Fraud Transaction Detection Using Machine Learning

1. Introduction

Digital payment systems are increasingly vulnerable to fraudulent activities. Detecting fraudulent transactions accurately and efficiently is critical for financial institutions. This project focuses on building an end-to-end machine learning–based fraud detection system using transactional data.

2. Dataset Description

The dataset consists of simulated transaction records stored as daily .pkl files. Each transaction contains:

- TRANSACTION_ID
- TX_DATETIME
- CUSTOMER_ID
- TERMINAL_ID
- TX_AMOUNT
- TX_FRAUD (target variable)

Fraud labels were generated using three scenarios:

1. High-amount fraud (TX_AMOUNT > 220)
2. Terminal compromise fraud
3. Customer credential leakage fraud

3. Exploratory Data Analysis

EDA revealed that fraudulent transactions form a very small portion of the dataset, reflecting real-world class imbalance. Fraudulent transactions showed significantly higher transaction amounts and abnormal patterns across certain customers and terminals.

4. Feature Engineering

To capture fraud behavior, the following features were engineered:

- **Time-based features:** transaction hour, day of week, weekend flag
- **Customer behavior features:** average transaction amount, transaction count, deviation from normal spending
- **Terminal risk features:** terminal transaction count and terminal fraud rate

These features directly align with the fraud generation logic in the dataset.

5. Model Development

Two models were trained:

- **Random Forest Classifier** (baseline)
- **XGBoost Classifier** (advanced model)

Class imbalance was handled using class weighting and scale_pos_weight.

6. Model Evaluation

Models were evaluated using:

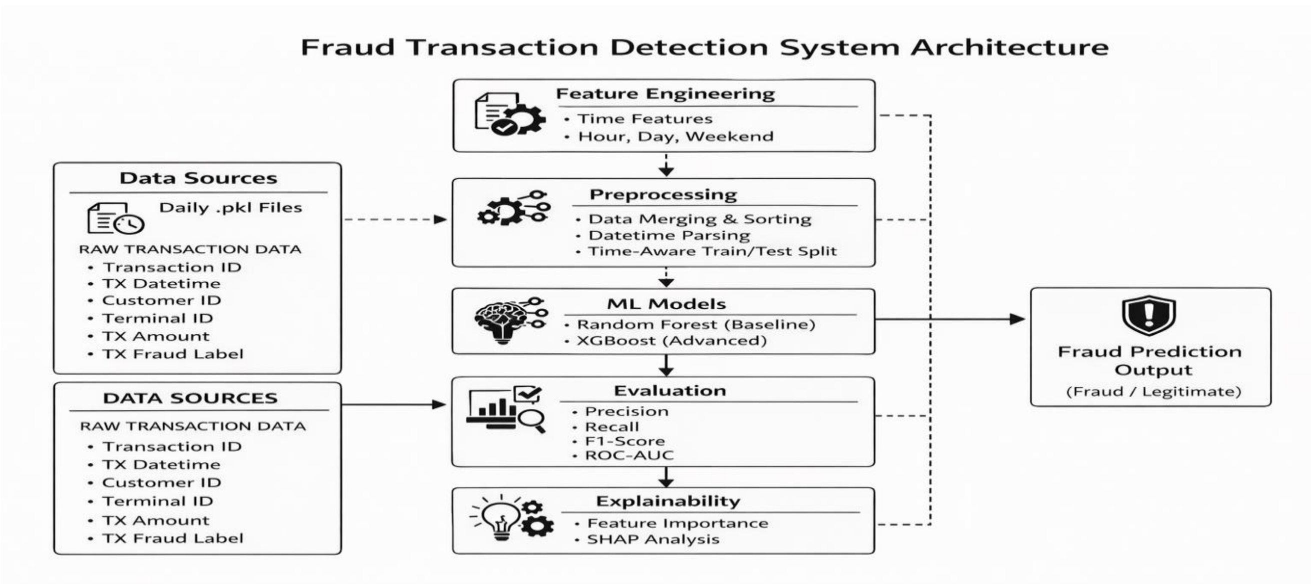
- Precision
- Recall
- F1-score
- ROC-AUC

Accuracy was avoided due to severe class imbalance. XGBoost achieved better recall and ROC-AUC, making it more suitable for fraud detection.

7. Explainability

Feature importance analysis showed that transaction amount, terminal fraud rate, and customer spending deviation were the strongest indicators of fraud. These results matched the known fraud simulation rules.

8. System Architecture



9. Conclusion

The project successfully demonstrates an end-to-end fraud detection pipeline. The final model captures multiple fraud patterns and provides reliable performance on imbalanced data. This system can be extended for real-world deployment with streaming data and real-time alerts.