**Fraud Detection System – Project Report**

**1. Introduction**

Financial fraud, especially in the form of credit card fraud, is a major concern for banks and e-commerce platforms. With millions of transactions processed every day, manually identifying fraud is impossible. This project aims to build a machine learning-based fraud detection system that automatically detects suspicious transactions with high accuracy.

We used the Credit Card Fraud Detection Dataset, which contains anonymized transaction data of European cardholders. Our system was built using supervised learning techniques, and it evaluates transactions based on historical data labeled as either fraudulent or legitimate.

**2. Dataset Description**

* Source: Kaggle Credit Card Fraud Dataset
* Size: 284,807 transactions
* Features: 30 anonymized features (V1–V28), Time, Amount
* Target: Class (0 = Legitimate, 1 = Fraudulent)
* Issue: Highly imbalanced data
  + Legitimate: ~99.83%
  + Fraudulent: ~0.17%

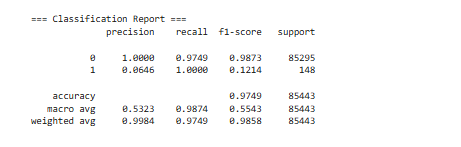
**3. Data Preprocessing**

* Feature Scaling: Applied StandardScaler to Time and Amount.
* Train-Test Split: Used 70% for training and 30% for testing with stratification.
* Imbalance Handling: Applied undersampling of the majority class to balance the dataset.
  + Fraudulent samples: 492
  + Undersampled legitimate samples: 492
  + Final training set size: 984 samples

**4. Model Development**

* We used a Random Forest Classifier:
  + Robust to outliers
  + Works well on imbalanced datasets
  + Easy to interpret and tune

**5. Explanation of Results**

****

**Interpretation:**

The classification report shows the performance of a fraud detection model on an imbalanced dataset. For legitimate transactions (class 0), the model performs exceptionally well. It achieved a precision of 1.0000, meaning that all transactions predicted as legitimate were truly legitimate. The recall is 0.9749, indicating that about 97.5% of actual legitimate transactions were correctly identified. This results in a strong F1-score of 0.9873, reflecting a good balance between precision and recall for the majority class.

On the other hand, the performance on fraudulent transactions (class 1) is mixed. The model achieved a recall of 1.0000, which means it successfully identified all actual fraud cases. This is a highly desirable outcome in fraud detection, as it ensures no fraudulent transaction goes undetected. However, the precision is very low at 0.0646, suggesting that a large number of transactions flagged as fraud were actually legitimate. This leads to a low F1-score of 0.1214, indicating a poor balance between precision and recall for the minority class.

The overall accuracy of the model is 97.49%, but due to class imbalance, this metric is misleading. Most of the transactions are legitimate, so high accuracy can still be achieved even if many fraud cases are misclassified. The macro average F1-score is 0.5543, reflecting the imbalance in performance across classes, while the weighted average F1-score is 0.9858, heavily influenced by the majority class.

In conclusion, the model is very effective at identifying all frauds (high recall), but it does so at the cost of incorrectly flagging many legitimate transactions as fraudulent (low precision). This could lead to customer dissatisfaction and unnecessary investigation efforts in real-world applications. Improving precision without compromising recall—possibly through threshold tuning, advanced sampling techniques, or cost-sensitive learning—would help build a more balanced and practical fraud detection system.

Git hub link:

<https://github.com/hania27808/fraud-detection-system>

Note:

Due to the large size of the dataset (more than 100 MB), it could not be uploaded directly to this GitHub repository.

You can download the original dataset from the following official source:  
Credit Card Fraud Detection Dataset – Kaggle