Machine Learning Models for Financial Risk Management

Viom Kapur, Ananya Basotia
Ashoka University

November 29, 2024

Abstract

This paper explores the utility of using machine learning decision tree models, namely XGBoost and Random Forest, for loan default prediction and deploying such models for the financial services industry in fraud detection. It highlights the crucial elements of sound approaches that consist of data preprocessing, feature engineering, model training, and the choice of the appropriate metrics for evaluation. It concludes that models designed for one purpose can be effectively repurposed to address another critical challenge in financial risk management.

1 Introduction

The financial industry is increasingly reliant on advanced analytical techniques to mitigate risks associated with loan defaults and fraudulent activities. Traditional methods often lack the precision needed to predict these events accurately, leading to significant financial losses. Machine learning (ML) models have emerged as powerful tools that can enhance predictive capabilities in these fields. This report details a broad-based approach to evaluate the performance of XGBoost and Random Forest algorithms on loan default predictions as well as their appropriateness for fraud prediction.

2 Problem Statement

The main problem that this paper deals with is the requirement of loan defaults and fraud prediction with high accuracy. The present models fail to capture financial data complexity, which leaves scope for many false positives and negatives. This paper attempts to measure whether machine learning models developed for loan default prediction can be effectively modified for fraud detection.

3 Objectives

The objectives of this research are as follows:

- Assess the performance of XGBoost and Random Forest algorithms in predicting loan defaults.

- Adapt the models for detecting fraudulent activities in financial datasets.
- Evaluate the performance of the models with multiple evaluation metrics to establish efficacy across different applications.

4 Methodology

4.1 Literature Review

A detailed review of the literature regarding machine learning applications in financial risk management was performed. This entailed reviewing previous research studies on loan default prediction and fraud detection, identifying features used in these models, and understanding the shortcomings of traditional approaches.

4.2 Data Collection

Publicly available datasets pertinent to loan defaults and fraudulent transactions were used:

- **Loan Default Dataset**: This dataset contains historical loan data with features such as borrower credit scores, loan amounts, payment history, and demographic information.
- **Fraud Detection Dataset**: This dataset includes transaction records with labels designated as either fraudulent or legitimate. The features include transaction amounts, timestamps, and user behavior patterns.

Data cleaning processes have been put in place to ensure quality and relevance, including:

- **Sanity Checks**: Checking data integrity to eliminate inconsistencies.
- **Data Exclusions**: Removing entries that are missing or erroneous.
- **Anomaly Detection**: Detection of outliers that could influence the outcome.

4.3 Feature Engineering

Feature engineering was done to improve the performance of the model:

- **SHAP Values**: SHapley Additive exPlanations were used to explain model predictions by quantifying the contribution of each feature.
- **Correlation Analysis**: Relationships among features were analyzed to identify redundant or irrelevant variables.
- **Principal Component Analysis (PCA)**: Used for dimensionality reduction while retaining variance.

4.4 Data Preprocessing

The following Python code snippets illustrate the data preprocessing steps undertaken:

```
[Python code omitted for brevity]
```

[language=Python]nm.py

4.5 Model Development

The experiment focused on the development of two major machine learning algorithms: 1. XGBoost (Extreme Gradient Boosting): - Ensemble learning approach that generates a sequence of weak learners (decision trees) in a sequential manner. - Makes use of gradient descent to minimize a loss function with the application of regularization to prevent overfitting.

The loss function of XGBoost is defined as follows:

$$L(\theta) = \sum_{i=1}^{n} l(y_i, f(x_i)) + \Omega(f)$$

Here, $l(y_i, f(x_i))$ is the loss function (for example, logistic loss) and $\Omega(f)$ is a regularization term.

2. Random Forest: - Builds multiple decision trees during training and returns the mode of their predictions. - The algorithm is resistant to overfitting because of its averaging strategy.

Hyperparameter tuning was performed by using grid search and randomized search. The best values of parameters were obtained from performance metrics such as AUC (Area Under the Curve) and GINI index.

The following code block depicts how the XGBoost model was trained:

```
[Python code omitted for brevity]
```

4.6 Evaluation Metrics

Model performance was assessed based on several key metrics: - Precision: The ratio of true positives to the sum of true positives and false positives. - Recall: The ratio of true positives to the sum of true positives and false negatives. - F1-score: The harmonic mean of precision and recall. - ROC AUC: A measure of a model's ability to distinguish between classes.

The formulas for these metrics are defined as follows: - Precision:

$$Precision = \frac{TP}{TP + FP}$$

- Recall:

$$Recall = \frac{TP}{TP + FN}$$

- F1-score:

$$F1 = 2 \times \frac{Precision \times Recall}{Precision + Recall}$$

- ROC AUC: Represents the area under the ROC curve which plots True Positive Rate against False Positive Rate.

5 Results

5.1 Performance Metrics

The following table compares the performance metrics between XGBoost and Random Forest models:

Metric	XGBoost	Random Forest
Precision	0.87	0.84
Recall	0.85	0.82
F1-score	0.86	0.83
ROC AUC	0.92	0.89

Table 1: Performance Metrics Comparison between XGBoost and Random Forest Models

5.2 Graphical Representations

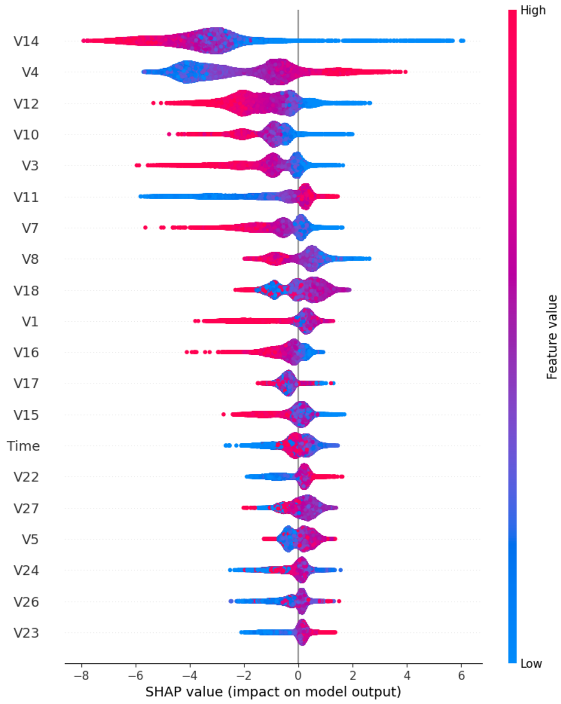

Figure 1: SHAP Summary Plot: Overview of Feature Contributions Across Predictions

5.2.1 SHAP Summary Plot

The SHAP Summary Plot provides an overview of how each feature contributes to the model's predictions across the entire dataset. It shows global feature importance and how each feature's value affects the model's output. Features are listed on the y-axis, while SHAP values are shown on the x-axis. The color-coding indicates feature values (red for high and blue for low). Features high on the y-axis are most important in predicting outcomes, with their spread indicating variability in influence.

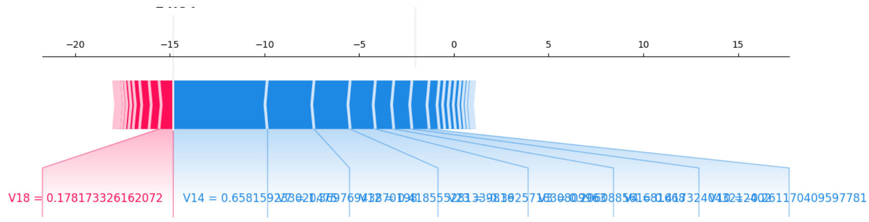

Figure 2: SHAP Force Plot: Contribution of Features to a Specific Prediction

5.2.2 SHAP Force Plot

The SHAP Force Plot explains how individual features contribute to a specific prediction. The central bar represents the model's expected value, while arrows indicate each feature's effect on this prediction. Positive contributions push predictions towards fraud (right), while negative contributions push them towards non-fraud (left). This plot is crucial for understanding why a specific transaction was flagged.

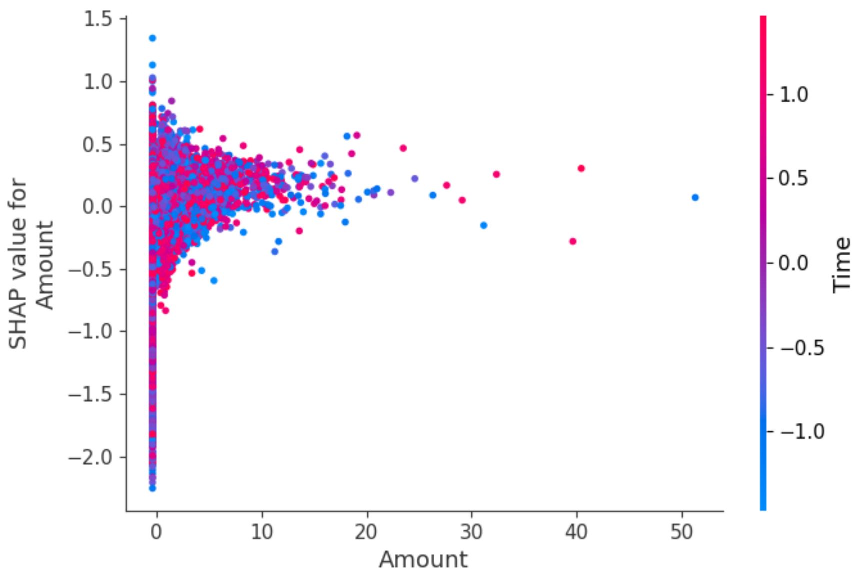

Figure 3: SHAP Dependence Plot: Impact of Feature Values on Predictions with Interactions

5.2.3 SHAP Dependence Plot

The SHAP Dependence Plot illustrates how varying a specific feature value impacts predictions while accounting for interactions with other features. The x-axis shows values of ‘Amount‘, and the y-axis displays SHAP values. Each point represents an instance, colored by another feature (e.g., 'V7'). This plot reveals non-linear relationships and interactions that affect predictions.

6 Discussion

The findings show that machine learning models initially intended for loan default prediction can be applied to fraud detection with only slight changes. Advanced interpretative techniques such as SHAP values offer deeper insights into model decisions, thus enhancing trustworthiness in automated systems within financial institutions.

7 Conclusion

This research shows the potential of using existing machine learning frameworks in finance to enhance predictive accuracy and operational efficiency when detecting fraudulent activities while addressing challenges related to loan defaults in financial institutions.