A PROJECT REPORT

on

“Fraudulent Transaction Detection Model”

Submitted to

CELEBAL TECHNOLOGIES

In Fulfilment of

Data Science Internship

Prepared by : Group 3

Name	Email
Aman Raj	2005362@kiit.ac.in
Rishabh Kumar	rishabhquasar23@gmail.com
Simran Bhardwaj	Simranbhardwaj2607@gmail.com
Vardaan Khosla	Khoslavardaan1@gmail.com
Sharad Kumar Agarwal	Skagarwal485@gmail.com
Dipti Verma	2006173@kiit.ac.in

UNDER THE GUIDANCE OF

Arpit Jain Sir

July 2023

Acknowledgement

It gives us immense pleasure to present before you our project titled “Fraud transaction detection model”. The joy and satisfaction that accompany the successful completion of any task would be incomplete without the mention of those who made it possible. We are glad to express our gratitude towards our prestigious Company **Celebal Technologies** for providing us with utmost knowledge, encouragement and the maximum facilities in undertaking this project. We express our deepest gratitude and special thanks to **Arpit Jain** Sir for his guidance and encouragement.

RISHABH KUMAR
AMAN RAJ
DIPTI VERMA
SHARAD KUMAR AGARWAL
SIMRAN BHARDWAJ
VARDAAN KHOSLA

ABSTRACT

Fraudulent transactions pose a significant threat to financial institutions and businesses, leading to substantial financial losses and damaged customer trust. To mitigate this risk, a robust and efficient fraud detection system is essential. This paper presents a machine learning-based fraudulent transaction detection model that leverages the power of artificial intelligence to detect and prevent fraudulent activities in real-time.

The proposed model utilizes a vast dataset of historical transaction records, including both legitimate and fraudulent transactions, to train and fine-tune several machine learning algorithms. These algorithms encompass a wide range of techniques such as logistic regression, random forests, gradient boosting, and deep neural networks. The features extracted from the transaction data include transaction amounts, timestamps, payment behaviour patterns.

Keywords:
Machine Learning, Classification, Fraud detection, Sampling.

CONTENTS

INTRODUCTION

In today's digital era, financial transactions have become an integral part of our daily lives, encompassing online shopping, electronic payments, and mobile banking. While this convenience has revolutionized the way we conduct business and manage our finances, it has also opened the door to a growing threat – fraudulent transactions. The surge in sophisticated fraud attempts poses significant challenges to financial institutions and businesses, necessitating the development of advanced and efficient fraud detection systems.

This project aims to address the pressing need for a robust and reliable fraud detection model using machine learning techniques. Traditional rule-based systems, which rely on predefined rules to flag suspicious transactions, often struggle to keep up with the ever-evolving tactics employed by fraudsters. As a consequence, legitimate transactions can be falsely identified as fraudulent (false positives), leading to unnecessary inconveniences for customers and negatively impacting user experience.

To bridge these gaps and improve fraud detection capabilities, machine learning-based solutions have emerged as a promising alternative. Machine learning algorithms can automatically learn from historical transaction data and identify intricate patterns and anomalies that might indicate fraudulent activities. By leveraging these techniques, the proposed model aims to significantly enhance fraud detection accuracy while minimizing false positives and false negatives.
This project will draw upon a diverse dataset encompassing both legitimate and fraudulent transactions, enabling the model to learn from real-world scenarios and recognize complex fraud patterns. Additionally, the model will be designed to adapt dynamically, continuously updating its algorithms based on new data to stay ahead of emerging fraud tactics.

The development of an effective machine learning-based fraudulent transaction detection model is crucial not only for the financial sector but also for businesses across various industries that process online payments and transactions. By implementing such a solution, organizations can bolster their security measures, protect their customers from financial losses, and safeguard their reputation. The recent developments in AI provide a clear view of future techniques that will be used with Machine Learning and will act as a boon to the society.

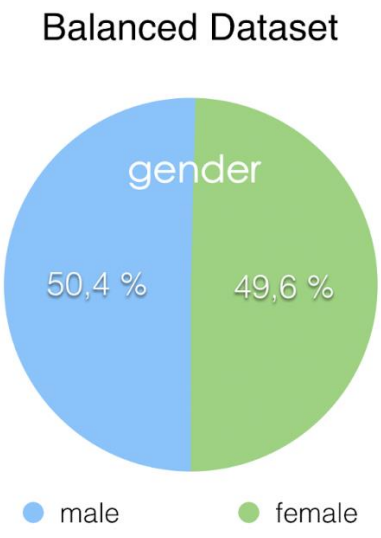
LITERATURE REVIEW

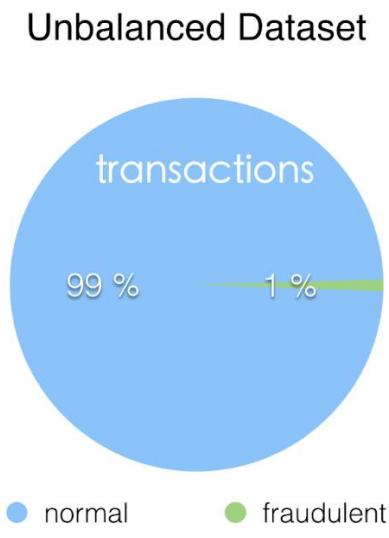
2.1 Handling Imbalanced Data

Imbalanced data refers to a situation, primarily in classification machine learning, where one target class represents a significant proportion of observations. Imbalanced datasets are those where there is a severe skew in the class distribution, such as 1:100 or 1:1000 examples in the minority class to the majority class.

Class Imbalance appear in many domains, including:

- Fraud detection (the vast majority of the transactions will be in the "Not-Fraud" class)
- Disease screening (the vast majority will be healthy)
- Subscription churn (the vast majority of customers stay with the service - the "No-Churn" class)
- Ad Serving (click prediction datasets don't have a high click-through rate)





There are several approaches to solving class imbalance problem before starting classification, such as:

- More samples from the minority class(es) should be acquired from the knowledge domain.
- Changing the loss function to give the failing minority class a higher cost.
- Oversampling the minority class.
- Undersampling the majority class.
- Any combination of previous approaches.

Oversampling methods duplicate or create new synthetic examples in the minority class, whereas undersampling methods delete or merge examples in the majority class.

2.2 Classification

Classification is a fundamental task in machine learning, where the goal is to assign input data points to predefined categories or classes based on their features. In the context of fraudulent transaction detection, classification methods are utilized to identify whether a given transaction is legitimate or fraudulent. There are several classification algorithms commonly employed for this purpose, each with its strengths and weaknesses. Here are some popular classification methods used in fraudulent transaction detection:

- Logistic Regression is a simple and interpretable classification algorithm that models the probability of an input belonging to a particular class. It works well for linearly separable data and is often used as a baseline model for binary classification tasks. In the context of fraudulent transaction detection, logistic regression can be used to predict the probability of a transaction being fraudulent based on relevant features.

- Decision Trees are non-linear models that partition the feature space into hierarchical segments, where each node represents a decision based on a specific feature. This makes them suitable for capturing non-linear relationships in the data. Decision Trees can be useful for identifying key features that contribute to fraudulent transactions and are often combined with other ensemble methods to improve their performance.

- Random Forests is an ensemble learning method that combines multiple decision trees to improve classification accuracy. It works by aggregating predictions from individual decision trees, reducing overfitting, and increasing generalization. Random Forests are robust and can handle large datasets with high-dimensional feature spaces, making them popular in fraud detection applications.

- SVM is a powerful classification algorithm that finds the optimal hyperplane to separate different classes in the feature space. SVM can handle both linearly separable and non-linearly separable data by employing different kernel functions. While SVMs have been used for fraud detection, their performance might be affected by the choice of the kernel and the dataset size.

- XGBoost is an optimized and scalable implementation of gradient boosting that often outperforms other algorithms in various machine learning tasks. It is well-suited for handling imbalanced data and is widely used in fraudulent transaction detection for its efficiency and accuracy.

- Naive Bayes is a probabilistic classifier that assumes independence between features given the class label. Despite its simplicity, Naive Bayes can perform surprisingly well on certain types of datasets and is computationally efficient, making it a viable option for quick initial experiments in fraud detection.

PROBLEM STATEMENT

Develop a machine learning model to identify fraudulent transactions in financial data, helping banks and credit card companies detect potential fraud and improve security.

3.1 Project Planning

Project Overview :
The goal of this project is to design and implement a transaction classification model that can accurately identify and classify between Fraudulent and Genuine transactions.

Project Scope :
• Collecting and pre-processing a dataset of transaction samples
• Data Encoding to handle object type features
• Undersampling to handle imbalanced data
• Scaling Dataset
• Classification models
• Application deployment

Timeline :
• Phase 1: Data Collection, Pre-processing (1 day)
• Phase 2: Model Selection and design (1 day)
• Phase 3: Model Training and Evaluation (2 days)
• Phase 4: Result analysis & app deployment(2 days)

Resources :
• A dataset of financial transactions with relevant features
• A computing environment with sufficient processing power and memory
• Machine learning libraries and frameworks (e.g., Scikit-learn)
• A cloud framework to deploy model application

Deliverables :

• A pre-processed dataset of known transaction samples
• Encoded, undersampled & scaled dataset
• A machine learning model capable of classifying transactions
• Working model application
• A report summarizing the performance of the model

Risks and Mitigation Strategies :

• Imbalanced data : To mitigate this risk, we will undersample the data.
• Deployment issues : To mitigate this risk, we will thoroughly test the model in a staging environment before deploying it to production.

Conclusion :

This project aims to develop a financial transaction classification model that can accurately identify and classify between fraudulent & genuine transactions. By following the proposed timeline and leveraging appropriate resources, we are confident that we can successfully deliver a model that meets the project objectives.

3.2 SRS

1. Introduction

1.1 Purpose
The purpose of this document is to specify the requirements for fraudulent transaction classification model using machine learning.

1.2 Scope
This software system model will provide a classification between fraud and genuine transactions based on their characteristics such as type, amount. The system model will be developed using machine learning techniques.

1.3 References
IEEE Std 830-1998: IEEE Recommended Practice for Software Requirements Specifications.

1.4 Overview
This document is divided into several sections, including an overview of the system, functional and non-functional requirements & constraints.

2. Overall Description

2.1 Project Perspective
The transaction classification model will be a standalone software system model that can be used by security professionals and researchers to classify different types of transactions.

2.2 Project Functions
The system will allow users to enter suspicious transaction data in form of some of the features like amount, mode of payment, etc. extract relevant features from the uploaded samples, train a machine learning model, and classify the samples. The system will also provide a user interface for interacting with the system, allowing users to view the classification results.

2.3 User Characteristics
The system will be used by security professionals and researchers who have knowledge of tackling financial frauds using and machine learning techniques.

2.4 Constraints
a) Data privacy: The system must comply with data privacy regulations.

b) Hardware limitations: The system must be able to run on standard hardware, such as a laptop, local server, or cloud without requiring specialized hardware or GPUs.

c) Time constraints: The development of the transaction classification model must be completed within a week.

2.5 Assumptions and Dependencies
The following assumptions and dependencies have been identified:
a) The system assumes that the uploaded transaction samples are not harmful and do not contain any sensitive or confidential information.

2.6 Data characteristics
Shape of the dataset : 6362620 rows × 11 columns

Features :

1. step: represents a unit of time where 1 step equals 1 hour
2. type: type of online transaction
3. amount: the amount of the transaction
4. nameOrig: customer starting the transaction
5. oldbalanceOrg: balance before the transaction
6. newbalanceOrig: balance after the transaction
7. nameDest: recipient of the transaction

8. oldbalanceDest: initial balance of recipient before the transaction
9. newbalanceDest: the new balance of recipient after the transaction
10. isFraud: fraud transaction
11. isflaggedfraud: This column wasnt included in the dataset information that was provided, so we will drop this column as the labeled column is already present.

3. System Features

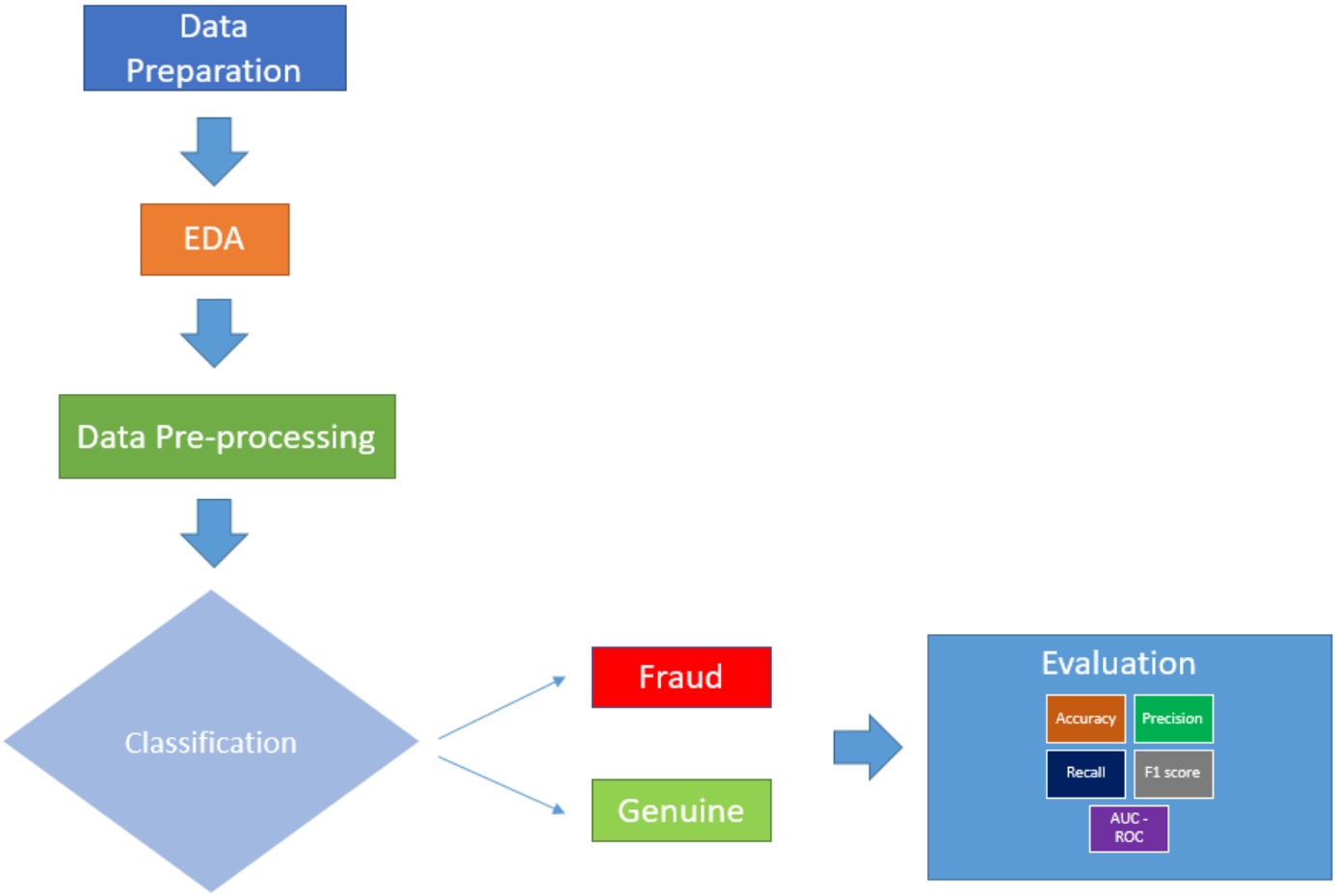
3.1 Functional Requirements

The following functional requirements describe the behavior of the classification model:
REQ-1: The system shall allow users to upload transaction samples dataset.
REQ-2: The system shall extract relevant features from the uploaded data like amount, type of payment, etc.
REQ-3: The system should encode, sample & scale the data efficiently.
REQ-4: The system shall allow users to view the classification results.
REQ-6: The system shall be scalable and able to handle increasing amounts of data and users

3.2 Non-Functional Requirements

The following non-functional requirements describe the performance, reliability, and usability of the classification model:
a) Performance
b) Reliability
c) Usability
d) Security
e) Maintainability

3.3 System Design



IMPLEMENTATION

4.1 Methodology

1. Data Preparation:
    - Collecting & loading the data
    - Cleaning & handling missing values
    - Feature engineering

2. EDA to get insights

3. Data Preprocessing
    - Dropping unnecessary features
    - Handling Outliers
    - Encoding categorical features
    - Splitting independent and target variable
    - Undersampling to handle data imbalance
    - Scaling to normalize data

4. Classification algorithms applied:
    - Logistic Regression
    - LDA
    - Decision Tree
    - KNN
    - NB

5. Evaluation:
    - F1 score - The F1 score is the harmonic mean of precision and recall. It balances precision and recall, making it useful when there is an uneven class distribution.
    - Precision - Precision is the proportion of true positive predictions out of all positive predictions (both true and false). It helps to assess the accuracy of positive predictions made by the model.
    - Accuracy - Accuracy is the ratio of correctly predicted instances to the total number of instances in the dataset. It provides a general overview of how well the model performs across all classes.
    - Recall - Recall is the proportion of true positive predictions out of all actual positive instances. It helps to evaluate the model's ability to correctly identify positive instances.

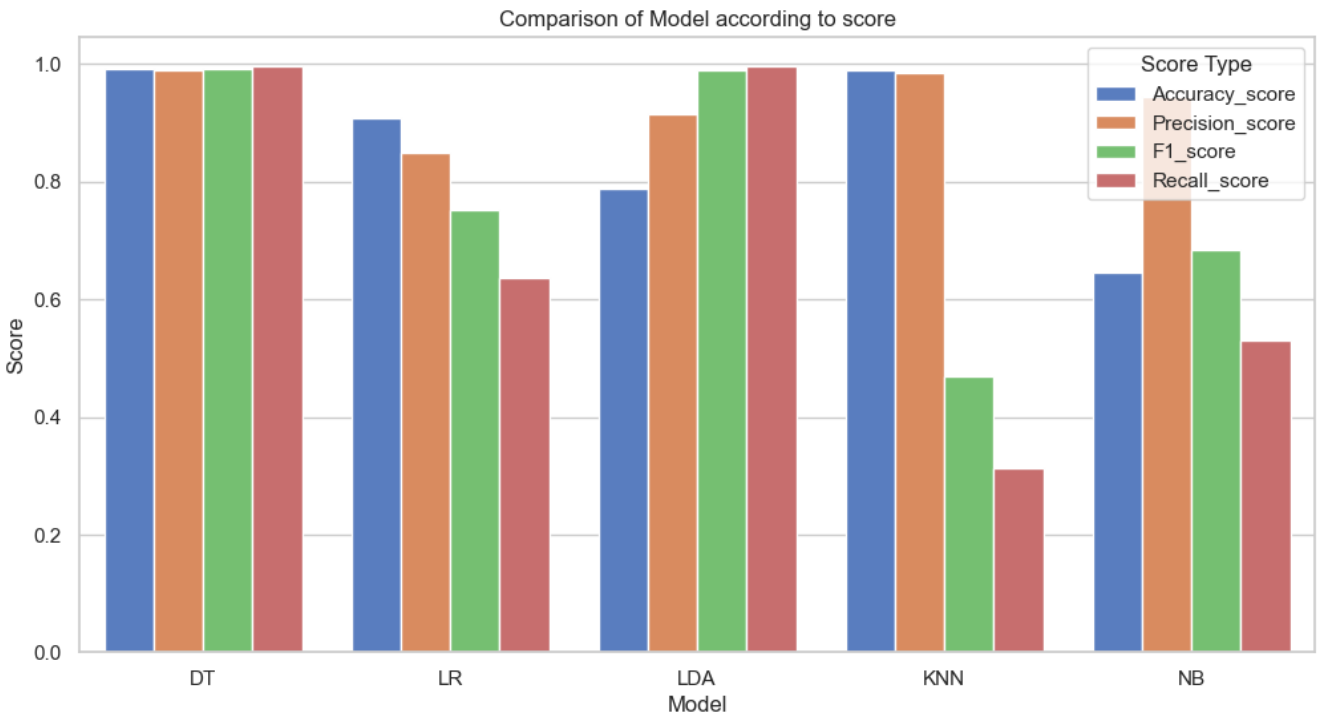
- AUC-ROC - The ROC curve plots the true positive rate (recall) against the false positive rate at various classification thresholds. The area under the ROC curve (AUC-ROC) is a measure of the model's overall performance, with a higher value indicating better performance.

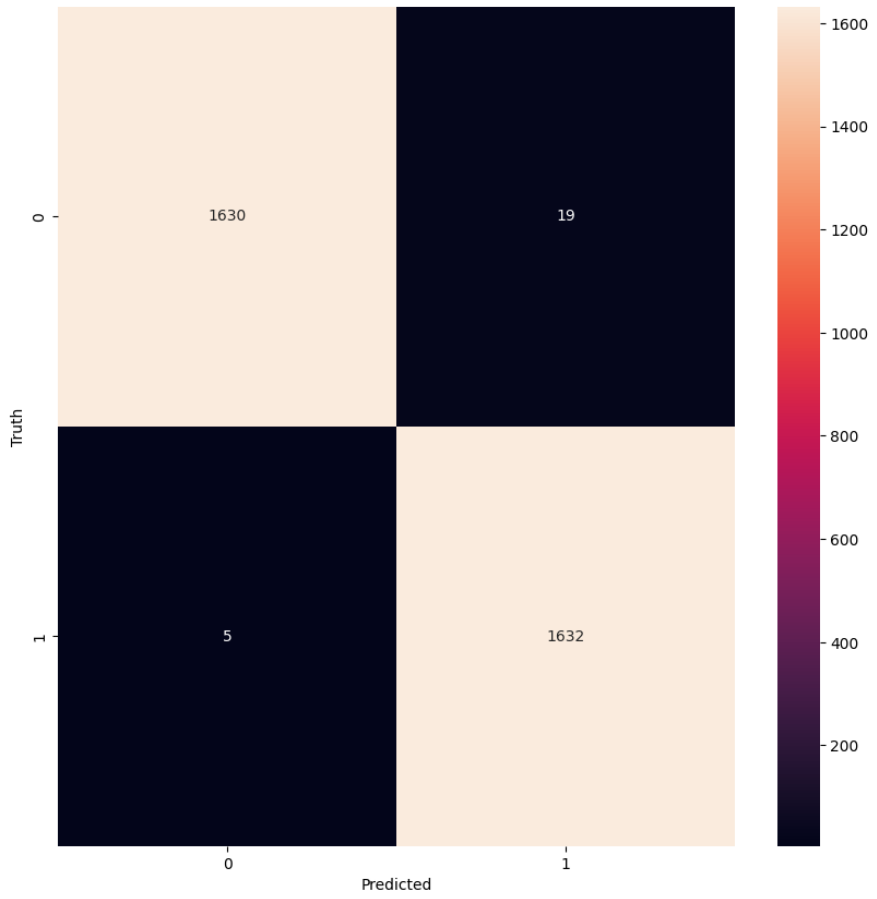
- Confusion Matrix - A confusion matrix is a table that summarizes the model's performance by comparing predicted labels with actual labels. It consists of four values: True Positive (TP), True Negative (TN), False Positive (FP), and False Negative (FN). From the confusion matrix, we can calculate various metrics such as accuracy, precision, recall (sensitivity), specificity, and F1 score.

6. Model Selection based on evaluation metrics

7. Model application development & deployment

4.2 Result Analysis





Model	Accuracy	Precision	F1	Recall
DT	0.993	0.989	0.992	0.996
LR	0.908	0.85	0.751	0.636
LDA	0.789	0.916	0.99	0.996
KNN	0.99	0.985	0.469	0.312
NB	0.646	0.944	0.684	0.53

CONCLUSION

Fraud transaction detection models in machine learning have proven to be highly effective and valuable tools in the fight against financial crimes. These models leverage advanced algorithms and sophisticated data processing techniques to identify fraudulent activities accurately and efficiently. The benefits of employing such models include: Enhanced Accuracy, Real-time Detection, Cost-effectiveness, Scalability, Continuous Improvement. However, it is crucial to acknowledge some potential challenges and considerations:Data Quality, False Positives, Adversarial Attacks, etc.

To address these challenges and maximize the potential benefits of ML-based fraud detection, continuous research, and development are necessary. Regular model retraining and staying up-to-date with the latest advancements in machine learning techniques are crucial to maintaining the model's effectiveness and keeping pace with evolving fraud tactics. Overall, ML-based fraud transaction detection models remain an indispensable tool in safeguarding financial systems and ensuring secure and reliable transactions for businesses and consumers alike.

References :

Dataset link :
https://www.kaggle.com/datasets/rupakroy/online-payments-fraud-detection-dataset

1. *https://www.kaggle.com/code/marcinrutecki/best-techniques-and-metrics-for-imbalanced-dataset/notebook*
2. *https://www.javatpoint.com/classification-algorithm-in-machine-learning*
3. *https://www.analyticsvidhya.com/blog/2021/07/metrics-to-evaluate-your-classification-model-to-take-the-right-decisions/*
4. *https://towardsdatascience.com/oversampling-and-undersampling-5e2bbaf56dcf*
5. *https://www.analyticsvidhya.com/blog/2020/07/10-techniques-to-deal-with-class-imbalance-in-machine-learning/*

INDIVIDUAL CONTRIBUTION REPORT :

Contributions:

Aman Raj - Project report / documentation

Rishabh Kumar - data cleaning, EDA, outlier

Sharad Kumar Agarwal - undersampling, deployment

Dipti Verma – classification, model deployment, evaluation metrics and comparision

Simran Bhardwaj - Ppt presentation

Vardaan Khosla - Ppt presentation