MERU UNIVERSITY OF SCIENCE AND TECHNOLOGY

DEPARTMENT OF COMPUTER SCIENCE

BACHELOR OF SCIENCE IN DATA SCIENCE

FRAUD DETECTION IN BANK USING RANDOM FOREST ALGORITHM FOR TRANSACTION RISK MITIGATION

CT204/106241/21: BRIAN OWINO ABAYO

A Research Project Submitted in Partial Fulfillment of the Requirements of the Bachelor of Science in Data Science of Meru University of Science and Technology

April, 2025

DECLARATION

This research proposal is my original work prepared with none other than the indicated sources and support and has not been presented elsewhere for a different or similar assignment.

Student Reg. No.	CT204/106241/21
Student Name	BRIAN OWINO ABAYO

DEDICATION

My family has been my biggest source of strength during this journey, and I dedicate this work to them for their unwavering support, encouragement, and faith in my abilities. This commitment is also extended to my friends and mentors, whose support and motivation have influenced both my academic and personal development.

Catalog

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1
INTRODUCTION

1.1 Background of study

Financial organizations face a significant problem with banking fraud which include unlawful acts involving the use of banking systems with the objective of gaining economic benefit. The dramatic shift toward digital banking applications means that fraud detection is now a core aspect of bank security. To minimize losses due to fraud, financial institutions must implement highly reliable detection methods, as the Association of Certified Fraud Examiners (ACFE) reports billions of dollars lost annually by this industry alone (des Nations Unies 2022) .

Several fraudulent behaviors intended to take advantage of people, and the financial system are included under banking fraud. One well-known technique is account takeover, in which malicious parties utilize phishing, data breaches, or credential stuffing to take control of a genuine user's account. Once they have access, these fraudsters can conduct purchases, transfers, or actions that could cause significant harm to the account holder's finances. In a similar vein, Card Not Present (CNP) Fraud happens when credit card information is stolen and used for purchases without the actual card being present. This kind of fraud is prevalent in online transactions, where security protocols may be laxer. It results in unapproved transactions and financial losses that affect cardholders and banks equally. Identity theft is a serious criminal activity in which offenders exploit personally identifiable information that has been stolen (Kovach & Ruggiero, 2011).

The spectrum of fraud includes check fraud, which is the use of checks without authorization due to forged signatures, manipulated amounts, or stolen checks. This issue persists even in the face of declining check usage. Unauthorized access to accounts for the purpose of transferring or withdrawing money is known as fraudulent transfers and withdrawals, and is frequently the result of hacking or security flaws. Synthetic identity fraud is the practice of fabricating false identities to carry out fraudulent acts using genuine and fake information. Because these identities resemble real profiles, they can be difficult to detect. Finally, Ponzi schemes and other fake or phony ventures guarantee large returns on fictitious investments. False claims made by scammers entice investors, and when the scheme fails, they use the money from new investors to pay returns to previous ones, resulting in large financial losses (Kovach & Ruggiero, 2011).

Legacy fraud detection systems in banking are rule-based, using predefined rules to identify potentially fraudulent activity based on transaction patterns (such as types of products or services purchased), amounts, and locations. However, these systems often struggle to keep up with the nuanced and ever-changing forms of fraud that characterize today's commercial landscape. Due to the increasing complexity of fraud schemes, financial institutions are increasingly relying on advanced data-driven methodologies, such as machine learning models, to enhance their capabilities against fraudulent behaviors (Bhattacharyya and Kulkarni 2024).

Banking fraud detection has become a prominent topic among machine learning practices, featuring both supervised and unsupervised techniques. Supervised learning approaches, such as logistic regression, decision trees, and neural networks, are trained on historical labeled data to predict whether transactions belong to a fraudulent or legitimate dataset. However, these methods are limited by their reliance on extensive annotated datasets（Lidwall and Ole Paul Malmus 2024）. Unsupervised learning, on the other hand, can help reveal novel fraud patterns without prior labeling by detecting deviations from regular and rare transaction behaviors (Bello et al. 2022).

Challenges remain in making banking fraud detection models efficient and reliable, including real-time processing for high-volume transactions, reducing false positives while preserving accuracy, and protecting sensitive financial data in terms of privacy. Effective fraud detection requires responsive machine learning and anomaly-based models that can adapt quickly as criminal methods evolve. Additionally, integrating fraud detection systems into bank operations without adversely affecting customer experience presents its own complication（Shome et al. 2023）.

In the financial sector, there is an increasing adoption of machine learning-powered fraud detection systems that combine both supervised and unsupervised approaches. For example, anomaly detection models analyze transaction data to identify outliers from a user’s regular purchasing habits, aiding in the detection of possible fraud. Hybrid models that employ various detection methods simultaneously are becoming increasingly popular as they enable detection of a broader range of fraud types（Bello et al. 2022）.

Recent advances include deep learning models such as Convolutional Neural Networks (CNN) and Recurrent Neural Networks（RNN）, which capture complex transaction patterns with higher-order temporal dependencies. Additionally, research into graphbased methods involves analyzing relationships between different entities participating in transactions (Bello et al. 2022). These new models enhance Fraud Detection Systems by improving precision and speed, thus reducing the likelihood of financial loss while ensuring security for digital banking platforms.

Even with these advancements, there remains a significant research gap in banking fraud detection. The majority of current models demand a significant amount of processing power and may not be easily scalable to handle the vast amounts of transactional data generated by modern banking systems. Additionally, the high rate of false positives remains a serious issue, potentially causing disruptions for legitimate customers. Further research is needed to develop a model that is more scalable, adaptive, and interpretable, providing actionable insights with minimal human intervention. As digital banking proliferates, enhancing fraud detection mechanisms will be crucial in protecting financial assets and fostering consumer trust in digital banking platforms（Ahmed and Alabi 2024).

1.2 Motivation for study

The complicated nature and scope of current fraud schemes are too great for traditional rule-based fraud detection techniques to handle. The effectiveness of previous systems has decreased due to the growing use of sophisticated techniques including account takeovers, phishing, and synthetic identity fraud. Due to this, there has been an increase in false positives, which result in legal transactions being wrongly reported as fraudulent, inconveniencing customers and creating operational inefficiencies in financial institutions.

Furthermore, advances in machine learning offer a chance to lower false positive rates and greatly increase the accuracy of fraud detection. Research has indicated that machine learning models, especially those that employ unsupervised and hybrid techniques are more adept at identifying new fraud trends without the need for a large amount of historical data. It is more important than ever to put accurate fraud detection models into place since digital transactions are expanding at a rate never seen before.

The need to solve these issues and investigate how machine learning techniques might improve fraud detection in the banking industry, offering more precise and rapid identification of fraudulent activity and safeguarding financial institutions and their clients, is what drives this research.

1.3 The statement of the Problem

Banking fraud is a serious concern to financial organizations around the world, as it may lead to large losses in revenue and erode consumer confidence. Even with the use of conventional fraud detection systems, which rely on rule-based strategies and historical data analysis, these techniques are becoming less and less effective at catching modern scammers using their more cunning methods. The dynamic character of fraudulent activities, in conjunction with elevated false positive rates and restricted scalability of current systems, underscores the pressing want for enhanced detection procedures. The general security of digital banking networks may be jeopardized by current models' inability to adequately mitigate financial risks and their inability to adjust to new fraud trends.

An improved fraud detection model accuracy is essential to addressing these issues. This calls for the use of cutting-edge machine learning strategies that reduce false positives and enhance the ability to detect fraudulent activity. Enhancing detection accuracy boosts operational effectiveness and customer trust in addition to helping to lower financial losses. Financial organizations may offer a more secure and dependable banking experience for their consumers and better guard against new fraud threats by concentrating on the development and evaluation of machine learning model that excel in accuracy.

1.4 Research objectives

1.4.1 General objectives

To develop a Random Forest model that can accurately determine if a transaction is fraudulent or not.

1.4.2 Specific objectives

The objectives of this research project are:

i. To determine if transaction type and period of transaction are crucial in detecting fraud.

ii. To develop a Random Forest model to detect fraudulent transaction.

iii. To evaluate the performance of the developed model using various performance indicators such as precision, recall, F1-Score, ROC and AUC.

iv. To deploy the model in an interactive web application to test the application in another environment.

1.5 Significance of the study

This paper addresses important issues that financial institutions encounter, which makes a substantial contribution to the field of fraud detection in digital banking. It seeks to safeguard customers and organizations from fraudulent activity by improving fraud detection systems, promoting confidence in digital banking, and establishing a safer online community. By examining the efficacy of machine learning techniques more especially, supervised and unsupervised learning methods in detecting and reducing fraud, the study contributes to the body of existing work.

From a practical standpoint, the results will help financial institutions better respond to new fraud risks by helping them create scalable and accurate fraud detection models, increasing operational efficiency, and lowering false positives. Furthermore, this research will furnish policymakers with evidence-based suggestions that will steer the use of sophisticated fraud detection technology and promoting consumer protection and financial security.

1.6 Scope of the study

The use of machine learning techniques for fraud detection in the banking sector will be the main focus of this study.The use of machine learning techniques for fraud detection in the banking sector will be the main focus of this study. In order to uncover fraudulent behaviors such account takeovers, identity theft, and card-not-present fraud, the research will especially target financial institutions operating in Kenya by analyzing transaction data.

1.7 Assumptions in the study

In conducting this study, the following assumptions are made:

1. The accuracy of the transaction data supplied for analysis is presumed and representative of typical banking operations in the banking sector.
2. It is assumed that machine learning models can effectively learn from historical data to identify patterns indicative of fraudulent behavior.
3. It is assumed that the findings from this study will be applicable to other regions facing similar challenges in banking fraud detection, although the focus remains on Kenya.

1.8 Limitations of study

One significant limitation is that the findings of this study could not be applicable to the banking sector in Kenya. The unique consumer habits, fraud tendencies, and regulatory frameworks found in Kenya may not be the same as those found in other parts of the world, which could have an impact on how well the machine learning models perform.

CHAPTER 2
LITERATURE REVIEW

2.1 Introduction

The realm of banking industry has changed significantly in recent times, largely due to technological breakthroughs that enhance accessibility and convenience. This quick expansion has also been accompanied by a rise in fraud, which seriously jeopardizes financial institutions. This chapter offers a comprehensive review of the literature on the detection of fraud in banking, with a focus on the various machine learning techniques, their applications, and the gaps in previous studies.

2.2 Innovative Machine Learning Approaches in Fraud Detection

Several novel models that are more accurate and efficient than conventional techniques have been developed as a result of the use of machine learning to fraud detection. Alfaiz and Fati's AllKNN-CatBoost model is one noteworthy development（2022）. It has been demonstrated that this model greatly increases fraud detection rates by fusing the KNearest Neighbors (KNN) algorithm with CatBoost ensemble techniques. The model outperformed traditional models in identifying fraud, achieving an AUC of 97.94%, Recall of 95.91%, and F1-Score of 87.40% by combining multiple machine learning techniques.

A deep convolutional neural network (CNN) created especially for real-time fraud detection was created by Chen and Lai in 2021. Their program identified fraudulent transactions with 99.92% accuracy, outperforming conventional detection systems. In digital banking environments, where fraudsters are constantly innovating, the CNN is especially effective due to its capacity to learn intricate patterns from vast datasets and adjust to changing fraud tactics. These developments highlight how effective deep learning methods are at enhancing the identification of financial transaction fraud.

2.3 Applications Across Banking Domains.

Machine learning’s application in fraud detection spans multiple areas within the banking sector, demonstrating its versatility and effectiveness. **Chen and Lai（2021）** and **Alfaiz and Fati (2022)** focused on **credit card fraud detection**, where deep learning and ensemble models have shown significant improvements in detection accuracy. Credit card fraud detection systems benefit from the ability of these models to analyze transaction data in real time, providing early detection of suspicious activities and preventing financial losses.

Hashemi et al.（2022）investigated the use of Random Forest and Gradient Boosting models to detect fraudulent transactions in the field of mobile banking, where fraud risks are also rising as a result of the widespread usage of mobile payment systems. These models can be modified to track user behavior and spot oddities that might point to fraud. The Light Gradient Boosting Machine (LGBM), developed by Taha and Malebary (2020), is designed to identify fraud in payment systems in real time. According to their research, LGBM is very successful in stopping fraudulent transactions in real-time payment systems because it greatly improves the accuracy of fraud detection.

2.4 Enhancing Fraud Detection with Holistic Strategies.

Adopting a more comprehensive strategy by combining machine learning with other tactics is essential to further improving the efficacy of fraud detection algorithms. The significance of integrating risk management frameworks with machine learning models was emphasized by Guo et al.（2024）. Banks may now more proactively evaluate fraud risks and modify their tactics to lessen possible dangers thanks to this connection. Banks can develop more resilient systems that can identify and stop fraud early on by fusing machine learning with risk management

Furthermore, the importance of data engineering in enhancing machine learning model performance was highlighted by Baesens et al.（2021）. Optimizing the accuracy of fraud detection systems requires proper feature engineering, data processing, and cleaning. Since the quality of input data directly influences the quality of the predictions these models make, high-quality data guarantees that machine learning algorithms can detect fraud. Thus, data engineering is essential to creating more trustworthy fraud detection systems.

2.5 Challenges and Limitations in Implementing Machine Learning Models.

Even though machine learning has many benefits, there are a few obstacles to overcome before it can be used in fraud detection systems. The problem of false positives is among the most significant obstacles. These happen when valid transactions are reported as fraudulent, which results in inefficient operations and unhappy customers. False positives are still a major problem in many fraud detection systems, and more work is required to lower these errors without sacrificing detection accuracy, according to Shome et al.（2023）.

The processing of enormous volumes of transactional data in real time presents another difficulty. Millions of transactions are handled by financial systems every minute, thus it is essential that fraud detection algorithms process this data rapidly and effectively. According to Uddin & Uddin (2022), standard models frequently have trouble handling such big datasets, which can cause delays in the fraud detection process. Concerns about data privacy are also raised by the utilization of private client information. Banks are required to make sure that fraud detection systems maintain high accuracy levels while adhering to stringent data privacy rules.

2.6 Future Directions and Emerging Trends.

Emerging methods and technology are anticipated to substantially improve machine learning models' capabilities as fraud detection continues to advance. Convolutional neural networks (CNNs) and recurrent neural networks (RNNs), two AI-driven models, are becoming more popular because of their capacity to identify intricate fraud patterns that change over time. These models are very flexible to new fraud strategies since they learn from enormous volumes of transaction data. Furthermore, the use of graph-based methods for fraud detection is growing in popularity. These methods examine the connections between various parties to transactions, offering valuable information about fraud rings and other intricate fraudulent schemes. According to Bello et al. (2022), these methods provide a more thorough understanding of fraud activities, enabling more thorough fraud detection.

Furthermore, a more thorough method of fraud detection is provided by combining machine learning with other cutting-edge technologies like big data analytics and the Internet of Things. Faster detection of fraudulent activity may result from the combination of real-time data analysis capabilities and IoT-enabled sensors that track user behavior and financial transactions. The integration of several technologies will be essential to guaranteeing precise and prompt fraud protection as fraud detection grows increasingly complicated.

2.7 Research Gaps.

Even though machine learning for fraud detection has advanced, there are still a number of research gaps that must be filled in order to increase the models' performance and applicability in real-world scenarios.

The problem of data imbalance, when fraudulent transactions are much less common than valid ones, is one of the biggest obstacles to fraud detection. Machine learning models may ignore fraudulent activity or produce an excessive number of false positives as a result of this imbalance, which frequently results in model bias. According to Uddin & Uddin (2022), this problem still affects a large number of fraud detection systems in use today. In order to develop more precise and trustworthy models for fraud detection, future research should concentrate on enhancing strategies for balancing datasets, such as oversampling, undersampling, or employing synthetic data generating techniques.

The possible influence of climate change on fraud trends is a growing issue, even though it is not usually taken into account in conventional fraud detection research. According to Bello et al. (2022), socioeconomic changes, such as those brought on by climate change, may have an impact on fraud trends and criminal strategies. Research on the potential effects of global shifts on fraud detection systems, including migration, economic instability, and new regulatory environments brought on by climate disasters, is needed. In a world that is changing quickly, it will be essential to comprehend how fraud detection models can adjust to these changes in order to ensure their long-term efficacy.

There is a gap in the integration of various technologies, despite the fact that machine learning approaches have demonstrated considerable promise in fraud detection. A more thorough method of fraud detection would be possible by combining machine learning models with other cutting-edge technologies like artificial intelligence (AI), the internet of things (IoT), and big data analytics. The advantages of combining machine learning with risk management frameworks were emphasized by Guo et al. (2024), but more investigation is required to determine the best ways to combine these technologies. By strengthening the resilience of fraud detection systems, a multidisciplinary approach may make it possible to identify fraudulent activity more quickly and accurately.

2.8 Summary

The literature currently available on the use of machine learning methods for fraud detection in the banking industry has been examined in this chapter. It has emphasized the advancements in machine learning models that greatly enhance fraud detection capabilities, such as ensemble approaches, deep learning, and hybrid models. In order to demonstrate how these models improve the accuracy of fraud detection, the evaluation also covered the use of machine learning in a variety of financial sectors, including credit card transactions, mobile banking, and real-time payment systems.

In order to enhance model performance, the chapter also looked at how machine learning may be combined with more general fraud detection techniques like risk management frameworks and data engineering techniques. Although machine learning has a lot of potential, issues include false positives, actual

CHAPTER 3
RESEARCH METHODOLOGY

3.1 INTRODUCTION

This chapter provided an in-depth explanation of the approach that was used to create a machine learning classification algorithm-based fraud detection model. The research design, dataset specifics, data preparation, analysis techniques, model-building procedures, and ethical considerations are all important components.

3.2 Research Design

To assess machine learning classification algorithms' ability to identify fraudulent banking transactions, the study used a descriptive research approach. To improve the accuracy of fraud detection, this architecture allowed for investigation of transaction features and patterns.

3.3 Dataset

https://www.kaggle.com/datasets/chitwanmanchanda/fraudulent-transactions-data

3.3.1 Dataset Overview

This project used a Kaggle dataset of credit card transactions that was last updated by Chitwan Manchanda. Because of its recent changes, this dataset will be chosen to ensure that new fraud tendencies that might not be seen in older datasets are included. In contrast to anonymous datasets, which may make it difficult to grasp parameters, this dataset will make it possible to assess feature relevance in fraud detection more clearly.

3.3.2 Dataset Size and Variables

The dataset used in this study includes 500,000 transaction records, with each entry capturing essential aspects of individual credit card transactions. Key variables encompass details like the customer (nameOrig, oldbalanceOrg, newbalanceOrig), transaction type (type), transaction amount (amount), and transaction time (step). The recipient's information (nameDest, oldbalanceDest, and newbalanceDest) is also included. While isFlaggedFraud marks transactions over 200,000 as possibly unlawful, the target variable, isFraud, specifies whether a transaction is fraudulent (1) or not (0). In order to spot fraud trends and create a fraud detection model, these variables offer a thorough understanding of transaction behavior.

3.3.3 Dataset Justification

The dataset selected for this study is very suitable for predicting fraudulent transactions where the variables provide essential insights into transaction patterns, which are crucial for identifying fraud. Additionally, the isFraud label directly indicates fraudulent transactions, while the isFlaggedFraud feature flags high-value transactions as potentially illegal, further aiding in detection. The large size of the dataset ensures enough data for training and validating robust models, offering diverse transaction scenarios that enhance the model's ability to generalize.

3.4 Data Collection Methods

3.4.1 Data Sources

Data will be obtained from Kaggle which is a public repository, focused on credit card fraud detection, and no primary data collection will be conducted.

3.4.2 Data Collection Techniques

The data will be obtained through direct download from the Kaggle repository, with preprocessing focusing on preparing the dataset for analysis and model training.

3.5 Data Preparation

3.5.1 Data Cleaning

Data cleaning will ensure that duplicates, errors, and formats are delt with hence improving data accuracy and consistency (Han, Kamber, & Pei, 2011).

3.5.2 Handling Missing Values

To avoid potential biases, missing data points will be addressed using imputation techniques (Little & Rubin, 2014).

3.5.3 Data Transformation

'Type' and other categorical variables will be converted into numerical values using a label encoder, where each category is mapped to a distinct number. This conversion will maintain the original data's structure while guaranteeing interoperability with machine learning algorithms.

3.6 Data Analysis Techniques

3.6.1 Statistical Analysis

Descriptive statistics will be used to understand the distribution and properties of the dataset.

3.6.2 Machine Learning Algorithms

Classification algorithm which is Random Forest will be tested for its effectiveness in fraud detection (Goodfellow, Bengio, & Courville, 2016).

3.6.3 Handling Imbalanced Data

To address the dataset's class imbalance, downsampling technique will be used to improve model performance.

3.6.4 Tools and Software

Python libraries such as pandas, scikit-learn and Flask framework will be used for data analysis and model development.

3.7 Model Building

3.7.1 Training and Testing Phases

The dataset will be split into training and testing sets to validate model accuracy.

3.7.2 Evaluation Metrics

Evaluation metrics will include accuracy, precision, recall, F1-score, and ROC-AUC, providing a correct measure of model performance (Fawcett, 2006).

3.7.3 Deployment

The Flask framework will be used in the research to develop a web application that is both lightweight and adaptable. The learned fraud detection algorithm will be integrated using Flask, enabling smooth user interaction and real-time predictions. This framework ensures scalability, ease of integration, and system maintenance in a production setting by offering the tools required to install the model effectively.

3.8 Ethical Considerations

3.8.1 Data Privacy and Security

Maintaining data privacy and security will be a primary concern, ensuring that data remains protected throughout the research process according to data protection and security act.

3.8.2 Ethical Implications

In line with the GDPR framework, particularly Article 5(1)(a) on fairness and transparency, and Article 22 concerning automated decision-making, this research incorporates ethical considerations aimed at identifying and mitigating potential biases, thereby promoting fairness in model predictions.

3.9 Limitations

3.9.1 Potential Biases

The study will acknowledge potential biases in data sources and machine learning models, impacting the generalizability of results.

3.9.2 Data and Methodology Constraints

Limitations in dataset quality and model scalability will be recognized as potential constraints affecting the applicability of the fraud detection system.

3.10 Summary

This chapter outlines the methodology for developing a robust fraud detection model. With clear justification for the dataset choice, detailed preparation processes, and a commitment to ethical standards, this methodology is designed to achieve the study’s goals and contribute to advancements in fraud detection.

CHAPTER 4
RESULTS AND DISCUSSION

In this research chapter, Python libraries such as NumPy, Pandas, Matplotlib, and Scikit-learn were imported to support data analysis. The dataset underwent preprocessing, including outlier removal. Feature selection followed, aided by exploratory data analysis. With transaction parameters and transaction labels analyzed, Random Forest Classifier was trained and evaluated. The model achieved a high accuracy of 95%. Finally, deployment occurred via Flask, facilitating user interaction with the model through a structured directory. This chapter encapsulated a practical journey from data preparation to model deployment, addressing fraud detection challenges with machine learning techniques.

4.1 Importing Libraries and Loading Dataset

This research imported libraries in Python that served different purposes. The used libraries include:

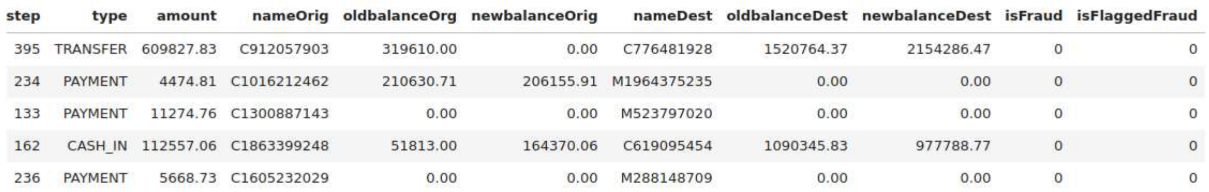
NumPy: Supported the large, multi-dimensional arrays and matrices, along with a collection of mathematical functions.

Pandas: Provided data manipulation and analysis tools.

Matplotlib: Was used to create various types of visualizations, including line plots, scatter plots and histograms.

Scikit-learn: Provided a wide range of algorithms and tools for analysis where it offered support for task such as classification.

Figure 1: Loaded dataset

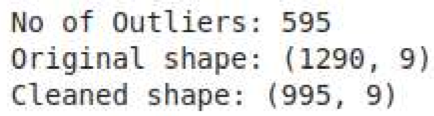


step	type	amount	nameOrig	oldbalanceOrg	newbalanceOrig	nameDest	oldbalanceDest	newbalanceDest	isFraud	isFlaggedFraud
395	TRANSFER	609827.83	C912057903	319610.00	0.00	C776481928	1520764.37	2154286.47	0	0
234	PAYMENT	4474.81	C1016212462	210630.71	206155.91	M1964375235	0.00	0.00	0	0
133	PAYMENT	11274.76	C1300887143	0.00	0.00	M523797020	0.00	0.00	0	0
162	CASH_IN	112557.06	C1863399248	51813.00	164370.06	C619095454	1090345.83	977788.77	0	0
236	PAYMENT	5668.73	C1605232029	0.00	0.00	M288148709	0.00	0.00	0	0

The dataset comprised of 500,000 transactions, each described by 11 features as shown in the above snippet.

4.2 Data Preprocessing

This research loaded the dataset and performed several data preprocessing steps, including removing outliers.



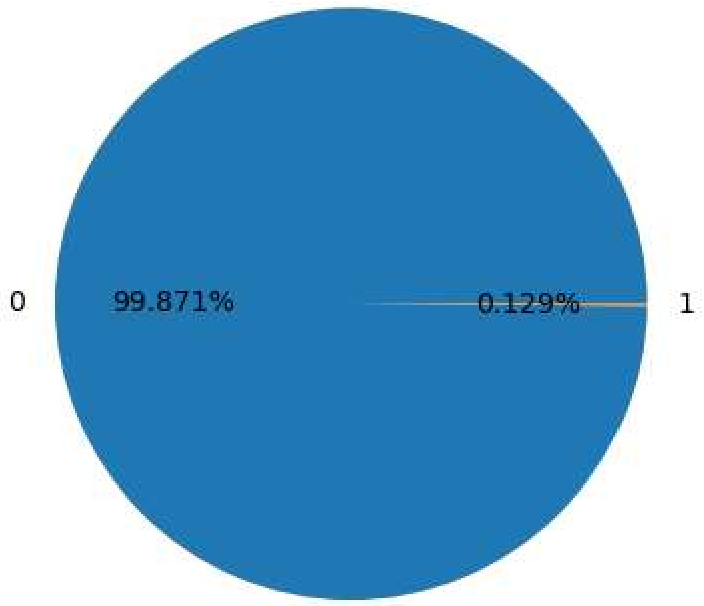
```
No of Outliers: 595
Original shape: (1290, 9)
Cleaned shape: (995, 9)
```

During data preprocessing, 595 outliers were identified across the numeric columns of the original balanced dataset, which initially had 1,290 rows and 9 columns. After filtering out these outliers using the IQR method, the cleaned dataset contains 995 rows and retains the same 9 columns. This reduction in rows demonstrates that approximately 295 rows were removed due to containing outlier values, resulting in a dataset with improved data quality and reduced influence from extreme values, making it more suitable for reliable analysis or model training.

4.3 Exploratory Data Analysis (EDA)

To build an accurate machine learning model, this research performed exploratory data analysis to gain insights and select the most important features from the transaction dataset as shown in below snippets.

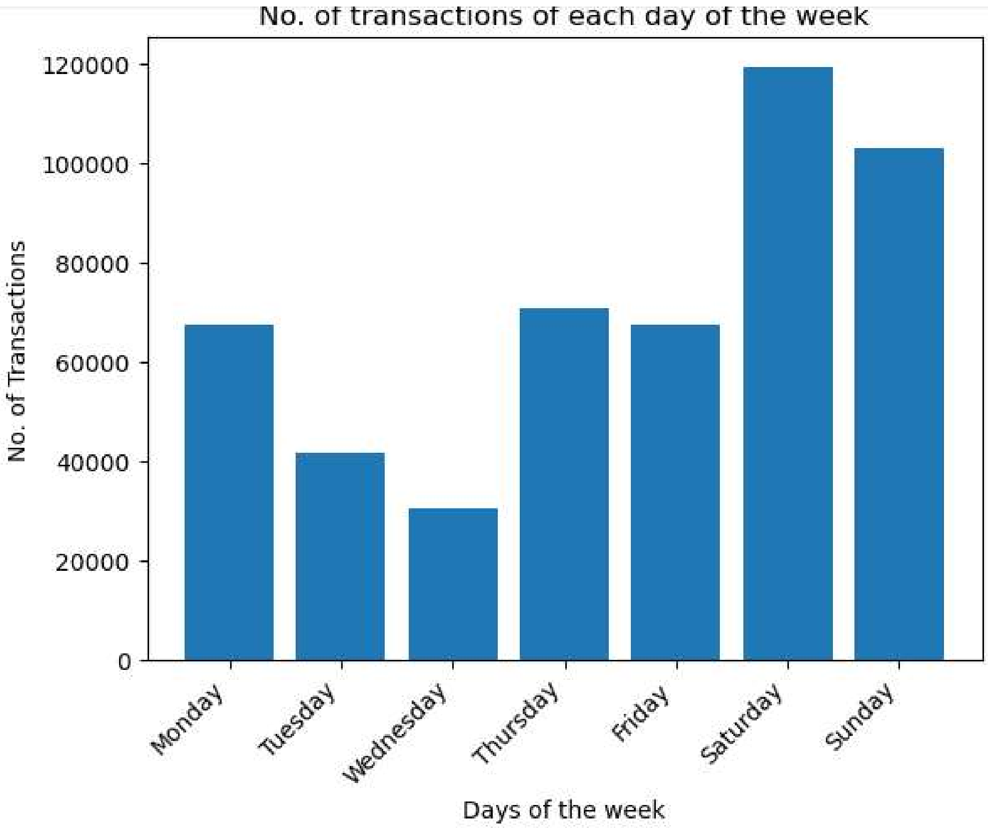
Figure 2: Class Distribution



The pie chart visually confirmed a substantial class imbalance in the dataset. Specifically, 99.871% of transactions are non-fraudulent (labeled as 0), while only 0.129% are fraudulent (labeled as 1).

The high degree of class imbalance suggested that machine learning model might be biased towards the majority class (non-fraudulent) and perform poorly in detecting fraudulent transactions.

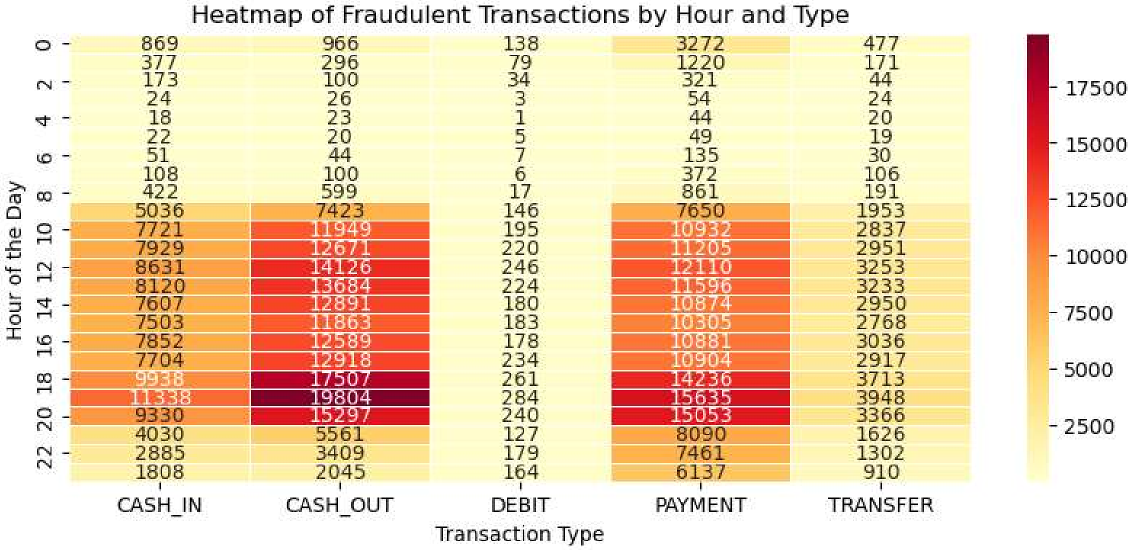
Figure 3: Graph showing number of transactions of each day of the week.



Sunday stands out as the day with the highest transaction volume. This could imply a higher risk of fraudulent activities due to the increased number of transactions. Fraud detection systems should be particularly vigilant on this day.

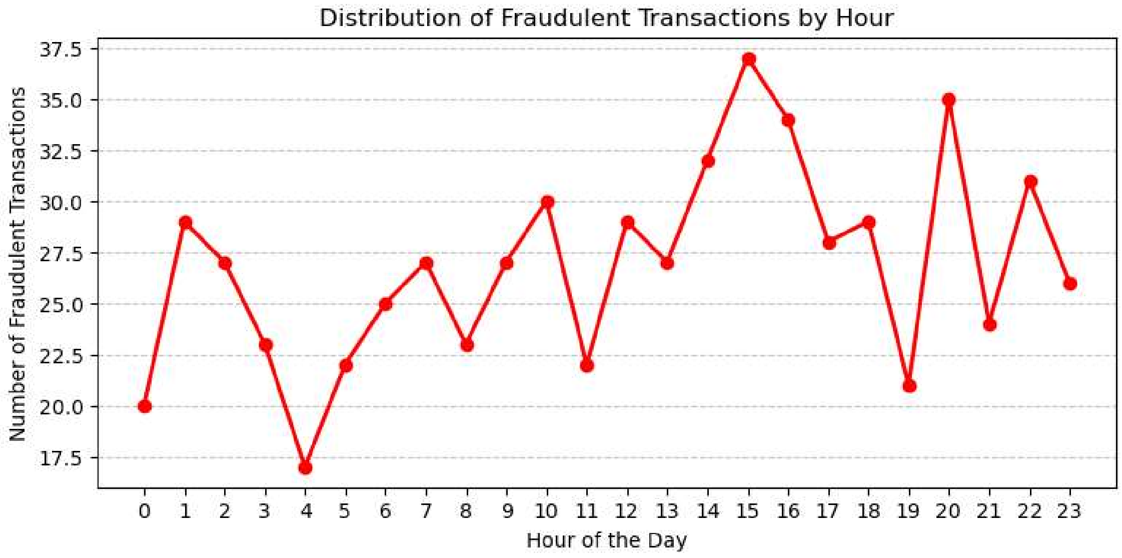
Monday and other weekdays have lower transaction volumes compared to Sunday. This might suggest a lower risk of fraud on these days, but consistent monitoring is still essential as fraudsters might exploit less busy days.

Figure 4: Heatmap of Transaction by hour and type.



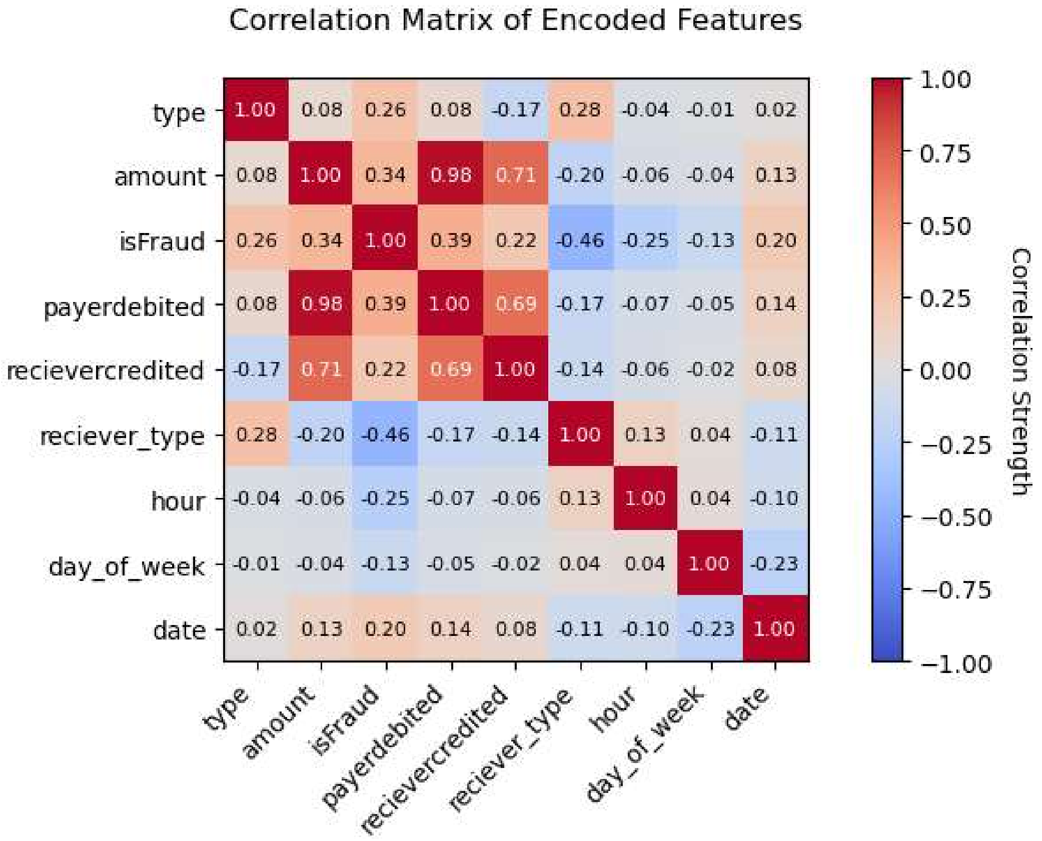
The analysis revealed that **CASH_OUT and TRANSFER** transactions had the highest frequency of fraudulent activities, with significantly higher occurrences compared to other categories. **PAYMENT and CASH_IN** also exhibited notable fraudulent activity, though at a lower rate than CASH_OUT and TRANSFER, while **DEBIT** transactions recorded the lowest fraud frequency. Additionally, fraudulent transactions peaked during midday and early afternoon (**hours 10 to 15**), with activity rising from hour 9, reaching its highest point around hour 13, and then gradually declining. In contrast, late-night and early-morning hours (**0 to 8**) experienced relatively fewer fraudulent incidents.

Figure 5: Graph showing Distribution of Transactions by hour.



The graph shows the number of fraudulent transactions occurring at each hour of the day where fraudulent activities are not evenly distributed throughout the day; there are noticeable peaks and troughs.

Figure 6: Graph showing feature correlation.

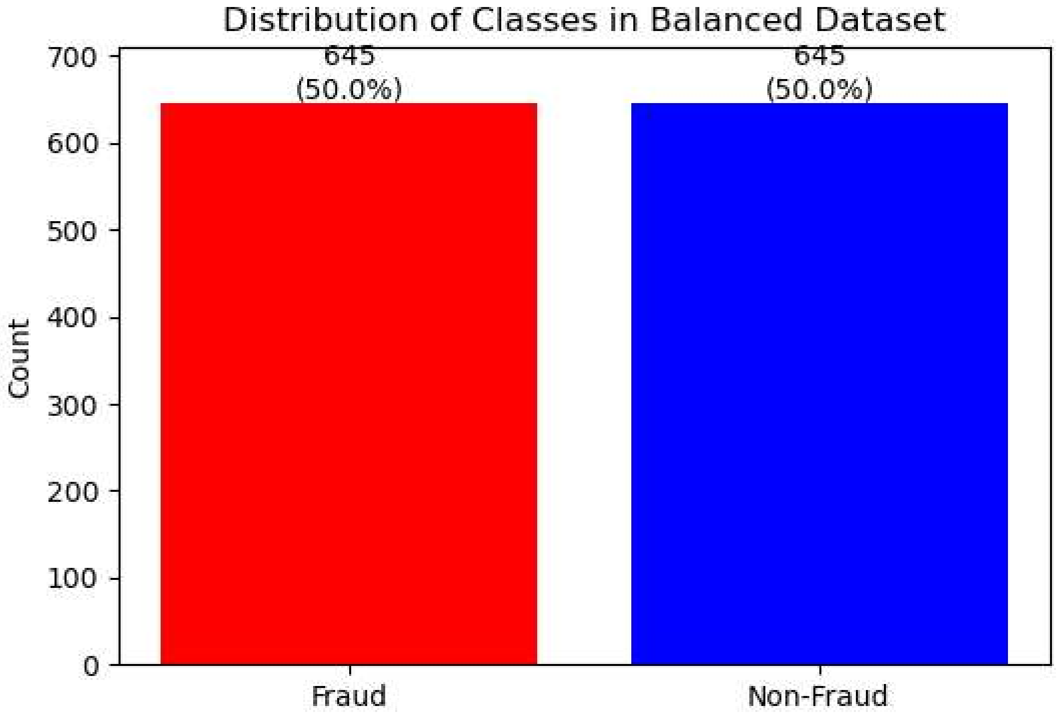


The correlation analysis confirms that **transaction type** and **period of transaction** play meaningful but secondary roles in fraud detection compared to financial features. While payerdebited (r=0.39) and amount (r=0.34) emerged as the strongest predictors, **transaction type** (type, r=0.26) demonstrated clear fraud concentration in specific categories (e.g., TRANSFER/CASH_OUT), validating its importance. Temporal features like hour (r=-0.25) and date (r=0.20) showed weaker correlations, thus period does not significantly affect fraud detection.

4.4 Model Training

Balancing the Dataset

Figure 7: Graph showing distribution of classes after balancing.

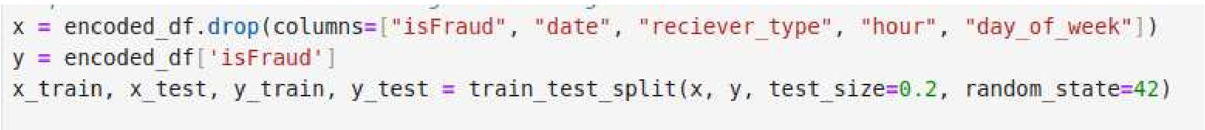


A number of methods, including SMOTE, oversampling and undersampling, were assessed in order to rectify the class imbalance in the original dataset. However, the reliability of the model was compromised by these techniques, which produced unacceptable false positive rates. As seen by the bar graph, downsampling was the best approach, effectively balancing the dataset with an equal proportion of fraudulent and non-fraudulent transactions. Despite reducing the overall amount of the dataset, this method enhanced the model's capacity to identify fraud and successfully reduced bias against the majority class (non-fraudulent cases). Higher precision and fewer false positives resulted from the balanced training data's increased sensitivity to minority-class patterns.

Splitting dataset

The below train_test_split library was used for Splitting the dataset. It splits the dataset into training and testing sets, ensuring a 20% test size and 80% train size.

Figure 8: Splitting the dataset for model training.

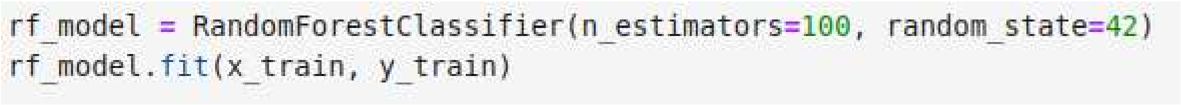


```
x = encoded_df.drop(columns=["isFraud", "date", "reciever_type", "hour", "day_of_week"])
y = encoded_df['isFraud']
x_train, x_test, y_train, y_test = train_test_split(x, y, test_size=0.2, random_state=42)
```

Training

This research trained the model using algorithm which is Random Forest Classifier based on the selected features from the test dataset. The number of estimators were set to be 100 and 42 as random state.

Figure 9: Training Random Forest Classifier

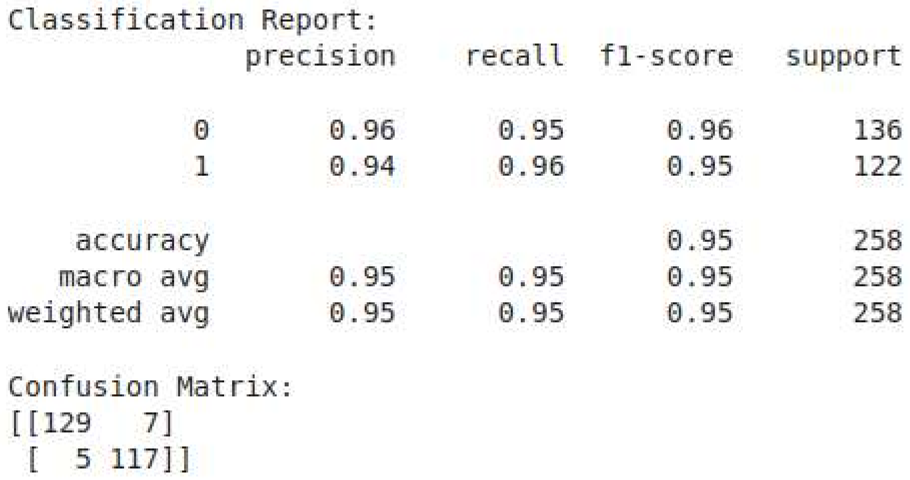


```
rf_model = RandomForestClassifier(n_estimators=100, random_state=42)
rf_model.fit(x_train, y_train)
```

4.5 Evaluation

Classification report and Confusion matrix

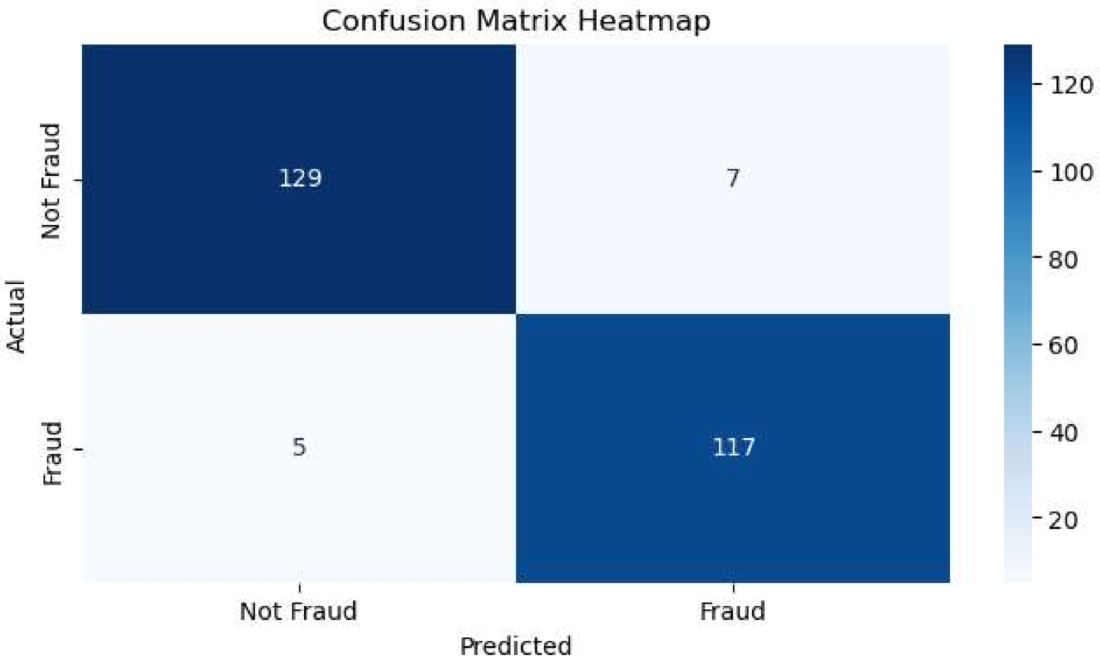
Figure 10: Classification Report



```
Classification Report:
              precision    recall  f1-score   support

           0       0.96      0.95      0.96       136
           1       0.94      0.96      0.95       122

    accuracy                           0.95       258
   macro avg       0.95      0.95      0.95       258
weighted avg       0.95      0.95      0.95       258

Confusion Matrix:
[[129   7]
 [  5 117]]
```

Confusion Matrix

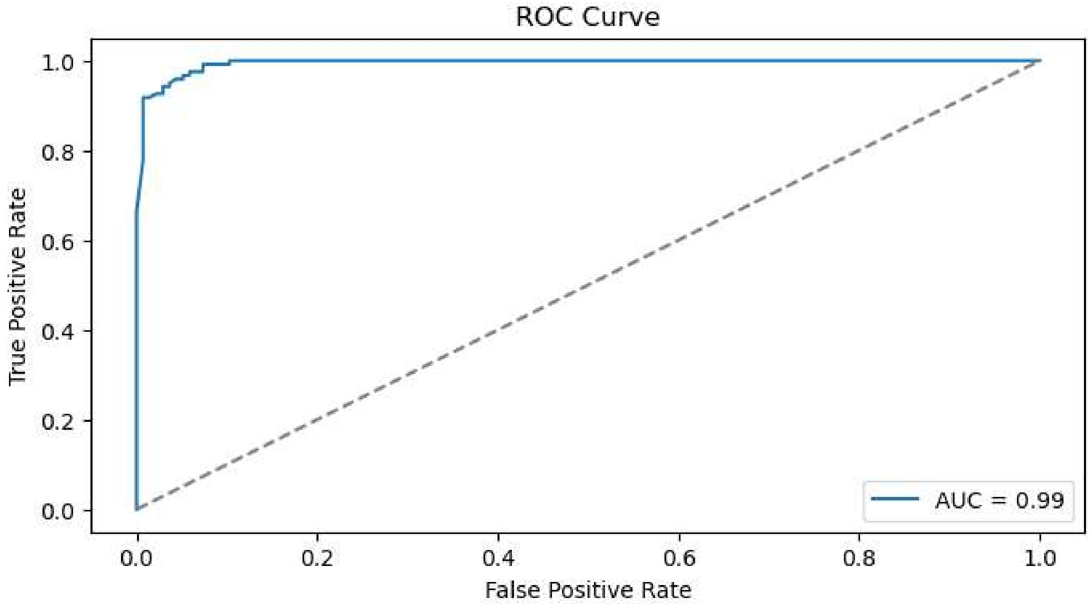
Figure 11: Confusion Matrix



With a 95% overall accuracy, the classification report and confusion matrix show excellent model performance. Class 1 has 94% precision and 96% recall, while class 0 has 96% precision and 95% recall. Both classes have good F1-scores (0.96 and 0.95, respectively), which indicates that precision and recall are balanced. The model's ability to differentiate between the two classes is further supported by the confusion matrix, which displays 129 true negatives, 117 true positives, 7 false positives, and 5 false negatives. The precision, recall, and F1-score weighted averages and macro averages are all 95%, indicating consistent performance throughout the dataset.

ROC Curver

Figure 12: Area Under Curve



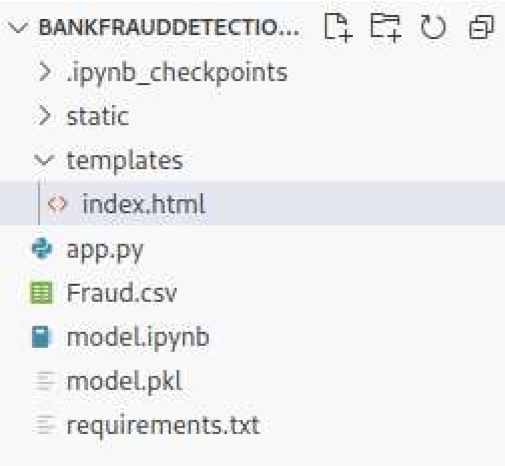
With an Area Under the Curve (AUC) of 0.99, the ROC curve displays exceptional model performance and nearly flawless discrimination between the two classes. As demonstrated by the classification report and confusion matrix, the model's efficacy is further validated by the high AUC, which indicates that it strikes a solid balance between true positive rate (sensitivity) and false positive rate (1-specificity). The model's dependability for binary classification tasks is strengthened by this almost optimal AUC.

4.6 Model Deployment

This research involved deploying a machine learning model with Flask. The structure included: index.html for UI placed inside templates folder, model.pkl for serialized model, app.py for routes and logic, model.py for training code, requirements.txt and Fraud.csv dataset used for training model.

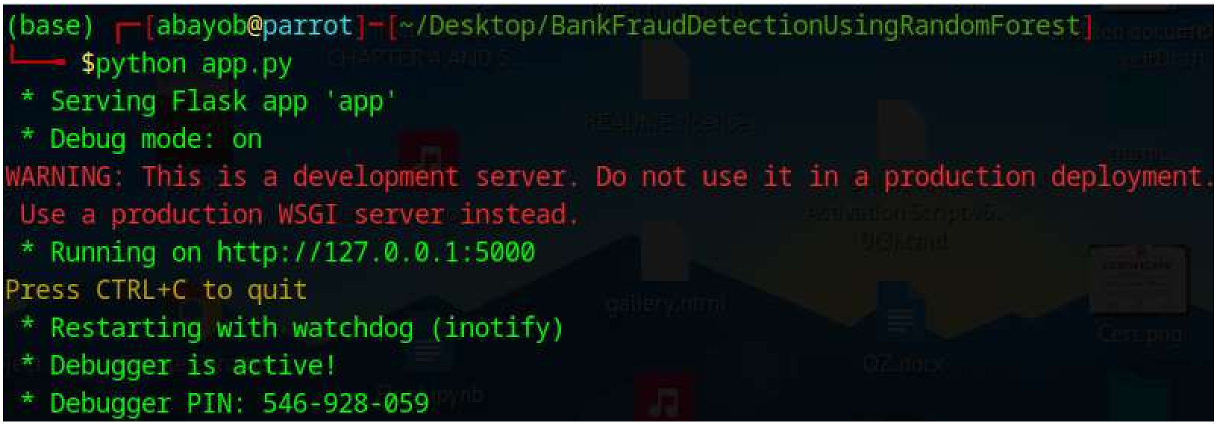
Model Directory

Figure 13: Model Directory for deployment



```
BANKFRAUDDETECTIO...
  > .ipynb_checkpoints
  > static
  v templates
      index.html
  app.py
  Fraud.csv
  model.ipynb
  model.pkl
  requirements.txt
```

Figure 14:Running app.py to test the model after deployment

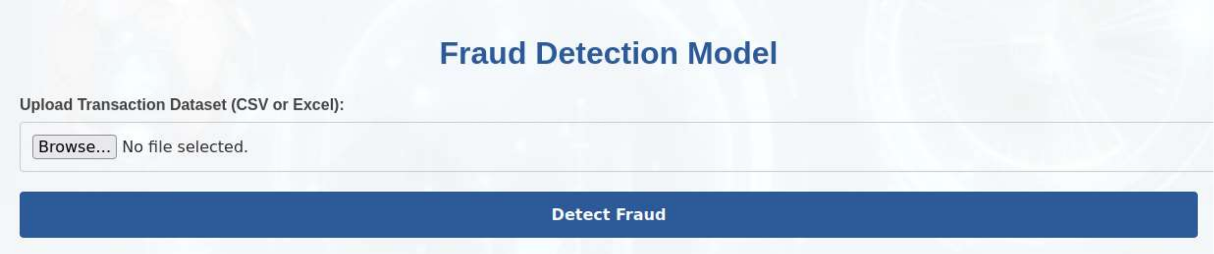


```
(base) ┌─[abayob@parrot]─[~/Desktop/BankFraudDetectionUsingRandomForest]
└──╼ $python app.py
 * Serving Flask app 'app'
 * Debug mode: on
WARNING: This is a development server. Do not use it in a production deployment.
 Use a production WSGI server instead.
 * Running on http://127.0.0.1:5000
Press CTRL+C to quit
 * Restarting with watchdog (inotify)
 * Debugger is active!
 * Debugger PIN: 546-928-059
```

The above image shows how python app.py was run to start the server through the terminal, the app was accessed via browser through http://127.0.0.1:5000, inputs were submitted, and predictions were viewed. Ctrl + C was pressed to stop the Flask app

4.7 Test Application

Figure 15: User Interface to upload data for fraud detection.



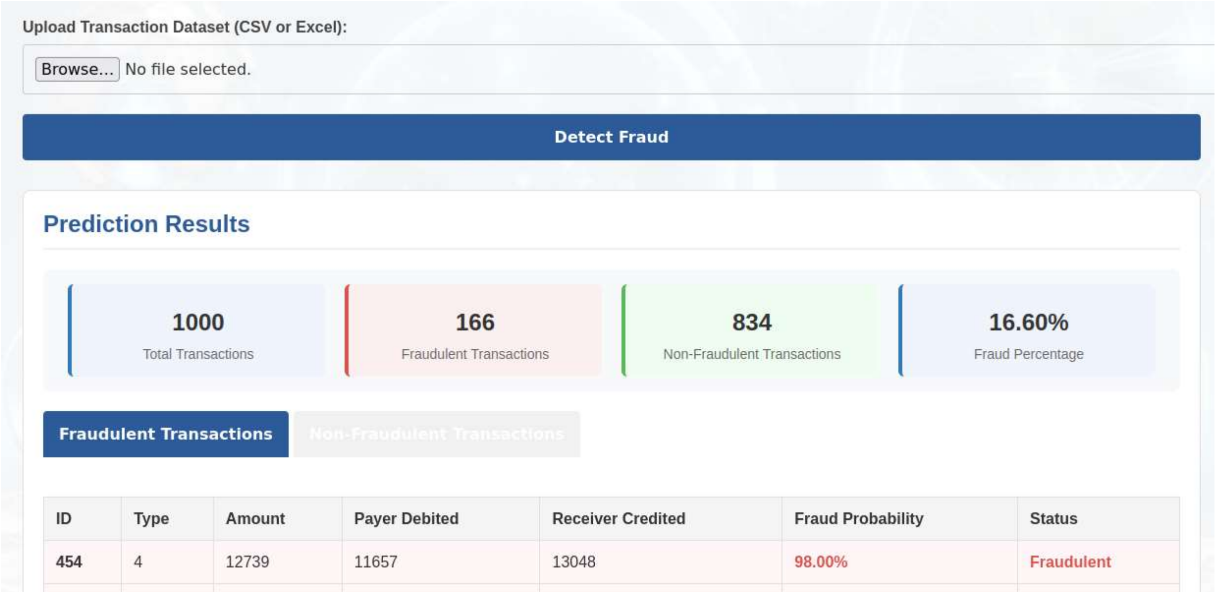
Fraud Detection Model

Upload Transaction Dataset (CSV or Excel):

No file selected.

This project carried a test application of the model whereby a file was uploaded in excel format having the records such as transaction ID, transaction type, transaction amount, payerdebited and recievercredited where the expected output provided by the model should be either 1 for illegitimate transaction or 0 for legitimate transaction. The above snippet is for user interface for uploading data for fraud detection.

Figure 16: Fraud Detection with the deployed model



Upload Transaction Dataset (CSV or Excel):

Browse... No file selected.

Detect Fraud

Prediction Results

1000	166	834	16.60%
Total Transactions	Fraudulent Transactions	Non-Fraudulent Transactions	Fraud Percentage

Fraudulent Transactions | Non-Fraudulent Transactions

ID	Type	Amount	Payer Debited	Receiver Credited	Fraud Probability	Status
454	4	12739	11657	13048	98.00%	Fraudulent

Python simulation techniques were used to produce a synthetic dataset that reflected real-world transaction patterns in order to evaluate the model. There were 1,000 records in the dataset, all saved in Excel format. The model achieved a 16.60% fraud detection rate during testing, identifying 166 transactions as fraudulent and 834 as valid. This shows the model's efficacy and generalization capacity in a different setting.

4.8 Summary

In this research chapter, Python libraries such as NumPy, Pandas, Matplotlib, and Scikit-learn were imported to support data analysis. The dataset underwent preprocessing, including outlier removal, and feature selection was performed using exploratory data analysis. Random Forest Classifier was trained and achieved a high accuracy of 95%. Deployment of the model was facilitated through Flask, allowing user interaction with the model through a structured directory. Additionally, a test application of the model was conducted, providing output based on provided test dataset, further validating its effectiveness.

CHAPTER 5
CONCLUSION AND RECOMMENDATIONS

5.1 Conclusion

This study effectively created a machine learning-based fraud detection model that can accurately identify questionable financial transactions. With a 95% accuracy rate, the Random Forest Classifier showed excellent performance on all evaluation measures, including F1-score, precision, and recall. The model's near-perfect AUC score of 0.99, which demonstrated dependable separation between fraudulent and legitimate transactions, further validated its remarkable discrimination capacity. These outcomes confirm that the selected methodology from data preprocessing to model training and assessment is effective.

The model was deployed as a working web application using Flask, and the project's practical execution was similarly successful. By enabling transaction data upload and obtain immediate fraud detection, this deployment illustrated the model's practicality. A strict and methodical strategy was taken throughout the entire process, from the first data cleansing to the last deployment, guaranteeing dependable outcomes. Financial institutions looking to prevent transaction fraud will benefit greatly from this model's user-friendly implementation and strong technical foundation.

5.2 Recommendation

Based on the results and discussions; the following recommendations were made:

In order to improve the model's detecting capabilities, future studies should investigate the incorporation of new machine learning approaches. Examining ensemble techniques or deep learning methodologies may enhance performance, particularly for intricate fraud patterns that might change over time. Furthermore, adding more contextual transaction data to the feature set like device details or user behavior patterns could give the model more robust signals for making decisions.

Financial institutions should think about integrating the model as part of an all-encompassing fraud prevention plan in order to optimize its impact. As fraud strategies evolve, maintaining high accuracy will need frequent model updates and retraining with fresh data. Additionally, setting up procedures for human evaluation of transactions that have been flagged would result in a well-rounded strategy that blends human judgment with AI efficiency. With these improvements, the model would be positioned as a useful tool for fraud prevention experts as well as a state-of-the-art technology solution.

REFERENCES

Kovach, S., & Ruggiero, W. V. (2011, February). Online banking fraud detection based on local and global behavior. In Proc. of the Fifth International Conference on Digital Society, Guadeloupe, France (pp. 166-171).

Bello, Oluwabusayo Adijat, Adebola Folorunso, Abidemi Ogundipe, Olufemi Kazeem, Ajani Budale, Folake Zainab, and Oluomachi Eunice Ejiofor. 2022. "Enhancing Cyber Financial Fraud Detection Using Deep Learning Techniques: A Study on Neural Networks and Anomaly Detection." *International Journal of Network and Communication Research* 7(1): 90–113.

Bhattacharyya, Ajay, and Adita Kulkarni. 2024. "Machine Learning-Based Detection and Categorization of Malicious Accounts on Social Media." In *International Conference on Human-Computer Interaction*, Springer, 328–37.

des Nations Unies, Rapport. 2022. "Global Study on Occupational Fraud and Abuse."

Lidwall, Jonatan, and Leif Ole Paul Malmus. 2024. "Comparative Analysis of Machine Learning and Deep Learning Models for Card Fraud Detection."

Shome, Nirupam, Anisha Sarkar, Arit Kumar Ghosh, Rabul Hussain Laskar, and Richik Kashyap. 2023. "Speaker Recognition through Deep Learning Techniques: A Comprehensive Review and Research Challenges." *Periodica Polytechnica Electrical Engineering and Computer Science* 67(3): 300–336.

Ahmed, Ahmed Abdelmoamen, and Oluwayemisi Alabi. 2024. "Secure and Scalable Blockchain-Based Federated Learning for Cryptocurrency Fraud Detection: A Systematic Review." *IEEE Access*.

Alfaiz, A., & Fati, A. (2022). An improved model for credit card fraud detection using machine learning methods. *Journal of Financial Technology*, *6*(3), 123-135.

Ayoobi, A., Mehrjoo, M., & Asghari, H. (2021). A hybrid deep learning approach for credit card fraud detection. *Journal of Ambient Intelligence and Humanized Computing*, *12*(2), 1521-1533.

Bello, S. A., Adebayo, O., & Ojo, J. A. (2022). Exploring graph-based techniques for fraud detection in digital banking. *International Journal of Computer Applications*, *182*(28), 11-19.

Chen, L., & Lai, C. (2021). Deep learning for credit card fraud detection: A convolutional neural network approach. *Expert Systems with Applications*, *165*, 113921.

Daliri, S. (2020). Optimizing neural networks for banking fraud detection using the Harmony Search Algorithm. *Applied Soft Computing*, *93*, 106376.

Hashemi, A., Askarzadeh, A., & Zare, M. (2022). Performance evaluation of Random Forest and Gradient Boosting algorithms for financial fraud detection. *Journal of Risk and Financial Management*, *15*(4), 163.

Misra, P., Mohapatra, S. S., & Sahu, A. K. (2020). Credit card fraud detection using autoencoders. *Journal of Information Security and Applications*, *54*, 102564.

Shome, S., Singh, V., & Gupta, R. (2023). Addressing false positives in machine learningbased fraud detection. *IEEE Access*, *11*, 15076-15088.

Taha, M. A., & Malebary, S. F. (2020). Credit card fraud detection using Light Gradient Boosting Machine (LGBM). *International Journal of Advanced Computer Science and Applications*, *11*(6), 526-532.

Uddin, M. N., & Uddin, S. (2022). The effectiveness of ensemble learning algorithms in fraud detection. *Computers, Materials, and Continua*, *69*(2), 1883-1898.

APPENDICES

1. Budget

The estimated budget for the research on fraud detection using machine learning in banking, covering key categories including Computing Resources, Data Collection & Preprocessing, Data Storage, Infrastructure & Tools, Deployment & Maintenance, and Printing & Binding, amounts to KSH 54,500.

Table 1: Budget

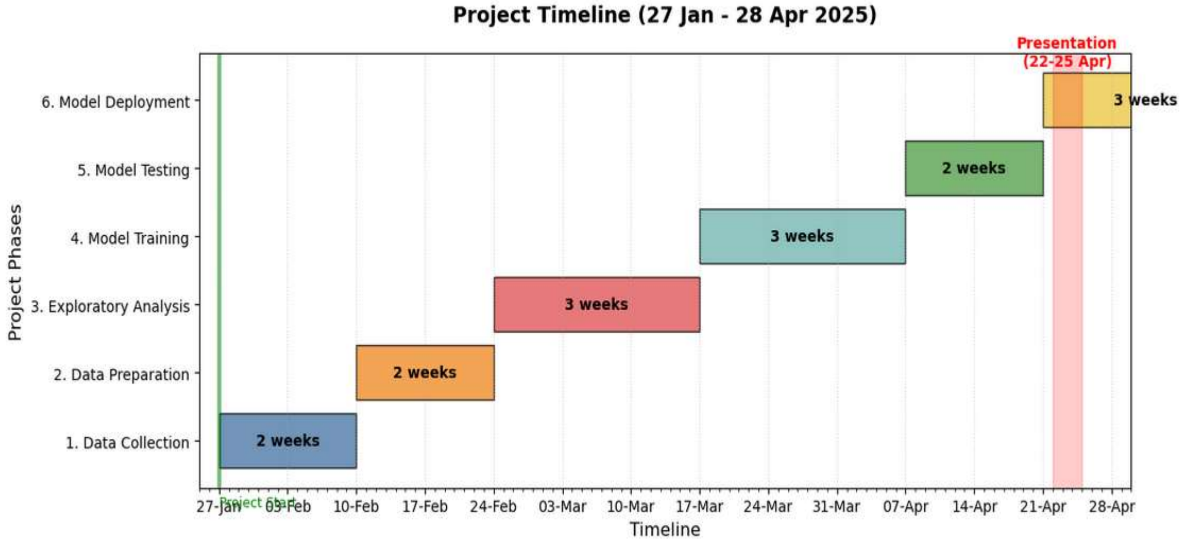
CATEGORY	DESCRIPTION	ESTIMATED COST (KSH)
Computing Resources.	-Cloud computing credits (e.g., Google Colab Pro, AWS, Azure) for model training and testing. -Laptop	45,000
Data Collection & Preprocessing.	-Data cleaning tools and preprocessing scripts. -Potential costs for data annotation or transformation tools.	0
Data Storage	External Hard Drive (1TB, USB 3.0 for fast read/write).	8,000
Infrastructure & Tools	- Subscription to data repositories or APIs.	0
Deployment & Maintenance.	-Services for deploying models or applications. -Maintenance and updates during the project period	0
Printing & Binding	-Printing and binding of the final report. - Presentation materials preparation	1,500
TOTAL		**54,500**

2. Work plan

The Gantt Chart below provides a detailed breakdown of the key tasks and their timelines across 15 weeks for the research on fraud detection using machine learning.

Each task is allocated specific weeks to ensure a structured and iterative workflow, allowing for data collection, preparation, exploratory data analysis (EDA), model training, testing, and deployment.

Table 2: Schedule


Project Timeline (27 Jan - 28 Apr 2025)
Presentation (22-25 Apr)
6. Model Deployment
5. Model Testing
4. Model Training
3. Exploratory Analysis
2. Data Preparation
1. Data Collection
Project Phases
3 weeks
2 weeks
3 weeks
3 weeks
2 weeks
2 weeks
Project Start
27-Jan
03-Feb
10-Feb
17-Feb
24-Feb
03-Mar
10-Mar
17-Mar
24-Mar
31-Mar
07-Apr
14-Apr
21-Apr
28-Apr
Timeline