Final Capstone Project Report: Credit Card Fraud Detection

1. Introduction

Problem Statement
Credit card fraud is a significant issue in the financial industry, causing substantial monetary losses annually. The objective of this project is to develop a machine learning model to detect fraudulent credit card transactions accurately. This will help minimize false positives while maintaining high recall for fraud detection.

Objectives
- Analyze the given dataset to understand the distribution of features and the imbalance in class labels.
- Build a machine learning model capable of classifying transactions as fraudulent or non-fraudulent.
- Optimize the model through hyperparameter tuning to improve performance.
- Evaluate the model using key metrics such as precision, recall, F1-score, and ROC-AUC.

2. Dataset Overview

Source
The dataset contains transactions made by European cardholders in September 2013. It includes:

- **284,807 transactions** over two days.
- **Highly imbalanced classes:** ~99.8% non-fraudulent (Class 0) and ~0.2% fraudulent (Class 1).

Features
- **Time:** Seconds elapsed between this transaction and the first transaction.
- **Amount**: The transaction amount.
- **V1 to V28:** Principal components derived from PCA for anonymization.
- **Class:** Target variable (0 = non-fraud, 1 = fraud).

Preprocessing Steps
- Handled class imbalance using **SMOTE.**
- Standardized `Time` and `Amount` features using **StandardScaler**.

3. Modeling Approach

Baseline Model
- Used a **Random Forest Classifier** to establish a baseline performance.
- Evaluated the model using precision, recall, and ROC-AUC metrics.

Hyperparameter Tuning
- Simplified approach: Instead of exhaustive hyperparameter tuning (e.g., GridSearchCV), selected minimal effective parameters:
    - n_estimators=100
    - max_depth=10
- This ensured faster training while maintaining strong performance.

Metrics for Evaluation
- **Precision**: Fraction of correctly identified fraud cases out of all cases predicted as fraud.
- **Recall:** Fraction of actual fraud cases correctly identified.
- **F1-Score**: Harmonic mean of precision and recall.
- **ROC-AUC**: Measures the model's ability to distinguish between classes.

4. Results

Best Model
- **Model**: Random Forest Classifier

- **Parameters Used:**

n_estimators=100
max_depth=10

Evaluation Metrics

Before Tuning:

- Precision: 0.87
- Recall: 0.85
- F1-Score: 0.86
- ROC-AUC: 0.9849

After Tuning:

- **Precision**: 0.62
- **Recall**: 0.89
- **F1-Score**: 0.73
- **ROC-AUC**: 0.9852

Confusion Matrix:

Actual/Predicted	Predicted non-fraud	Predicted Fraud
Non-fraud (0)	56,810	54
Fraud (1)	11	87

5. Model Deployment

Saving the Model

- Saved the best model using **joblib**:

joblib.dump(loaded_model, "final_rf_model.pkl")

Loading the Model

- Reloaded the model for deployment:

deployed_model = joblib.load("final_rf_model.pkl")
print("Model loaded successfully")

Predictions on New Data

- Example predictions on the test dataset:
  - **Predictions**: [1, 0, 0, 0, 0]
  - **Fraud Probabilities**: [0.99944777, 0.0309337, 0.02403235, 0.01659746, 0.00282702]

7. Conclusion

The project successfully developed a machine learning model to detect fraudulent transactions with high precision and recall. The model can be deployed in real-world applications to assist financial institutions in mitigating fraud risks effectively.