Credit Card Fraud Detection Capstone Project

Details:

- ***Name: Priya Kharote***
- ***Batch:*** Data Scientist bootcamp
- ## Introduction:

- The Credit Card Fraud Detection project focuses on enhancing financial security through advanced machine learning and data analysis techniques.
- Its primary goal is to develop a predictive model that can proactively distinguish between legitimate and fraudulent credit card transactions.
- Leveraging machine learning, specifically supervised learning and anomaly detection, this project addresses the dynamic nature of fraud patterns, surpassing the limitations of traditional rule-based systems.
- Key components involve data preprocessing, feature engineering, model selection, and evaluation metrics.
- The exploration of machine learning algorithms, including logistic regression, decision trees, random forests, and support vector machines, aims to identify the most effective approach for fraud detection.
- Ultimately, the project aims to provide a robust, efficient, and adaptive solution to safeguard financial transactions from the evolving landscape of fraudulent activities.

Project Objectives

- In this project, the goal is to leverage machine learning models to predict fraudulent credit card transactions. The process typically involves preprocessing and exploring the dataset, which may include features such as transaction amount, location, time, and previous transaction history.
- After splitting the dataset into training and testing sets, various machine learning algorithms such as logistic regression, decision trees, random forests, or support vector machines can be employed to build predictive models.

- The models are trained on a labeled dataset where instances of fraudulent and non-fraudulent transactions are identified. Evaluation metrics like precision, recall, and the F1 score are commonly used to assess the model's performance. Continuous improvement may involve tuning hyperparameters, employing ensemble methods, or exploring more advanced techniques like anomaly detection.

- The final model aims to accurately identify and prevent fraudulent credit card transactions by learning patterns from historical data.

Project Understanding

- Suppose you get a call from your bank, and the customer care executive informs you that your card is about to expire in a week. Immediately, you check your card details and realise that it will expire in the next eight days. Now, to renew your membership, the executive asks you to verify a few details such as your credit card number, the expiry date and the CVV number. Will you share these details with the executive?

- In such situations, you need to be careful because the details that you might share with them could grant them unhindered access to your credit card account.

- Although digital transactions in India registered a 51% growth in 2018–2019, their safety remains a concern. Fraudulent activities have increased severalfold, with approximately 52,304 cases of credit/debit card fraud reported in FY 2019 alone. Owing to this steep increase in banking frauds, it is the need of the hour to detect these fraudulent transactions in time to help consumers and banks that are losing their credit worth each day. Machine learning can play a vital role in detecting fraudulent transactions.

- So far, you have learnt about the different types of machine learning models. Now, you will learn which model to choose for your purpose and the reason for it. Understanding models based on different scenarios is an important skill that a data scientist / machine learning engineer should possess. In addition, tuning your model is equally important to get the best fit for your given data.

- By the end of this module, you will learn how you can build a machine learning model that is capable of detecting fraudulent transactions. You will also learn how to handle class imbalances present in any data set, along with model selection and hyperparameter tuning.

Problem Statement

- The problem statement chosen for this project is to predict fraudulent credit card transactions with the help of machine learning models.

Business Problem Overview

- Retaining highly profitable clients is the primary business objective for many banks. For some banks, however, this objective is seriously threatened by banking fraud. Regarding significant monetary losses, credibility, and trust, this is a worry for banks as well as customers.

- According to the Nilson Report, banking scams are expected to cause 30 billion in losses globally by 2020. New and varied methods of fraudulent transactions are being committed as digital payment channels proliferate.

- Machine learning-based credit card fraud detection is not only popular but also required in the banking sector to implement proactive monitoring and fraud prevention measures. These organizations are benefiting from machine learning by having less time-consuming manual reviews, expensive chargebacks and fees, and denials of valid transactions.

Understanding and Defining Fraud Logic

Credit card fraud is any dishonest act or behavior to obtain information without proper authorization from the account holder for financial gain. Among different ways of committing frauds, skimming is the most common one, which is a way of duplicating information located on the magnetic strip of the card. Apart from this, following are the other ways:

- Manipulation/alteration of genuine cards
- Creation of counterfeit cards
- Stealing/loss of credit cards
- Fraudulent telemarketing

About the Dataset

- The data set is taken from the Kaggle website and has a total of 2,84,807 transactions; out of these, 492 are fraudulent. Since the data set is highly imbalanced, it needs to be handled before model building.

- It is important that credit card companies are able to recognize fraudulent credit card transactions so that customers are not charged for items that they did not purchase.

- 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.

- It contains only numerical input variables resulting from a PCA transformation. Unfortunately, due to confidentiality issues, we cannot provide the original features and more background information about the data. Features V1, V2, … V28 are the principal components obtained with PCA; the only features not transformed with PCA are 'Time' and 'Amount'. Feature 'Time' contains the seconds elapsed between each transaction and

the first transaction in the dataset. The feature 'Amount' is the transaction amount, which can be used for example-dependent cost-sensitive learning. Feature 'Class' is the response variable and takes value 1 in case of fraud and 0 otherwise.

- Given the class imbalance ratio, we recommend measuring accuracy using the Area Under the Precision-Recall Curve (AUPRC). The confusion matrix accuracy is not meaningful for unbalanced classification.

Metric Used

ROC-AUC Score

- One often used metric to assess the effectiveness of binary classifiers is the ROC-AUC (Receiver Operating Characteristic - Area Under the Curve) score. By computing the area under the receiver operating characteristic curve's curve, a model's capacity to discriminate between positive and negative classes is evaluated.

- Because the ROC-AUC score is insensitive to class imbalance, it can be a useful tool for imbalanced datasets. Thus, even in cases when the dataset's positive and negative classes are unbalanced, the ROC-AUC score will continue to offer a trustworthy indicator of the model's capacity to distinguish between the two classes.

F1 Score

- It's crucial to remember that the ROC-AUC score does not reveal details about the model's precise performance for every class. The model might perform well in the larger class but poorly in the smaller class, for instance, if one class is noticeably smaller than the other. The ROC-AUC score might not show this. Therefore, while assessing a model's performance on imbalanced datasets, it's crucial to take into account additional metrics like accuracy, recall, F1-score, or confusion matrix.

- A popular metric for assessing the effectiveness of binary classifiers is the F1-score. It gives a measure of the overall accuracy of the model by combining recall and precision into a single score.

Precision

- A classification or prediction model's precision is a gauge of its accuracy. It can be defined as the ratio in the model's output between the number of true positives (positive cases successfully predicted) and the total number of false positives (positive cases wrongly predicted). To put it another way, precision calculates the percentage of positive situations that are actually anticipated to be positive.

- When a model has a high precision, it means that it is highly effective at finding positive cases and that its output contains few false positives. A poor precision, on the other hand, indicates a higher rate of false positives in the model, which may produce inaccurate or misleading findings.

Recall

- The completeness of a categorization or prediction model is gauged by recall. In the model's output, it is defined as the ratio of true positives (positive cases that were correctly predicted) to the total of true positives and false negatives (positive cases that were missed). Put differently, recall quantifies the percentage of real positive cases that the model accurately recognizes.

- A high recall means that few positive examples are overlooked by the model, demonstrating its excellent ability to recognize positive situations. Conversely, a low recall indicates a larger likelihood of missing positive cases in the model, which may potentially produce inaccurate or deceptive results.