Project Proposal: Fraud Detection Using Machine Learning

CISC 5800

Xurui Zhang

1. Introduction and Summary

The goal of this project is to develop a robust machine learning model for fraud detection using a synthetic dataset of financial transactions. The dataset contains numerical, categorical, and temporal features, enabling a binary classification task to distinguish fraudulent transactions from legitimate ones. Financial fraud poses significant risks to both institutions and consumers, and this project aims to explore how machine learning techniques can enhance fraud detection systems by improving accuracy and interpretability.

This project will focus on implementing and comparing classical and advanced machine learning algorithms covered in the course, such as logistic regression, decision trees, support vector machines (SVMs), and neural networks. The results will highlight the strengths and limitations of different approaches in addressing real-world fraud detection challenges.

---

2. Anticipated Objectives

The primary objectives of this project are:

1. **Develop High-Performance Models**: Build fraud detection models using machine learning techniques learned in class, prioritizing high recall to minimize missed fraud cases while controlling false positives.
2. **Feature Analysis**: Identify key features driving fraudulent transactions through statistical analysis and model interpretation.
3. **Algorithm Comparison**: Compare the performance of logistic regression, decision trees, SVMs, and neural networks in fraud detection.
4. **End-to-End Pipeline**: Design a reproducible pipeline encompassing data preprocessing, feature engineering, model training, and evaluation.

5. **Model Transparency**: Provide interpretable explanations of model predictions to support decision-making in financial systems.

---

3. Proposed Tasks

To achieve the objectives, the following tasks will be completed:

1. **Data Preprocessing**:
    - Handle missing values via imputation or removal.
    - Encode categorical features (e.g., Transaction_Type, Device_Type) using One-Hot Encoding or ordinal encoding.
    - Normalize numerical features (e.g., Transaction_Amount, Account_Balance) for consistency.
2. **Exploratory Data Analysis (EDA)**:
    - Analyze distributions of features (e.g., fraud vs. non-fraud transactions by Transaction_Type or Location).
    - Visualize correlations between features and the target variable (Fraud_Label).
    - Detect outliers and class imbalance issues.
3. **Feature Engineering**:
    - Extract temporal features from Timestamp (e.g., hour of day, weekend vs. weekday).
    - Create behavioral features, such as transaction frequency over time or deviation from a user's average spending pattern.
    - Combine Risk_Score and Previous_Fraudulent_Activity to generate a composite risk indicator.
4. **Model Implementation**:
    - Implement logistic regression as a baseline model.
    - Train decision tree-based models (e.g., Random Forest) to capture nonlinear relationships.
    - Explore kernel-based methods (e.g., SVM with RBF kernel) for nonlinear classification.
    - Design a neural network to evaluate deep learning's potential in fraud detection.
5. **Performance Evaluation**:
    - Evaluate models using metrics tailored to imbalanced data: Precision, Recall, F1-Score, and AUC-ROC.
    - Compare training efficiency and computational costs across algorithms.

    - Analyze confusion matrices to balance false positives and false negatives.
6. **Model Interpretation**:
    - Use SHAP (SHapley Additive exPlanations) to interpret complex models like Random Forest and neural networks.
    - Visualize decision boundaries for simpler models (e.g., logistic regression and SVM).
7. **Final Report**:
    - Summarize methodologies, results, and practical insights.
    - Provide code documentation and reproducibility guidelines.
    - Discuss ethical considerations (e.g., bias in fraud detection systems).

---

4. Schedule

- **March 28, 2025**: Submit project proposal.
- **April 1 - April 14, 2025**: Data preprocessing and EDA.
- **April 15 - April 28, 2025**: Feature engineering and model implementation.
- **April 29 - May 10, 2025**: Model evaluation, interpretation, and optimization.
- **May 11 - May 15, 2025**: Finalize report and submission.

---

5. References

1. Kaggle. "Fraud Detection Transactions Dataset." [Dataset Source]
2. Pedregosa, F., et al. (2011). "Scikit-learn: Machine Learning in Python." *Journal of Machine Learning Research.*
3. Hastie, T., Tibshirani, R., & Friedman, J. (2009). *The Elements of Statistical Learning.* Springer.
4. Lundberg, S. M., & Lee, S.-I. (2017). "A Unified Approach to Interpretable Machine Learning Predictions." *Advances in Neural Information Processing Systems.*