine Learning, this project aims to model and detect fraudulent credit card transactions with high accuracy. The primary focus is on analayzing historical transaction data, identifying patterns associated with fraud, and applying anomaly detection techniques to classify new transactions as either normal or fraudulent in this project, we work with a dataset of past credit card transactions, including both genuine and fraudulent cases. The goal is to develop a model capable of accurately identifying 100% of fraudulent activities while decreasing false positives. This classification problem is addressed using machine learning techniques, particularly anomaly detection algorithms such as Local Outlier Factor (LOF) and Isolation Forest. To enhance model performance and efficiency, Principal Component Analysis (PCA) is applied to reduce data dimensionality. Through careful data preprocessing, model training, and evaluation, this project demonstrates the practical application of machine learning in detecting credit card fraud and highlights its significance in enhancing financial security

IndexTerms - credit card fraud detection, machine Learning algorithms,dataset models, preprocessing techniques.uml diagrams,logistic regression and random forest algorithms,knn algorithm

INTRODUCTION

Credit card fraud refers to the unauthorized and illegitimate use of a credit card by someone other than the cardholder, without their knowledge or consent.[5] It involves exploiting an account for personal gain while the rightful owner and the issuing authority remain unaware of the activity. Preventing such abuse is essential, and understanding the behaveior behind fraudulent transactions plays a crucial role in minimizing future occurrences and strengthening security systems.

Fraud detection involves continuously monitoring user activity to identify, predict, or prevent objectionable behavior such as fraud, intrusion, or default.[12] It is a critical issue in the financial domain, where solutions require advanced techniques from fields like machine learning and data science to enable automation and real-time analysis.

One of the primary challenges in fraud detection is class imbalance—fraudulent transactions represent only a small fraction of the total, making them harder to detect. Furthermore, transaction patterns evolve over time, leading to concept drift, which can affect the accuracy and reliability of predictive models.

Real-world fraud detection systems must process vast volumes of payment requests in real-time.[20] These systems rely on automated tools and machine learning algorithms to analyze transactions and flag suspicious activity.[2] Flagged transactions are reviewed by fraud investigation teams who verify their authenticity by contacting the cardholder.

The feedback obtained from these investigations is crucial—it is used to retrain and update the fraud detection models, thereby enhancing their accuracy and adaptability over time.[10] This continuous learning loop helps build more robust and responsive fraud detection systems capable of adapting to evolving fraud patterns.

EXISTING SYSTEM.

The existing system for credit card fraud detection primarily relies on traditional rule-based engines combined with manual verification processes.[16] These systems operate by checking each transaction against a predefined set of static rules, such as detecting unusually high amounts, transactions in unfamiliar locations, or multiple rapid transactions within a short time span. While this approach offers some level of security, it is limited in its ability to adapt to evolving fraud techniques. Fraudsters often find new ways to bypass these rules, making the system less effective over time. Moreover, these systems tend to generate a high number of false positives, flagging many legitimate transactions as suspicious, which leads to unnecessary inconvenience

for customers and an increased workload for investigation teams. Each flagged transaction usually undergoes manual review, where investigators must contact cardholders to confirm the transaction's legitimacy, making the process time-consuming and inefficient.Additionally the system does not learn from past data, meaning that any new fraud patterns require manual rule updates.[4] Another major challenge is the issue of class imbalance, where fraudulent transactions represent only a small portion of the data, making accurate detection even more difficult. Furthermore, the system struggles with processing the high volume of real-time transactions, limiting its effectiveness in identifying sophisticated fraud attempts.[21] Despite providing a basic framework for fraud detection, the existing system lacks the adaptability, scalability, and intelligence required to keep up with modern fraud tactics.

3.1 CHALLENGES

Data collection: The first step in the project is to collect a dataset of credit card transactions that includes both fraudulent and valid transactions. The dataset used in the project was obtained from Kaggle.

- Data preprocessing: The collected dataset was preprocessed to remove any duplicates and missing values.[18] The data was also standardized to ensure that all features have a similar scale.
- Feature engineering: The next step was to extract relevant features from the preprocessed dataset that are likely to be useful in detecting fraud. The selected features included transaction amount, time, and location.
- Model training: The Random Forest Classifier algorithm was used to train a model on the preprocessed and feature-engineered dataset.[23] The dataset was split into training and testing sets in a 70:30 ratio.
- Model evaluation: Once the model was trained, it was evaluated using various performance metrics, including accuracy, precision, recall, F1-score, and ROC. A confusion matrix was also generated to visualize the performance of the model.
- Model deployment: The final step in the project is to deploy the trained model in production,[26] where it can be used to monitor credit card transactions in real-time.

3.2 PROPOSED SYSTEM

In the proposed system, machine learning algorithms are applied to effectively classify credit card transactions and detect fraudulent activities. Specifically, the Random Forest Classifier is utilized due to its robustness, accuracy, and ability to handle imbalanced datasets. Random Forest is an ensemble learning method used for both classification and regression tasks.[19] It operates by constructing multiple decision trees during training and outputting the majority vote for classification tasks. One of its key advantages over a single decision tree is its ability to reduce overfitting, as combines the results of many weak learners (decision trees) to produce a more stable and generalized model.

In this approach, random subsets of the training data and features are used to train each decision tree, introducing diversity and reducing the correlation between individual models.[15] This not only enhances performance but also improves the model's capability to generalize well to unseen data. Additionally, Random Forest is highly efficient, as the individual trees can be trained in parallel, making it scalable even for large datasets with numerous features.[27] The algorithm has shown strong resistance to overfitting and is capable of providing reliable estimates of generalization error. Due to these advantages, Random Forest serves as a powerful and effective method for detecting credit card fraud in real-time applications

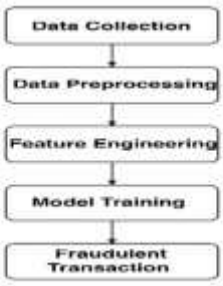


Fig: 1 Proposed Diagram

3.3 ADVANTAGES

1. **High Accuracy and Performance:** Random Forest provides high classification accuracy, making it effective in distinguishing between fraudulent and legitimate transactions.
2. **Reduced Overfitting:** Unlike traditional decision trees, Random Forest minimizes the risk of overfitting by averaging the results of multiple trees, improving generalization to new data.
3. **Handles Imbalanced Data:** The algorithm performs well even when fraudulent transactions are significantly fewer than valid ones, which is a common scenario in fraud detection.
4. **Efficient on Large Datasets:** The algorithm is scalable and can efficiently handle large datasets with many features, due to the parallel training of decision trees.
5. **Fast Prediction Time:** Once trained, the model can quickly classify new transactions, making it suitable for real-time fraud detection systems.

ARCHITECTURE:

The architecture of the proposed credit card fraud detection system is structured to ensure efficient data handling, model training, and real-time prediction.[11] The process begins with the data collection layer, where transaction data is gathered from reliable sources, such as Kaggle, containing both legitimate and fraudulent transactions. This raw data then moves into the data preprocessing layer, where it is cleaned by removing duplicates and missing values, and standardized to ensure consistent scaling across features.[3] Following this, the feature engineering layer extracts and selects the most relevant features—such as transaction amount, time, and location—to enhance the model's ability to distinguish fraudulent activity.

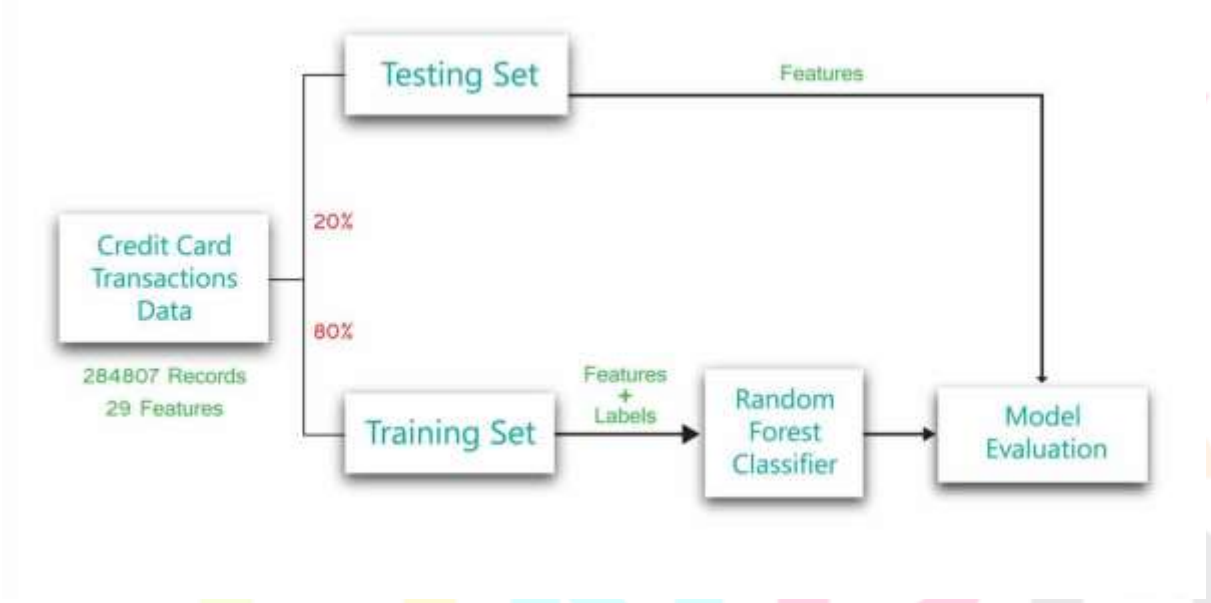


Fig:2 Architecture

2.2 AlGORITHM:

Credit card fraud detection leverages a variety of intelligent algorithms to identify suspicious activities effectively. [9] Artificial NeuralArtifical Nural Networks (ANNs) mimic the human brain's interconnected neurons to detect complex patterns in transaction data, making them particularly effective in recognizing subtle fraud indicators. [28] Fuzzy Logic is used to handle uncertainty and imprecise information, enabling systems to make decisions that resemble human reasoning in ambiguous scenarios.[17] Genetic Algorithms optimize detection strategies by evolving solutions over time, improving the accuracy of identifying fraudulent transactions. Logistic Regression, a statistical method, is widely used for binary classification problems, such as determining whether a transaction is fraudulent or legitimate, based on input features. Decision Trees offer a transparent and interpretable way to make decisions by splitting data based on attribute values, which helps in tracing the rationale behind fraud detection. Support Vector Machines (SVM) classify transactions by finding the optimal boundary that separates fraudulent from non-fraudulent cases, especially effective in high-dimensional spaces.[24] Bayesian Networks use probabilistic inference to model the relationships between different variables, enabling prediction even with missing or uncertain data. Hidden Markov Models (HMMs) are particularly useful in analyzing sequences of transactions, detecting unusual behavior patterns over time. Finally, K-Nearest Neighbors (KNN) classifies transactions based on the similarity to past labeled examples, allowing the system to detect fraud by comparing new transactions with known fraudulent and legitimate ones.[30] Together these algorithms provide a comprehensive toolkit for developing robust and adaptive credit card fraud detection systems.

2.3 TECHNIQUES:

This project applies advanced machine learning techniques to detect and prevent fraudulent credit card transactions. Initially, a robust and comprehensive dataset containing historical transaction records is collected.[6] These records include features such as transaction amount, time, merchant information, location, and anonymized user identifiers.

The dataset is then subjected to thorough preprocessing, which includes handling missing values, feature scaling (e.g., normalization or standardization), encoding categorical variables, and balancing class distribution using techniques like SMOTE (Synthetic Minority Over-sampling Technique). These steps ensure data quality, model stability, and effective learning, especially given the highclass imbalance typically found in fraud detection datasets.[14]

Following preprocessing, various machine learning algorithms—such as Logistic Regression, Random Forest, and Gradient Boosting—are trained and evaluated.[22] Feature selection and engineering are applied to improve model performance by identifying the most relevant transaction patterns and behaviors associated with fraudulent activity

For deployment and testing, transaction data is fed into the model in real time or batch mode to flag suspicious activities. The system can be integrated with existing banking platforms or fraud monitoring tools, providing an efficient, scalable, and automated solution for early detection and prevention of credit card fraud.

2.4 TOOLS:

The project utilizes various machine learning models to detect credit card fraud, including Gaussian Naive Bayes, Support Vector Machine, AdaBoost Classifier, Gradient Boosting Classifier, Bagging Classifier, Extra Trees Classifier, Stochastic Gradient Descent Classifier, Voting Classifier, K-Nearest Neighbors Classifier, and Logistic Regression.[13] These models are evaluated using metrics such as accuracy score and precision score. The dataset is split into training and testing sets to validate the performance of the models..The project benefits from improved accuracy and enhanced security, enabling real-time detection of credit card fraud.[29] However, challenges such as class imbalance, feature engineering, and model interpretability need to be addressed. Future work includes hyperparameter tuning, exploring new features, and ensemble methods to improve overall performance

2.5 METHODS:

There are various fraudulent activities detection techniques has implemented in credit card transactions have been kept in researcher minds to methods to develop models based on artificial intelligence data mining, fuzzy logic and machine learning.[25] Credit card fraud detection is significantly difficult, but also popular problem to solve. In our proposed system we built the credit card fraud detection using Machine learning.[8] With the advancement of machine learning techniques. Machine learning has been identified as a successful measure for fraud detection. A large amount of data is transferred during online transaction processes, resulting in a binary result: genuine or fraudulent. Within the sample fraudulent datasets, features are constructed. These are data points namely the age and value of the customer account, as well as the origin of the credit card. There are hundreds of features and each contributes, to varying extents, towards the fraud probability

III. METHODOLOGY

3.1 Input:

The model is trained on a dataset that includes information about credit card transactions, including features such as the transaction amount, time, and location. [21] The goal is to predict whether a given transaction is fraudulent or not, based on these features. The accuracy, precision, recall, F1-score, and ROC of the model are evaluated using appropriate metrics, and a confusion matrix is generated to visualize the performance of the model.[14] The ultimate objective of this project is to build a reliable and effective fraud detection system for credit card companies, which can help prevent fraudulent transactions and protect customers from financial losses

```
from sklearn.metrics import accuracy_score, f1_score, precision_score, recall_score, RocCurveDisplay # corrected import

# Assuming y_test and y_pred are defined from your previous classification task

acc = accuracy_score(y_test, y_pred)
prec = precision_score(y_test, y_pred, zero_division=0) # Added zero_division to handle potential division by zero
rec = recall_score(y_test, y_pred, zero_division=0) # Added zero_division to handle potential division by zero
f1 = f1_score(y_test, y_pred, zero_division=0) # Added zero_division to handle potential division by zero
print('accuracy:%0.4f'%acc,'\tprecision:%0.4f'%prec,'\trecall:%0.4f'%rec,'\tf1-score:%0.4f'%f1)

# Example of plotting ROC curve (requires model and X_test)
# If you want to plot the roc curve, you need the classifier and the test data.
#Example:
#from sklearn.linear_model import LogisticRegression
#clf = LogisticRegression(solver='liblinear') # or whatever your classifier is.
#clf.fit(X_train, y_train)
#RocCurveDisplay.from_estimator(clf, X_test, y_test)
#plt.show() # to show the plot.

Python
accuracy:0.9995        precision:0.9487        recall:0.7551   F1-score:0.8409
```

Fig 1: classification report of accuracy,precision,recall

```python
from imblearn.over_sampling import SMOTE
import numpy as np
import pandas as pd # added pandas import

# Assuming X and y are defined (replace with your actual data)
# Example dummy data:
X = np.random.rand(100, 10)
y = pd.DataFrame({'Class': np.random.randint(0, 2, 100)}) # y as DataFrame with 'Class' column

try:
    smote = SMOTE()
    X_resampled, y_resampled = smote.fit_resample(X, y['Class']) # Resample using 'Class' column
    print('Number of total transactions before SMOTE upsampling: ', len(y), '...after SMOTE upsampling: ', len(y_resampled))
    print('Number of fraudulent transactions before SMOTE upsampling: ', len(y[y.Class==1]), '...after SMOTE upsampling: ', np.sum(y_resam

except NameError as e:
    print(f"NameError: {e}. Make sure SMOTE has been executed.")
except AttributeError as e:
    print(f"AttributeError: {e}. Ensure you have the latest imbalanced-learn version.")
except Exception as e:
    print(f"An unexpected error occurred: {e}")
```

Python

```
Number of total transactions before SMOTE upsampling:  100 ...after SMOTE upsampling:  104
Number of fraudulent transactions before SMOTE upsampling:  52 ...after SMOTE upsampling:  52
```

Fig 2: Total tranctions and fraudulent transactions before and after SMOTE up sampling

```
y_resampled DataFrame:
   0
0  1
1  1
2  0
3  1
4  0

X_resampled DataFrame:
          0         1         2         3         4         5         6  \
0  0.765680  0.425209  0.875793  0.263495  0.464103  0.496256  0.773253
1  0.261157  0.067737  0.121492  0.933112  0.038179  0.086057  0.363810
2  0.106243  0.611593  0.952293  0.889171  0.452410  0.130263  0.050552
3  0.062274  0.238353  0.151274  0.591844  0.275266  0.786121  0.767606
4  0.126739  0.530245  0.617846  0.535218  0.067760  0.080183  0.345466

          7         8         9
0  0.765828  0.517002  0.738153
1  0.130391  0.593392  0.447265
2  0.950660  0.519637  0.902120
3  0.923804  0.813285  0.479141
4  0.175465  0.241132  0.920568
```

Fig3: oversampling using smote analysis

```python
from imblearn.over_sampling import SMOTE
import numpy as np

# Assuming X and y are defined (replace with your actual data)
# Example dummy data:
X = np.random.rand(100, 10)
y = np.random.randint(0, 2, 100)

try:
    smote = SMOTE()
    X_resampled, y_resampled = smote.fit_resample(X, y) # Corrected function name
    print("SMOTE applied successfully.")
    print("X_resampled shape:", X_resampled.shape)
    print("y_resampled shape:", y_resampled.shape)

except AttributeError as e:
    print(f"AttributeError: {e}. Ensure you have the latest imbalanced-learn version.")
except Exception as e:
    print(f"An unexpected error occurred: {e}")
```

Python

```
SMOTE applied successfully.
X_resampled shape: (104, 10)
y_resampled shape: (104,)
```

3.2 Method of Process:

The Real time credit card fraud detection project involves a multi-step process that includes data preparation, model development, model deployment, and model monitoring and maintenance. Initially, the project requires collecting and preprocessing credit card transaction data, followed by feature engineering to extract relevant features. Various machine learning models are then developed and trained using the preprocessed data, including Gaussian Naive Bayes, Support Vector Machine, and ensemble methods like AdaBoost and Gradient Boosting. The models are evaluated using metrics such as accuracy score and precision score, and the best-performing model is selected for deployment.Once deployed, the model makes real-time predictions on new transactions, enabling swift action to be taken against potential fraud. The model's performance is continuously monitored, and it is updated periodically to adapt to changing patterns in the data.[7] Regular maintenance tasks, such as data preprocessing and feature engineering, ensure the model remains effective in detecting credit card fraud. By leveraging machine learning and data analysis, the project aims to provide a robust and efficient solution for credit card fraud detection, protecting financial institutions and cardholders from losses.The project is an ongoing effort, and future updates may include exploring new machine learning models, incorporating additional features, and improving the model's interpretability and explainability. By staying up-to-date with the latest advancements in machine learning and data analysis, the project can continue to enhance its capabilities and provide a more effective solution for credit card fraud detection.

3.3 Output:

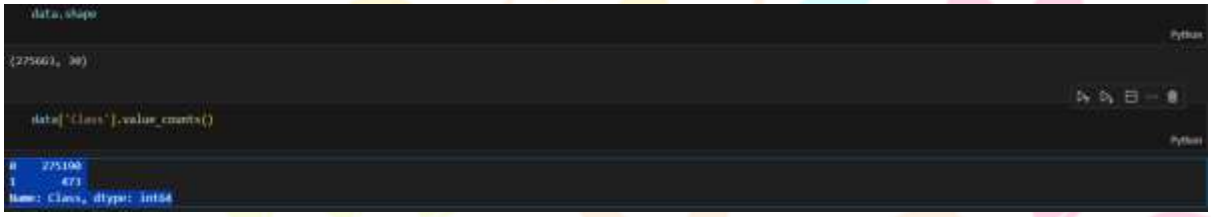


Fig: imbalanced dataset

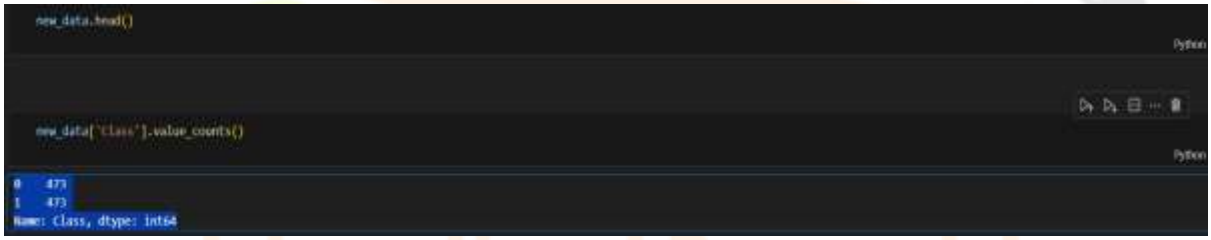
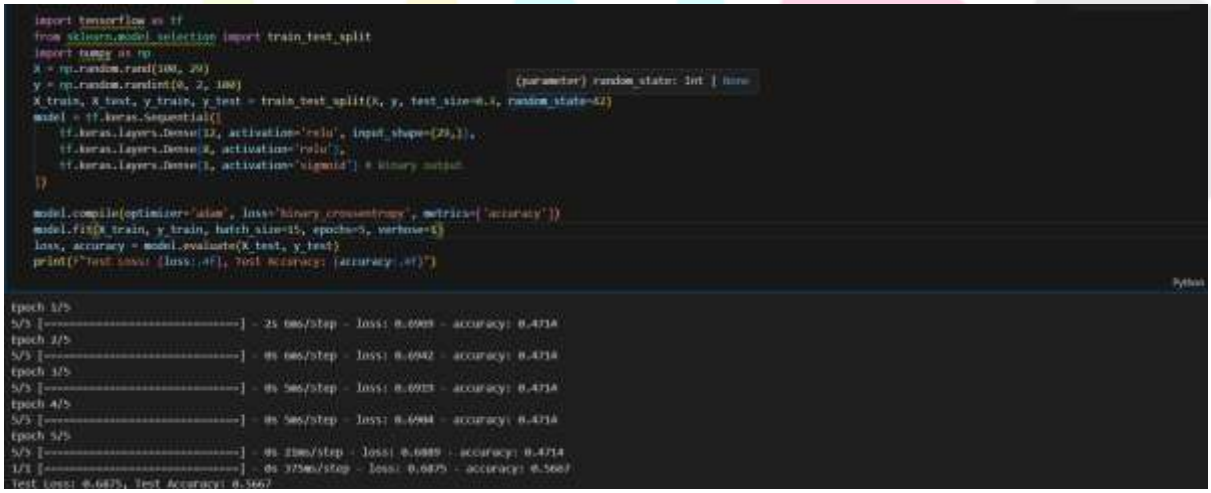


Fig: balanced dataset



IV. RESULTS:

In this project we are using python logistic regression algorithm and machine learning techiniques to detect fraud transaction in credit cards. Using datasetc called 'CreditCardFraud.csv' file we will train some machine learning algorithms algorithms and then we will upload test data file and this test data will be applied on machine learning techiniques train model to predict whether test data contains normal or fraud transaction signatures. When we upload test data then it will contain only transaction data no class label will be there application will predict and give the result

V. DISCUSSIONS:

This project helps to find out the normal transactions and fruadlent transactions in credit card transactions by applying machine learning algorithms. Fraud detection methods are continuously developed to defend criminals in adapting to their fraudulent strategies. These frauds are classified as: Credit Card Frauds: Online and Offline • Card Theft • Account Bankruptcy • Device Intrusion • Application Fraud • Counterfeit Card • Telecommunication Fraud.

VI.CONCLUSION

In conclusion, this project on credit card fraud detection using Random Forest Classifier, Isolation tree model, Decision tree model, Logistic Regression and Naïve Bayes model is an effective example of how machine learning algorithms can be applied to real world problems. The project involved collecting a dataset of credit card transactions, preprocessing the data, engineering relevant features, training a Random Forest Classifier model, evaluating the model's performance using various metrics, and finally, deploying the model in production. Overall, the project highlights the importance of data preprocessing, feature engineering, and selecting appropriate machine learning algorithms for solving complex problems. The project also demonstrates the potential of machine learning algorithms in the financial industry for detecting fraud and improving security

VII. FUTURE SCOPE:

Application of more pre-processing techniques would also help. The SVM algorithm still suffers from the imbalanced dataset problem and requires more pre-processing to give better results at the results shown by SVM is great but it could have been better if more pre-processing have been done on the data.New adavanced techiniques and algoithms should be used to develop credit card fraud detection in more efficient way

VIII. ACKNOWLEDGEMENT:

Kandhati Tulasi Krishna Kumar Nainar: Training & Placement Officer with 15 years' experience in training & placing the students into IT, ITES & Core profiles & trained more than 9,700 UG, PG candidates & trained more than 450 faculty through FDPs. Authored various books for the benefit of the diploma, pharmacy, engineering & pure science graduating students. He is a Certified Campus Recruitment Trainer from JNTUA, did his Master of Technology degree in CSE from VTA and in process of his Doctoral research. He is a professional in Pro-E, CNC certified by CITD He is recognized as an editorial member of IJIT (International Journal for Information Technology & member in IAAC, IEEE, MISTE, IAENG, ISOC, ISQEM, and SDIWC. He published 6 books, 55 articles in various international journals ONDatabases,SoftwareEngineering,HumanResourseManagementandCampus Recruit ment&Training.

Potnuri Jogibabu is pursuing his final semester MCA in Sanketika Vidya Parishad Engineering College, accredited with A grade by NAAC, affiliated by Andhra University and approved by AICTE. With interest in Machine learning P Jogibabu has taken up his PG project on REAL TIME CREDIT CARD FRUAD DETECTION BASED ON LOGISTIC REGRESSION IN MACHINE LEARNING and published the paper in connection to the project under the guidance of K TULASI KRISHNA KUMAR, Assistant Professor, Training and Placement officer, SVPEC

REFERENCES:

[1] A Feature engineering strategies for credit card fraud detection
https://www.sciencedirect.com/science/article/abs/pii/S0957417415008386
[2] A article of Credit Card Fraud Detection using Machine Learning Algorithms
https://www.sciencedirect.com/science/article/pii/S187705092030065X

[3] A **Review of Machine Learning Approach on Credit Card Fraud Detection**
https://link.springer.com/article/10.1007/s44230-022-00004-0
[4] Credit Card Fraud Detection Using Machine Learning As Data Mining Technique
https://jtec.utem.edu.my/jtec/article/view/3571
[5] Autonomous credit card fraud detection using machine learning approach
https://www.sciencedirect.com/science/article/abs/pii/S0045790622003822
[6] A machine learning based credit card fraud detection using the GA algorithm for feature selection
https://link.springer.com/article/10.1186/s40537-022-00573-8
[7] A Review of Machine Learning Applications for Credit Card Fraud Detection with A Case study
https://www.journal.seisense.com/jom/article/view/770
[8] A survey of machine-learning and nature-inspired based credit card fraud detection techniques
https://link.springer.com/article/10.1007/s13198-016-0551-y
[9] Uncertainty-aware credit card fraud detection using deep learning
https://www.sciencedirect.com/science/article/abs/pii/S0952197623004323
[10] Credit card fraud detection in the era of disruptive technologies: A systematic review
https://www.sciencedirect.com/science/article/pii/S1319157822004062
[11] Champion-challenger analysis for credit card fraud detection: Hybrid ensemble and deep learning
https://www.sciencedirect.com/science/article/abs/pii/S0957417419302167
[12] Unbalanced Credit Card Fraud Detection Data: A Machine Learning-Oriented Comparative Study of Balancing Techniques
https://www.sciencedirect.com/science/article/pii/S1877050923002314
[13] Predictive Modelling For Credit Card Fraud Detection Using Data Analytics
https://www.sciencedirect.com/science/article/pii/S1877050918309347
[14] Anomaly Credit Card Fraud Detection Using Deep Learning
https://link.springer.com/chapter/10.1007/978-3-030-75855-4_12
[15] Enhancing Credit Card Fraud Detection: An Ensemble Machine Learning Approach
https://www.mdpi.com/2504-2289/8/1/6
[16] Fraud Detection in Credit Card Data Using Machine Learning Techniques
https://link.springer.com/chapter/10.1007/978-981-15-6318-8_31
[17] A systematic review of literature on credit card cyber fraud detection using machine and deep learning
https://peerj.com/articles/cs-1278/
[18] Credit Card Fraud Detection using Machine Learning: A Study
https://arxiv.org/abs/2108.10005
[19] A survey of machine-learning and nature-inspired based credit card fraud detection techniques
https://link.springer.com/article/10.1007/s13198-016-0551-y
[20] A Review of Machine Learning Algorithms for Fraud Detection in Credit Card Transaction
https://koreascience.kr/article/JAKO202129436693259.page
[21] Autonomous credit card fraud detection using machine learning approach
https://www.sciencedirect.com/science/article/abs/pii/S0045790622003822
[22] Credit card fraud detection using a deep learning multistage model
https://link.springer.com/article/10.1007/s11227-022-04465-9
[23] Credit Card Fraud Detection Using K-Means and Fuzzy C-Means
https://www.igi-global.com/chapter/credit-card-fraud-detection-using-k-means-and-fuzzy-c-means/285690
[24] Credit card fraud detection: A fusion approach using Dempster–Shafer theory and Bayesian learning
https://www.sciencedirect.com/science/article/abs/pii/S1566253509000141
[25] Credit Card Fraud Detection Using Convolutional Neural Networks
https://link.springer.com/chapter/10.1007/978-3-319-46675-0_53
[26] Using generative adversarial networks for improving classification effectiveness in credit card fraud detection
https://www.sciencedirect.com/science/article/abs/pii/S0020025517311519
[27] Refined Weighted Random Forest and Its Application to Credit Card Fraud Detection
https://link.springer.com/chapter/10.1007/978-3-030-04648-4_29
[28] A systematic review of literature on credit card cyber fraud detection using machine and deep learning
https://peerj.com/articles/cs-1278/
[29] Classification of Credit Card Frauds Using Autoencoded Features
https://link.springer.com/chapter/10.1007/978-981-19-4162-7_2