Task 2: Credit Card Fraud Detection

Sharlene Moetjie – Data Science Intern

Objective:

- The objective of the credit card fraud detection is to identify and distinguish between legitimate and fraudulent transactions. This task involves training machine learning models and evaluating their performance to ensure they can effectively classify and detect fraudulent transactions.

1.Project Selection

- The aim is to train a credit card fraud detection model that accurately classifies transactions as legitimate or fraudulent. This involves using statistical methods such as the mean values of each transaction column for both classes to understand the patterns and behaviours of legitimate and fraudulent transactions.

2.Data Selection

- The dataset, sourced from Kaggle, contains credit card transactions over two days, including 492 frauds and 284,807 legitimate transactions. The dataset is highly unbalanced and contains information regarding the time in seconds elapsed between transactions, amount and classes.

3. Model Development

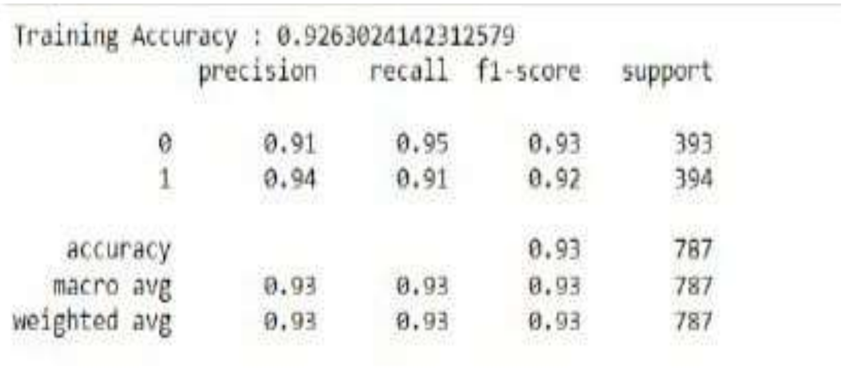
- I used a systematic process approach that included: data preprocessing, feature extraction, model training and evaluation. The implementations are as follows:
    - **Data Collection and Preprocessing:**
        1. Imported the dataset and analysed the distribution of the transactions.
        2. Used statistical measures to compare legitimate and fraudulent transactions.
        3. Balanced the dataset by sampling legitimate transactions to match the number of fraudulent ones so as to train the model with a uniform sample dataset.
    - **Train_Test_Split:** To split the dataset into training and testing sets to evaluate the model's performance on seen and unseen data.
    - **Model Training:** Train the classifier model on the split uniform sample data sets.
    - **Model Evaluation:** Evaluate the model's performance using the training and testing sample datasets.

5.Training and Evaluation

- The training and evaluation phase includes splitting the data, training the model and evaluating its performance using appropriate metrics such as accuracy, precision, recall and F1-score.

Results Presentation

CLASSIFICATION REPORT ON TRAINING (SEEN) DATA:

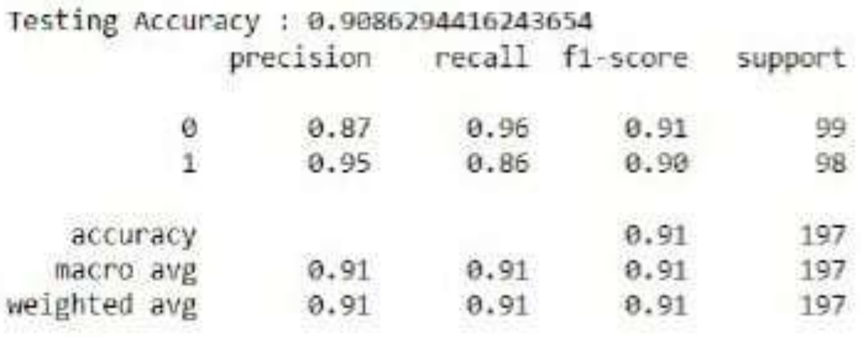


```
Training Accuracy : 0.9263024142312579
              precision    recall  f1-score   support

           0       0.91      0.95      0.93       393
           1       0.94      0.91      0.92       394

    accuracy                           0.93       787
   macro avg       0.93      0.93      0.93       787
weighted avg       0.93      0.93      0.93       787
```

CLASSIFICATION REPORT ON TESTING (UNSEEN) DATA:



```
Testing Accuracy : 0.9086294416243654
              precision    recall  f1-score   support

           0       0.87      0.96      0.91        99
           1       0.95      0.86      0.90        98

    accuracy                           0.91       197
   macro avg       0.91      0.91      0.91       197
weighted avg       0.91      0.91      0.91       197
```

Summary

- The results indicate that the model performs well on both trained and testing datasets, displaying a strong ability to generalize to new, unseen data. The relatively small difference between the training and testing accuracies entails that the model is not overfitting.

References

- Siddhardhan. Credit Card Fraud Detection Using Machine Learning in Python. [https://www.youtube.com/watch?v=NCgjcHLFNDg&t=329s]. YouTube.