**MODULES**

**Data Collection and Preprocessing:**

*Objective:* Gather relevant datasets containing banking transactions, ensuring a diverse representation of both genuine and fraudulent activities. Perform preprocessing tasks, including handling missing values, addressing outliers, and resampling to mitigate class imbalances.

**Feature Engineering and Selection:**

*Objective:* Identify and select features that are most relevant to fraud detection. This module involves analyzing the dataset to create new features or transform existing ones, enhancing the machine learning model's ability to discern patterns associated with fraudulent transactions.

**Machine Learning Model Training:**

*Objective:* Implement various machine learning algorithms, such as logistic regression, decision trees, random forest, support vector machines, or gradient boosting models. Train these models on the preprocessed dataset to learn and capture the patterns indicative of fraudulent activities.

**Real-time Transaction Verification:**

*Objective:* Develop a module for real-time transaction verification, leveraging the trained machine learning model. This module should facilitate the quick and efficient verification of transactions as they occur, ensuring timely detection and prevention of fraudulent activities.

**Model Evaluation and Continuous Monitoring:**

*Objective:* Assess the performance of the trained machine learning model using metrics like accuracy, precision, recall, and F1-score. Implement continuous monitoring mechanisms to track the model's effectiveness over time, enabling timely updates and adaptations to address emerging fraud patterns.