Credit Card Fraud Detection Using Statistical Machine Learning

Understanding Credit Card Fraud

Defining Fraud

Fraud occurs when unauthorised individuals use stolen or compromised credit card details for transactions, leading to financial loss for both cardholders and financial institutions.

Common Types

- Card Not Present (CNP): Online or phone transactions without the physical card.
- Account Takeover (ATO): Fraudsters gain control of a legitimate account.
- Skimming: Devices illegally capture card information at point-of-sale terminals.
- Phishing: Deceptive emails or websites to trick users into revealing card details.

Rising Risk in India

With a significant 40% surge in digital payments in India during 2024, the potential for credit card fraud has also increased substantially, necessitating robust detection mechanisms.

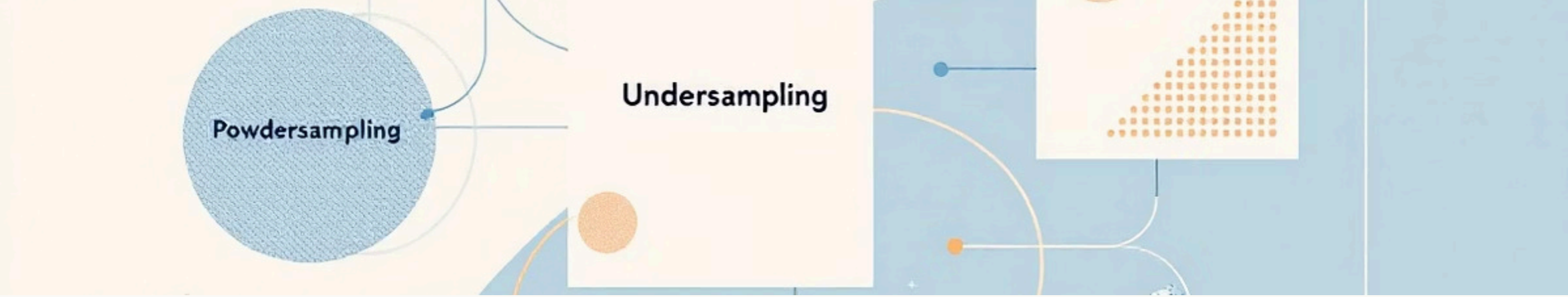
The Challenge: Detecting Fraud in Real-Time

Credit card fraud presents a unique challenge due to its rarity. Fraudulent transactions constitute less than 0.2% of all transactions, leading to highly imbalanced datasets for machine learning models.

Traditional rule-based systems, while effective for known patterns, struggle to adapt to the evolving tactics of fraudsters. This often results in a high number of false positives, inconveniencing legitimate customers and increasing operational costs for banks.

Dataset Overview

- The dataset, sourced from Kaggle, comprises **284,807 credit card transactions**.
- It includes **32 features**: V1 to V28, which are anonymised PCA (Principal Component Analysis) transformed components, along with 'Amount' and 'Time' of transaction.
- The 'Class' label indicates transaction type: **0 for legitimate transactions** and **1 for fraudulent ones**.
- A significant challenge is the **extreme class imbalance**: only 492 cases (~0.17%) are fraudulent, making accurate detection difficult without proper handling.



Data Preprocessing & Balancing Techniques

Addressing the severe class imbalance is crucial for building effective fraud detection models.

Random Oversampling

Duplicates instances of the minority class (fraudulent transactions) to increase its representation.

Random Undersampling

Reduces the number of instances in the majority class (legitimate transactions) to balance the dataset.

SMOTE (Synthetic Minority Over-sampling Technique)

Generates synthetic samples for the minority class, rather than just duplicating existing ones, offering a more robust approach.

Furthermore, feature scaling and normalisation were applied to ensure all features contribute equally to the model, improving stability and performance.

Supervised Machine Learning Models Used

Support Vector Machine (SVM)

SVM is a powerful binary classifier that finds an optimal hyperplane to separate data points into different classes. It performs effectively in fraud detection tasks due to its ability to handle complex decision boundaries.

XGBoost (Extreme Gradient Boosting)

An advanced ensemble method, XGBoost builds a strong predictive model by combining multiple weak prediction models, typically decision trees. It is highly efficient and robust against overfitting, making it ideal for imbalanced datasets.

Random Forest

This model constructs a multitude of decision trees during training and outputs the class that is the mode of the classes (classification) or mean prediction (regression) of the individual trees. It enhances robustness and reduces overfitting effectively.

How XGBoost Works for Fraud Detection

XGBoost is particularly effective for fraud detection due to its sophisticated approach to model building and error correction.

Sequential Tree Building

It sequentially builds decision trees, with each new tree correcting the errors of the previous ones, iteratively improving prediction accuracy.

Missing Data Handling

XGBoost natively handles missing data by learning the best imputation values for splits, ensuring no valuable information is lost.

Regularisation for Overfitting

It incorporates regularisation terms to penalise complex models, effectively preventing overfitting and enhancing generalisation to unseen data.

Parameter Tuning

Key parameters like learning rate (eta), max_depth of trees, gamma (minimum loss reduction), and the number of boosting rounds are meticulously tuned for optimal performance.

High Precision & Recall

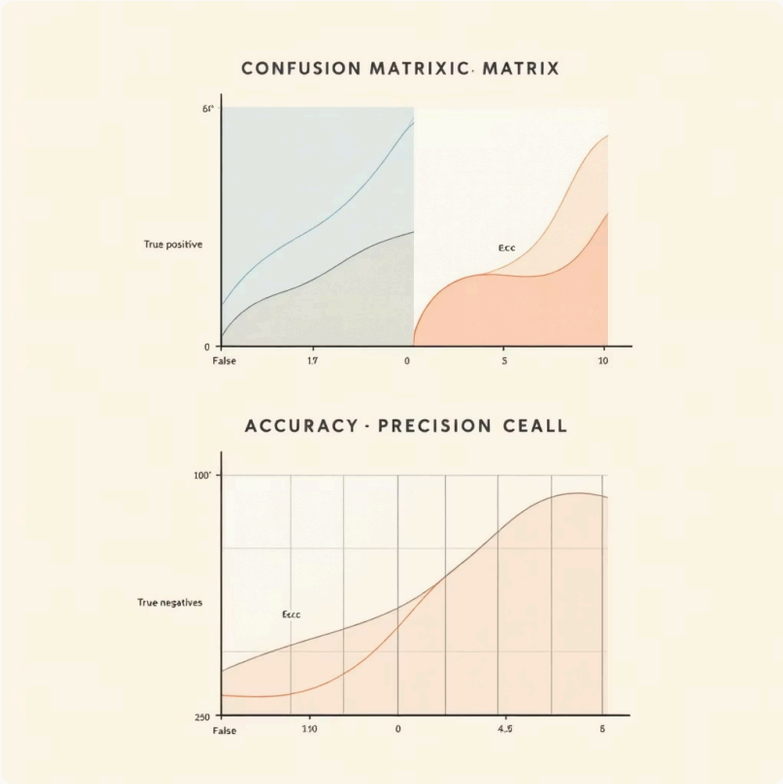
Through its iterative learning and robust optimisation, XGBoost achieves high precision and recall on the fraud class, crucial for identifying elusive fraudulent transactions.

Model Evaluation Metrics

Confusion Matrix

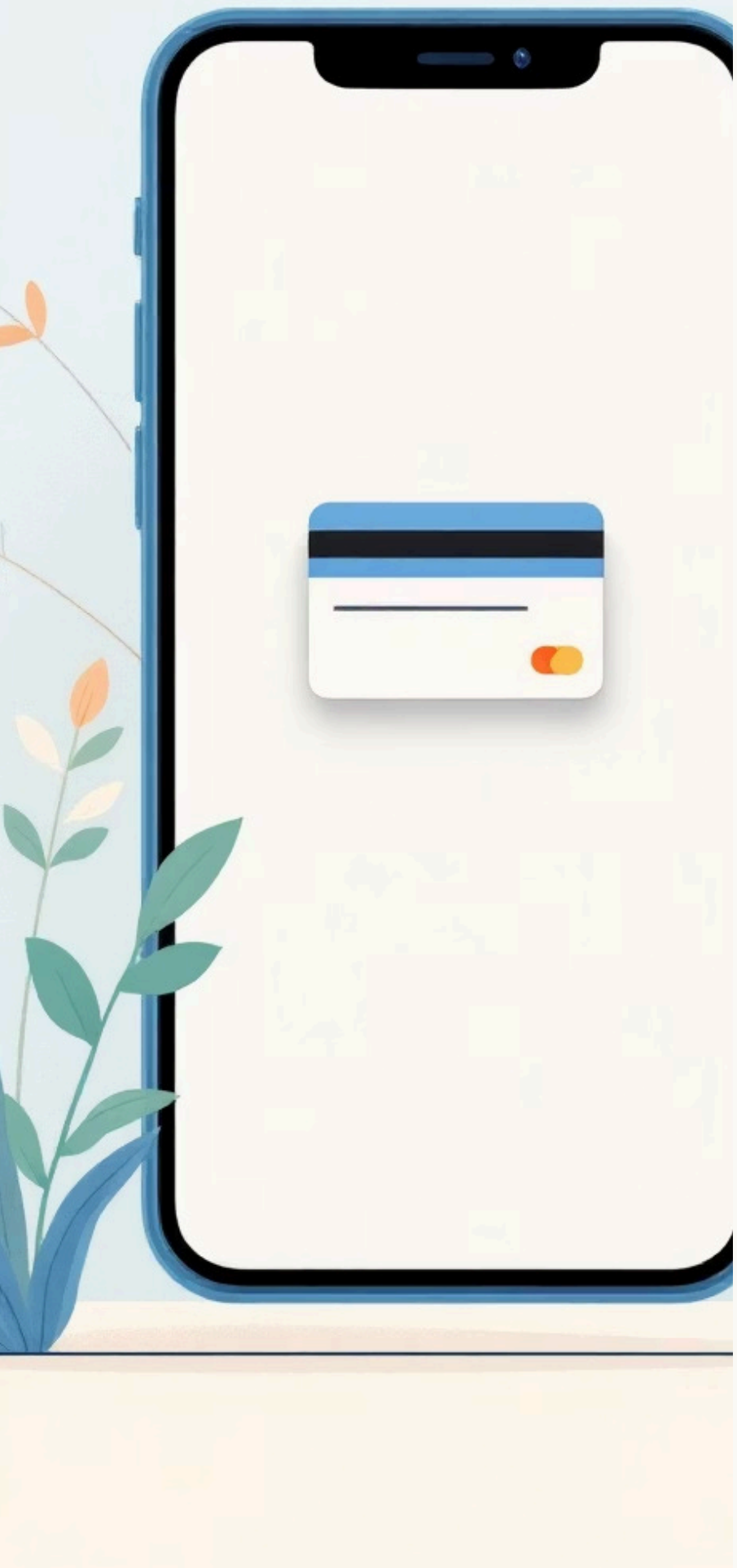
A crucial tool for assessing classifier performance, particularly with imbalanced data:

- **True Positives (TP)**: Actual fraudulent transactions correctly identified as fraud.
- **False Positives (FP)**: Legitimate transactions incorrectly flagged as fraud.
- **True Negatives (TN)**: Actual legitimate transactions correctly identified as legitimate.
- **False Negatives (FN)**: Actual fraudulent transactions incorrectly identified as legitimate.



Key Metrics

- **Accuracy**: Overall correctness of the model.
- **Precision**: (TP / (TP + FP)) - Measures the proportion of correctly predicted positive observations out of all predicted positives.
- **Recall (Sensitivity)**: (TP / (TP + FN)) - Measures the proportion of actual positives correctly identified.
- **F1-Score**: Harmonic mean of Precision and Recall, providing a balance between the two.



Real-World Impact & Benefits

Reduced Financial Losses

Early detection of fraudulent activities significantly minimises financial losses for both banks and their customers, safeguarding assets.

Enhanced Digital Trust

By ensuring secure transactions, AI-driven fraud detection builds greater trust in digital payment systems, vital for India's rapidly expanding e-commerce sector.

Scalable Processing

AI models can efficiently process millions of transactions daily with minimal latency, providing real-time protection without system slowdowns.

Seamless Security

These advanced security layers operate discreetly in the background, offering robust protection without inconveniencing genuine users or disrupting their payment experience.

Conclusion & Future Directions

Powerful Tools

Supervised ML models SVM offer robust capabilities for detecting credit card fraud.

Continuous Adaptation

Regular model retraining is essential to adapt to the dynamic and evolving patterns of fraud.

Advanced Techniques

Future work includes integrating unsupervised anomaly detection and deep learning for even higher accuracy.

Safeguarding India's Digital Economy

AI-driven fraud detection is crucial for protecting financial integrity and consumer confidence in India.