**Credit Card Fraud Detection**

Madhuri Basava

Bellevue University

Applied Data Science DSC680

Amirfarrokh Iranitalab

**Milestone 3- White Paper**

**Topic:** The project I chose is Credit Card Fraud Detection.

This project focuses on detecting Credit Card Fraud by creating models that can predict the likelihood of fraud based on the given features.

**Business Problem**:

Nowadays, Credit Card Fraud has become a common problem in the financial sector that results in significant losses for financial institutions and cardholders. This reduces customer trust and satisfaction, leading to customer churn.

**Background/History:**

Credit Card fraud has been a persistent issue since the introduction of credit cards. Initially, there was physical theft of cards and forgery. These initial cards lack security features, making them easy targets for fraud. Later, the advent of magnetic stripes led to skimming and counterfeiting. The rise of the internet in the 1990s and the implementation of chip technology in 2000s introduced digital fraud as criminals exploited online transactions.

**Research Questions:**

1. Which features are most relevant for detecting fraud?
2. How to handle imbalanced datasets?
3. Which models are suitable for credit card fraud detection?
4. What criteria should be used to evaluate the performance of the model?
5. Is the model capable of detecting real-time fraudulent transactions?
6. What measures can be implemented to ensure the privacy and security of customer data used in fraud detection?
7. What are the best practices for handling false positives to minimize inconvenience to legitimate users?
8. How can credit card fraud detection models be adapted for use in other domains such as online shopping fraud?
9. How does the accuracy of fraud detection models impact customer trust and satisfaction?
10. What are the best strategies for continuous learning and updating of fraud detection models?

**Dataset:**

The dataset contains transactions made by credit cards in **September 2013** by European cardholders. This dataset presents transactions that occurred in two days, where we have **492 frauds** out of **284,807 transactions**. The dataset is **highly unbalanced**, the **positive class (frauds)** accounts for **0.172%** of all transactions

The dataset is taken from the Kaggle website.

[Credit Card Fraud Detection (kaggle.com)](https://www.kaggle.com/code/baherhamada/credit-card-fraud-detection/input?select=creditcard.csv)

**Data Description:** There are a total of 31 fields.

Time: Number of seconds elapsed between this transaction and the first transaction in the dataset.

Amount: Transaction Amount

V1-V28:  Result of a PCA Dimensionality reduction to protect user identities and sensitive features.

Class: 1 – fraudulent transactions and 0 – non fraudulent

**Methods and analysis:**

Performed prediction analysis with five different models as below.

1. Random Forest Classifier
2. Ada Boost Classifier
3. Cat Boost Classifier
4. XGBoost Classifier
5. Logistic Regression

I chose these models to improve accuracy and reduce false positives and false negatives (Inaccurate predictions).

I plan to evaluate the results by calculating the Area under the ROC curve.

It measures the overall performance of the binary classification model. As both TPR (True Positive Rate) and FPR (False Positive Rate) range between 0 to 1, the area will always lie between 0 and 1, and a greater value of AUC denotes better model performance.

I followed the below steps to evaluate these results.

1. Load the data set into a data frame.
2. Perform the Exploratory Data Analysis to understand the characteristics of the data set.
3. Clean the data set. Remove the unnecessary features.
4. Evaluate the correlation between the variables in the dataset.
5. Divide the data set into a train and test data set and apply various models.
6. Create a confusion matrix to show the performance of each model to evaluate the predicted values from the model vs. the actual values from the test dataset.
7. Calculate the AUC-ROC for each model and choose the best model.

**Correlation Matrix**:

A graph with a blue line

Description automatically generated with medium confidence

Below is the Confusion Matrix for each of the 5 models.

1. Random Forest Classifier

A blue and white diagram

Description automatically generated

1. Ada Boost Classifier

A blue and white diagram

Description automatically generated

1. Cat Boost Classifier

A blue and white diagram

Description automatically generated

1. XGBoost Classifier

A blue and white diagram

Description automatically generated

1. Logistic Regression

A screenshot of a computer

Description automatically generated

**Answers to the Research Questions:**

1. Which features are most relevant for detecting fraud?

The below chart from the XG Boost Classifier shows that V14, V4, V17, Transaction Amount, V10, V12, V26, V3 and Time of Transaction features are important.A green and white graph

Description automatically generated

1. How to handle imbalanced datasets?

Using techniques like oversampling the minority class and undersampling the majority class and ensemble techniques can handle data imbalance.

1. Which models are suitable for credit card fraud detection?

Random Forest, ADA Boost Classifier, Cat Boost Classifier, XG Boost Classifier and Logistic Regression algorithms are suitable for modeling. Ensemble methods like Random Forest and Gradient Boosting perform well due to their ability to handle complex interactions between various features.

1. What criteria should be used to evaluate the performance of the model?

Confusion Matrix which consists of predicted values from the model vs. the actual values from the test dataset and AUC-ROC scores should be used to evaluate the performance of the model.

1. Is the model capable of detecting real-time fraudulent transactions?

The model needs to be complimented with data consistency, low latency, and using frameworks like Apache Kafka to detect fraud in real-time.

1. What measures can be implemented to ensure the privacy and security of customer data used in fraud detection?

Data needs to be encrypted either in transit or at rest. Sensitive data needs to be provided based on the user role. Personally Identifiable Information (PII) data needs to be removed and sensitive data needs to be masked in non-production environments.

1. What are the best practices for handling false positives to minimize inconvenience to legitimate users?

False Positives can be handled by providing easy ways to verify transactions, and clear communications to users that will minimize disruptions to legitimate transactions.

1. How can credit card fraud detection models be adapted for use in other domains such as online shopping fraud?

Existing models can be fine-tuned to detect the unique patterns and behaviors of customers in online shopping. It may need the new data injection related to online shopping and retrain the model by adjusting the parameters.

1. How does the accuracy of fraud detection models impact customer trust and satisfaction?

High accuracy in models can lead to a lower incidence of false positives (unnecessary transaction declines) which in turn improves customer satisfaction.

1. What are the best strategies for continuous learning and updating of fraud detection models?

Best Strategies for continuous learning include using ensemble methods to integrate new models with old ones, continuous monitoring of the model’s performance to detect the changes in fraud patterns, and periodic training of the models with recent data.

**Conclusion**:

In summary, building a good credit card fraud detection system requires careful handling of data, real-time detection, and making sure the system is easy to understand and fair. Using advanced machine learning, updating the models regularly, and protecting user data are key steps. These systems can also be used in other areas like insurance and healthcare. Ethical concerns like avoiding bias and maintaining privacy are crucial for trust and compliance. A strong fraud detection system helps prevent financial losses, improves customer satisfaction, and offers good returns on investment. Regular monitoring and clear decision-making help keep the system effective and trustworthy.

**Assumptions:**

It is assumed that the data is representative of the population in the data set and is correctly recorded. Handling of missing data through imputation or other techniques is assumed to be correct. Also, assumed that the selected features have good predictive power. The selected models do not introduce any biases and are enough to achieve accurate results.

**Limitations:**

The dataset might not be representative of the entire population due to sampling bias.

The dataset may contain errors. The models may perform well on training data but may be poorly on unseen data. Handling sensitive data involves strict privacy requirements. Financial Institutions should understand the model and use it effectively.

**Challenges/Issues:**

* There will be an imbalance in the data set as fraudulent transactions are very few when compared to total transactions.
* Identifying features that are related to fraudulent activities can be complex.
* Real-time Fraud Detection can be a challenge.
* Handling sensitive data can be a challenge.

**Future Uses/Additional Applications:**

This project can be extended to future use for detecting fraud across different countries, money laundering, and other illegal activities. These models can be used for offering personalized services by understanding customer behavior. They can also be used to improve cybersecurity by detecting unusual activities and preventing identity theft.

**Recommendations:**

The recommendations for this project are to use high-quality data and keep the models updated to catch the new fraud patterns. It's important to explain how the models work so people trust them. Businesses should balance catching fraud with avoiding false alarms that can annoy customers. They should protect customer data and follow privacy laws. They should also think about using these models in online shopping to catch fraud.

**Implementation Plan:**

To implement the Credit Card Fraud Detection project, start by collecting and cleaning high-quality, representative data, ensuring it is anonymized and compliant with privacy regulations. Perform feature selection and engineering based on domain knowledge and statistical techniques, followed by experimenting with various machine learning models and ensemble methods, using cross-validation to ensure performance and avoid overfitting. Develop an interpretable model and deploy it using scalable cloud services and receive predictions with explanations. Implement continuous monitoring and a retraining pipeline to maintain model accuracy, and regularly audit the model for biases to ensure fairness. Document the process thoroughly and provide transparency regarding the model's limitations and ethical considerations to build trust and support.

**Ethical Considerations:**

The model should not discriminate against users based on protected attributes such as race, gender, or age. Biases in the data or model predictions may lead to unfair treatment of certain user groups. Individuals need to be notified about the limitations, implications, and potential consequences of the prediction.

**References:**

* *Credit Card Fraud Detection dataset is retrieved from the Kaggle website:*

[*Credit Card Fraud Detection Predictive Models (kaggle.com)*](https://www.kaggle.com/code/gpreda/credit-card-fraud-detection-predictive-models)

* [*IEEE Credit Card Fraud Detection - EDA (kaggle.com)*](https://www.kaggle.com/code/anbinhbui/ieee-credit-card-fraud-detection-eda/notebook)
* [*Credit Card Fraud Detection Project (kaggle.com)*](https://www.kaggle.com/code/santapiyaphon/credit-card-fraud-detection-project)
* [*Credit Card Fraud Detection Guide - Best Practices & Solutions (datadome.co)*](https://datadome.co/learning-center/credit-card-fraud-detection/)
* [*The History and Evolution of Fraud | Fraud.com*](https://www.fraud.com/post/the-history-and-evolution-of-fraud)