**UNIVERSITY OF HERTFORDSHIRE**

**MODULE**  
**7COM1040 – Computer Science Master’s Project**

**ASSIGNMENT ON**

***Cyber Profiling for Fraud Detection using Machine Learning Techniques***

**Supervised by**

**Julia Goncharenko  
  
Submitted by**

**Rutuja Tummewar  
2302573  
  
2024 - 2025**

Table of Contents

[1. Introduction 1](#_Toc191837647)

[1.1 Aim of Project 1](#_Toc191837648)

[1.2 Background 1](#_Toc191837649)

[1.3 Objectives 2](#_Toc191837650)

[1.4 Research Questions 2](#_Toc191837651)

[2. Summary of Progress to Date 2](#_Toc191837652)

[2.1 Literature Review 2](#_Toc191837653)

[2.1.1 Supervised machine learning for fraud detection 2](#_Toc191837654)

[2.2 Supervised Machine learning models 3](#_Toc191837655)

[2.3 Background Research 5](#_Toc191837656)

[2.3.1 Studies Comparison 7](#_Toc191837657)

[2.4 Datasets 8](#_Toc191837658)

[2.4.1 Selected Datasets progress up to date 8](#_Toc191837659)

[2.4.2 Merging Multiple Datasets 9](#_Toc191837660)

[2.5 Data Visualization 11](#_Toc191837661)

[3. Consideration of Ethical, Legal, Professional, and Social Issues 14](#_Toc191837662)

[3.1 Legal Issues 14](#_Toc191837663)

[3.2 Social Issues 14](#_Toc191837664)

[3.3 Professional Issues 14](#_Toc191837665)

[3.4 Ethical Issues 15](#_Toc191837666)

[4. Project Plan 15](#_Toc191837667)

[4.1 Completed Tasks 16](#_Toc191837668)

[4.2 Remaining Tasks 16](#_Toc191837669)

[5. Level Of The Project 16](#_Toc191837670)

[5.1 Project Artefact 16](#_Toc191837671)

[5.2 Level of investigation 16](#_Toc191837672)

[5.3 Appropriation 17](#_Toc191837673)

[6. References 17](#_Toc191837674)

[7. Appendices: 19](#_Toc191837675)

# 1. Introduction

The rapid evolution of mobile devices and web technologies has led to increasingly sophisticated attack methods that bypass traditional signature-based defenses. Cyber profiling, an advanced approach, analyzes online behavior patterns to identify fraudulent activities. With the growing prevalence of social media, e-commerce, and online transactions, cybercriminals exploit vulnerabilities to commit fraud, rendering conventional detection methods ineffective. Machine learning (ML) offers promising solutions to these complex challenges, as it can quickly adapt to new and unforeseen scenarios. In today’s digital era, cyber fraud has emerged as a significant global threat, affecting individuals, businesses, and governments. Traditional monitoring systems often fail to detect intricate fraud patterns, leading to financial losses and reputational damage. To address this, there is a pressing need for proactive, adaptive, and intelligent fraud detection systems. By leveraging machine learning and cyber profiling—which analyze user behavior and transaction patterns to create unique digital profiles—organizations can significantly enhance their ability to detect and prevent fraud.

## Aim of Project

The primary objective of this research is to leverage advanced machine learning techniques to develop an effective fraud detection system based on cyber profiling. The study seeks to create comprehensive cyber profiles of users by analyzing various behavioral patterns, utilizing a range of machine learning methods. To build a more efficient and time-effective model, the project will explore different machine learning algorithms and evaluate strategies such as handling data imbalance, feature engineering, feature selection, and model optimization techniques. This approach aims to enhance the accuracy and reliability of fraud detection systems in identifying suspicious activities.

## Background

Cyber profiling encompasses a series of approaches uniting law enforcement and psychology to predict the general characteristics of individuals likely to commit cybercrimes. It not only helps with fraud detection by having a process of elaborating the pattern and characteristics of fraudsters but also one where more effective systems can be developed. Different machine learning techniques such as Naive Bayes (NB), Logistic Regression (NB), K-Nearest Neighbors (KNN), Random Forest (RF), Decision Tree (DT), and Support Vector Machines (SVM) have been widely used to address credit card fraud issues but have been constrained by issues such as imbalanced datasets and ever-changing fraud patterns Bada, and Nurse, (2021). Techniques such as SMOTE have been developed to mitigate the issue of class imbalance. The confluence of cyber profiling and machine learning techniques will certainly enhance fraud detection through a holistic understanding of fraudster behaviour. Cyber profiling, by way of analysing psychological and behavioural traits, will assist not only in revealing potential fraud patterns that machine learning models may miss but also in leading to the design of more effective anti-fraud and preventive measures.

## Objectives

* **Development of a Cyber Profiling-Based Fraud Detection System**: To design and implement a fraud detection system that leverages cyber profiling to identify fraudulent activities by applying various machine learning (ML) techniques.
* **Identification of Effective Feature Engineering Techniques**: To investigate and assess feature extraction and selection methods to enhance the performance and effectiveness of the fraud detection system.
* **Comparison of Machine Learning Models for Cyber Profiling-Based Fraud Detection**: To analyze and compare different machine learning models based on their time complexity, accuracy, and efficiency in detecting fraudulent behavior.
* **Optimization of Model Performance Using Advanced Techniques**: To employ and evaluate parameter optimization techniques to improve computational efficiency and accuracy in fraud detection.

## Research Questions

* How can machine learning techniques be leveraged to build an effective cyber profiling system for fraud detection?
* How can optimization techniques be employed to enhance model accuracy and computational efficiency?

# 2. Summary of Progress to Date

In this project, key initial tasks have been completed, including dataset selection, literature review, and data exploration and preprocessing. The dataset has been merged, cleaned, and visualized to identify patterns. Moving forward, my focus will be on balancing the dataset to address class imbalance, followed by feature engineering to extract relevant features. Parameter optimization will fine-tune hyperparameters for Decision Tree, KNN, and SVM classifiers. The models will then be trained and evaluated using metrics like accuracy, precision, and recall.

## 2.1 Literature Review

### 2.1.1 Supervised machine learning for fraud detection

In many different fields, machine learning (ML), encompassing supervised, unsupervised, and reinforcement machine learning, is an essential method for handling and evaluating data. By identifying trends in enormous volumes of data, it aids in the detection and prevention of fraud (Btoush, et al. 2023). Effective machine learning algorithms can distinguish among illegal and legal operations and can gradually adjust to new methods. This requires accurate execution of thousands of calculations in milliseconds.

A ML approach called supervised learning uses annotated collections of data and customizable information with specified parameter objectives for training algorithms. It encompasses deduction, regression, however, and categorization. The most prevalent machine learning method depends on correctly tagged transactions that are either valid or fraudulent. Fraud detection is one of the numerous learning tasks for which machine learning has many branches and methods. Solid detection classifiers are built using supervised and machine learning techniques, such as methods like Logistic Regression, Decision Tree, Support Vector Machine, and Naïve Bayes. These methods can be used in conjunction with ensemble methods to improve fraud detection.

**2.1.2 Data Preprocessing:**

The data preprocessing the foundation to build a robust machine learning model for cyber profiling & fraud detection. The data processing methods utilize in order to make the raw data into the structured and clear & meaning full format so that machine learning models should be enable to find out the fraudulent patterns and activities in the dataset to make cyber profiling of fraudulent activities and detection of fraud. The concerned dataset may contain the missing values & outliers that can distort the model’s performance. The missing values can be handled through different such as imputing the numerical fields with taking the mean or median of dataset values & replacing the missing categorical values with placeholders. A further essential aspect of data preprocessing is handling outliers and discrepancies. Because outliers can skew statistical analysis, it can be challenging to identify real fraud. Outliers can be managed by converting the information, employing statistical techniques, or evaluating the veracity of the data sources utilizing specialist knowledge.

The selected dataset can be imbalance with non-equal number of target entries (fraudulent activities with comparison to the normal activities) in the targeted label So handling this situation is compulsory. The resampling techniques like SMOTE is widely used technique to handle the imbalance situation of dataset. By generating fresh instances in the vicinity of the minority class, the SMOTE employs a technique to lessen the disparity in class (Lucas and Jurgovsky, 2020). This entails combining both categories and nearby examples. Although the method enhances the efficiency of classifiers, it ignores surrounding samples' labels, which could result in overlapping among minority and dominant categories. Class imbalance can be lessened with the help of this rebalance technique.

## 2.2 Supervised Machine learning models

**Random Forest:**

A machine learning (ML) technique called random forest solves regressive and categorization issues by utilizing a decision tree (DT) methodology. It combines numerous classifications to get very accurate output predictions for big collections (Darwish, 2020). A rise in the number of trees increases the accuracy of the method, which forecasts a typical average of outputs generated by additional trees. It assists in removing the drawbacks of tree-based techniques. Additionally, it reduces information pulling improving accuracy. A landscape contains multiple decision-trees, each of which functions as an ineffective learning but when combined, they produce an excellent learner. When dealing with enormous numbers of information sets, including imbalanced ones, and the Random Forest (RF) approach is quick and efficient. Nevertheless, a RF approach presents limits when it comes to learning from a variety of information sets, particularly in regression applications.

**Support Vector Machine (SVM):**

Support Vector Machine is taken into consideration for classification and performs regression analysis for a variety of issues. Using this method, researchers frequently examine consumer credit card usage trends. From the databases, the clients' payment habits were gathered. Consumption behaviors are categorized according to illegal or Legal activities using the SVM approach (Sasank, et al. 2019). Whenever less characteristics form the dataset are employed, the Support Vector Machine approach is effective and yields precise outcomes. The issue arises, though, when a greater number of datasets are employed. Support Vector Machine is ineffective when employed in actual time because of the magnitude of the data set when it comes to fraud detection.

In order to identify fraud risk, (Rtayli and Enneya, 2020) have created a combination method that combines SVM and random forest. The characteristic choice of forged deals in sizable, unbalanced datasets served as the technique's inspiration. The framework was assessed using criteria like confusion metrics parameters. That hybrid approach exhibited significant correctness and process decrease, leading in enhanced fraud detection in big databases and unbalanced information. Nevertheless, this approach restricts transactional confidentiality in regard to assessment metrics for correctness and recall.

**Artificial Neural Network (ANN):**

An algorithm for machine learning called an artificial neural network (ANN) works comparable to the way a human mind. Supervised and unsupervised methods are the two main approaches on which ANNs are usually built (Ogwueleka, 2011). The supervised artificial neural network looks for comparable trends among the current holders of credit cards and those from previous transactions. Assume that there is a correlation between the information in the present transactions and the information from earlier ones. ANN techniques are very resilient to errors. As an illustration, even when there is distortion in one or more cells, result is still generated.

A model for detecting credit card fraud has been produced by (Patidar and Sharma, 2011) utilizing artificial neural networks (ANN). For training and testing, the algorithm utilizes 80-20 ratios of client data. The approach outperformed the prior model in real-time fraud detection, achieving a noteworthy result with good accuracy. During banking transactions using credit cards, an approach that satisfies all privacy and security requirements is required. When they used the algorithm for instruction, they made no indication about information security.

**K-Nearest Neighbour (KNN):**

One kind of supervised machine learning technique that is useful for issue classification and predictive assessment is K-Nearest Neighbor. It is a successful supervised learning technique. It aids in enhancing identification and lowering the likelihood of false alarms (Alam, et al. 2021). It establishes the existence of fraud in debit card transactions using a controlled method. Two estimations are needed by the K-Nearest Neighbor fraudulent identification method: the transactional association and the proximity among the frequency of transactions in the dataset. Illegal behavior around transaction duration can be detected using the K-Nearest Neighbor approach. It may be possible to identify the abnormalities in the objectives by over sampling and information separation. A popular tool for finding comparable trends in past cardholder activities is the K-Nearest Neighbor. K-Nearest Neighbor performs optimally on all measures and offers an acceptable efficiency rate in identifying forged activities. However, if given a lot of information, K-Nearest Neighbor can cause efficiency loss since it uses a lot of memory and ramps up unnecessary information properties (Awoyemi, et al. 2017). The fraudulent activity detection procedure's recall and precision matrices are impacted by these limitations. K-Nearest Neighbor has demonstrated encouraging results in identifying fraud regardless of these drawbacks.

**Decision Tree:**

A popular ML method for categorization problems is the decision tree. They offer a methodical approach to choosing a group of data. With this approach, a tree-like model is produced, with every inner node standing for an operation, every branch representing for a choice according to that function's characteristics, and every node in the leaf for a category name or expected result (Shetty and Malghan, 2023). Decision trees' main concept is to separate the information according to the levels of various attributes in order to produce subgroups that have values as close to the desired parameter as feasible. The splitting process chooses the optimal split position for a particular relevant characteristic of every inside component.

## 2.3 Background Research

Methods from data mining might be used to detect financial fraud, which is a serious threat to the economy. It can be difficult to spot fraudulent activity over time and with biased datasets, though. The effectiveness of several approaches, including LR, NB, RF, KNN, AdaBoost, Multilayer Perceptron, Pipelining, and Ensemble Learning, in detecting credit card fraud is compared using a methodology put forward by (Bagga et al. 2020). The efficacy of fraud identification is affected by the factors and methodology employed. Their results showed the RF produced the highest accuracy 99.7% comparing to the supervised learning algorithms. Several machine learning and deep learning techniques are employed to identify fraud with credit cards, and methods like NB, LR, KNN, RF, and SCNN are biased to train the other typical and anomalous transactions characteristics in order to identify fraudulent use of credit cards (Mehbodniya et al. 2021). The random forest achieved the highest accuracy of 97.5% and the others such as NB, LR, KNN & SCNN achieved the accuracy rate 96%, 95%,96% & 92% respectively.

(Darwish, 2020) discusses the shortcomings of fraud detection systems and suggests a sophisticated system that uses the ABC optimization process to fix these problems. In order to save time and money, the system concentrates on identifying the optimal response rather than identifying several intermediate solutions. To link parameters with human significance, the method utilizes an optimized a classification technique, dynamically fused k-mean classification algorithm, and ABC optimization rather than straightforward methods like data analysis. Specific characteristics are chosen from a big dataset using a rule engine. The model's overall performance leads to improved accuracy and shorter calculation times.

In order to identify fraud, (Dal Pozzolo et al. 2017) suggested three important contributions. They defined the problem, showed how to apply pertinent assessment metrics, created a novel learning strategy to address class imbalance, idea drift, and confirmation delay, and illustrated the impact of these problems in a real-time data stream that allowed more than 75 million transactions over a span of three years. To train the behavior features of both normal and abnormal transactions, they used two different kinds of random forests.

The effectiveness of several approaches, such as Naive Bayes, KNN, and Logistic Regression, in identifying skewed credit card fraudulent information was examined by (Awoyemi et al. 2017). To rectify the imbalance in the dataset, they employed a hybrid sampling strategy. They used a Python-based machine learning environment to test the ML techniques Naive Bayes, K closest neighbor, and logistic regression. According to the findings, the accuracy ratings of K nearest neighbor, Naive Bayes, and Logistic Regression were 97.9%, 54.8%, and 97.6%, correspondingly. The researchers were unwilling to investigate the viability of using a characteristic selecting technique.

To determine if a transaction was fraudulent or lawful, (Varmedja et al. 2019) utilized the credit card fraud recognition data. The information set was split into training and test data, and the inconsistent dataset was oversampled using the SMOTE method. The methods that were employed were Multilayer Perceptron, RF, NB, and LR. According to the report, every technology has a high success rate for identifying credit card fraud but RF outperformed others with good accuracy rate. Since credit card fraud detection systems depend on supervised learning techniques, the structure can be utilized to find more irregularities. The authors recommend more study to enhance feature selection techniques for various machine learning techniques.

(Alfaiz & Fati, 2022) uses a real-world dataset of European consumers' credit card theft to assess 66 machine learning algorithms. The top three methods are selected for further implementation in the subsequent stage after nine methods are examined in the initial phase. Having an AUC of 97%, an average recall of 95%, and a F1 scores of 87%, the All-KNN under sampling approach and CatBoost (AllKNN-CatBoost) model is regarded as the best, surpassing earlier models.

(Khare & Sait 2018) used several ML techniques, such as LR, DT, SVM, and RF, to create a system for detecting fraud. The European cardholder dataset, which had a significantly lopsided proportion of fraudulent to non-fraudulent interactions, was used to test these methods. According to the findings, the correctness ratings of the Logistic Regression, Decision Tree, Support Vector Machine, and Random Forest were 97.7%, 95.5%, 97.5%, and 98.6%, correspondingly. According to the researchers, sophisticated pre-processing methods might enhance the classifications' effectiveness. From their results The Random Forest model has outperformed the others.

The effectiveness of machine learning methods for fraud detection was carried out by (Khatri et al. 2020) They assessed every technique's accuracy using an extremely imbalanced collection of European consumers. According to the findings, the decision tree, random forest, K nearest neighbour, and logistic regression all had corresponding experimental accuracy of 85.1%, 91.1%, 87.5%, 89.7%, and 96.5%. (Ileberi, et al. 2022) suggests a machine learning (ML)-based fraud detection system that selects features utilizing the genetic algorithm (GA). The subsequent ML methods for categorizing, including DT, RF, LR, ANN, and NB, are used in their suggested detection process followed the choice of optimum features. With validation5, the GA-based random forest obtained a 99.9% accuracy rate, while with validation1, the GA-based decision tree obtained a 99.9% accuracy rate.

Utilizing machine learning methods like Random Forest (RF) and Gradient Boosting (GB), (Trivedi et al. 2020) created a fraud detection system. They used the European cardholder’s dataset to assess various approaches. The findings demonstrated that 94% accuracy was attained by both Random Forest and Gradient Boosting. Utilizing the same dataset, (Sailusha, et al. 2020) created a framework for detecting credit card fraud utilizing machine learning methods. To solve the data collection's class imbalance problems, they employed an under-sampling strategy. Accuracy was the primary effectiveness parameter, and the authors employed logistic regression and random forest as machine learning techniques. The success rate of identifying fraud was 91% for the random forest approach and 95% for the logistic regression methods. To find the best performances for positive as well as negative classes, the confusion matrix was calculated. The paper recommends more research be done on the class imbalance problems dataset.

Using imbalanced data sets, (Ileberi, et al. 2021) created a machine learning (ML) system for detecting fraud using credit cards. To correct for class imbalance, they re-sampled the dataset utilizing the SMOTE techniques. Several machine learning techniques, such as SVM, LR, RF, XGBoost, DT, and Extra Tree (ET), were used to assess the architecture. To enhance categorization excellence, the Adaptive Boosting (AdaBoost) technique was integrated with machine learning algorithms. The methods were assessed using AUC and the confusion matrix.

### 2.3.1 Studies Comparison

|  |  |  |  |
| --- | --- | --- | --- |
| Study | Method | Utilized models | Most efficient model |
| Bagga et al. (2020) | Supervised Learning | LR, NB, RF, KNN, AdaBoost, MLP, Pipelining, Ensemble | RF |
| Mehbodniya et al. (2021) | Supervised Learning | NB, LR, KNN, RF, SCNN | RF |
| Darwish (2020) | ABC Optimization | Dynamic K-means, ABC Optimized Classification | ABC Optimization |
| Dal Pozzolo et al. (2017) | Random Forests | Two types of RF | RF (Optimized for large datasets) |
| Awoyemi et al. (2017) | Hybrid Sampling, ML | NB, KNN, LR | KNN |
| Varmedja et al. (2019) | SMOTE, Supervised Learning | MLP, RF, NB, LR | RF |
| Alfaiz & Fati (2022) | Undersampling, ML | 66 ML models (Top 3 selected) | AllKNN-CatBoost |
| Khare & Sait (2018) | Supervised Learning | LR, DT, SVM, RF | RF |
| Khatri et al. (2020) | Imbalanced Data Handling, ML | DT, RF, KNN, LR | LR |
| Ileberi et al. (2022) | Feature Selection (GA), ML | DT, RF, LR, ANN, NB | GA-based RF & GA-based DT |
| Trivedi et al. (2020) | ML-based Fraud Detection | RF, GB | RF & GB |
| Sailusha et al. (2020) | Under-Sampling, ML | LR, RF | LR |
| Ileberi et al. (2021) | SMOTE, ML, Adaptive Boosting | SVM, LR, RF, XGBoost, DT, ET, AdaBoost | AdaBoost + ML Combination |

**Reasoning :**

In the comparison of various studies on fraud detection using machine learning techniques, **Random Forest (RF)** consistently emerges as one of the most efficient models. For instance, studies by Bagga et al. (2020), Mehbodniya et al. (2021), and Khare & Sait (2018) demonstrate that Random Forest achieved the highest accuracy rates (99.7%, 97.5%, and 98.6% respectively) compared to other models like Logistic Regression, Decision Tree, and Support Vector Machine. This indicates that **Random Forest is highly effective in handling imbalanced datasets and capturing complex fraud patterns**, making it a reliable choice for developing robust fraud detection systems. Its ability to reduce overfitting and provide interpretable results further strengthens its suitability for cyber profiling and fraud detection tasks.

## 2.4 Datasets

### 2.4.1 Selected Datasets progress up to date

The "Financial Fraud Detection Dataset," a Kaggle dataset that has been chosen, includes information on financial transactions and suspicious trends. For the intent of training and assessing machine learning algorithms for fraud detection, it was created. The dataset is arranged in the "data" directory and has multiple sub-folders, each of which has CSV files with particular data on client profiles, financial transactions, fraudulent activity, transaction values, and vendor details. The structure of the dataset is as follows:

**Transaction data:**

transaction\_records.csv: It includes transaction records that include information such as the customer ID, date, amount, and transaction ID.

ransaction\_metadata.csv: It contains additional metadata for each transaction.

**Costumer Data:**

customer\_data.csv: Includes customer profiles with information such as name, age, address, and contact details.

account\_activity.csv: Provides details of customer account activity, including account balance, transaction history, and account status.

**Fraudulent patterns:**

fraud\_indicators.csv: Contains indicators of fraudulent patterns and suspicious activities.

suspicious\_activity.csv: Provides specific details of transactions flagged as suspicious.

**Transactions amounts:**

amount\_data.csv: Includes transaction amounts for each transaction.

anomaly\_scores.csv: Provides anomaly scores for transaction amounts, indicating potential fraudulence.

**Merchant Information:**

merchant\_data.csv: Contains information about merchants involved in transactions.

transaction\_category\_labels.csv: Provides category labels for different transaction types.

**Dataset Source:** https://www.kaggle.com/datasets/majidiqbalvhr/fraud-detection-dataset/data

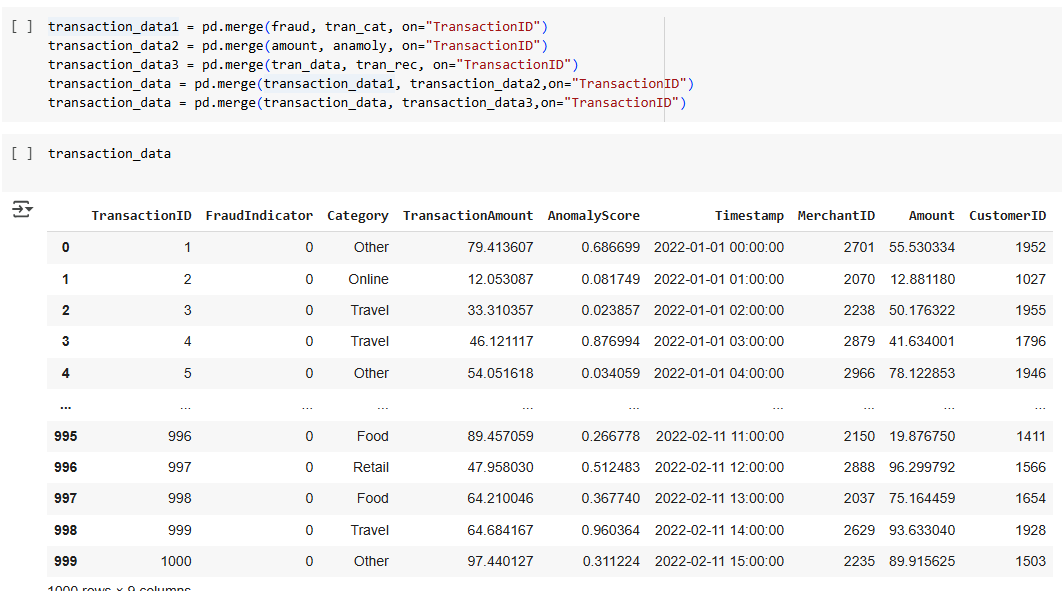
### 2.4.2 Merging Multiple Datasets

Our selected datasets contain the multiple sub-folders of different categories such as customer-data, Account-activity, Fraudulent-indicators, Merchant-data, Suspicious-activity, Transaction-category-labels, Amount-data. Anomaly-scores, Transaction-meta-data & Transaction-records. Therefore, we have merged these files to make a single data contain all these sub-folder entries.



**Figure 1: Figure of merging customer data**

In above figure, from the exploration of the dataset there is Customer-ID column exist in different sub-folders such as Suspicious-activity, Account-activity & Customer-data therefore we have merged these subfolders as one folder data such as customer-data based on customer-ID.



**Figure 2: Figure of merging customer data**

In above figure, there is Transaction-ID column exist in different sub-folders such as Fraudulent-indicators, Merchant-data, Transaction-category-labels, Amount-data. Anomaly-scores, Transaction-meta-data & Transaction-records therefore we have merged these subfolders as one folder data such as Transaction-data on the basis of transaction-ID.

A screenshot of a computer

AI-generated content may be incorrect.

**Figure 3: Figure of merging customer data & transaction data**

In above figure, after making the 2 subfolders of dataset as Customer-data & Transaction-data we have merged these subfolders into one main data.

## 2.5 Data Visualization

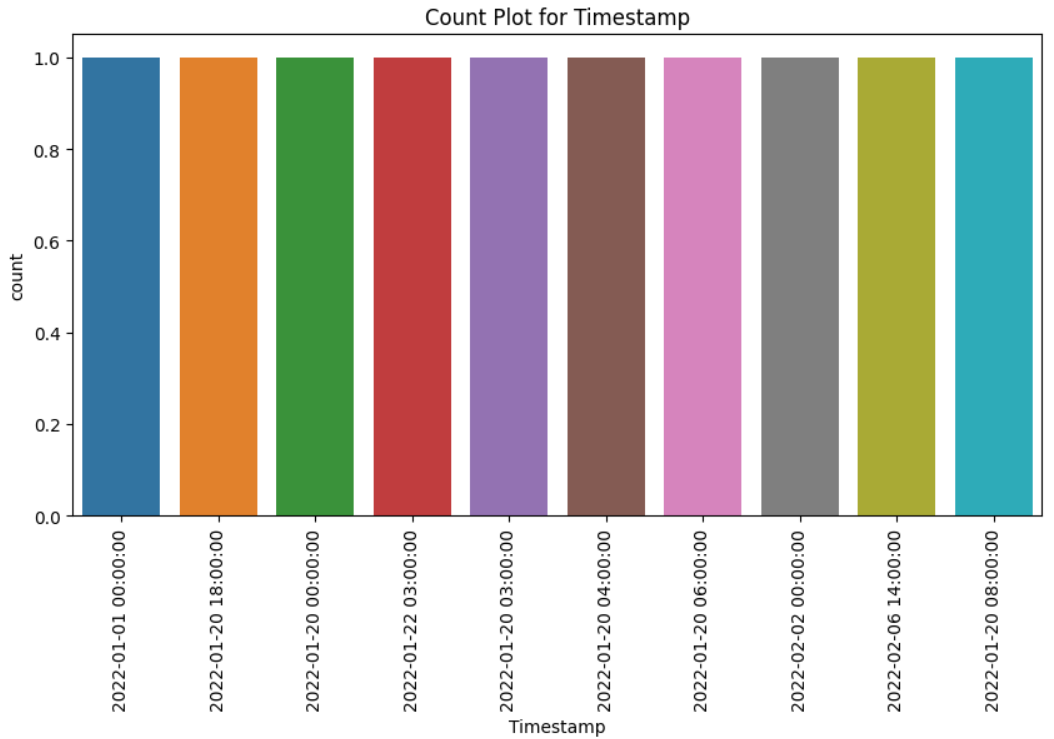
The data visualization technique has been implemented to see the patterns and trends in the dataset relevant to transactions category and timestamp.

A bar graph with different colored rectangles

AI-generated content may be incorrect.

**Figure 4: Count plot for category**

The Category Count Plot displays the distribution of various categories, such as "Other," "Food," "Travel," "Online," and "Retail," to detect unusual activity and identify areas for further fraud detection analysis.



**Figure 5: Count plot for Timestamp**

There might not be numerous transactions that occur at the exact same timestamp, as indicated by the Timestamp Count Plot, which merely shows individual instances while displaying the frequency of timestamps.

**Box Plots:**

A box plot is a type of graphic that shows information from a list of five numbers along with an overall trend measurement. It's utilized to find irregular distributions and possible outliers in big data sets, but it isn't as thorough as a summary or leaf and stem graph. Large data sets can be compared with the use of boxplots. Therefore, we have utilized the box plot analyzing data distribution and identifying outliers in dataset.

Box plots provide important information about fraudulent transactions, such as unexpected transaction amounts, anomaly scores, account balances, and binary indicators like Fraud-Indicator and Suspicious-Flag. These indicators can be used to indicate possible fraud cases, spot outliers, and spot odd distributions. Knowing these characteristics can make it easier to spot account balance fluctuations and how they relate to fraudulent activity.

**Dataset targeted label:**

A graph of a flag

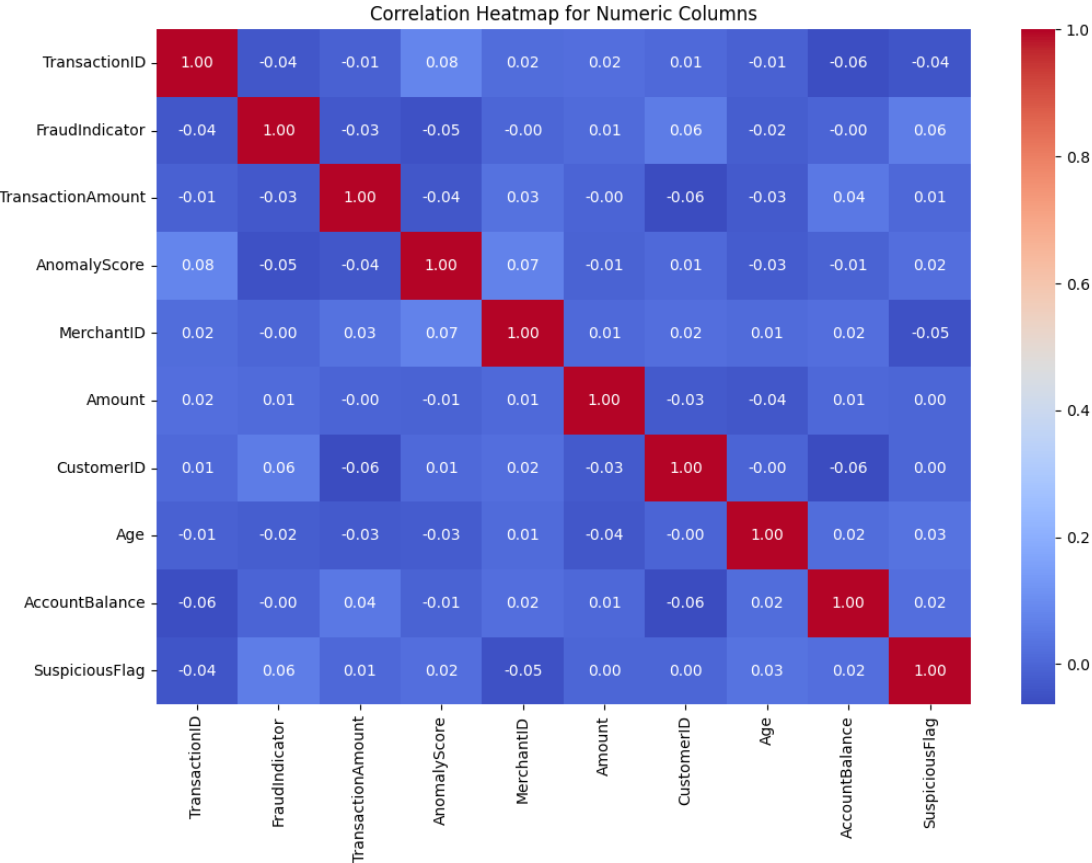
AI-generated content may be incorrect.

**Figure 6: Count plot for Suspicious flag**

With exploration of the targeted label suspicious-flag which shows that the dataset is highly imbalanced, which can affect the performance of machine learning models, especially if accuracy is the primary evaluation metric. This situation may also lead to the model biased toward the majority class 0 which may lead to the poor detection of fraudulent cases. To handle this situation, we have to utilize the resampling techniques to make it equal in numbers.

**Heatmap Correlation:**

To show row-column correlations in crosstab information, heatmaps are tabulated charts with various color codes superimposed within every cell in various either light or dark colored pattern. They give data in visual form by using different color tones to convey various numbers (Gupta, et al. 2023). Data analysts utilize heatmaps because they offer a thorough method of displaying the relationships among factors or features in information. These might be applied to a variety of analysis of data tasks, including analyzing data elements, defining the relationship and impact of one feature on another, and in certain situations, detecting human activity.



**Figure 7: Correlation heatmap**

The heatmap correlation provides the insights about the correlations between the numerical features of the dataset. The target variable for fraud detection is represented by the Fraud Indicator column, and correlation values show how much each attribute contributes. A slight positive connection between Suspicious Flag and Fraud Indicator suggests that it has an impact on fraud detection. Strong linear relationships are indicated by low or almost zero correlation values, but duplicated information may be indicated by large correlations.

# 3. ****Consideration of**** ****Ethical, Legal, Professional, and Social Issues****

## 3.1 Legal Issues

* **Data privacy & protection**: The data privacy & protection compliance is crucial with concerning the features extraction and model development. The key issues related to data privacy and ensuring the compliance with laws with determining the legal basis for processing the personal data.
* **Legal liability**: The legal liability may arise if personal identification information is leaked or misused due to the vulnerabilities.
* **Legality of automated decision making**: If a fraud detection model results in false positives, leading to wrongful accusations, the affected individuals might seek legal recourse.

## 3.2 Social Issues

* **Privacy violations**: The cyber profiling & fraud detection involves the collection and analyzation of different amount of personal and other behavioural data which can lead to the data privacy breaches.
* **Identity theft**: The machine learning techniques & models can enhance the fraud detection but there is also presents the risk of identity theft.
* **Misinformation & Social Manipulation**: The fake profiles are often used to spread the misinformation & engage in social manipulations which impacts public opinion & social norms.
* **Dependence on technology**: The enhancement of reliance on automated system can reduce human oversight that can potentially allowing the sophisticated fraud tactics than can go undetected if the machine learning algorithm fail to detect.

## 3.3 Professional Issues

* **Data quality & availability**: The collection of high-quality data is compulsory for development of robust model; However, the data can be incomplete and outdated or inaccurate which can impact the performance of machine learning model.
* **Model Biasness**: The machine learning models can be biased and can produced the unfair profiling of individuals based on the data through which they are trained which may lead to the ethical concern about discrimination in fraud detection process.
* **Security attacks**: Adversarial attacks, such as model poisoning, in which scammers insert false data to taint the system, can affect machine learning models. It is essential to protect these models from cyberattacks and data tampering.
* **Data disparity & Imbalance**: The fraudulent transactions in dataset can be rare which lead to dataset imbalance and Cyber-profiling data often contains noise or missing values which complicating feature extraction and model training. So, there is a challenge to handle these situations.

## 3.4 Ethical Issues

* **Confidentiality**: Handling the personal and sensitive information may raise the ethical issue due to the security concerns which requires strict data confidentiality measures.
* **Informed consent**: It is essential to obtain explicit consent to the person or individual whose data is being used. It is essential that they are informed about how their data will be used.
* **Fairness and Equity**: It is essential to ensure that the fraud detection framework do not unfairly disadvantage specific demographics. Biases in cyber profiling could lead to wrongful suspicion or discrimination against certain individuals or groups.

# 4. Project Plan

This section provides the comprehensive roadmap to complete the project with timeline. Some of the work has been done with in the time line. Every task of project has assigned time according to work in order to complete the project in time. Here the below Table of tasks with timeline defines the task importance and its retrospective time to be completed.

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Tasks** | **February** | | | | **March** | | | | **April** | | | |
| **1-7** | **8-15** | **16-22** | **23-28** | **1-7** | **8-15** | **16-22** | **23-31** | **1-5** | **6-10** | **11-15** | **16-20** |
| **Dataset** |  |  |  |  |  |  |  |  |  |  |  |  |
| **Literature Review** |  |  |  |  |  |  |  |  |  |  |  |  |
| **Data exploration** |  |  |  |  |  |  |  |  |  |  |  |  |
| **Data preprocessing** |  |  |  |  |  |  |  |  |  |  |  |  |
| **Data balance** |  |  |  |  |  |  |  |  |  |  |  |  |
| **Features Extraction** |  |  |  |  |  |  |  |  |  |  |  |  |
| **Parameter optimization** |  |  |  |  |  |  |  |  |  |  |  |  |
| **Model training** |  |  |  |  |  |  |  |  |  |  |  |  |
| **Model Evaluation** |  |  |  |  |  |  |  |  |  |  |  |  |
| **Final Report** |  |  |  |  |  |  |  |  |  |  |  |  |

**Figure 8: Gantt Chart**

## 4.1 Completed Tasks

* Data Selection.
* Literature Review.
* Data exploration & preprocessing.

## 4.2 Remaining Tasks

Making dataset balance: Utilization of under sampling & oversampling techniques balancing the targeted label.

Time line: 28-february to 1-March

**Features engineering**: This task phase will focus on to extract most import features from dataset through utilization of feature extraction techniques such as features extraction using random regressor & handling the date and time columns in dataset.

Time line: 1-March to 07-March

**Parameter optimization**: This task phase involves utilization of parameter optimization technique such as gridsearchCV to extract optimized parameters for decision tree, KNN and SVM classifiers.

Time line: 8-March to 15-March

**Model training**: This phase involves training of decision tree, KNN and SVM classifiers through cross validation technique on training dataset.

Time line: 16-March to 31-March

**Model Evaluation**: This phase involves in evaluating the trained machine learning models through key metrics such as accuracy, F1-score, precision & recall.

Time line: 01-April to 10-April.

# 5. Level Of The Project

## 5.1 Project Artefact

To find irregularities in fraud, it examines user activity and transaction trends. To enhance data quality, the system makes use of sophisticated feature engineering techniques. To find the best approach, it uses a variety of machine learning models, such as deep learning and conventional classifiers. To achieve accuracy, speed, and efficiency standards for real-world applications, the system will go through a thorough performance evaluation.

## 5.2 Level of investigation

The research includes the different critical aspects and techniques for fraud detection using the cyber profiling in order to make it extensive investigation. The investigation involves:

* Deployment and exploration of different supervised machine learning algorithms for fraud detection with evaluating their capabilities.
* Investigating the features extraction and selection techniques to extract the most relevant cyber profiling features.
* Addressing the data imbalance issues with state-of-the-art technique such as SMOTE to enhance model prediction ability.
* Employing the parameter optimization techniques to improve model performance.

## 5.3 Appropriation

The chosen methodology aligns with the research objectives and research questions. The methodology is structures below:

Scalability and Adaptability: The proposed system can efficiently process the large data with concerning the fraud detection through cyber profiling.

Data-Driven Decision Making: The utilization of features engineering and extraction techniques ensure the development of model on high quality data.

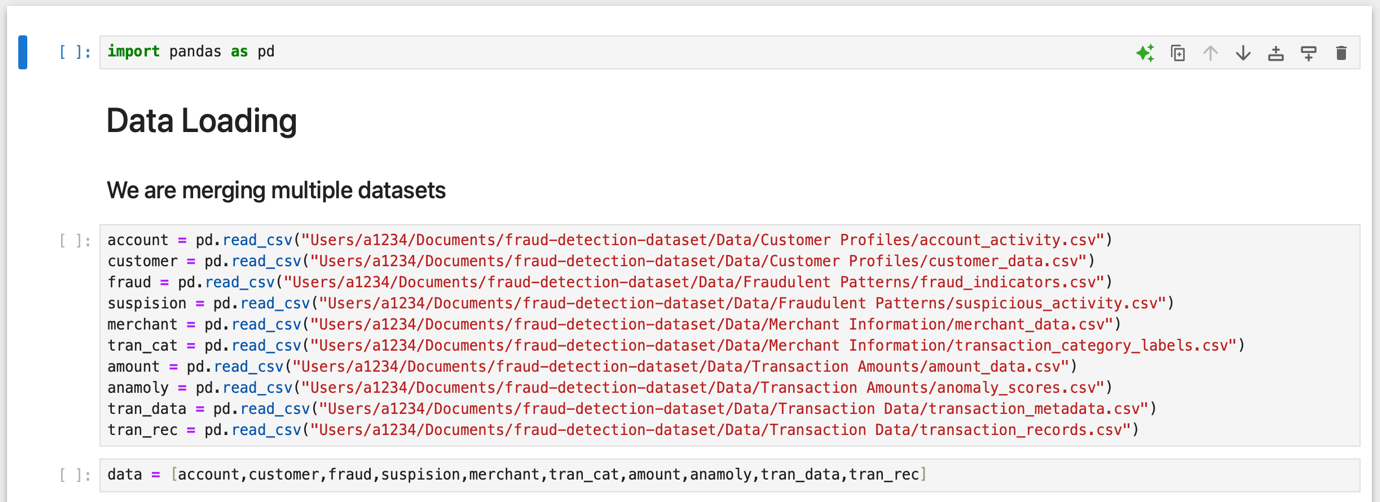
Comparative and Experimental setup: The research’s approach of evaluating different models, feature engineering techniques, and optimization strategies ensures a thorough analysis of the most effective fraud detection methods.

# 6. References

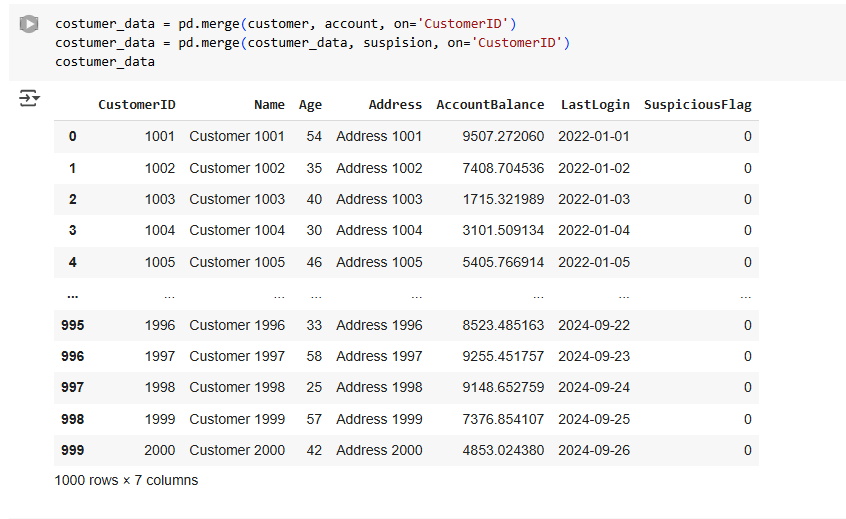
1. Alam, M.N., Podder, P., Bharati, S. and Mondal, M.R.H., 2021. Effective machine learning approaches for credit card fraud detection. In Innovations in Bio-Inspired Computing and Applications: Proceedings of the 11th International Conference on Innovations in Bio-Inspired Computing and Applications (IBICA 2020), pp. 154-163. Springer International Publishing.
2. Alfaiz, N.S. and Fati, S.M., 2022. Enhanced credit card fraud detection model using machine learning. Electronics, 11(4), p.662.
3. Awoyemi, J.O., Adetunmbi, A.O. and Oluwadare, S.A., 2017. Credit card fraud detection using machine learning techniques: A comparative analysis. In 2017 International Conference on Computing Networking and Informatics (ICCNI), pp. 1-9. IEEE.
4. Bada, M. and Nurse, J.R., 2021. Profiling the cybercriminal: A systematic review of research. In 2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), pp. 1-8. IEEE.
5. Btoush, E.A.L.M., Zhou, X., Gururajan, R., Chan, K.C., Genrich, R. and Sankaran, P., 2023. A systematic review of literature on credit card cyber fraud detection using machine and deep learning. PeerJ Computer Science, 9, p.e1278.
6. Chhabra Roy, N. and Prabhakaran, S., 2023. Internal-led cyber frauds in Indian banks: an effective machine learning–based defense system to fraud detection, prioritization and prevention. Aslib Journal of Information Management, 75(2), pp.246-296.
7. Dal Pozzolo, A., Boracchi, G., Caelen, O., Alippi, C. and Bontempi, G., 2017. Credit card fraud detection: a realistic modeling and a novel learning strategy. IEEE Transactions on Neural Networks and Learning Systems, 29(8), pp.3784-3797.
8. Darwish, S.M., 2020. An intelligent credit card fraud detection approach based on semantic fusion of two classifiers. Soft Computing, 24(2), pp.1243-1253.
9. Ford, V. and Siraj, A., 2014. Applications of machine learning in cyber security. In Proceedings of the 27th International Conference on Computer Applications in Industry and Engineering, Vol. 118. Kota Kinabalu, Malaysia: IEEE Xplore.
10. Gupta, A., Lohani, M.C. and Manchanda, M., 2023. Utilizing mathematical concepts of heat map for an intelligent and secure approach to efficiently detect credit card fraud. Journal of Interdisciplinary Mathematics, 26(8), pp.1837-1854.
11. Ileberi, E., Sun, Y. and Wang, Z., 2021. Performance evaluation of machine learning methods for credit card fraud detection using SMOTE and AdaBoost. IEEE Access, 9, pp.165286-165294.
12. Ileberi, E., Sun, Y. and Wang, Z., 2022. A machine learning based credit card fraud detection using the GA algorithm for feature selection. Journal of Big Data, 9(1), p.24.
13. Khare, N. and Sait, S.Y., 2018. Credit card fraud detection using machine learning models and collating machine learning models. International Journal of Pure and Applied Mathematics, 118(20), pp.825-838.
14. Khatri, S., Arora, A. and Agrawal, A.P., 2020. Supervised machine learning algorithms for credit card fraud detection: a comparison. In 2020 10th International Conference on Cloud Computing, Data Science & Engineering (Confluence), pp. 680-683. IEEE.
15. Lucas, Y. and Jurgovsky, J., 2020. Credit card fraud detection using machine learning: A survey. arXiv preprint arXiv:2010.06479.
16. Mehbodniya, A., Alam, I., Pande, S., Neware, R., Rane, K.P., Shabaz, M. and Madhavan, M.V., 2021. [Retracted] Financial Fraud Detection in Healthcare Using Machine Learning and Deep Learning Techniques. Security and Communication Networks, 2021(1), p.9293877.
17. Minastireanu, E.A. and Mesnita, G., 2019. An Analysis of the Most Used Machine Learning Algorithms for Online Fraud Detection. Informatica Economica, 23(1).
18. Ogwueleka, F.N., 2011. Data mining application in credit card fraud detection system. Journal of Engineering Science and Technology, 6(3), pp.311-322.
19. Patidar, R. and Sharma, L., 2011. Credit card fraud detection using neural network. International Journal of Soft Computing and Engineering (IJSCE), 1(32-38).
20. Rtayli, N. and Enneya, N., 2020. Selection features and support vector machine for credit card risk identification. Procedia Manufacturing, 46, pp.941-948.
21. Sailusha, R., Gnaneswar, V., Ramesh, R. and Rao, G.R., 2020. Credit card fraud detection using machine learning. In 2020 4th International Conference on Intelligent Computing and Control Systems (ICICCS), pp. 1264-1270. IEEE.
22. Sasank, J.S., Sahith, G.R., Abhinav, K. and Belwal, M., 2019. Credit card fraud detection using various classification and sampling techniques: a comparative study. In 2019 International Conference on Communication and Electronics Systems (ICCES), pp. 1713-1718. IEEE.
23. Shetty, V.R. and Malghan, R.L., 2023. Safeguarding against cyber threats: machine learning-based approaches for real-time fraud detection and prevention. Engineering Proceedings, 59(1), p.111.
24. Susto, G.A., Terzi, M., Masiero, C., Pampuri, S. and Schirru, A., 2018. A fraud detection decision support system via human on-line behavior characterization and machine learning. In 2018 First International Conference on Artificial Intelligence for Industries (AI4I), pp. 9-14. IEEE.
25. Trivedi, N.K., Simaiya, S., Lilhore, U.K. and Sharma, S.K., 2020. An efficient credit card fraud detection model based on machine learning methods. International Journal of Advanced Science and Technology, 29(5), pp.3414-3424.
26. Udoeyop, A.W., 2010. Cyber profiling for insider threat detection.
27. Varmedja, D., Karanovic, M., Sladojevic, S., Arsenovic, M. and Anderla, A., 2019. Credit card fraud detection-machine learning methods. In 2019 18th International Symposium INFOTEH-JAHORINA (INFOTEH), pp. 1-5. IEEE.

# 7. Appendices:

**Data Loading**

****

**Merging Customer Data**

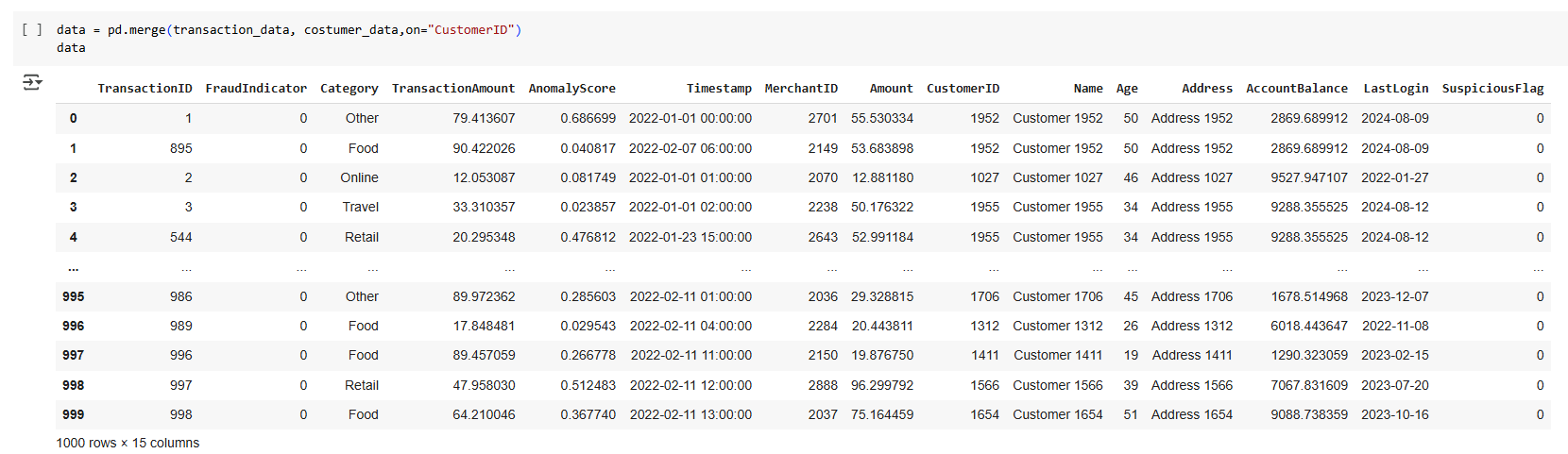


**Merging transaction Data**

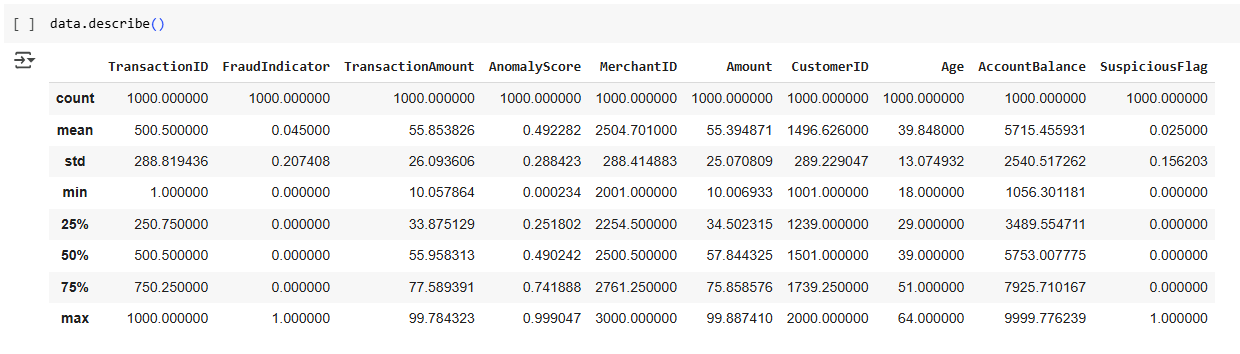
A screenshot of a computer

AI-generated content may be incorrect.

**Merging customer & transaction data:**



**Data Exploration:**



**Data Visualization Code**

A screenshot of a computer code

AI-generated content may be incorrect.

**Count plot for category:**

A graph of a bar graph

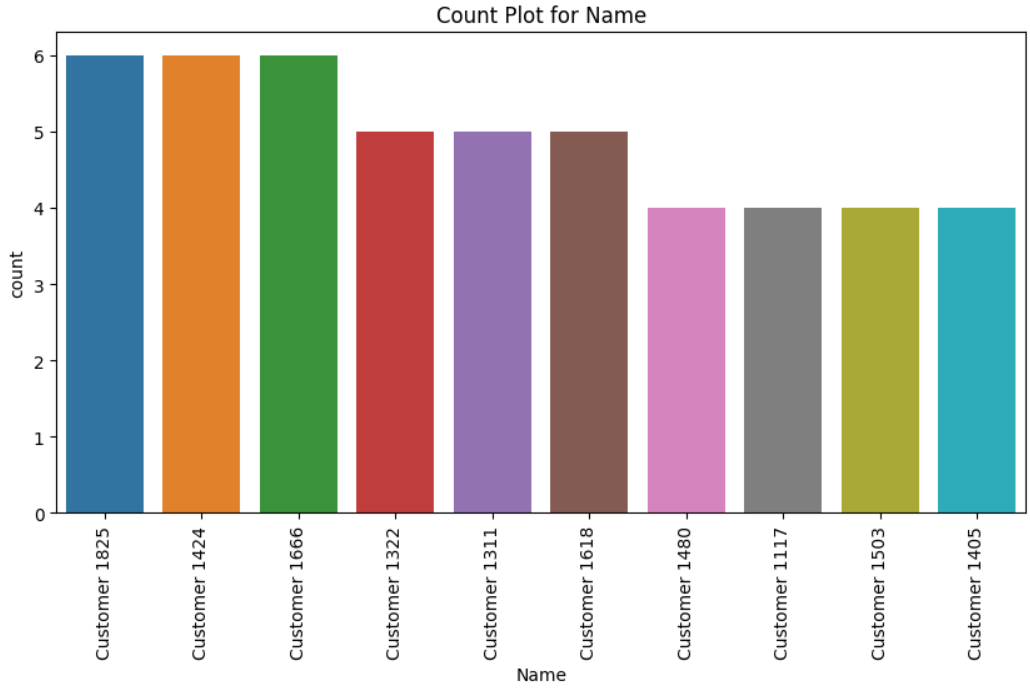
AI-generated content may be incorrect.

**Count plot for time stamp:**

A graph showing different colored vertical bars

AI-generated content may be incorrect.

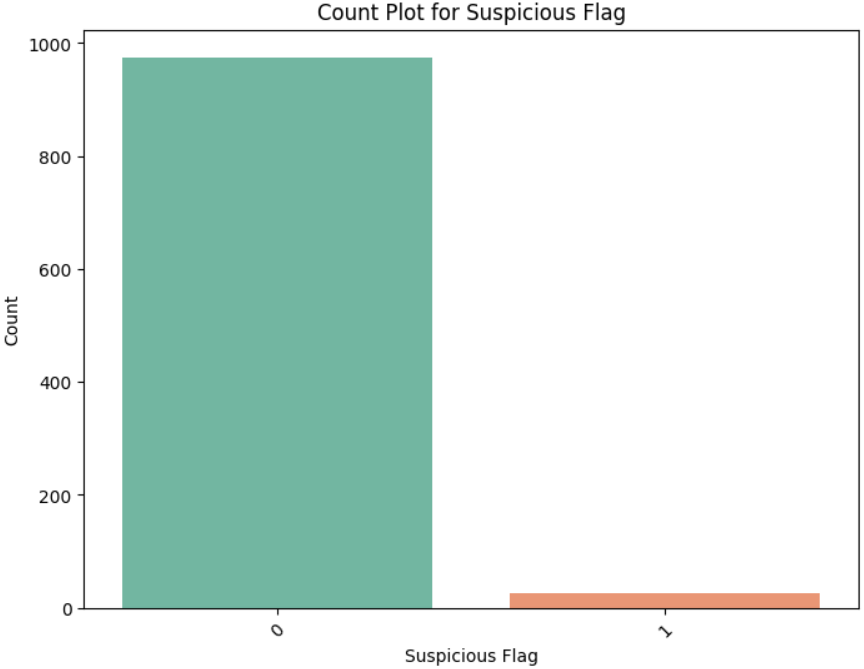
**Count plot for Name:**



**Count plot for suspicious flag Code**

A screen shot of a computer code

AI-generated content may be incorrect.



**Heatmap Correlations Code**

