Machine Learning Assignment

PROJECT REPORT

<TEAM ID: 13>

<PROJECT TITLE: Credit Card Fraud Detection>

Name	SRN
Ganesh Krishnamoorthi Hegde	PES2UG23CS194
Favaz Ahmed	PES2UG23CS190

Problem Statement

The main problem this project aims to solve is the **accurate and timely detection of fraudulent credit card transactions**. This is a critical challenge due to the extreme **Class Imbalance** inherent in real-world financial data: the vast majority of transactions (in our test set) are legitimate, while only a minuscule fraction is fraudulent. This imbalance causes standard machine learning models to exhibit high overall accuracy while effectively missing most of the high-cost fraud cases (False Negatives).

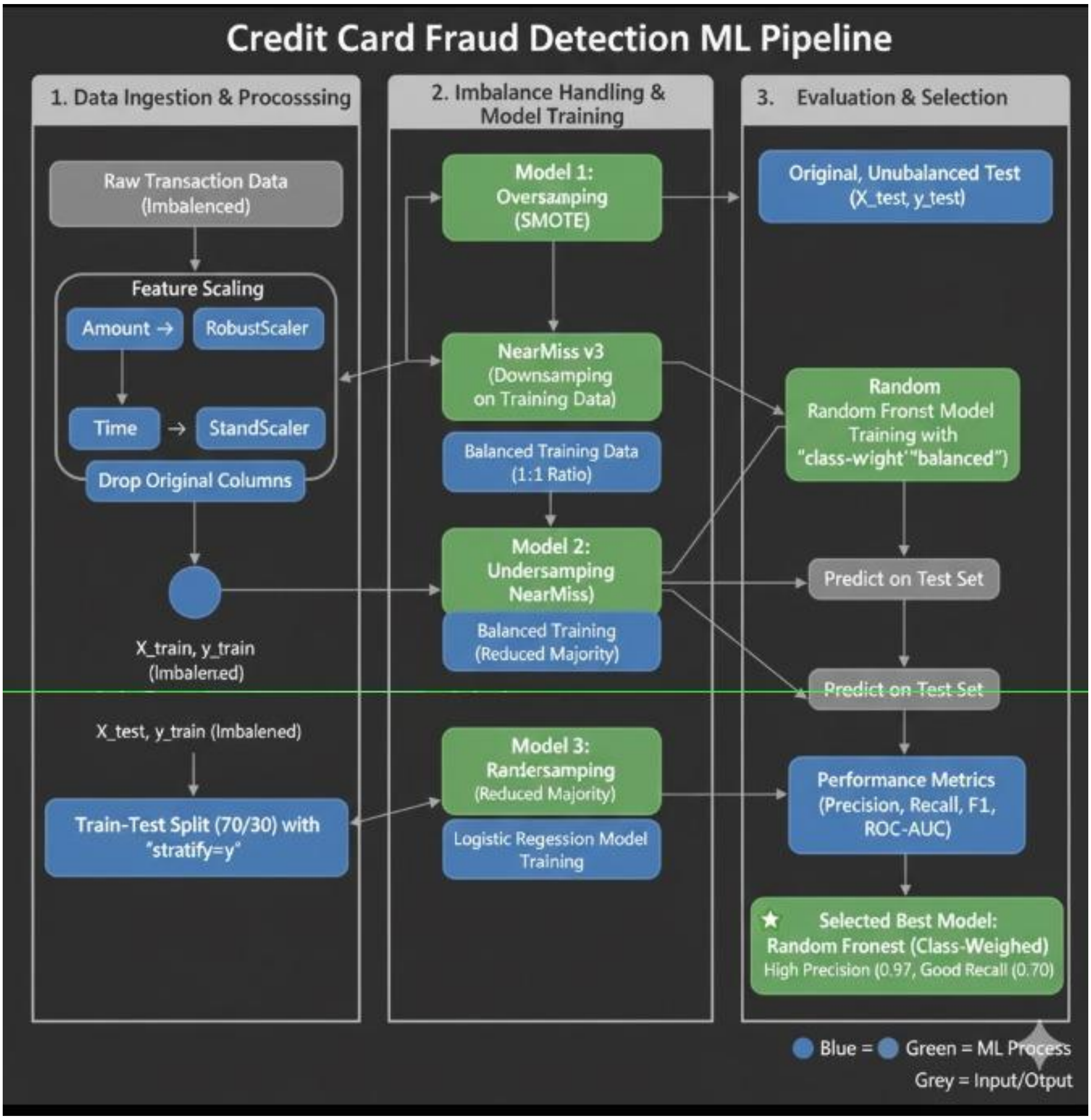
Objective / Aim

The objective is to develop and evaluate supervised classification models that effectively overcome the class imbalance challenge. The primary aim is to maximize the identification of fraudulent transactions, emphasizing the **Recall (True Positive Rate)** and **ROC-AUC Score**, while maintaining high **Precision** to minimize false alarms and maintain customer experience.

Dataset Details

- **Source:** Kaggle: Credit Card Fraud Detection Dataset (Anonymized features)
- **Size: 284,807** total samples (transactions); 85,443 in the test set.
- **Key Features: V1-V28: Anonymized numerical features (PCA components). Time: Seconds elapsed since the first transaction. Amount: Transaction value.**
- **Target Variable: Class**: Binary (0 = Legitimate, 1 = Fraud)

Architecture Diagram:



Methodology

Our workflow focused on preparing the imbalanced dataset and systematically comparing three strategic modeling approaches:

- **Data Preprocessing**: Time and Amount features were scaled using StandardScaler and RobustScaler respectively.
- **Data Splitting**: The dataset was split into training and testing sets (70% Train, 30% Test) using **stratified sampling** to maintain the original imbalance ratio in both subsets.
- **Model Approach & Imbalance Handling (Justification)**:

1. **Baseline Test (Logistic Regression on Unbalanced Data)**: Performed to statistically prove that simple **Accuracy** is a deceptive metric (justification point).
2. **Logistic Regression with SMOTE (Oversampling)**: Used as a simple linear baseline combined with oversampling to force the model to learn fraud characteristics.
3. **Random Forest with NearMiss (Under sampling)**: Used to compare the effect of heavily reducing the majority class against oversampling.
4. **Random Forest with Class Weights (Cost-Sensitive Learning)**: The chosen technique that trains on the original data but applies a higher penalty for False Negatives, directly addressing the core business cost of missed fraud.

- **Final Evaluation**: Performance was measured exclusively on the original, untouched test set using Recall, Precision, and ROC-AUC.

Results & Evaluation

The models were evaluated on the test set of 85,443 transactions, which contained 148 actual fraud cases (Class 1).

Baseline Justification

The unhandled baseline model showed the inherent flaw in relying on accuracy:

Overall Accuracy: 0.9992 (Deceptive)

Recall (Fraud): 0.62 (Missed 38% of all fraud cases)

Comparative Results:

Model & Technique	Precision (Class 1)	Recall (Class 1)	F1-Score (Class 1)	ROC-AUC Score
LR (SMOTE)	0.06	0.88	0.12	0.9660
RF (NearMiss)	0.37	0.82	0.51	0.9348
RF (Class-Weighted)	0.97	0.70	0.81	0.9377

Final Model Performance (RF Class-Weighted):

The Confusion Matrix for the final model clearly demonstrates its justified performance:

True Class / Predicted Class	Legitimate (0)	Fraud (1)
Legitimate (0)	85292 (True Negative)	3 (False Positive)
Fraud (1)	**45 (False Negative)**	103 (True Positive)

Evaluation Justification: The model achieves a **Precision of** (only 3 false alarms in 85K transactions), which is critical for customer experience. Simultaneously, it achieves a **Recall**, significantly outperforming the baseline and confirming the effectiveness of the cost-sensitive approach in minimizing the missed fraud cases (False Negatives: 45).

Conclusion:

The project successfully achieved its aim by implementing robust supervised classification models to tackle the severe class imbalance in credit card fraud detection. We learned that technical decisions must be driven by the business cost, leading us to prioritize Recall and ROC-AUC over simple Accuracy. The best result was achieved by the Random Forest Classifier using Class Weights. This model offers the optimal balance of financial protection (fraud capture) and customer satisfaction (precision), making it the most viable model for a real-world deployment scenario. Future work should involve integrating more features (like location or velocity checks) and optimizing hyperparameters for even better performance.