Enhancing Credit Card Fraud Detection Accuracy by Optimisation of Anomaly Detection Algorithms and Resampling Techniques

MSc Research Project
Data Analytics

Aafreen Shan Asmath
Student ID: x23231335

School of Computing
National College of Ireland

Supervisor: Prof. Christian Horn

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Aafreen Shan Asmath		
Student ID:	x23231335		
Programme:	MSc Data Analytics	**Year:**	2024 - 25
Module:	MSc Research Project		
Supervisor:	Prof. Christian Horn		
Submission Due Date:	29/01/2025		
Project Title:	Enhancing Credit Card Fraud Detection Accuracy by Optimisation of Anomaly Detection Algorithms and Resampling Techniques		
Word Count:	8545	**Page Count:**	25

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: Aafreen Shan Asmath

Date: 29/01/2025

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Enhancing Credit Card Fraud Detection Accuracy by Optimisation of Anomaly Detection Algorithms and Resampling Techniques

Aafreen Shan Asmath
x23231335

Abstract

Credit card fraud has become a major threat to the financial systems, resulting in losses of billions of dollars and reducing the financial trust. Detection methodologies, such as rule-based systems and manual audits, are no longer effective in catching up with the rapidly changing patterns of fraud, besides the challenges posed by an imbalanced dataset. This work attempts to improve the fraud detection accuracy by combining the anomaly detection algorithms, that is, Isolation Forest and Local Outlier Factor with the state-of-the-art resampling techniques, that is, SMOTE, SMOTE-ENN, and Random Undersampling. The publicly available credit card transaction dataset is employed within this study through preprocessing and feature engineering to handle class imbalance and the data quality. The methodology combines unsupervised anomaly detection techniques with supervised logistic regression, to compare the performance across metrics such as accuracy, precision, recall, the F1 score, and AUC-ROC. It is revealed by the results that logistic regression using SMOTE-ENN obtains the highest AUC value (0.9364) and recall value (0,94), which is effective at detecting fraud transactions and minimizes false positives. Isolation forest with random undersampling reflects promise but has precision-specific limitations. This study thus emphasizes on how resampling techniques address class imbalance issues along with highlighting logistic regression using SMOTE-ENN as the best solution for fraud detection. Future studies could dwell upon hybrid models and advanced ensemble techniques to improve fraud detection systems in terms of their accuracy, scalability, and robustness.

Keywords: Credit Card Fraud Detection, Anomaly Detection, SMOTE-ENN, Isolation Forest, Machine Learning, Resampling Techniques.

1 Introduction

While digitization of financial transactions has added a lot of value by saving consumers and businesses time, it has also increased the amount of fraud taking place. Addressing the rise of smarter, more digital, and financial fraud has surpassed the capabilities of traditional detection systems, requiring innovative approaches to keep up. Fraudulent transactions result in direct financial losses and a gradual loss of trust in financial institutions. Current techniques, like manual audits or rule- based systems, prove insufficient to these challenges because they do not adapt well to the evolution of fraud, and they will not work with a large transaction volume.

As a result, machine learning is a promising weapon for fighting fraud. Machine learning algorithms use patterns within data to catch outliers and fraudulent activities more accurately. Nonetheless, a number of challenges exist, including the class imbalance problem, where fraud transactions make up a very small subset of the dataset. This imbalance can lead those machine learning models to underperform at detecting fraud. This Project is intended to build up an effective framework of customers for the detection of the fraud with the help of the advanced machine learning methods. The study combines anomaly detection models and resampling strategies to tackle the main challenges; class imbalance and high dimensional data. This strategy is scalable, interpretable, and also flexible regarding the evolution of financial fraud.

1.1 Background and Motivation

Financial fraud is a world-wide threat that undermines governments, businesses, and individuals. Modern statistics show that it is a problem, that incurs losses of billions of dollars each year which can be even greater in the future with the advancement of technology. Finance crimes become ever more complex, making it increasingly difficult to detect. Existing fraud detection systems that are based on either fixed rules or manual checks are inadequate in addressing current fraud scenarios. These systems also tend to result in a high number of false alarms which wastes resources and also frustrates customers.

The imbalance in transaction datasets deepens the issue at hand. Since fraud is rare and constitutes less than 1% of the transaction in most cases. Models trained on these kinds of datasets tend always to be biased towards the majority class, which is non-fraud, and will therefore have very low or even no detection of fraud. The vast majority of studies attempting to address the problem of fraud detection do focus on imbalanced data.

The driving force behind this project is the necessity of coming up with a solution that addresses these limitations. To perform data balancing, more advanced techniques such as the SMOTE (Synthetic Minority Oversampling Technique) and the SMOTE-ENN (SMOTE with Edited Nearest Neighbors) are employed. Moreover, outlier detection approaches such as Isolation Forest and the Local Outlier Factor are investigated in the context of their potential to detect rare events. The combination of such approaches will offer a more robust approach to detection of fraud activities in financial systems in practice.

1.2 Research Question and Objectives

The proposed research question for this study:

“How can Isolation Forest, Local Outlier Factor, and Logistic Regression combined with resampling techniques (SMOTE, SMOTE-ENN and Random Undersampling) improve the accuracy and reliability of credit card fraud detection models on highly imbalanced datasets?”

The main objective of this project is to make credit card fraud detection models more accurate and reliable by using anomaly detection algorithms (Isolation Forest and Local Outlier Factor) and combining them with different resampling techniques. The first objective is to preprocess and purge the dataset, thus tackling the missing values, duplicates, and outliers so that the data is now ready for model training. Second, doing research and implementing a few resampling techniques, such as SMOTE (Synthetic Minority Oversampling Technique), SMOTE-ENN (SMOTE with Edited Nearest Neighbors), Non-SMOTE and Random Undersampling, will be the next step of the project, which aims to resolve the class imbalance that prevails in fraud detection datasets since the fraudulent transactions are most of the time, very scarce. The purpose of this evaluation is to check the extent to which these approaches help in data balancing and the detection of fraudulent transactions.

The project will also try to contrast the results received through the Isolation Forest, Local Outlier Factor, and Logistic Regression models by measuring important performance metrics such as accuracy, precision, recall, F1-score, and AUC-ROC. The project will lastly propose a fraud detection structure that consists of these top-performing models blended, together with the resampling strategies relationships used to accomplish high fraud detection rates, while at the same time lowering the false positives to a bare minimum, hence guaranteeing that the model will be robust and that scalability is possible for real-world credit card fraud detection systems.

1.3 Document Structure

The structure of the paper is organized as follows: Section 1 will give an introduction to the background, motivation, and objectives of the project. Section 2 deals with an exhaustive survey of the available research on anomaly detection algorithms and resampling techniques in the area of fraud detection. Section 3 is the part that consists of the methodology together with the data preparation, manipulation of class imbalance, and feature selection. Section 4 lists the method of the fraud detection models which include the Isolation Forest, Local Outlier Factor, and Logistic Regression. Section 5 is the stage where the development of the process, including the training of the model and optimization, is done. Section 6 will be used to check the performance of the models. And lastly, Section 7 gives a conclusion of the paper as well as the direction for the future of the study.

2 Related Work

In the domain of credit card fraud detection, the focus is on various machine learning methods, especially anomaly detection and resampling procedures. The isolation forest and local outlier factor are the most common types of methods used to identify the outliers in datasets with class imbalance because they are very accurate in spotting rare fraudulent transactions. In addition, SMOTE and its derivative methods (SMOTE-ENN) have been used when the class is highly imbalanced. The technique in turn gives the performance of the model an uplift by making synthetic data for the minority class. Besides, Logistic Regression has been the classifier used in most situations of fraud detection and anomaly detection technique, at times parallel to these, for greater accuracy as well as a reduction of the number of false positives.

2.1 Machine Learning in Fraud Detection

Machine learning methods have advanced to a state as a leading tool for credit card fraud detection, delivering innovative approaches to the prevention of fraudulent activities in the financial service industry. Therefore, many studies have attempted to identify what is the optimal way to implement the various ML algorithms for this task. For instance, (R. Sailusha et al. 2020) applied Random Forest and AdaBoost for imbalanced data and obtained better performance in the case of preprocessed data and resampling strategy. Similarly, F. K. (Alarfaj et al. 2022) benchmarked deep learning algorithms (including some Support Vector Machines and Random Forests) for the real time handling of the problem/class (class imbalance) in the context of fraud detection. In particular, as a short introduction, (I. D. Mienye and N. Jere 2024) have considered deep learning architectures (i.e., LSTM, CNN and GRU) for fraud detection, with a special attention to the issues of paucity of data and concept drift, which leads to the insurances of fraud detection systems.

The work of (D. Prajapati et al. 2021) Competition between the application of Random Forest, XGBoost and the Artificial Neural Networks (ANNs) with regard to feature selection and optimization of the algorithmic parameters aiming towards the enhancement of performance in fraudulent transaction detection is described. Further, (P. Murkute et al. 2023) reported the application of Random Forest, Logistic Regression, and Gradient Boosting Machines and the use of evaluation parameters (e.g., AUC-ROC, AUPRC) to recover the financial fraud using blueprint metrics suitable for insuring the financial exchanges. At the same time, it is explained how the ML/DL models have played a key role in the evolution of systems towards the issue of fraud detection, which has made a relevant contribution to the field of insurance and confidentiality of financial operations.

2.2 Anomaly Detection Algorithms in Fraud Detection

Isolation Forest (IF) and Local Outlier Factor (LOF) are recently studied machine learning algorithms, and applied to credit card transaction fraud detection. (Zadafiya et al. 2022) also indicated that those algorithms actually operate on recognizing aberrant patterns in the transaction data by means of unsupervised learning methods, i.e., on imbalanced datasets. The authors showed that the techniques IF and LOF are valuable in the sense that they allow to classify fraudulent behavior from legitimate transactions by using the outliers and the local data density. Similarly, (Ghevariya et al. 2021) further exploited IF and LOF, and reported their effectiveness in big data computational for limited computional resources. Through their reversibility, these algorithms are suitable for real-world applications, such as real-time applications of fraud detection in the financial sector. (Singh et al. 2024) generalizes this paradigm by giving rise to preprocessing procedures such as random undersampling and SMOTE (Synthetic Minority Over-sampling Technique) for cases where class imbalance emerges and is addressed by the algorithm in order to compensate. These type of imbalanced classes have been worked on using anomaly detection classifier classes and the advantage has been discussed of using an IF, LOF and SMOTE based approach in combination to achieve better performance and accuracy for the credit card fraud detection. On the basis of comparative studies between classifiers and data analysis techniques, the two accompanying papers demonstrate that machine learning has great potential in credit card fraud deterrence and offers a nascent step toward understanding the future research required in optimization of financial security models.

2.3 Resampling Techniques for Handling Class Imbalance

In the present study about the application of imbalanced datasets in automatic credit card fraud detection, a good number of new contributions about imbalanced dataset treatment can be found. (Alamri and Ykhlef 2024) study hybrid undersampling and oversampling methods and, more specifically, the integration of Borderline SMOTE and Tomek links to remedy class imbalance in a credit card fraud dataset. Their method, which has also been confirmed for synthetic data generated by PaySim simulator, also resulted in improved sensitivity, i.e., owing to the absence of the benign contaminating noise and an appropriate model learning. To this end, (Xie and Huang 2024) further proposed to mix Mahalanobis distance and SMOTE-ENN hybridized sampling and Random Forest which can improve not only outlier detection, but also classification performance of a fraud detection system. (Samant et al. 2024) Investigate the effectiveness of Synthetic Minority Over-sampling Technique (SMOTE) for overcoming class imbalance and notable improvements to recall (RY) and precision (PE), which are of critical importance to real-time fraud detection. (Varmedja et al. 2019) explored machine learning models, Random Forest, Naive Bayes and Neural Network and confirmed their feasibility for creating fraud classifiers and used those classifiers. According to the paper, Random Forest would, in principle, yield robust and consistent results. All these papers, unanimously, also infer that for the financial system case, problems in data imbalance, in the application, and in the parameter tuning of these methods to a particular (e.g., a specific fraud detection) task are all issues that must be considered. Indicated by techniques, like SMOTE, hybrid samplings methods and robusing classifiers (random forests), yet also valuable information is also mentioned in system, to give better performance and efficiency of fraud detection systems for electronic credit card transactions.

2.4 Performance Metrics in Fraud Detection

The credit card fraud detection problem has also driven substantial research into suitable machine learning techniques to reach their maximum accuracy achievable, in particular the best possible accuracy of imbalanced datasets. (Leevy, Khoshgoftaar, and Hancock 2022) showed that in terms of the classification of schemes (Extremely Randomized Trees, XGBoost, Cat-Boost, LightGBM, and Random Forest), one must determine the right set of assessment metrics (e.g., AUC and AUPRC) for handling the class imbalance of fraud detection (Leevy et al., 2022). Similarly, Abdulghani et al. (Abdulghani et al., 2021) applied machine learning methods such as Logistic Regression and linear discriminant analysis with fuzzy membership approach for Discrete behavior of transaction data and eventually those are contributing to fraud detection of the fraud detection system (Abdulghani et al., 2021), and so on. (Ileberi, Sun, and Wang 2021) analyzed the combination of SMOTE (Synthetic Minority Over-sampling Technique) with AdaBoost for the correction of model errors due to data-balancing procedures and boosting algorithms, including those applied to the enhancement of fraud detection performance when the distribution of fraud and norminal transactions is imbalanced (Ileberi et al., 2021).

In addition, (Isangediok and Gajamannage 2022) focused, not only on the hyperparameter tuning and fine tuning of machine learning constructs, but also on the use of different classifiers in order to enhance the performance of fraud detection for imbalanced classes and in what manner these could be optimized in order to enhance the robustness of deployed practical financial protection applications. These works show that the application of combined application of the proposed methods such as the usage of boosting algorithms and other methods such as fuzzy logic combined with data balancing algorithms for the design of fraud detection systems is required to obtain more robust, dependable and effective results with respect to credit/debit card fraud. By suitable models, and metrics appropriate to the task, these approaches have the potential to improve performance in the field of fraud detection (class imbalances), and, as cybercrime methods advance along with technical capabilities, so too do these.

3 Research Methodology

This section outlines the research methodology, detailing essential steps for successful implementation and providing a technical perspective. The objective is to detect fraudulent credit card transactions and identify critical features influencing detection. Following the Knowledge Discovery in Databases (KDD) process, the methodology begins with data pre-processing, including cleaning duplicates, normalizing transaction amounts, transforming time features, and addressing missing values to ensure data quality. Feature selection and engineering are applied to refine the dataset and enhance model performance. This structured approach ensures the data is well-prepared for machine learning, enabling accurate and reliable fraud detection.

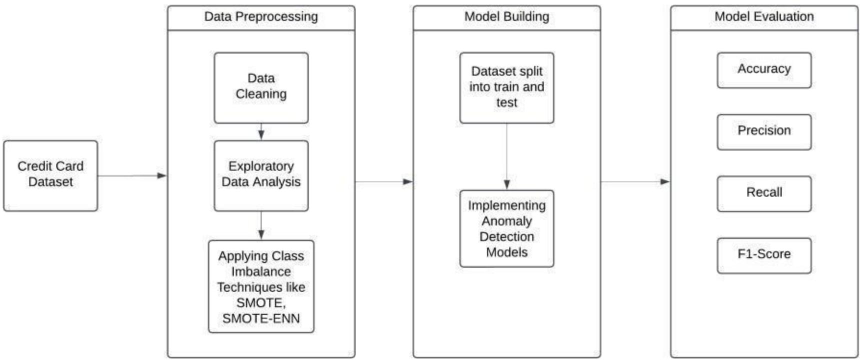

Credit Card Dataset
Data Preprocessing
Data Cleaning
Exploratory Data Analysis
Applying Class Imbalance Techniques like SMOTE, SMOTE-ENN
Model Building
Dataset split into train and test
Implementing Anomaly Detection Models
Model Evaluation
Accuracy
Precision
Recall
F1-Score

Figure 1: Research Methodology

3.1 Data Selection

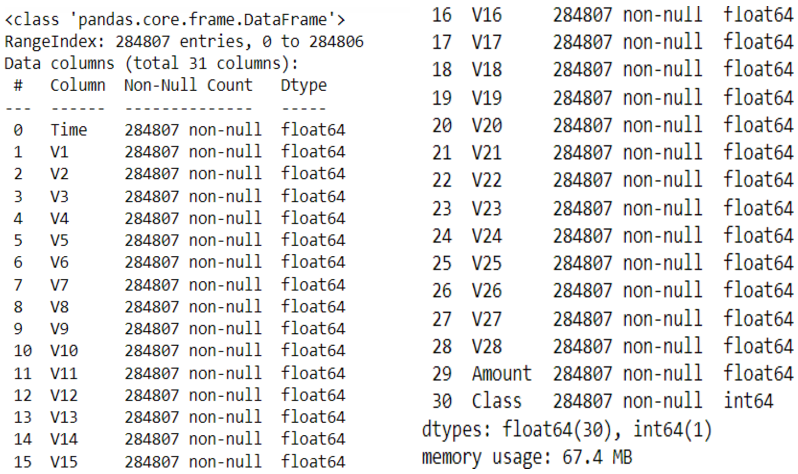
In this research project. I have took Public dataset which is creditcard.csv , which contains 284,807 entries with 31 different features including Time, Amount, and a series of anonymized variables (V1 to V28). The dependent variable, Class, indicates whether a transaction is fraudulent, coded 1, or non-fraudulent, coded 0. To make analysis really tough, the data also show reality complexity, especially with serious imbalance classes, in which less than 1% of entries account for fraudulent transactions. The above-mentioned scenario requires advanced techniques for effective fraud detection. This data set, thus, forms the basis of research that should point at the patterns and aspects that play a critical role in the separation of legitimate and fraudulent transactions, hence more secure financial systems.

3.2 Data Pre-Processing

This data preprocessing is the first and most essential step to be undertaken after data collection and before EDA and actual model building. Another core feature of the first phase of pre-processing is the cleaning of data from unnecessary columns, duplicates, and redundant data, which might affect model performance. The dataset is loaded into a dataframe, using the Python and pandas library, for efficiency. Since it is a publicly available dataset, there are no missing values, although the dataset has a few duplicate rows that the user has to identify and remove. For instance, some features-groups under transaction time (Time) and transaction amount (Amount) are transformed for further model performance. Amount feature is log-transformed while the time feature is normalized into hours to enhance interpretability-by reducing the skewness in the amount feature. After cleaning and transforming the data, the dataset is ready for analysis in that it incorporates only relevant features for the analysis, as illustrated in the pre-processed dataset that is used for EDA.

3.2.1 Data Cleaning

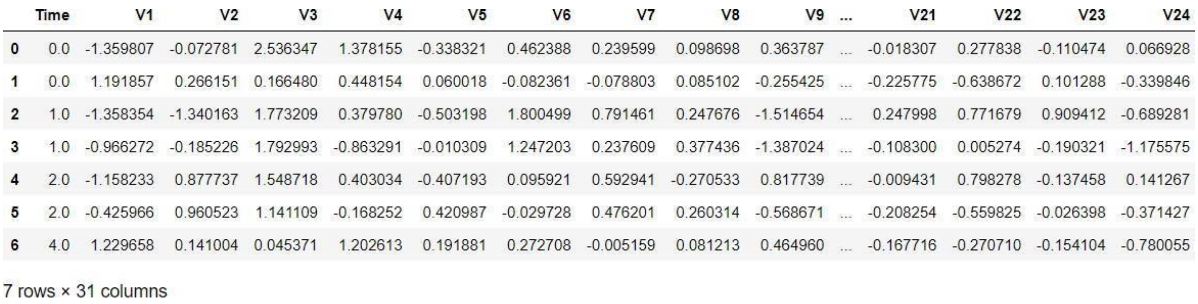
The data cleaning phase begins with an examination of the dataset to ensure that it is free of missing or null values. The dataset is loaded and evaluated with the help of the pandas library, which results in the conclusion that not one column associated with Time, V1 to V28, Amount, and Class - the target variable - has any null values. Most of the columns have data types as float64, except one column, Classastype, which is int64. .duplicated() check was run for the dataset even though there was no missing data, and discovered that the dataset has duplicate rows found 1081 and removed them. Cleaning ensures that redundancy does not compromise the analysis or performance of the model. The cleaning process takes the dataset to an investigation and transformation level, whereby removing duplicates and all columns with valid, non-null data that are important for the next project steps comprise the dataset.



```
<class 'pandas.core.frame.DataFrame'>
RangeIndex: 284807 entries, 0 to 284806
Data columns (total 31 columns):
 #   Column  Non-Null Count   Dtype
---  ------  --------------   -----
 0   Time    284807 non-null  float64
 1   V1      284807 non-null  float64
 2   V2      284807 non-null  float64
 3   V3      284807 non-null  float64
 4   V4      284807 non-null  float64
 5   V5      284807 non-null  float64
 6   V6      284807 non-null  float64
 7   V7      284807 non-null  float64
 8   V8      284807 non-null  float64
 9   V9      284807 non-null  float64
 10  V10     284807 non-null  float64
 11  V11     284807 non-null  float64
 12  V12     284807 non-null  float64
 13  V13     284807 non-null  float64
 14  V14     284807 non-null  float64
 15  V15     284807 non-null  float64
 16  V16     284807 non-null  float64
 17  V17     284807 non-null  float64
 18  V18     284807 non-null  float64
 19  V19     284807 non-null  float64
 20  V20     284807 non-null  float64
 21  V21     284807 non-null  float64
 22  V22     284807 non-null  float64
 23  V23     284807 non-null  float64
 24  V24     284807 non-null  float64
 25  V25     284807 non-null  float64
 26  V26     284807 non-null  float64
 27  V27     284807 non-null  float64
 28  V28     284807 non-null  float64
 29  Amount  284807 non-null  float64
 30  Class   284807 non-null  int64
dtypes: float64(30), int64(1)
memory usage: 67.4 MB
```

Figure 2: Overview of column Datatypes

The dataset is made of 284807 rows and 31 columns and has anonymized transaction features and labels. These columns have Time (hours from the first transaction), Amount (transaction value), and V1 to V28 (anonymized features developed through PCA). The column Class marks whether the transaction can be considered fraudulent (1) or non-fraudulent (0). Each specific transaction is assigned a row, with the values comprising V1 to V28 considerable as factors that contribute to the transaction; in contrast, the Amount and Time more specific details concerning the transaction. The dataset offers a varied range of feature values, from positive to negative numbers. They are normalized or transformed data to maintain their privacy. The target variable Class allows for the binary classification of fraudulent and non-fraudulent transactions. It is very easy to carry further analysis which opens to trends in the data that helps in fraud identification with advancements in detection quality.

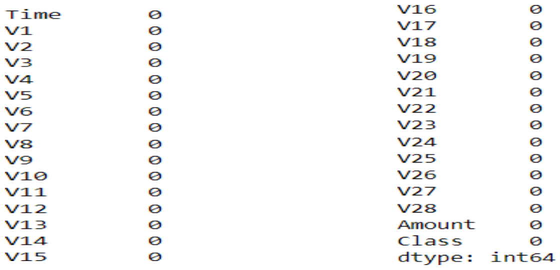


	Time	V1	V2	V3	V4	V5	V6	V7	V8	V9	...	V21	V22	V23	V24
0	0.0	-1.359807	-0.072781	2.536347	1.378155	-0.338321	0.462388	0.239599	0.098698	0.363787	...	-0.018307	0.277838	-0.110474	0.066928
1	0.0	1.191857	0.266151	0.166480	0.448154	0.060018	-0.082361	-0.078803	0.085102	-0.255425	...	-0.225775	-0.638672	0.101288	-0.339846
2	1.0	-1.358354	-1.340163	1.773209	0.379780	-0.503198	1.800499	0.791461	0.247676	-1.514654	...	0.247998	0.771679	0.909412	-0.689281
3	1.0	-0.966272	-0.185226	1.792993	-0.863291	-0.010309	1.247203	0.237609	0.377436	-1.387024	...	-0.108300	0.005274	-0.190321	-1.175575
4	2.0	-1.158233	0.877737	1.548718	0.403034	-0.407193	0.095921	0.592941	-0.270533	0.817739	...	-0.009431	0.798278	-0.137458	0.141267
5	2.0	-0.425966	0.960523	1.141109	-0.168252	0.420987	-0.029728	0.476201	0.260314	-0.568671	...	-0.208254	-0.559825	-0.026398	-0.371427
6	4.0	1.229658	0.141004	0.045371	1.202613	0.191881	0.272708	-0.005159	0.081213	0.464960	...	-0.167716	-0.270710	-0.154104	-0.780055

7 rows × 31 columns

Figure 3: Overview of Data frame

Missing values were checked using.isnull().sum, which revealed that the dataset had no missing values. However, there were 1081 duplicated rows which were detected using the.duplicated method. These rows were dropped using the.drop_duplicates method thereby dropping the dataset to 283,726 rows from the initial 284,707 rows. This step also made sure that the data was clean and free from any form of bias as we proceed with the analysis.



```
                                  V16       0
Time      0                       V17       0
V1        0                       V18       0
V2        0                       V19       0
V3        0                       V20       0
V4        0                       V21       0
V5        0                       V22       0
V6        0                       V23       0
V7        0                       V24       0
V8        0                       V25       0
V9        0                       V26       0
V10       0                       V27       0
V11       0                       V28       0
V12       0                       Amount    0
V13       0                       Class     0
V14       0                       dtype: int64
V15       0
```

Figure 4: Missing Values

3.2.2 Exploratory Data Analysis

Exploratory Data Analysis (EDA) is a vital step within which a data set is learned, patterns identified, and the set prepared for machine learning. Initially, it would analyze the distributions of each feature, starting with visualizations that show relationships between each variable.

To tackle the skewness in the Amount feature, a logarithmic (log1p) transformation was done. The transformation normalized the distribution to follow less skewed distribution patterns, making it more analysis friendly. Histogram of the transformed Amount was found to give a more normal distribution, which now tells the different transaction values. Similarly, the Time feature, in which the seconds since the first transaction were interpreted this time, was converted into hourly intervals to better interpret. Histograms of the Time feature indicated that transactions were made at different times, with some periodic time patterns indicating the trend.

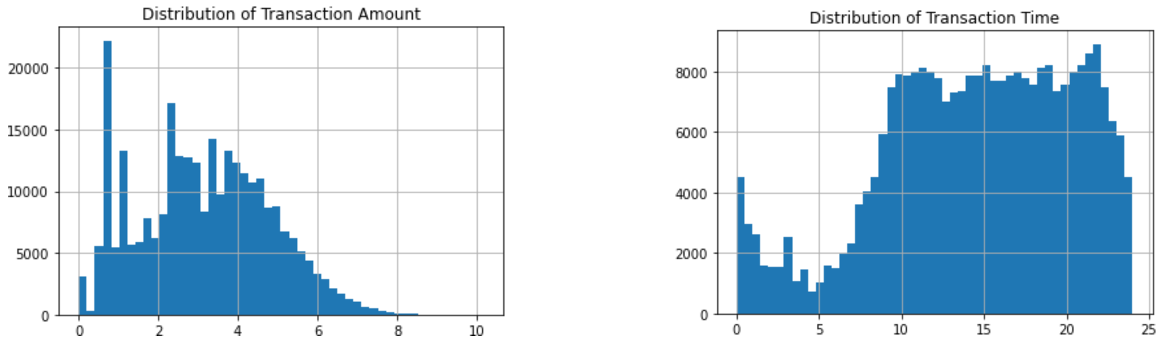


Figure 5: Logarithmic Transaction Amount and Time

The count plot was used to visualize the class distribution (Column Class) of the data with respect to whether it was a fraud (1) or non-fraud (0). The plot very well highlighted the class imbalance: fraudulent transactions comprised less than 1% of the data. That corroborated the necessity of balancing techniques to increase model performance.

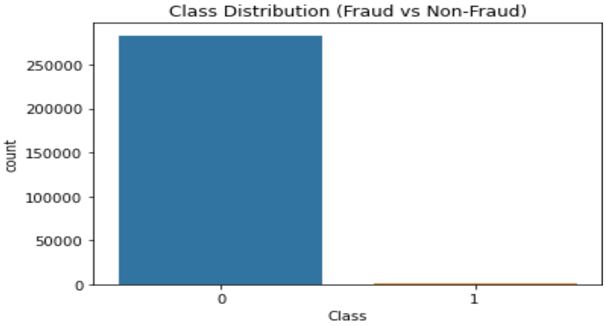


Figure 6: Fraud vs non-fraud

Boxplots have been visualized for Amount and Time and generated with respect to Overall and across the classes. It helped us identify the outlier data points and also the distinguished pattern of fraudulent transactions. For example, it indicated the concentration of such fraudulent transactions in a few time intervals. One of the scatter plots between the selected features (V1 and V2) showed clustering behavior characteristic to fraud compared to the non-fraud ones.

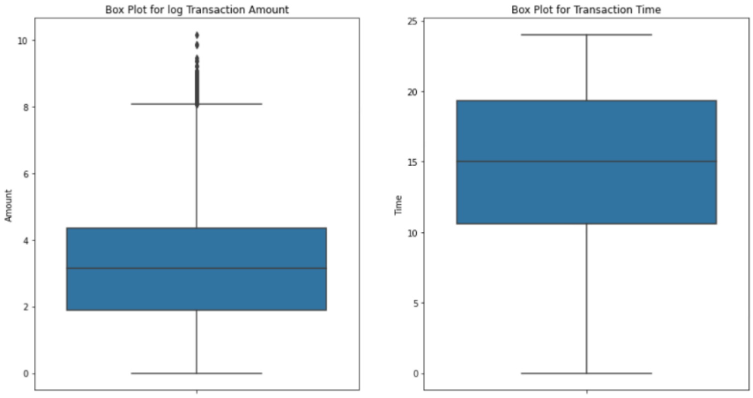


Figure 7: Amount and Time of Transaction

The correlation matrix made a broad picture of the relationships between the characteristics. Although most features were characterized by weak correlations, some of them had stronger ties with fraud, thus guiding feature selection for the model.

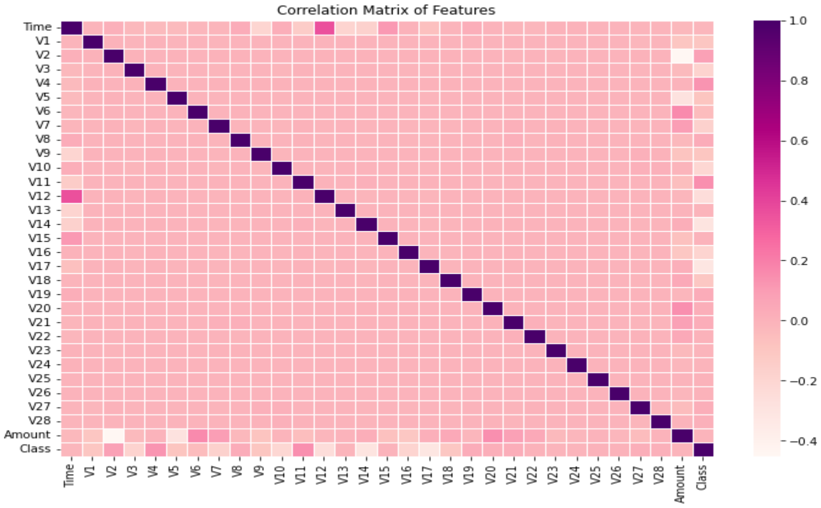


Figure 8: Correlation Matrix

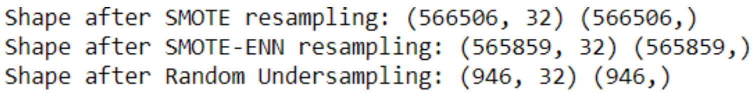
3.2.3 Data Balancing Techniques

Class imbalance is an important problem in the field of fraud detection. A dataset generally contains much fewer fraudulent transactions than non-fraudulent transactions. Hence, to balance the dataset, methods such as SMOTE, SMOTE-ENN, and Random Undersampling are three data balancing techniques that work on making the training dataset appropriate for machine learning algorithms without bias towards the majority class. The SMOTE method has been implemented for the generation of new artificial samples for the minority class. The method builds data points by interpolating between existing samples, hence preserving the original characteristics of data. With the application of SMOTE, the balanced dataset now contains 566,506 samples, of which both fraud (1) and non-fraud (0) classes are equally represented. Hence, excellent foundation for training models while keeping basic fraud characteristics was set.

SMOTE-ENN combines the use of SMOTE with ENN, an additional cleaning step for the removal of non-informative and borderline samples. Thus, this hybrid guarantees that the synthetic samples are very polished, that they improve performance in the models. This would yield a dataset within 565,859 samples, both class-distributed evenly and with points reduced for noise. Random Undersampling reduced the majority class by randomly selecting non-fraudulent samples for removal. This would balance the data set with respect to two classes, downside being extreme losses in honor of the majority class. The undersampled version had 946 samples with equal representation of both classes. Effective for balancing but leaves a lot of information which could have been useful for the majority.

While employing these techniques to ameliorate model accuracy and recall, diverse strategies against class imbalance will be provided for experimentation in the choice of best approaches. Particularly, three techniques: SMOTE, and SMOTE-ENN, are very good at keeping important patterns formed by the input data, whereas Random Undersampling gives the best possible alternative for simplicity at the expense of other aspects in data collection.

As a result, this prepared data can effectively meet the criterion of training fraud detection models counterbalancing the symmetry in performance effects from such training.



```
Shape after SMOTE resampling: (566506, 32) (566506,)
Shape after SMOTE-ENN resampling: (565859, 32) (565859,)
Shape after Random Undersampling: (946, 32) (946,)
```

Figure 9: Balanced Dataset

4 Design Specification

This is the technical methodology followed in the project during the design specification to solve the problem of fraud detection. Models and resampling strategies were applied to the highly imbalanced classes combined with the dataset's complexity. Hence, these factors make the system robust and very efficient in detecting fraudulent transactions.

4.1 Modelling Techniques

The project employs three primary modelling techniques: Isolation Forest, Local Outlier Factor (LOF), and Logistic Regression. Each technique brings unique strengths to the task of identifying anomalies and classifying transactions based on patterns observed in the data.

4.1.1 Isolation forest

Isolation Forest is an unsupervised algorithm for anomaly detection based on trees. The principle of isolation forest is recursively partitioning the data and separating every data point with random splits. In such cases, a fraudulent transaction is an anomaly because it requires fewer splits to be isolated than a non-fraudulent transaction. The algorithm thus assigns an anomaly score to each transaction, indicating high values as potentially fraudulent.

Isolation Forest was applied to the datasets resampled with SMOTE, SMOTE-ENN, and Random Undersampling. Tune the significant hyperparameters of contamination (proportion of outliers in the dataset) and maximum features for optimization. The algorithm's ability to isolate the records in their category makes it useful for fraud detection when the pattern does not match significantly with fraud cases. Results will be evaluated using precision, recall, F1-score, and ROC-AUC for a holistic view of the model from different resampled datasets.

4.1.2 Local Outlier Factor

It is also an anomaly detection algorithm which measures how much the density of data point differs from its neighbors. Data points with very low density as compared to their neighbors are considered outliers by LOF. LOF works quite well in terms of detecting fraudulent transactions since density can be distinguished in a high-dimensional data set. The LOF model was trained on both original and resampling datasets. Also, the number of neighbors, n_neighbors, an important hyperparameter determining local density in LOF, was tuned in order to maximize model accuracy. Crowned by local density variations, LOF effectively captures complex fraud patterns and is therefore a great tool for fraud detection

4.1.3 Logistic Regression

Logistic Regression is a way of supervised learning and often uses this technique to find the possibility of fraud detection in transactions. The relationship between independent variables (features) and the binary target variable (Class) develops and provides probabilities as an output. Logistic Regression is applied on both original as well as resampled datasets. Hyperparameter tuning using grid searches was done to optimize parameters including regularization strength (C) and penalty type (L1 or L2). The simplicity and interpretable nature of this algorithm make it trustworthy for being adopted particularly for binary classification purposes. Performance metrics such as precision, recall, F1 score, and ROC-AUC are used to evaluate how well the algorithm distinguishes between fraud cases and genuine transaction cases. Every model is tried on some resampled datasets, which give scope for future studies to compare the different models on their effectiveness for fraud detection. The project is holistic in identifying fraudulent transactions through the use of both anomaly detection and supervised learning techniques.

4.2 Resampling Techniques

Class imbalance is a critical challenge in fraud detection. Fraudulent transactions (Class = 1) constitute less than 1% of the entire dataset. The dataset was resampled to establish a balance whereby models would learn efficiently in both classes. Three resampling strategies were employed:

4.2.1 Synthetic Minority Oversampling Technique (SMOTE)

SMOTE is an oversampling method in which synthetic samples are created for the minority class. It does this by first choosing a sample of the minority class, and then it interpolates new samples along the line segments between the chosen small sample and its closest neighbors. This way of generating new samples effectively increases representation for the minority class, not just duplicating existing samples. After applying SMOTE, the database comprises balanced samples being 566,506, fraud and non-fraud equally distributed across them. By such balancing, the models were now trained on data accurately representing both classes and resulting in less bias toward the majority class. SMOTE retains the inherent patterns of the minority class, hence preferred for improving model performance.

4.2.2 SMOTE-ENN (Synthetic Minority Oversampling Technique - Edited Nearest Neighbors)

SMOTE-ENN is a hybrid approach that combines oversampling with data cleaning. The ENN method uses nearest-neighbor techniques to classify both classes into border and noisy samples after applying SMOTE to oversample the minority class. This gives a pure, much more reliable dataset which can now improve the quality of data that is used in training models. The use of SMOTE-ENN produced a dataset that was well balanced with 565,859 samples. This removes unreliable samples to illustrate the reduction of overfitting risk, thus improving precision and recall of the models. This was also very useful in preserving the dataset integrity to enhance generalization of application during model testing.

4.2.3 Random Undersampling

Random Undersampling decreases the size of majority classes randomly selecting a fraction of non-fraudulent transactions. This method produces a balanced dataset by making the number of samples in the majority class equal to that in the minority class. However, it was successful at achieving class imbalance. Irrespective of this point, it can lose some invaluable patterns in the majority class that can impact the models' generalizability. Even if this is the case, it would still serve as a good baseline to compare with the performance of other resampling techniques. Every dataset was split for training and testing purposes in an 80:20 ratio by resamples. It implies that new samples are used after resampling for evaluation purposes, hence providing performance measures that are realistic.

Finally, such resampling techniques would be integrated into superior modelling methods to address such problems of class imbalance and provide a reliable ground for fraud detection. The methodology of integrating modelling techniques with highly sophisticated resampling techniques assures the robustness and efficiency of the system toward fraudulent transaction identification.

5 Implementation

Implementing a theoretical design into a pragmatic and functional fraud detection system is the significant phase of the activity. In other words, it includes use of appropriate tools within the framework of a structured workflow, paying close attention to challenges such as class imbalance, and use of anomaly detection models. This detailed approach would make the system robust, efficient, and highly accurate in identifying fraud transactions.

5.1 Tools Utilised

The diversity of software tools and libraries employed for data processing, visualization, modelling, and evaluation created a solid framework to optimize the work and give strong solutions to complex challenges when developing the fraud detection system.

Python is that programming language in which everything is written. Its flexibility and ecosystem of libraries make it the best tool for data analysis and machine learning.

Pandas for efficient manipulation and cleaning, and numerical operations of the dataset; it is mainly directed to handle primary data while NumPy takes in complex mathematics.

Matplotlib and Seaborn libraries of visualization that helped to create histograms, boxplots, scatter plots, and heatmaps, which are fabulously useful in revealing patterns, outliers, and correlations within the dataset.

Scikit-learn a machine-learning library implemented algorithms like Logistic Regression, Isolation Forest, and Local Outlier Factor on it. Also contained vital model evaluation tools such as precision, recall, F1-score, and ROC-AUC metrics.

Imbalanced-learn (imblearn). This library was meant for dealing with class imbalance using SMOTE, SMOTE-ENN, and Random Undersampling techniques. Such approaches were essential in reinventing balanced datasets to enable fair and effective training of machine learning models.

5.2 Implemented Workflow

The fraud detection system encompassed an organized workflow addressing all challenges posed by the dataset specifically imbalanced class: the workflow included preprocessing, resampling, training model and evaluation. - and the systems that were built for such challenges were found to be equalized to a satisfactory level of effectiveness.

5.2.1 Handling Class Imbalance

It presented a major challenge in the dataset as the class mismatch was very high, in such a way that fraudulent transactions accounted for less than 1% of the total data. Because of this class imbalance, it had been very unfair for the standard algorithms to learn any meaningful patterns from the minority class because most of the time they would give biased predictions. To overcome the problem, three resampling techniques have been applied to ensure a balanced and fair representation of both classes during model training.

The first such technique, called SMOTE: synthetic minority oversampling technique, involved generating synthetic samples for minority classes through multiple interpolation techniques between data points now knotted to-and-fro their nearest neighbors. The technique allows for increased representation. The method nevertheless upholds fraudulent transaction patterns and enables modelling with an evenly balanced dataset. A more refined method is SMOTE-ENN, which basically does the same thing as SMOTE but with the addition of edited nearest neighbors after the oversampling stage to further improve data quality by eliminating noise and borderline instances.

This technique provided a better matched, cleaner data set for training and indeed robust performance of the final model. Random Undersampling, however, randomly downsizes the majority class to yield about the same size setup as that of the minority class. Though it is a remedy to achieving the successfully balanced setup, this technique is expected to delete some important patterns from the majority class, which in turn affects the ability of the model to generalize. Altogether, these strategies for resampling enable class imbalance correction to facilitate detection of fraud by the models.

5.2.2 Anomaly Detection Models

Three different models were developed to deal with the unique challenges arising from fraud datasets in order to detect different fraudulent transactions. Isolation Forest is an unsupervised anomaly detection algorithm though it isolates data points recursively through partitioning. In the case of fraudulent transactions, the anomaly gets identified quite sooner than the non-fraudulent transactions. Thus, the algorithm assigns an anomaly score for further judgment of classifying those transactions based on their scores. Isolation Forest was applied on original and resampled datasets, and hyperparameter tuning was done to get the optimum settings that would improve the performance of the algorithm. It was evaluated with the help of precision, recall, and ROC-AUC metrics to ensure the algorithm can rely on highlighting fraudulent outliers.

Another model is the Local Outlier Factor (LOF), which computes a local density of points with respect to their neighbors to scatter potential anomalies. It indicates outliers when identified with very low densities and thus captures a wide diversity of subtle and localized fraud patterns. It is run on the original and resampled data for assessment against varied class distributions to test its performance. Also, Logistic Regression is a supervised learning algorithm to forecast the probability of fraud occurring given a design of input features. It was trained with up sampled samples to deal with the issue of class imbalance while maintaining interpretability. Hyperparameter tuning was conducted for this logical available equation, and then performance was assessed through metrics such as F1-score and ROC-AUC. With these models, fraud detection proved very efficient among these combined.

6 Result and Evaluation

The performance of models when detection is done on different models such as Isolation Forest, Local Outlier Factor (LOF), and Logistic Regression but applied with different remodeling techniques to balance the class of the dataset. This work presents the metrics of measurement such as accuracy, precision, recall, F1 Score, and AUC for the effectiveness of the model with respect to fraudulent transactions. All the Resampling methods considered in this study include Synthetic Minority Oversampling Technique: SMOTE, SMOTE-ENN-the hybrid between SMOTE and Edited Nearest Neighbors, and Random Undersampling. Indeed, fraud detection within highly imbalanced datasets is a critical one in machine learning which is still an emerging field that needs innovative approaches for accuracy and scalability.

6.1 Case Study 1: Isolation Forest

The anomaly detection methodology Isolation Forest here generates decision trees for isolation of outliers. It has proven to be quite a promising method for application in fraud detection, for which anomaly detection is in proposition. Performance, however, varies considerably with the type of resampling technique being used. An in-depth analysis follows here:

Isolation forest with SMOTE: Balancing classes would become redundant as a result of classification by using oversampling on the minority class through synthetic sample creation. The output of the model upon integrating this with Isolation Forest was demonstrated to be as follows: an AUC of 0.6039, a precision of 0.75, and a recall of 0.6. The change in recall evidently shows that it has improved the fraudulent transaction detection capability of the model. But at the same time, it has been stated that it has achieved all this without a corresponding increase in the F1-score, which continues to get suspended at 0.54.

Isolation Forest with SMOTE-ENN: It also has potential to enhance the quality of data further because it takes care of oversampling and noise. This aspect could, therefore, quite marginally improve the performance of the model over SMOTE, resulting in an AUC of 0.6065 and a recall of 0.61. Precision remains unchanged at 75, thus establishing the importance for noise reduction as evidenced by SMOTE-ENN without any impact on the precision.

Random Undersampling with Isolation Forest: It can be said to balance the datasets through an attrition from class majority to bring about data loss. However, this was the highest AUC (0.619) recorded across the different Isolation Forest configurations. The precision also improved up to 0.78, while recall reached 0.62 giving an F1-score of 0.55. This means that undersampling works to correct the imbalance but compromises the representation of data.

Isolation Forest without Resampling: It was able to achieve AUC of 0.8901 on the non-re-sampled imbalanced dataset but recall and precision stood at 0.89 and 0.52 respectively. Hence, high recall indicates that the model is good at fetching the fraud cases, but low precision indicates a high false-positive result. All of those lead to the urgency of resampling techniques to improve overall performance. Isolation Forest did perform well using different resampling strategies; however, Random Undersampling was the most useful in terms of AUC and recall. Nevertheless, the model underperformed in terms of precision in the absence of any resampling, making the necessity of class imbalance admit.

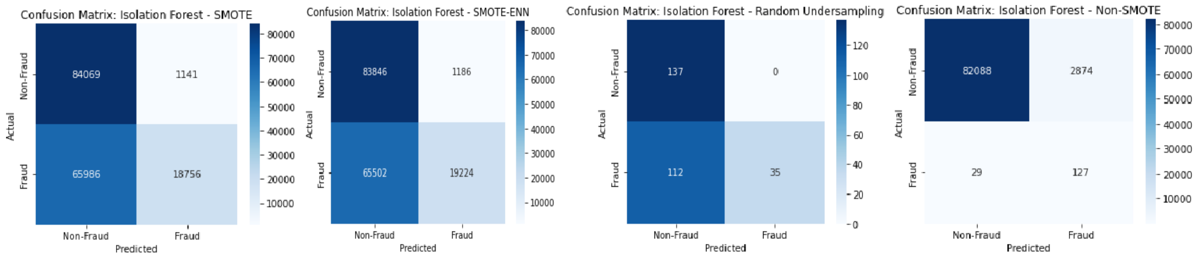


Figure 9: Confusion Matrix for Isolation Forest

6.2 Case Study 2: Local Outlier Factor

Local Outlier Factor (LOF) is a method used for anomaly detection that compares local densities. Although LOF is a good method for anomaly detection, it performs rather differently in fraud detection because of the different types of resampling that can be used.

LOF with SMOTE: With SMOTE, LOF provided an AUC of 0.5058, with precision at 0.53 and recall at 0.51. These results do show a marginal improvement over the approaches which did not use resampling. The low AUC indicates the fact that LOF is unable to separate fraudulent transactions from normal ones, even with synthetic oversampling.

LOF with SMOTE-ENN: SMOTE-ENN offers just slight improvement to LOF, bringing into the fore an AUC of 0.508 and precision of 0.54, whereas recall has remained at 0.51, signifying that noise reduction was not very effective at modifying the recognition of a fraudulent case by this model.

LOF with Random Undersampling: For LOF, Random Undersampling yielded the best AUC (0.5129) and maximum precision (0.59). Recall remained 0.51 with overall F1 score standing at 0.37. This shows that data reduction has a negative impact on recall performance by the model.

LOF without Resampling: LOF without any form of resampling produced an AUC score of 0.5903, precision and recall at 0.51 and 0.59, respectively. While the model achieved a very high accuracy of 0.97, it could not effectively detect fraudulent cases, demonstrating its limitations in imbalanced datasets.

LOF showed minor crawl improvement by the different resampling strategies, with an almost negligible gain in AUC and precision. This means that LOF could be even less efficient than Isolation Forest in fraud detection task where imbalances exist.

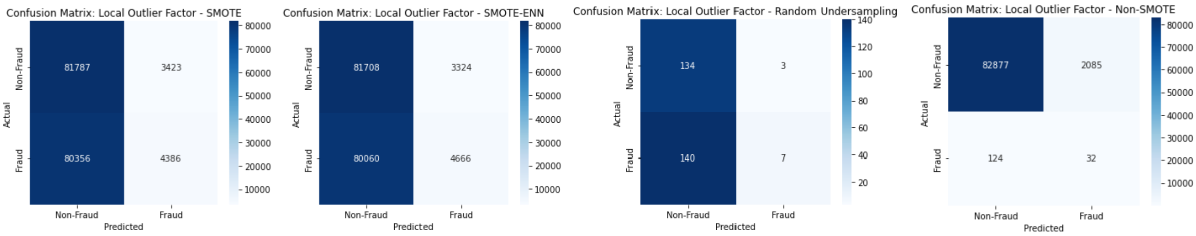


Figure 10: Confusion Matrix for LOF

6.3 Case Study 3: Logistic Regression

Logistic regression is a classification model for predicting probabilities and is popular for use in fraud detection. The performance of logistic regression was examined across different resampling techniques for class imbalance issues.

Logistic regression with SMOTE: The model was able to achieve perfect accuracy (0.94), precision of 0.97, and recall of 0.91, resulting in achieving F1 score of 0.94. The AUC was equal to 0.9708; therefore, it indicated that it was good at detecting fraud transactions. However, there was a minor drop in precision due to the overlaps caused by synthetic samples.

Logistic regression with SMOTE-ENN: This further improvement of logistic regression by that of SMOTE-ENN was the outcome of better quality of data and possible reduction in overlap. The best AUC (0.9712) and recall (0.94) of the models tested were occupied by this configuration. The performance for precision, however, only managed a score of 0.91 against the other models tested, although the corresponding F1 score remained reasonable at 0.94. These results affirm that the option of SMOTE-ENN would be the best maximizing recall, which really is a very critical parameter in fraud detection.

Logistic Regression with Random Under sampling: It has balanced the data set; reduced the majority class; AUC is 0.928 with a recall of 0.93. Its precision stood at 0.52 owing to challenges associated with data loss. The F1 score was at 0.53, implying performance is reasonable and affected by the data under this representation.

Logistic Regression without Resampling: It produced an AUC of 0.8027, precision to 0.92, recall at 0.8, and an F1 score is 0.85. These results are similar to the configuration under SMOTE, showing that Logistic Regression performs well in the detection, but it is highly imbalanced.

SMOTE-ENN with logistic regression produced the best results regarding highest AUC and recall. This shows how important combining rigorous resampling techniques with a classifier model is for fraud detection.

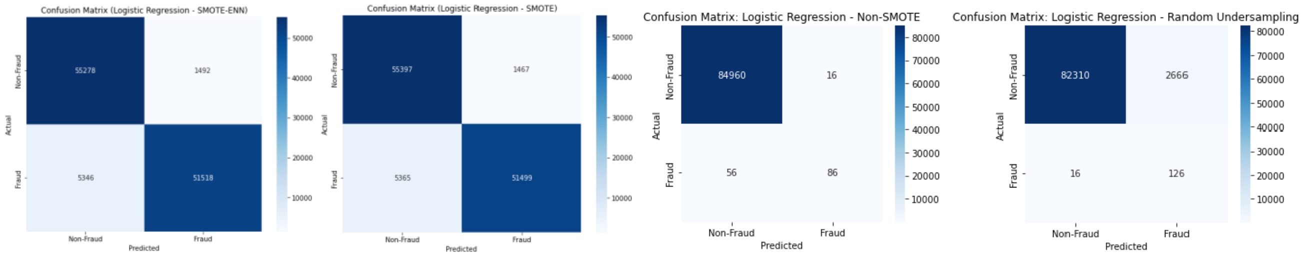


Figure 10: Confusion Matrix for Logistic Regression

6.4 Discussion

The evaluation has shown how to manage the class imbalance problem in fraud detection. Among those tested for models and resampling strategies, Logistic Regression with SMOTE-ENN is the best combination that scored the highest AUC (0.9712) and recall (0.94). This is interpreted as having a better probability of detecting fraudulent transactions with good balance in precision and recall. Under anomaly detection models, Isolation Forest and LOF performed quite differently when subjected to different resampling techniques. For example, Isolation Forest together with Random Undersampling produced the best performance in terms of using AUC (0.619) and recall (0.62) in the various anomaly detection models. However, those features did not provide any favorable precisions or F1-scores against what one could otherwise expect with this entirely method. Performance within LOF was limited, showing a bit of improvement from resampling, proving thus very sensitive to issues concerning data representation.

It showed much variation in performance across the model because of different resampling techniques. It was found that SMOTE and SMOTE-ENN performed quite consistently at improving fraud detection metrics because of addressing class imbalance and still further improving the data quality. On the other hand, while Random Undersampling increased recall much, it usually resulted in a very large data loss and hence affected precision and overall performance of the model quite badly. Non-SMOTE methods had unsuccessful biased models with the need to apply proper resampling techniques to deal with imbalanced datasets. As it can be concluded from the work, model-resampling matching is crucial in fraud detection. The most appropriate and viable among those evaluated is given by the Logistic Regression with SMOTE-ENN, which then becomes scalable and effective. Further research could investigate more advanced measurements of combination-based ensemble models for building hybrid models that continue improving fraud detection capabilities on highly imbalanced datasets.

Minimizing False Negative Rate (FNR) and False Positive Rate (FPR) is crucial in fraud detection so that the customers can enjoy a safe and effective fraud detection system. The denial of the threat from FNR is to indicate fraudulent transactions that remain undiscovered, which can lead to chargebacks; whereas FPR reflects the ratio of real buyers whose legitimate transactions are bent toward fraud detection. The values of FNR and FPR for Logistic Regression (SMOTE) and Isolation Forest (Non-SMOTE) are as follows.

Formulae

1. False Negative Rate (FNR):

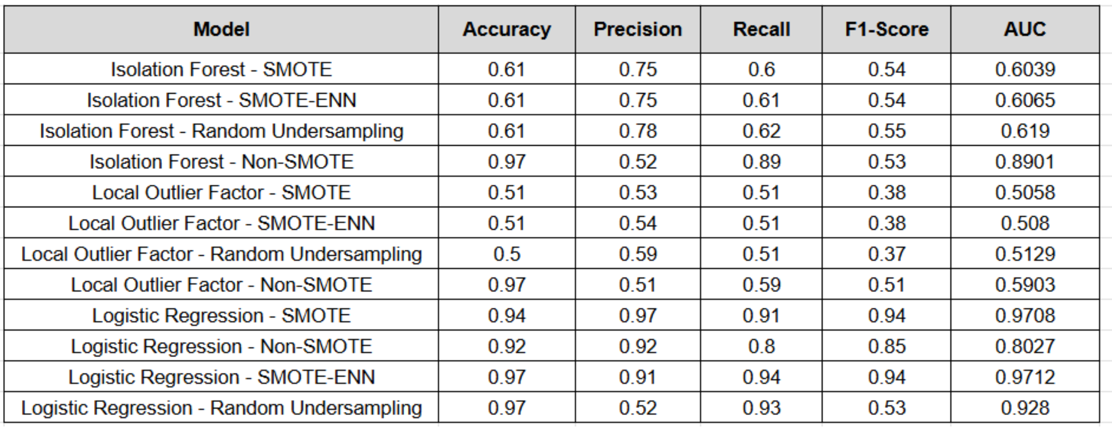
$$\mathrm{FNR} = \frac{\mathrm{FN}}{\mathrm{FN} + \mathrm{TP}}$$

This measures the proportion of undetected fraud cases (false negatives) out of all fraudulent transactions.

2. False Positive Rate (FPR):

$$\mathrm{FPR} = \frac{\mathrm{FP}}{\mathrm{FP} + \mathrm{TN}}$$

This indicates the proportion of legitimate transactions flagged as fraudulent.



Model	Accuracy	Precision	Recall	F1-Score	AUC
Isolation Forest - SMOTE	0.61	0.75	0.6	0.54	0.6039
Isolation Forest - SMOTE-ENN	0.61	0.75	0.61	0.54	0.6065
Isolation Forest - Random Undersampling	0.61	0.78	0.62	0.55	0.619
Isolation Forest - Non-SMOTE	0.97	0.52	0.89	0.53	0.8901
Local Outlier Factor - SMOTE	0.51	0.53	0.51	0.38	0.5058
Local Outlier Factor - SMOTE-ENN	0.51	0.54	0.51	0.38	0.508
Local Outlier Factor - Random Undersampling	0.5	0.59	0.51	0.37	0.5129
Local Outlier Factor - Non-SMOTE	0.97	0.51	0.59	0.51	0.5903
Logistic Regression - SMOTE	0.94	0.97	0.91	0.94	0.9708
Logistic Regression - Non-SMOTE	0.92	0.92	0.8	0.85	0.8027
Logistic Regression - SMOTE-ENN	0.97	0.91	0.94	0.94	0.9712
Logistic Regression - Random Undersampling	0.97	0.52	0.93	0.53	0.928

Figure 10: Model Evaluation

7 Conclusion and Future Work

This study evaluated three different models namely Isolation Forest, Local Outlier Factor (LOF), and Logistic Regression for class imbalance arising out of fraud detection and associated them with resampling techniques like SMOTE, SMOTE-ENN, and Random Undersampling. The outcome betokened how much well did rather than all others showed that Logistic Regression with SMOTE-ENN was the best concerning the model performance having the highest AUC (0.9712) and recall (0.94), thus proving precision among them and had merely superior performance for the identification of fraud transaction as the best for highly imbalanced datasets. Isolation Forest was also appreciable under Random Undersampling, where recall was pushed to 0.62, but it faced low on precision, therefore remained a cost in terms of recall against precision. LOF finally had very minor improvements after resampling techniques, pointing to its troubles in discontinuing fraud transactions, even when the data was adjusted. Cardinally, much of the out sample improvement models could be grounded upon resampling, especially by SMOTE and SMOTE-ENN, for addressing class imbalance and induce recall improvement. Not just detection, SMOTE-ENN improved the quality of data, while Random Undersampling had the positive effect of increasing the recall measure, which again took along a lot of data, leading to reduced precision. The present study stresses the need for appropriate resampling to sort the problems related to imbalanced datasets. Looking ahead, future research could focus on ensemble techniques merging possible model gains into a coherent one for high precision and recall. Hybrid models combining anomaly detection and classification approaches would be probably more robust, whereas advances in fraud detection could be achieved using deep learning models by automatically learning feature representation. Yet, designing novel hybrid resampling techniques for optimum oversampling and undersampling without degrading data quality would be very desirable. Inclusion of domain knowledge or the creation of specific features intended for fraud detection could result in even better accuracy. As a result, Logistic Regression with SMOTE-ENN seems to be the best approach tested until now, but the future innovation into machine learning techniques might come up with better solutions for fraud detection in highly imbalanced datasets.

References

Abdulghani, A.Q., Ucan, O.N., and Ali Alheeti, K.M., 2021. Credit card fraud detection system using machine learning algorithms and fuzzy membership. 2021 International Conference of Modern Trends in Information and Communication Technology Industry (MTICTI), Sana'a, Yemen, pp.1-6. doi: 10.1109/MTICTI53925.2021.9664789.

Alarfaj, F.K., Malik, I., Khan, H.U., Almusallam, N., Ramzan, M., and Ahmed, M., 2022. Credit card fraud detection using state-of-the-art machine learning and deep learning algorithms. IEEE Access, 10, pp.39700-39715. doi: 10.1109/ACCESS.2022.3166891.

Alamri, M., and Ykhlef, M., 2024. Hybrid undersampling and oversampling for handling imbalanced credit card data. IEEE Access, 12, pp.14050-14060. doi: 10.1109/ACCESS.2024.3357091.

Ghevariya, R., Desai, R., Bohara, M.H., and Garg, D., 2021. Credit card fraud detection using local outlier factor and isolation forest algorithms: A complete analysis. 2021 5th International Conference on Electronics, Communication and Aerospace Technology (ICECA), Coimbatore, India, pp.1679-1685. doi: 10.1109/ICECA52323.2021.9675971.

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. doi: 10.1109/ACCESS.2021.3134330.

Isangediok, M., and Gajamannage, K., 2022. Fraud detection using optimized machine learning tools under imbalance classes. 2022 IEEE International Conference on Big Data (Big Data), Osaka, Japan, pp.4275-4284. doi: 10.1109/BigData55660.2022.10020723.

Leevy, J.L., Khoshgoftaar, T.M., and Hancock, J., 2022. Evaluating performance metrics for credit card fraud classification. 2022 IEEE 34th International Conference on Tools with Artificial Intelligence (ICTAI), Macao, China, pp.1336-1341. doi: 10.1109/ICTAI56018.2022.00202.

Mienye, I.D., and Jere, N., 2024. Deep learning for credit card fraud detection: A review of algorithms, challenges, and solutions. IEEE Access, 12, pp.96893-96910. doi: 10.1109/ACCESS.2024.3426955.

Murkute, P., Dhule, C., Lipte, P., Agrawal, R., and Chavhan, N., 2023. Credit card fraud detection using machine learning techniques. 2023 First International Conference on Advances in Electrical, Electronics and Computational Intelligence (ICAEECI), Tiruchengode, India, pp.1-8. doi: 10.1109/ICAEECI58247.2023.10370832.

Prajapati, D., Tripathi, A., Mehta, J., Jhaveri, K., and Kelkar, V., 2021. Credit card fraud detection using machine learning. 2021 International Conference on Advances in Computing, Communication, and Control (ICAC3), Mumbai, India, pp.1-6. doi: 10.1109/ICAC353642.2021.9697227.

Sailusha, R., Gnaneswar, V., Ramesh, R., and Rao, G.R., 2020. Credit card fraud detection using machine learning. 2020 4th International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, India, pp.1264-1270. doi: 10.1109/ICICCS48265.2020.9121114.

Samant, S., Joshi, P., Jain, S., Bankar, S., and Ahuja, S., 2024. SMOTE-based credit card fraud detection for imbalanced data: Performance analysis. 2024 OPJU International Technology Conference (OTCON) on Smart Computing for Innovation and Advancement in Industry 4.0, Raigarh, India, pp.1-6. doi: 10.1109/OTCON60325.2024.10688312.

Singh, P., Singla, K., Piyush, P., and Chugh, B., 2024. Anomaly detection classifiers for detecting credit card fraudulent transactions. 2024 Fourth International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies (ICAECT), Bhilai, India, pp.1-6. doi: 10.1109/ICAECT60202.2024.10469194.

Varmedja, D., Karanovic, M., Sladojevic, S., Arsenovic, M., and Anderla, A., 2019. Credit card fraud detection - Machine learning methods. 2019 18th International Symposium INFOTEH-JAHORINA (INFOTEH), East Sarajevo, Bosnia and Herzegovina, pp.1-5. doi: 10.1109/INFOTEH.2019.8717766.

Xie, Z., and Huang, X., 2024. A credit card fraud detection method based on Mahalanobis distance hybrid sampling and random forest algorithm. IEEE Access, 12, pp.162788-162798. doi: 10.1109/ACCESS.2024.3421316.

Zadafiya, N., Karasariya, J., Kanani, P., and Nayak, A., 2022. Detecting credit card frauds using isolation forest and local outlier factor - Analytical insights. 2022 4th International Conference on Smart Systems and Inventive Technology (ICSSIT), Tirunelveli, India, pp.1588-1594. doi: 10.1109/ICSSIT53264.2022.9716541.