Title of the Project

Credit Card Fraud Detection

Submitted By

Nazia Tasnim

ID: 201-16-509

Department of Computing & Information System

Daffodil International University

Supervised By

Mr. Md. Faruk Hosen

Lecturer

Department of Computing & Information System

Daffodil International University

Department of Computing and Information System

Daffodil International University.

Dhaka, Bangladesh

Submission Date: 08.01.2025

Approval

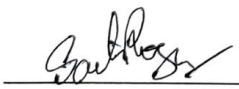
This Project titled "Credit Card Fraud Detection", Submitted by Nazia Tasnim, ID No: 201-16-509 to the Department of Computing & Information System, Daffodil International University has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of B.Sc. in Computing & Information System and approved as to its style and contents. The presentation has been held on 13-01-2025.

BOARD OF EXAMINERS

Md Sarwar Hossain Mollah — **Chairman**
Associate Professor and Head
Department of Computing & Information Systems
Faculty of Science & Information Technology
Daffodil International University

Md. Nasimul Kader — **Internal Examiner**
Assistant Professor
Department of Computing & Information Systems
Faculty of Science & Information Technology
Daffodil International University

Md. Mehedi Hassan — **Internal Examiner**
Lecturer (Senior Scale)
Department of Computing & Information Systems
Faculty of Science & Information Technology
Daffodil International University



Ahmed Saif Reza — **External Examiner**
Managing Director & Chief Technology Officer
Medico Bio Limited

Declaration

I hereby declare that; this project has been done by me under supervision of **Md. Faruk Hosen**, **Lecturer**, department of Computing and Information System (CIS) of Daffodil International University. I am also declaring that this project or any part of there has never been submitted anywhere else for the award of any educational degree like, B.Sc., M.Sc., Diploma or other qualifications.

Supervised By

13-01-25

Md. Faruk Hosen
Lecturer
Department of CIS
Daffodil International University

Submitted By

Nazia

Name: Nazia Tasnim
ID: 201-16-509
Department of CIS
Daffodil International University

Acknowledgment

Researching and finishing the "Credit Card Fraud Detection" project was a delight. I am thankful to Allah for his favor in my education.

My profound appreciation goes out to my supervisor, Md. Faruk Hosen of Daffodil International University's CIS Department, for giving his invaluable time, counsel, and inspiration during my research and academic career. I congratulate him and wish him well for his constant support, good judgment, relevant insights, and thorough comprehension of all the different aspects that were essential in making this project a success. His work has been crucial in making sure I understand what is required to do this job properly.

My sincere gratitude goes out to Md. Faruk Hosen a Lecturer in the Daffodil International University's CIS Department, as well as all of my lecturers for their unwavering support and tolerance during the completion of this thesis work.

Abstract

This thesis focuses on building a machine learning model for detecting fraud in credit card transactions using a data set consisting of 100,000 transactions with 92,785 non-fraudulent and 7,192 fraudulent instances containing information about each of the transactions along with their merchant group or demographics information. The paper tackles imbalanced data problems using Extra Trees, Random Forests, K-Nearest Neighbors (KNN), Support Vector Machine (SVM), and Logistic Regression machine learning models.

The ensemble methods, Trees and Random Performed had 96.87% highest accuracy with precision, recall, and balanced F1 score (Score). when it comes to classifying fraud transactions among all of the models, it is also noticed that KNN had a fairly good performance with an accuracy of 96.29%, being only slightly lower than the ensemble model results. The best-performing model was the SVM (94.32% detection rate accuracy) and the worst one, but a really good performer in terms of complexity (the simpler model had 91.04% accuracy) was logistic regression. This study showcases the power of ensemble methods in the management of imbalanced data, offering high accuracies without sacrificing balance in performance metrics. The ensemble of Extra Trees, Random Forest, and KNN provided a trade-off between effectiveness and reliability making it the best choice to deploy in credit card fraud detection systems due to consistent and stable performance.

These models could be improved in future work by applying deep learning techniques to represent more complex patterns, increasing the data set size with other types of transactions, and making use of synthetic data generated by generative models. In addition to offering real-time processing capabilities, so the system can analyze data as it comes in and detect anomalies more quickly, these techniques for detecting fraud should provide increased speed and accuracy. As such systems approach a production environment, compliance with data privacy rules like GDPR will be vital. It addresses fundamental differences between machine learning models and presents a thorough analysis to act as a guide in the choice of model for credit card fraud detection, thus laying the groundwork for future research.

Table of Contents

List of Figers

Chapter 1
Introduction

1.1 Introduction

Credit card fraud remains one of the largest problems in the financial sector and poses massive risks for consumers, businesses, and even capital market companies. Credit card misuse-based fraudulent activities are a variety from unauthorized transactions made with stolen card details to sophisticated counterfeit and cloned cards [1]. Such fraudulent activities can have implications for an individual's financial position, destroy consumer confidence, and ruin the public image of a business which is liable to lose customer trust. At the same time, monetary penalties are imposed on banks as well. With digital and online transactions rising, especially during the COVID-19 pandemic (when remote working became a key part of daily work life), credit card fraud is becoming more pervasive -many organizations will point to this as an area of increasing concern. E-commerce is an example that has disrupted not merely related industries, but every ('nearly' does justice to very few industries) one of them; online money transfer (and banking) and digital wallets have opened many multiples more avenues for fraudsters to exploit. All of these are convenience developments for the consumer but have introduced new opportunities that cybercriminals can exploit in fraudulent schemes. The need for more powerful and complex fraud detection mechanisms stems from the changing nature of the hashers, who use new tricks to remain undetected [3]. Despite this, traditional means of fraud detection (hand review) and rule-based systems are no longer appropriate for preventing the dynamic nature that credit card fraud. These legacy systems rely on preset rules and patterns that may not be applicable to detect brand-new types of fraud happening right now. Rule-based systems are also generally static, meaning they fail to leverage this new dataset-aware approach with the dynamic nature of digital fraud.

To work through these constraints, organizations have turned heavily towards leveraging modern tools — and especially artificial intelligence (AI) and machine learning (ML) — to bolster the effectiveness of their fraud detection measures. This technology allows huge transaction data to be processed in real-time and uncover some patterns/ anomalies that may

hint at fraud activity [3]. Credit card fraud detection is such an area where machine learning algorithms are very beneficial as they can learn from historical data and recognize the patterns that keep on changing concerning many behaviors in a very complex manner. This adaptive learning feature enables machine learning models to refine the fraud detection progressively with more accuracy over time as well as the bad actors improve their tactics. Fraud detection systems with AI or ML work more responsively than static rule-based approaches seen in the past because they learn from new data regularly (often continuously) and can catch emerging fraud trends. This can involve detecting outliers or anomalous transactions, which may happen to step out from a cardholder's normal spending activities using unsupervised learning techniques. However, supervised learning approaches can be run on labeled data and be trained with increasing accuracy to differentiate between real transactions from fraudulent ones [4]. As a result, financial services are now capable of detecting fraud as it happens rather than days or weeks after.

AI-driven fraud detection has already proven its impact in a range of real-world instances. For example, in the United Kingdom financial fraud losses due to payment cards and remote banking saw £844.8 million lost by consumers in 2018 overall but mitigation from proactive efforts like fraud detection prevented a total of over an additional £1.66 billion being taken away that customers would have been defrauded for without it! That is the equivalent of 2 in every 3 pounds sought to be defrauded being successfully prevented [5]. This demonstrates just how critical it can be to use fraud detection systems properly for institutions not to experience crippling blows. Still, credit card fraud continues to plague consumers, despite such advances. In the U.S. alone, for instance, some 50% of all Americans have seen a fraudulent credit or debit card charge at least once — showing just how large and pervasive this issue is [6]. This research paper attempts to explore the methods and technologies used in credit card fraud detection, with an emphasis on using AI and ML algorithms. The paper will review case studies and live implementations to analyze the efficiency of these advanced systems in decreasing fraud occurrences and securing consumer information. However, the paper will also explore a different kind of challenges being faced one after another in the implementation of AI-based solutions. As an example; While AI and ML systems offer huge benefits, they also raise issues regarding data privacy as these system needs to see the entire transactional information of individuals. Badly-trained models that inadvertently doom some users to be

discriminated against by algorithmic bias. As cybercriminals adjust, AI-driven systems must also be refined and upgraded to sustain fraud detection capabilities against more recent threats. This comprehensive analysis hopes to add to the wider community of interest as it seeks a conceptual contribution to enhancing financial security and minimizing credit card fraud risk. This paper will examine where AI and ML excel, as well as the limitations of these technologies in financial services use cases to highlight opportunities for improvement in cybersecurity efficacy. In the end, this post aims to provide a better perspective on where fraud detection currently lives and perhaps some of the paths we may want it to take.

1.2 Motivation

Introduction Credit card fraud is on the increase to the extent that it has become possible for thieves and crooks in this digital age to steal your financial life by just obtaining unauthorized access directly or indirectly (Allen et al, 2003). Even with all the security measures in place, fraudsters have found new ways to bypass them and commit significantly more costly attacks - making it necessary for organizations that do detect/stop only a fraction of this malicious activity to act promptly. Newer technologies like AI and ML have made it possible for computer examination of thousands of records in less time to be largely error-free — all we need is a dataset large enough. Configuration of various technologies is widely used for reducing financial losses and enhancing security, this research is focused on investigating these aspects more thoroughly to evaluate potential effectiveness. Finally, this paper will discuss some of the obstacles to translating implementation challenges where these complex methods are implemented into sustainable solutions in a way that can help understand and address many concerns around data privacy issues just as much as algorithm biases. The final objective of research intending to investigate the topic in greater detail is to offer additional insights and contribute to a holistic prevention against consumer-based credit card fraud given its impact on financial systems.

1.3 Objectives

The research paper will consist of goals:

1. Other Key Takeaways: Learn About The Utility Of AI And ML Technologies In Fraud Prevention — Look into how the fraud detection models have evolved from traditional techniques to intelligent algorithms based on artificial intelligence and machine learning.

2. Analyze Case Studies and Real-World Implementations: Furthermore, study case studies of ML/AI in credit card fraud detection to see whether it is effective or not.

3. Understand Challenges & Limitations: Study the challenges of incorporating AI and ML for fraud detection, such as privacy issues concerning data collection, bias by design in models, and systems heterogeneity.

4. Compare Detection Methods: Evaluate how the hyped AI and ML detection methods perform in comparison to traditional fraud detection techniques for identifying fraudulent activities.

5. Regulatory and Ethical considerations: A conversation about the regulatory environment leading to deploying AI/ML technologies for fraud detection (e.g. DPA compliance) addressing biases against ethical concerns, in addition to other discussion points ranging from data protection topics as well

6. Provide Suggestions for Improvement: Provide recommendations on how to improve the effectiveness of fraud detection systems based on AI and ML, including potential technological advancements and any needed policy work.

7. Support Financial Security Innovations: Advance the financial security conversation by contributing new ideas and approaches to preventing credit card fraud, and protecting consumers (long-term).

1.4 Research Outcome

Results and Discussion The results of the paper make an important contribution to credit card fraud detection as they focus on how information in datasets can be used for building more accurate models. The research shows a properly implemented analysis of credit card transaction datasets

plays an important role when it comes to building a more powerful fraud detection system. Using richer, more multi-dimensional data and employing depth of knowledge through AI (Artificial Intelligence) and ML (Machine Learning), the research demonstrates that models can be more accurate in detecting fraud. This suggests if we include more quality features in our datasets it will help the model to identify subtle and complex fraud patterns. Additionally, the paper puts special emphasis on improving data pre-processing and feature selection processes to enhance model performance. By elucidating these observations, this work contributes not only to the knowledge of how dataset-driven fraud detection works but also aims to give empirical suggestions that could increase both the precision and efficiency of AI/ML systems against credit card usage.

1.5 Scope of the Study

One of the biggest data analytics case studies is to find credit card fraud detection using Artificial Intelligence (AI) and Machine Learning (ML). This paper investigates how advanced technologies can be better employed for analyzing credit card transaction data to detect and prevent fraud. In this thesis, we provide an in-depth survey of existing methodologies and algorithms regarding AI/ML techniques to implement self-healing artificial systems. It also deals with data privacy, algorithmic bias, and system adaptability challenges to present a comprehensive picture of the factors that influence performance incentives for fraud detection systems. In addition to such a scope, it provides tangible takeaways on developing more efficient models in the wild that may be of help to both researchers and practitioners. This research seeks to improve comprehension and adoption of sophisticated fraud detection technological advancements within the financial services industry by focusing on these elements.

Chapter 2

Literature Review

2.1 Related Work

The ongoing battle against fraudulent activities has spurred significant research efforts to develop robust detection mechanisms. As fraud continues to result in substantial financial losses, a multitude of approaches have been investigated, ranging from classical machine learning algorithms to advanced deep learning techniques.

Classical algorithms, including Gradient Boosting (GB), Support Vector Machines (SVM), Decision Trees (DT), Logistic Regression (LR), and Random Forest (RF), have demonstrated varying degrees of effectiveness in fraud detection. A notable study [8] employed GB, LR, RD, and SVM, achieving a recall rate exceeding 91% on a European dataset. This high recall was contingent upon the implementation of under-sampling techniques to balance the dataset. Similarly, research [9] compared LR, DT, and RF on the same dataset, revealing RF as the most effective model with an accuracy of 95.5%. This was followed by DT with 94.3% and LR with 90%. These findings underscore RF's superior performance in handling fraud detection tasks compared to other classical methods.

The k-Nearest Neighbors (KNN) algorithm and outlier detection techniques have also been explored for their efficacy in fraud detection. Research [10] and [11] demonstrated that these methods effectively minimize false alarm rates and enhance fraud detection rates. KNN's performance was particularly notable in [12], where it was compared with other classical algorithms and showed promising results in identifying fraudulent transactions.

A comparative analysis of classical algorithms and deep learning techniques was conducted in [13]. This study found that both categories of methods achieved an accuracy of approximately 80%. In another comprehensive evaluation [14], a range of algorithms, including RF, GB, LR, SVM, DT, KNN, Naive Bayes (NB), XG Boost (XGB), Multi-Layer Perceptron (MLP), and stacking classifiers, were tested using a European dataset. Despite extensive data preprocessing,

the accuracy of these algorithms hovered around 90%, with the stacking classifier emerging as the most successful approach. The study presented in [15] investigated a neural network optimized with the Whale algorithm, achieving an accuracy of 96.40% and a recall of 97.83% on a European dataset. While this demonstrates the potential of neural networks in fraud detection, it also highlights the significant computational resources required. Furthermore, papers [16] and [17] illustrated the effectiveness of ensemble techniques applied to neural networks, further improving fraud detection outcomes.

Despite the promising results of deep learning models, their high computational demands and reliance on large datasets may limit their practical application [19]. This raises the question of whether comparable results can be achieved with less resource-intensive methods. Accordingly, this paper aims to explore the effectiveness of various machine learning algorithms—specifically Logistic Regression (LR), Random Forest (RF), Naive Bayes (NB), and Multi-Layer Perceptron (MLP)—in fraud detection. The study will investigate whether these algorithms, when combined with appropriate preprocessing techniques, such as oversampling, can provide satisfactory results. This approach seeks to address the limitations of under-sampling techniques commonly used in previous research, offering an alternative strategy for effective fraud detection.

2.2 Limitation of Existing Work

Data Imbalance: The lack of available credit card transaction data for modeling presents challenges since there are many more legitimate transactions than fraudulent ones. When this distribution imbalance is present in our data, model predictions can be "off" and the efficacy of fraud detection algorithms (and others) will suffer.

Data Privacy and Accessibility: Real-world transaction data is largely inaccessible due to privacy regulations. As a result, most research uses synthetic or anonymized data that do not necessarily reflect the complexity of real situations of fraud and potentially limits our ability to generalize results.

High computational costs Advanced techniques, especially deep learning models are computationally expensive in terms of both training the model and its deployment. This high

computational demand can present a challenge to implementation, especially for smaller organizations without as much technical ability.

Complex Feature Engineering: To detect fraud well, one typically needs to do complex feature engineering that can only come from the deep knowledge of fraudulent behavior. Feature engineering is complicated and time-consuming and we may not be able to get good model performance.

Adapting to changing fraud patterns: The problem with existing models is that the techniques of fraudsters are always evolving and therefore it becomes difficult for them to adapt fast enough. Most of the models need to be retrained and updated more frequently to catch up with newer fraud patterns which could become an overhead with resource consumption.

Categorical Data Treatment: Credit card transaction datasets often comprise categorical attributes, and many machine learning algorithms are not good at working with categorical variables. It is a different story if you take these categorical variables and change them analogously to describe something for analysis purposes (which could have effects on the detection models).

Overfitting: Generalization Models that are particularly complex (complex algorithms, deep learning) often overfit to the training data and as a result generalize poorly on new unseen data. This problem is additionally complicated by the absence of varied and depictive datasets in your research.

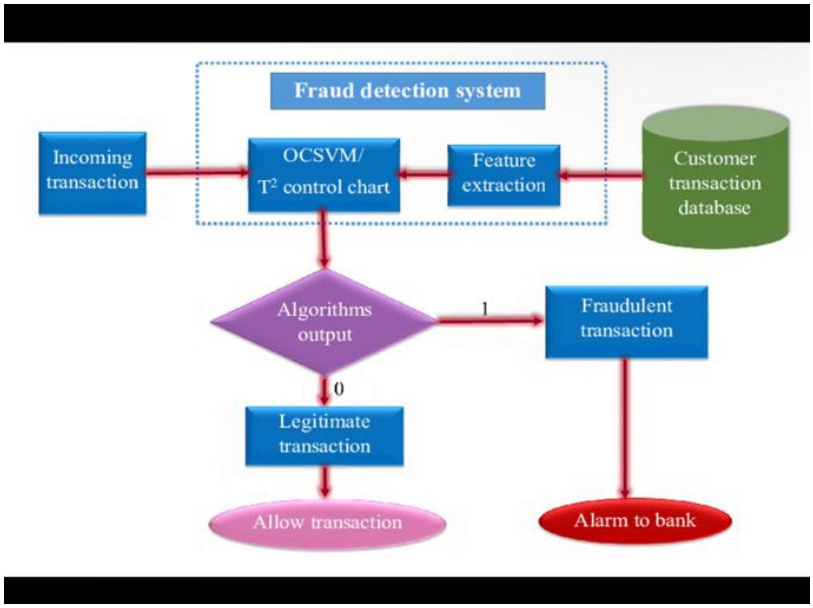
False Positive Rate: A common issue with many fraud detection models is that they come up with a high false positive rate which means the system wrongly flags falsely as fraudulent. This can result in unhappy customers and increased operational costs to review and verify manually.

Chapter 3

Methodology

3.1 Introduction

This study runs on a dataset that contains 100 thousand credit card transactions from an online e-commerce service and provides informative grounds for analysis toward fraudulent detection. Three examples are 'Transaction ID', 'Fraud', where the type of card and mode must be one-hot encoded before being fed to a model, four-column temporal variables such as the date that need finer resolution (e.g., split into periods or bins), five data exploration controls ('Merchant Group'?, Admin District?) with weak feature-extraction potential relative to known nominal/ordinal criteria like shipping country name effect or numeric features. Marked 0 in the Method bucket Phase (recent) Label Distributions. The imbalanced distribution in the dataset is observed as 92,785 instances of non-fraudulent transactions and, 192 fraudulent transactions. This setup makes possible a deep dive into the patterns of fraud displays and fast prototyping machine learning models that aim to make detection more accurate. This is very useful in generating fine-grained parameters for detecting fraud and therefore better detection strategies.



3.2 Dataset Collection

In this study, we have big data on a level of 100K transaction records meticulously collected from an online platform as our dataset. This was done through a collection of data from different sources to include most channels about credit card transactions. It contains several features with transaction identifiers, timestamps, and amount details as well as card type, and entry mode details along with merchant information and some demographic information of the holder. Both transactional and contextual data are fed into Pro Insight Secure to help analyze as well as prevent fraudulent activities; accommodating a comprehensive approach to the same. Its balanced class distribution of the dataset (92,785 non-fraudulent transactions and 7,192 fraudulent ones) provides a solid picture of what makes fraudulent transactions different from genuine ones. They utilized this comprehensive and systematic procedure of collecting data to prepare a dataset for the development, training, testing as well as validating machine learning models that are generally useful in improving credit card fraud detection systems.

3.2.1 Dataset Features

The dataset utilized in this research, sourced from an online platform, consists of the following key attributes:

1. **Size and Structure**: The dataset comprises 100,000 records and includes 16 features.

2. **Features:**

- Transaction ID: A unique identifier for each transaction.
- Date: The date on which the transaction occurred.
- Day of Week: The specific day of the week when the transaction took place.
- Time: The exact time of the transaction.
- Type of Card: The category or type of credit card used for the transaction.
- Entry Mode: The method used to enter card information (e.g., chip, magnetic stripe).
- Amount: The monetary value of the transaction.

- Type of Transaction: The nature or category of the transaction (e.g., purchase, refund).
- Merchant Group: The category of the merchant where the transaction occurred.
- Country of Transaction: The country where the transaction was processed.
- Shipping Address: The address where the purchased goods were shipped.
- Country of Residence: The country of the cardholder's residence.
- Gender: The gender of the cardholder.
- Age: The age of the cardholder.
- Bank: The financial institution that issued the card.
- Fraud: The target variable indicating whether the transaction was fraudulent (1) or non-fraudulent (0).

3. **Class Distribution**:

- Non-Fraudulent Transactions: 92,785 instances (Fraud = 0).
- Fraudulent Transactions: 7,192 instances (Fraud = 1).

This dataset provides a diverse set of features relevant to credit card transactions, enabling a thorough analysis of patterns and anomalies associated with fraudulent activities. The balanced representation of fraudulent and non-fraudulent transactions supports the development and evaluation of predictive models aimed at detecting credit card fraud.

3.3 Data analysis

The dataset under analysis exhibits a significant class imbalance, with 92,785 non-fraudulent transactions and 7,192 fraudulent transactions. This uneven distribution highlights the challenge of detecting fraudulent activities, as the majority of transactions are non-fraudulent.

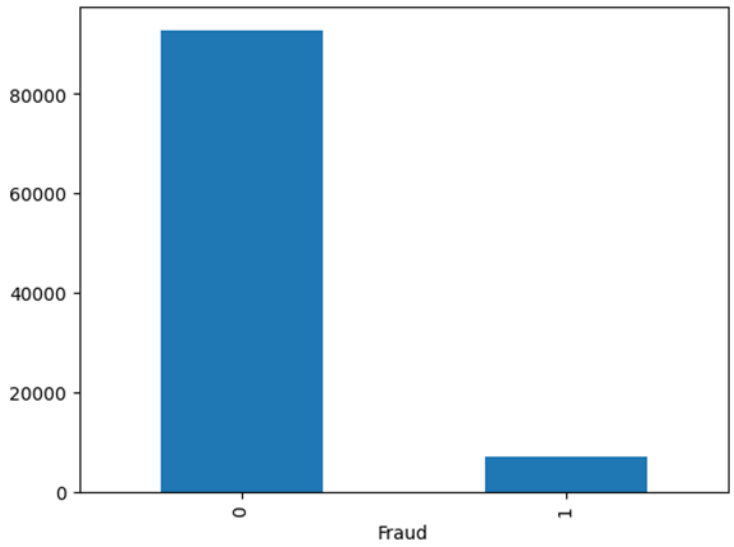


Figure 3.1: Data Distribution of Fraud

Such imbalances can lead to biased model performance, where the model may favor the majority class and overlook the minority class. Consequently, special techniques such as oversampling the minority class or under sampling the majority class, alongside advanced algorithmic approaches, are essential to address this imbalance. Analyzing and mitigating these imbalances is crucial for developing effective fraud detection models that accurately identify fraudulent transactions amidst the prevalent non-fraudulent ones.

The data analysis revealed that fraudulent transactions are notably rare during the hours from 0 to 6, indicating a low incidence of fraud in these early morning hours. This temporal pattern suggests that fraud detection strategies may need to account for variations in transaction timings to improve accuracy.

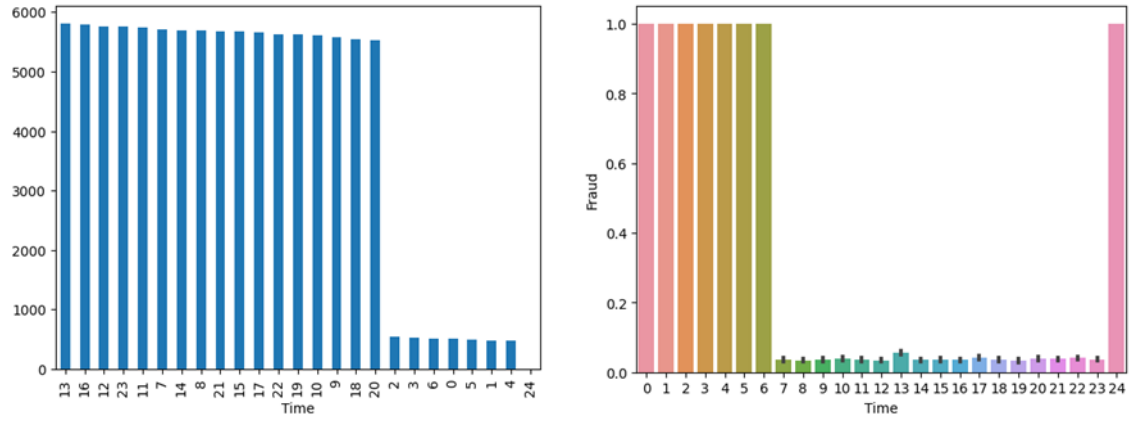


Figure 3.2: Correlation between Time and Fraud

Understanding these time-based trends is crucial for refining detection models and focusing resources on periods with higher fraud activity.

The analysis of the dataset indicates that ATM transactions are associated with the highest incidence of fraud compared to online and POS transactions. This finding suggests that ATM transactions are a significant risk factor for fraudulent activity and highlights the need for enhanced monitoring and security measures specifically targeting ATM transactions.

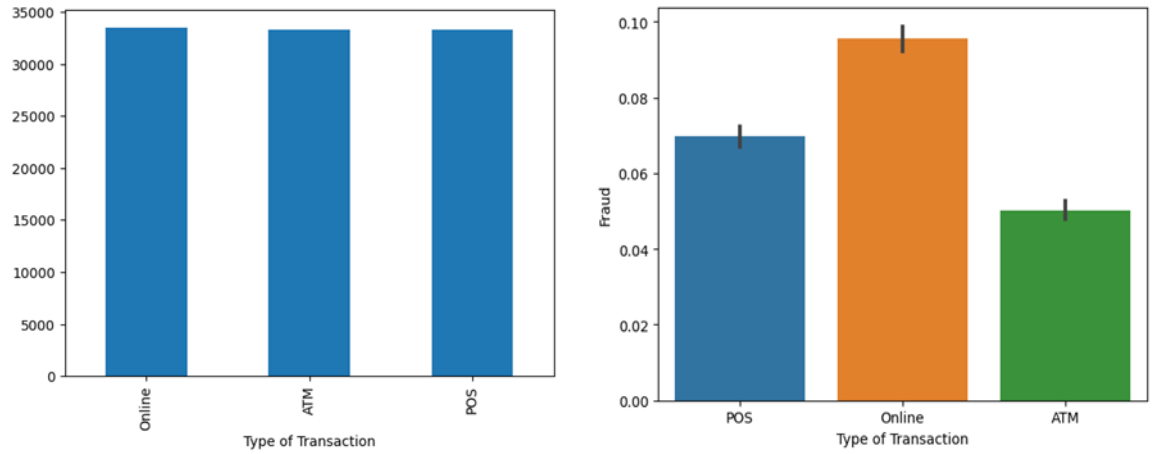


Figure 3.3: Correlation between Type of Transaction and Fraud

The dataset analysis indicates that the UK has the highest number of transactions compared to other countries like the USA, Russia, China, and India. However, despite the high transaction

volume, the fraud rate in the UK is significantly lower. This lower incidence of fraud in the UK suggests a more secure environment for credit card transactions compared to the other countries in the dataset, highlighting the relative safety of credit card usage in the UK.

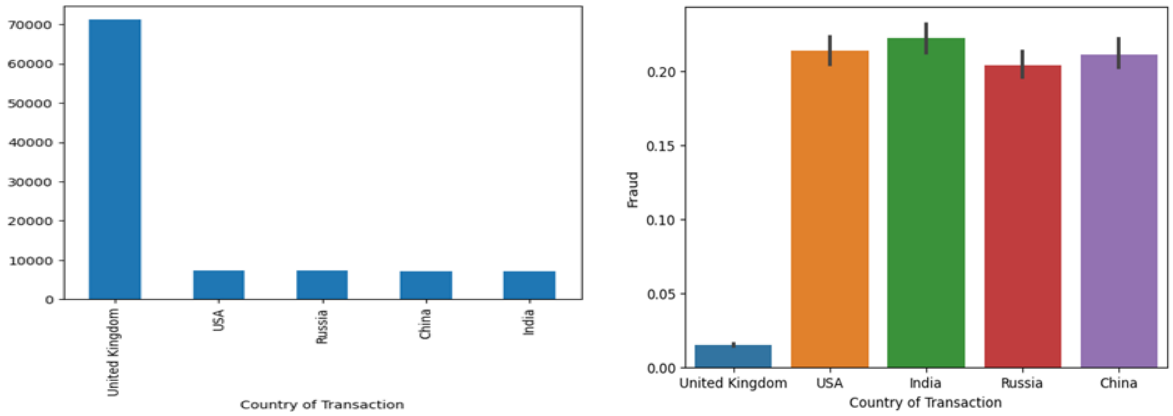


Figure 3.4: Correlation between Country of Transaction and Fraud

This finding emphasizes the importance of considering geographical differences in fraud detection strategies and suggests that further investigation into the factors contributing to the UK's lower fraud rate could provide valuable insights for improving fraud prevention measures globally.

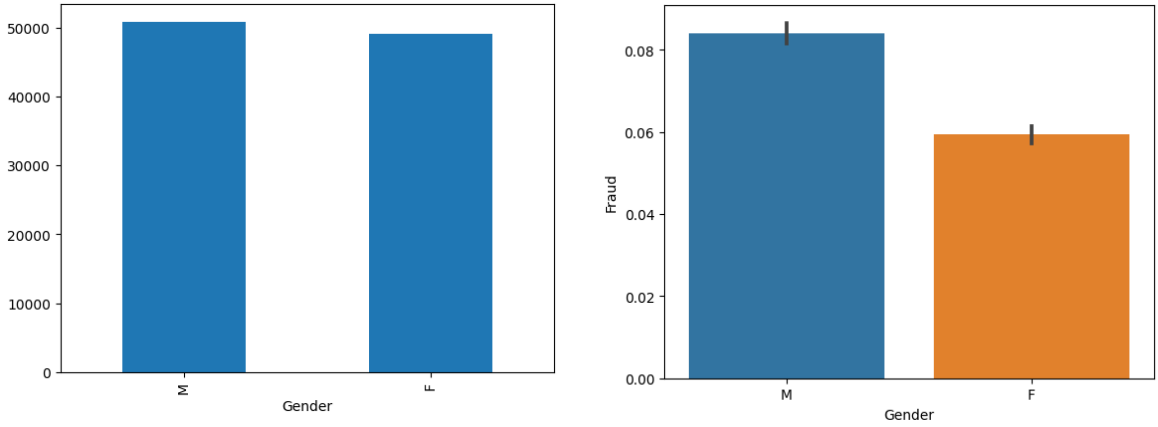


Figure 3.5: Correlation between Gender and Fraud

The analysis of the dataset reveals a notable trend where males exhibit a significantly higher incidence of fraud compared to females. This observation suggests that males are

disproportionately represented in fraudulent transactions, indicating a potential gender-related pattern in fraud activities. Understanding this disparity may help tailor more effective fraud detection strategies and prevention measures targeted at this demographic.

3.4 Data Preprocessing

In the data preprocessing phase, several critical steps were undertaken to ensure the quality and usability of the dataset. Initially, the dataset's shape was verified, and issues such as null values and duplicate records were addressed.

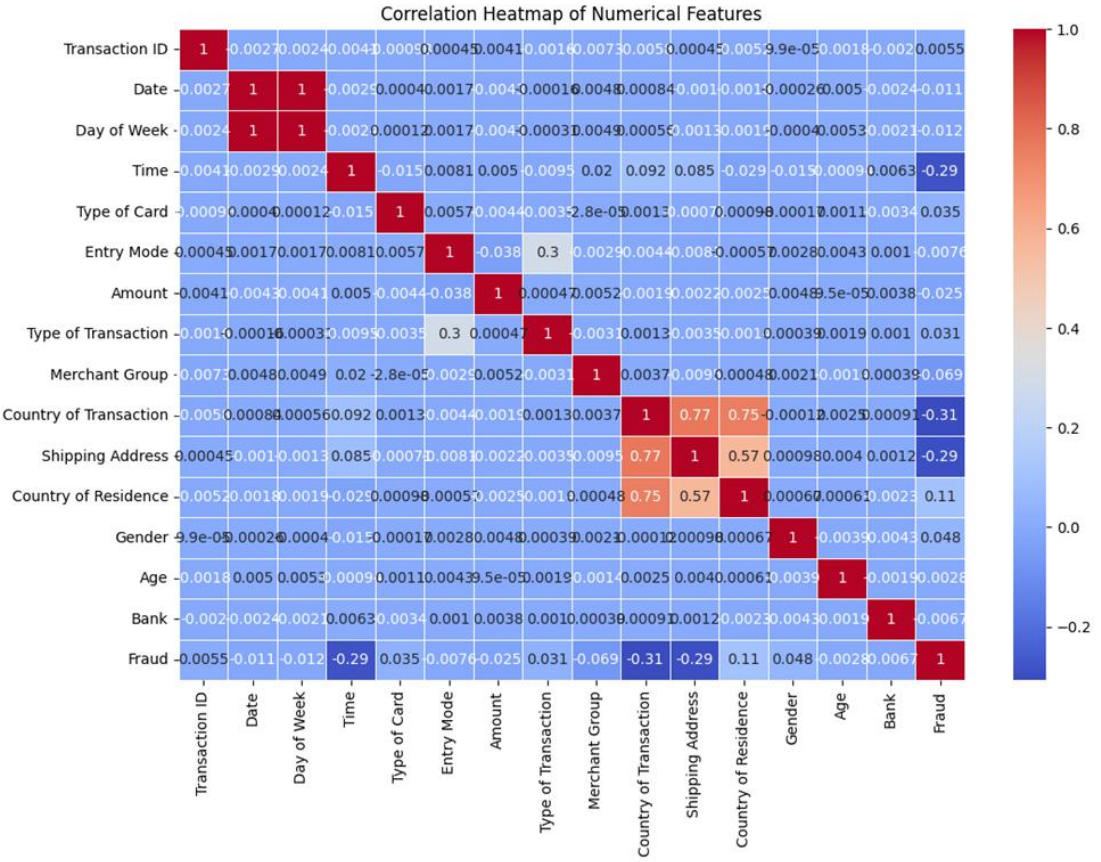


Figure 3.6 : Correlation between Dataset Columns

All records with null values were removed to maintain data integrity, and duplicate entries were eliminated to avoid redundancy. To address the class imbalance, Synthetic Minority Over-sampling Technique (SMOTE) was employed, enhancing the representation of fraudulent transactions and thereby improving the balance between fraudulent and non-fraudulent instances. Additionally, correlation analysis was conducted to identify relationships between features, which informed feature selection and model development. These preprocessing steps collectively refined the dataset, setting a solid foundation for accurate and reliable machine learning model training.

3.4.1 Data Oversampling

Synthetic Minority Over-sampling Technique (SMOTE): To counteract the imbalanced data problem, SMOTE was utilized in this study. One of the most well-known oversampling techniques is SMOTE, which aims to balance out class distribution by artificially creating hallucinated instances in minority classes. In this dataset, heart attack risk is much less common than no risk of a heart attack and SMOTE needs to be used so that the model can better learn patterns associated with the minority class. These are the steps in the oversampling process :

- Identification of Minority Class Instances: Start with identifying instances that are from the minority class, which in this case is heart attack risk (class 1)
- Selection of Individual Instances: For every individual minority class instance select k-nearest neighbors from the entire dataset. The parameter k is set depending on how much oversampling you want, and it can be tuned up or down respectively.
- Create Synthetic Instances: Here we generate synthetic instances on the line segments joining minority class instances & their selected neighbors. It provides you a good control over how many synthetic instances to generate, so the level of oversampling is regulated.

Joining with the dataset: Merge these artificial instances concerning the original data, thus creating a similar distribution for entry.

Behind the scenes, this oversampling process employed by using SMOTE improves the representation of minority class thus helping model in better generalization that helps to predict actual heart attack risk cases. This strategy is even more important in cases of data imbalance that

could skew model results. Items Source — The numbers tell it all! Using SMOTE creates a more balanced and consistent training set leading to the model being better tuned to predict minority class samples, hence improving overall performance.

3.5 Model Selection

Continuous war on refundable credit card fraud requires an elaborate detection system When it comes to credit card fraud we are talking about unauthorized transactions made with this type of payment card that allow people to obtain goods/services/funds through temporarily borrowed money such as in bank loaning or some sort. Logging your sensitive information may cost you a lot and give you another headache for local financial institutions. The use of machine learning algorithms for improving detection accuracy and speed is becoming necessary as fraud techniques continue to grow more sophisticated.

The actual paper gives definitive figures for the best machine learning models (Random Forest, Support Vector Machine (SVM), K-Nearest Neighbor (KNN), Extra Trees, and Logistic Regression) on fraud detection. These models are selected based on their use of various methods and historical performance in classification problems. As an ensemble method, Random Forest and Extra Trees give us quite good performance by combining multiple decision trees. SVM works well in high-dimensional spaces, KNN is good for transaction data that has subtle patterns that can be identified from neighborhood points and Logistic Regression gives a probabilistic perspective.

This study will compare these models to determine the most efficient methods for credit card fraud detection and thus development of a secure credit card fraud prevention system, in turn reducing financial losses.

3.5.1 Logistic Regression

In this case, Logistic Regression is applied which is a very basic and interpretable classification algorithm on the processed credit card transaction data to get initial intuition about the relationship between different features contributing towards fraudulent activity. This model is highly

compatible with our data due to its linear decision boundary and simple nature of this model. Logistic Regression works by predicting the probability that an instance belongs to some category (0,1 or yes, no) For every instance in Logistic it applies a logistic(framed with Sigmoid function)function which guarantees values ranged b/w 0 and also 1.

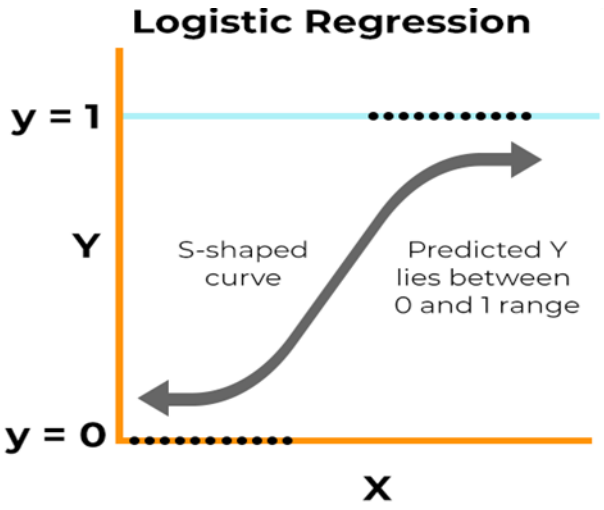


Figure 3.7: Logistic Regression Model

Logistic Regression here analyzes the relationships between each of the features (e.g. transaction amount, transaction time, and merchant category) with whether or not a given transaction is frauded in credit card cases. With its simple parameterization and interpretability, Logistic Regression gives information about how linearly separable the dataset is making it a very good first-step model to have so that all other complex algorithms can be analyzed above this. This approach is useful factor analysis for identifying the fundamental patterns of fraud and serves as a reality check for alternative machine learning models to ultimately create an effective, end-to-end system.

3.5.2 Extra trees

We used The Extra Trees Classifier which is an ensemble learning method specifically designed for high dimensional data sources to improve the predictive accuracy and control over-fitting on our clean credit card transaction dataset. This and Random Forest — during the training phase of

this model, it constructs a huge forest (like lots) with several trees same as a random forest but even more botanical in its randomness. That is, extra trees can explain the behavior, further randomizing feature selection and decision tree splitting. This will help to replicate patterns in the data but reduce overfitted.

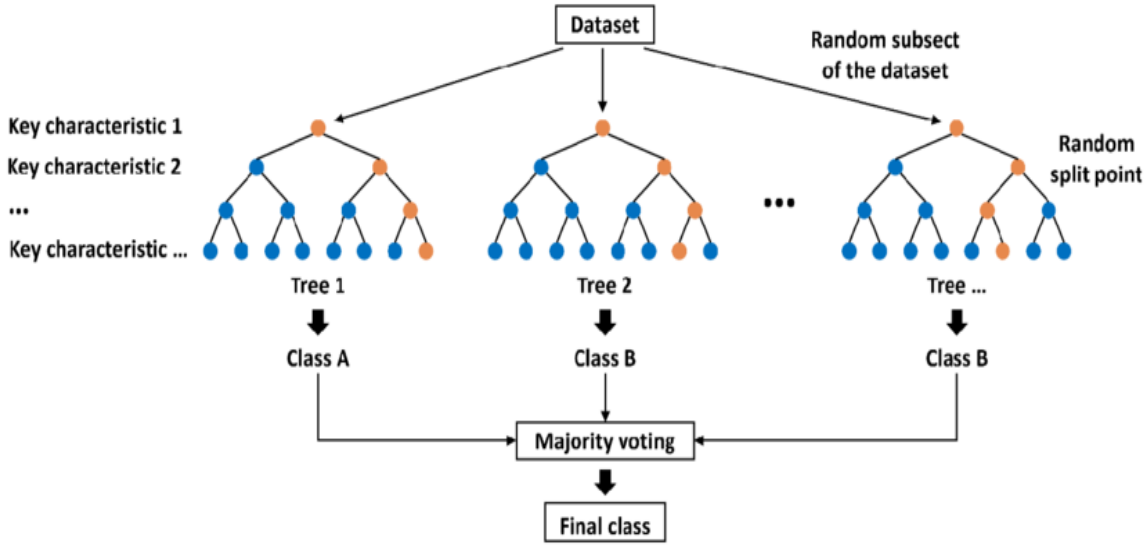


Figure 3.8: Extra trees Model

The Extra Trees Classifier works well in the high dimensionality and variability of transactional data, which is what credit card fraud detection usually deals with. This happens through an ensemble learning method of averaging the predictions from a large number of highly randomized trees to improve accuracy, generalization, and control over-fitting. This is especially helpful in detecting fraudulent patterns that are subtle and difficult to detect by a single decision tree. The high randomness in Extra Trees allows for a vast exploration of decision boundaries making it less likely to overfit and therefore more successful in fraud detection. Hence, Extra Trees becomes a handy tool in our framework to assist us build a powerful and robust credit card fraud detection system.

3.5.3 Support Vector Classifier

We use a Support Vector Classifier (SVC) on the preprocessed credit card transaction dataset because SVC works well with complex decision boundaries. SVC (Support Vector Classification): SVC is based on the idea of finding a hyperplane that best separates instances opposing classes inside high-dimensional feature spaces. And for our specific dataset, where the relationship between different features and being fraudulent is not linear this is a huge plus point.

SVC does this by using what is called a kernel trick to map the data into high-dimension, allowing for the detection of complex patterns that may not be detectable in lower dimensions. SVC can capture multi-dimensional relationships between hundreds of transaction attributes and the probability of fraud by relaxing constraints on defining class boundaries consequently making it more flexible. Consequently, since SVC can manage non-linearities as well as intricate data structures it becomes super helpful in our credit card fraud detection framework and adds to the predictiveness of the model. This way we can find and identify even more sophisticated false-positive fraudulent transactions to improve the effectiveness of our general fraud detection system.

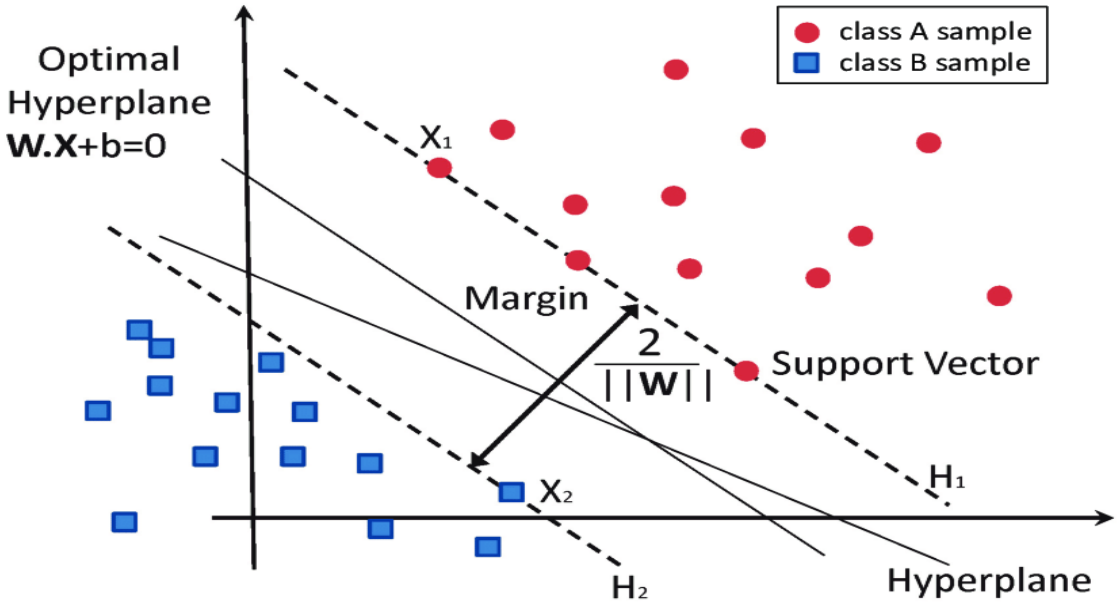


Figure 3.9: Support Vector Classifier

3.5.4 Random Forest Classifier

Here we used Random Forest Classifier, a handy ensemble learning algorithm that can manage complex relationships and reduce overall fitting for our processed credit card transaction dataset. This classifier works by creating multiple examples of decision trees in the training state and during testing, all these decisions are collected together through the voting process. Considering our dataset on credit card fraud detection, Random Forest is capable of capturing multiple feature interactions effectively which can produce stronger predictions. Every decision tree in the ensemble learns some part of that data, and when they come together to make predictions their averaging capabilities allow them not to be biased.

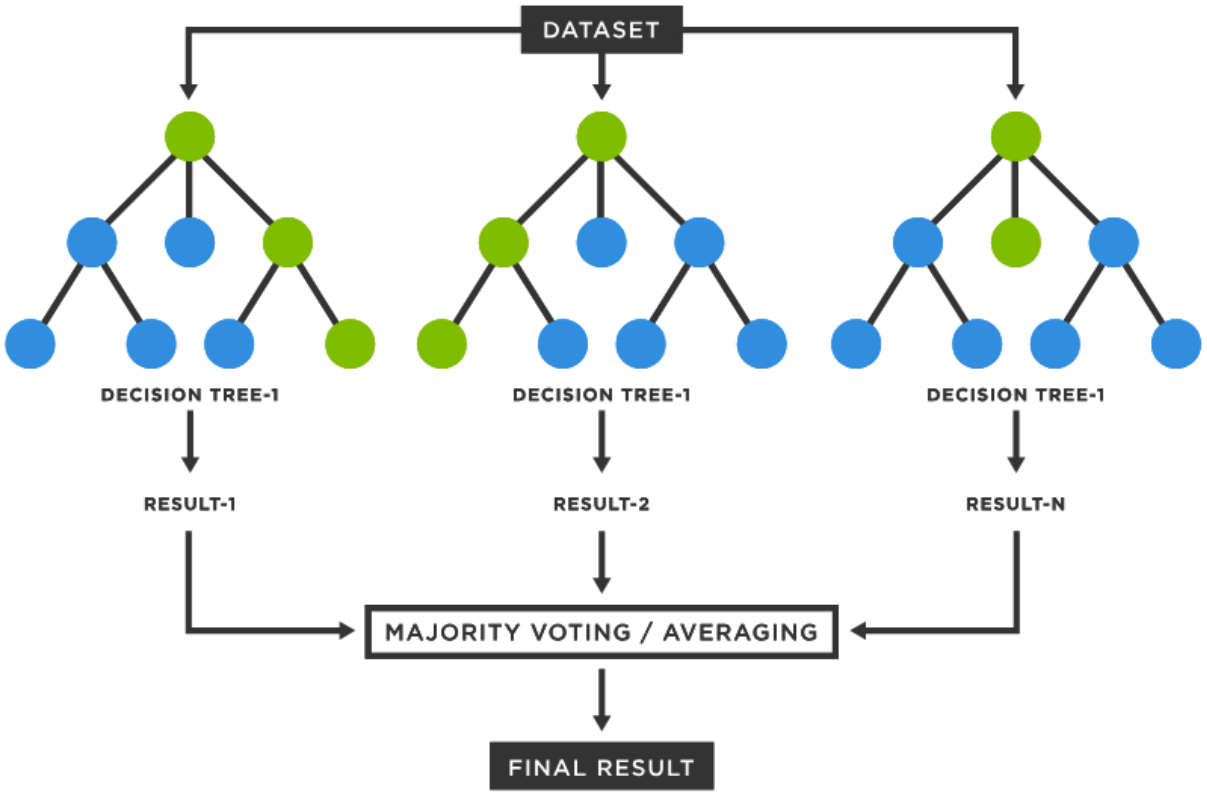


Figure 3.10: Random Forest Classifier

This characteristic is rather useful for our dataset having a variety of different transaction attributes. Random Forest also uses bootstrapping and random feature selection which leads to better generalisation of the model on new unseen data. When we build our fraud detection system,

the predictions must be highly accurate so utilizing several decision trees at once to self-validate each other makes Random Forest an excellent candidate for this. This provides a wider range of transaction patterns to recognize and results in far fewer false positives or negatives, thus increasing the security and trustability of the fraud detection system as a whole.

3.5.5 K-Nearest Neighbors

Our preprocessed credit card transaction dataset used the K-Nearest Neighbors (KNN) algorithm due to its simple classification yet effectiveness as well. In the prediction paradigms of KNN, prediction is made by measuring the similarity between a point and its nearest neighbors in feature space. It breaks down as classifying a transaction by the most common class of 'k' nearest neighbors; where k is the inputted number.

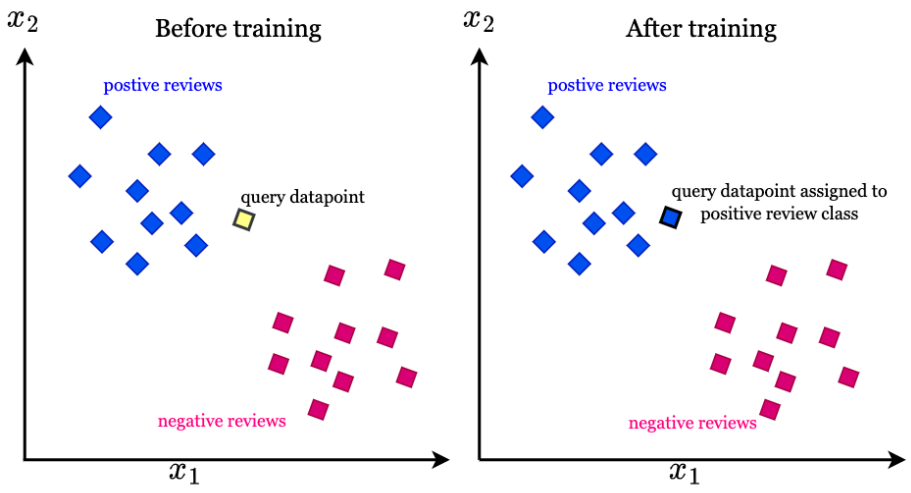


Figure 3.11:K-Nearest Neighbors model

For credit card fraud detection, KNN is suitable because of its nature being non-parametric and the intuition to know what a neighborhood looks like locally. KNN makes inferences based on how transactions should or shouldn't cluster together (by looking at the distance between a transaction and its neighbors). We find this approach to be especially valuable when the fraudulent transactions have a pattern of their own which is not visible in global models. The downside of

KNN is that it can be drastically affected by the choice of 'k' and distance metric, meaning that proper parametric tuning is required for good results.

While KNN has these properties, it can also cost a lot of processing time to compute and as the dataset grows further gets less efficient (since we need this calculation for all transactions and then calculate distance from hundreds/thousands/millions of other data points) However, despite not allowing a diagonal line through the Euclidian space of automated discretized features gives KNN an almost unexplainable level with world-class local pattern recognition and easy classification.

3.6 Model Training

The research used the partition of the dataset for training and testing, which is a robust approach for evaluating and validating machine learning models selected regarding credit card fraud detection. More specifically, 80% of the completely preprocessed dataset was planned for training means which will read data from X-train and get an insight into recognizing patterns or correlations among inputs. The last 20% of the data was kept as a holdout test set, acting entirely separate from training while checking to ensure models were not too adapted in predicting new unseen transactions. This helps in avoiding overfitting the models, as they are tested on unseen data. The study applies an 80-20 split, resulting in balanced considerations of the amount of data available to train models while still holding them accountable for predictive performance thus bolstering the confidence and effectiveness of fraud detection.

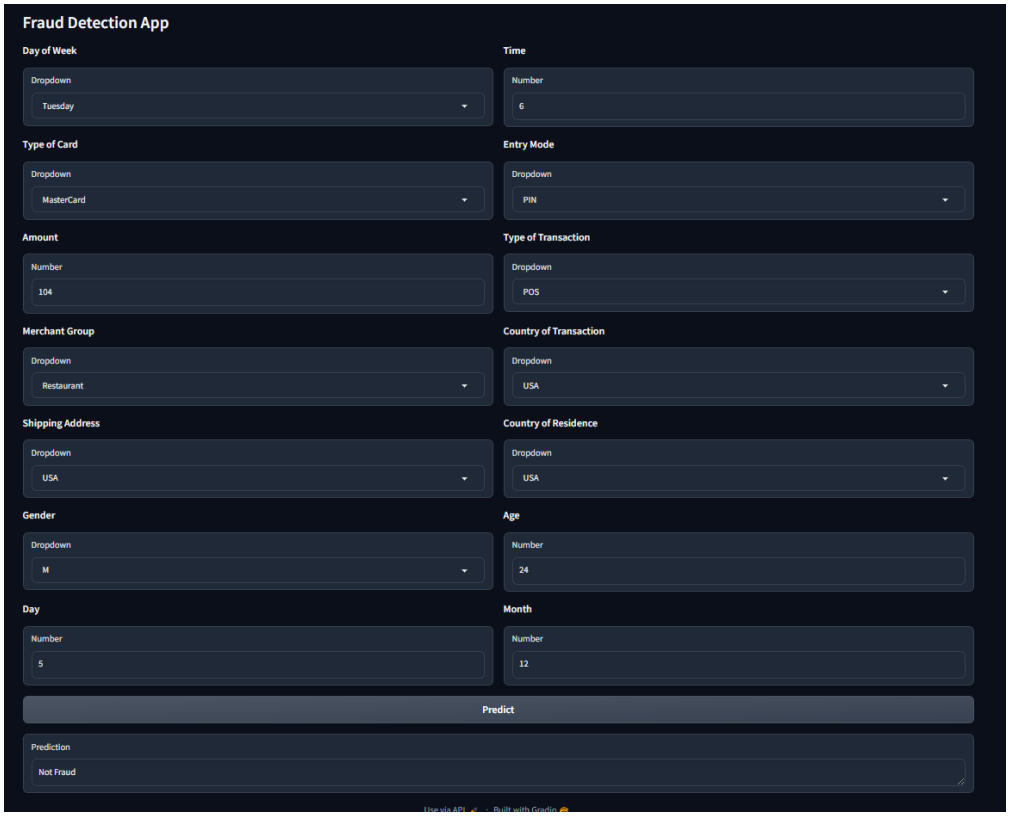
3.7 Result Evaluation

A comprehensive evaluation was done after training machine learning models on 80% of the dataset reserved for the train. This assessment measured performance across a range of vectors and utilized confusion matrices as key measures to better understand the strengths and weaknesses in each model. A confuse matrix gives the information between true positives, True negatives, and False positives, False Negative Which is importance in checking model accuracy and how it is good or bad by which we can find miss classification. Upon extensive examination and study, a smart criterion was employed to find out the best model that can be used for credit card fraud

detection. This decision-making, which we will detail in the next chapter is crucial to assess properly and without bias all of these models leading to a very robust Fraud detection system.

3.8 Deployment

To deploy the credit card fraud detection model the following technologies were used to provide a user-friendly interface and good prediction handling. Having used Gradio it is nice to build web-based interfaces for your machine-learning models with just a few lines of code. Gradio provides an interactive, easy-to-use interface for users to enter transaction parameters and get predictions of fraud on the fly.



There is a Random Forest model trained on the historical transaction data that powers the backend of this deployment. In the deployment script, we load the model which was saved using Joplin to maintain a consistent prediction across environments. The user input data is generally in table form, for this purpose we make use of pandas which allows the system to preprocess and shape this input data. To handle categorical variables, we will use Label Encoder available from sci-kit-

learn. It converts category fields such as card type, merchant group, or country for easy interpretations of the model to see them in the number forms. To normalize the numerical inputs like transaction amount, time, or age and standardize their values to match the format that the model had seen during training Standard Scaler is applied.

The user inputs, such as the card type, entry mode, and transaction amount are read by the sliders and drop-downs in the Gradio interface The input is transmitted to the predict fraud function when the user sends the data; where encoding, scaling, and model inference happen. This model then returns a binary result, indicating whether the transaction is categorized as Fraud or Not Fraud Finally, the application is served with Gradio, callable launcher, the model via a web browser so stakeholders can leverage it easily.

Chapter 4

Result Evaluation

4.1 Introduction

Evaluation of Machine Learning models is done using standard metrics like the confusion matrix, accuracy precision, and f1 score. A confusion matrix explains true positive, true negative, false positive, and false negative predictions in more detail which helps us to perform a detailed analysis of how well the model is doing for classification. Indeed, precision can be defined as the proportion of true positive predictions among all positive predictions while recall is analyzing the percentage of actual positives correctly predicted by the model. The F1 score — which is the harmonic mean of precision and recall gives you both false positives, negatives. Accuracy refers to how frequently the model is correct. The model that performs the best in these various metrics is chosen as the one with the election of having elite performance, after this extensive evaluation. The selected model is finally deployed on a web-based platform to provide the best user-friendly real-time credit card fraud detection interface that makes it accessible and practically usable!

4.2 Model Evaluation

4.2.1 Precision

Precision is an important model evaluation score that provides information about how accurate the positive predictions of a model are in binary classification. It is the proportion of all true positive predictions that were correct and it is calculated by dividing the number of true positives by to sum of True Positives + False Positives. A high precision score means that the model makes few false positive predictions and is therefore highly relevant for use cases where False Positives (FP) are expensive. For example in medical diagnoses, a high precision means that whenever the model says something is serious, it occurs only in a few cases and your real intervention could be concentrated better via here by not wasting resources.

$$recision = \frac{TP}{TP + FP}$$

4.2.2 Recall

Recall(also known as sensitivity, or true positive rate): the ability of a model to find all possible instances of misclassification in a positive class. Recall is also known as sensitivity and it measures the fraction of instances from positive classes that are correctly identified by a model, this is given in terms of all identified classes. Since the model identifies almost all positive instances, high recall is essential in applications where missing just one positive case would be costly. In medical cases, for example, high recall makes sure that the model can not miss possibly critical cases even if it gets a lot of false positives.

$$Recall = \frac{TP}{TP + FN}$$

4.2.3 F1 Score

The F1 Score, on the other hand, is a balanced metric that takes into account both precision and recall by calculating their harmonic mean. It is especially helpful in situations where the class distribution is skewed as it aims for a balance of precision and recall. The F1 score is 2* precision-recall/(precision + recall) High F1 Score implies the model has both good precision and recall, meaning it finds a lot of true positives for very few false positives and negatives. In the cases where it is crucial not to compromise a trade-off between precision and recall, you will find the F1 score an extremely valuable metric.

$$F1\ Score = \frac{Precision \times Recall}{Precision + Recall}$$

4.2.4 Accuracy

Accuracy is a fundamental metric that measures the overall correctness of a model's predictions, considering both true positives and true negatives. It is calculated as the ratio of correctly predicted instances to the total number of instances. While accuracy provides a comprehensive view of a model's performance, it may not be suitable in situations with imbalanced class distribution. For example, in fraud detection, where the majority of transactions are non-fraudulent, a high accuracy score might be misleading. It is essential to consider accuracy in conjunction with precision, recall, and F1 Score to gain a comprehensive understanding of a model's effectiveness.

$$Accuracy = \frac{TP}{TP + TN + FP + FN}$$

4.2.5 Confusion Matrix

The confusion matrix is one of the most useful tools to measure performance in a model for machine learning classification problems. It is highly used in binary or multi-class classification problems. A matrix is a square table that correlates both the model predictions based upon test data and true labels in the dataset. The matrix is organized in the following manner – True Positive (TP), False Negative (FN), False Positive (FP), and True Negative (TN). When it comes to deciding which observations are true and false: a True Positive is when cases were correctly predicted as positive, on the other hand, a True Negative means that they are not positives. False Positive: Instances where the model predicted positive but negative, False Negative: instances it protected as negative but actual answer is Positive. These parts include the metrics to be calculated and also involve a confusion matrix (accuracy, precision, recall, and F1 score) for getting detailed insights into how good or bad is our model. Likewise, the confusion matrix gives a clear insight into whether something is wrong with the classifier and what changes should you make to build a better model that predicts well.

4.3 Result

4.3.1 Result of Extra trees

In the field of credit card fraud detection, I find that the Extra Trees model performs well. With 96.87% accuracy, in general, the model does a good job at determining whether or not transactions are fraudulent for our dataset 96.89% Precision: The metric provides that for predictions that our model says as fraud transactions then those would be the correct or true predicted values and false positive are minimizes with help of this measure Since the recall is 99.09%, it indicates that model has very successfully pinpointed real cases of fraud, establishing its strength where fraudulent activity identification is concerned. The 96.87% F1 Score also describes a good balance of the precision-recall trade-off, resulting in a solid performance across both metrics without bias to either side. This evidence underpins the credit card fraud detecting mechanism through the Extra Trees model, which can serve as a potential resource in supplementing and strengthening existing fraud prevention strategies.

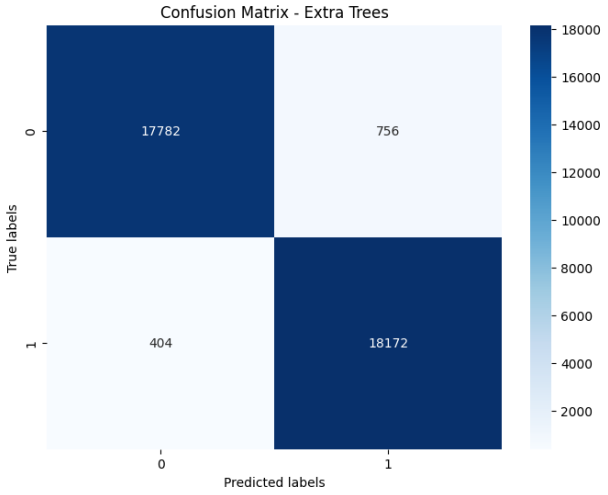


Figure 4.1: Confusion Matrix of Extra trees

4.3.2 Result of Support Vector Classifier

The accuracy score that it gave on test data is 94.32% and performance against credit card fraud detection problem seems to be good with optimal hyper parameters used in this implementation. Thus, this high accuracy suggests that the model can well differentiate between fraudulent and non-fraudulent transactions. The SVM model has precision and recall scores at 94.32, which proves to successfully detect fraud without making a lot of false positives(fake alerts) or missing fraudulent (fraud sample). This makes the F1 Score 94.32% also a very close value, stating a decent performance in both precision and recall features together evenly. In total, the high metrics of the SVM model show that this is a highly dependable and effective way to conduct fraud detection for other systems.

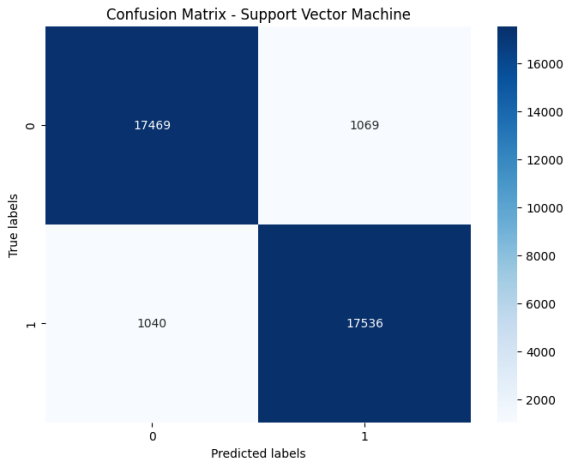


Figure 4.2: Confusion Matrix of Support Vector Classifier

4.3.3 Result of Logistic Regression

As a result, you can see that the Logistic Regression model comes out great in understanding credit card fraud detection, giving an accuracy of 91.04%. This shows that the model does not only classify fraudulent transactions correctly but also classifies all non-fraudulent ones. Precision is a bit higher, at 91.18%, which means the model does quite well in reducing false positives and not calling something fraud if it isn't so The recall is similar to the overall accuracy at 91.04% which

means that the model also succeeds in identifying a large percentage of fraudulent transactions The F1 Score at 91.03% shows the well-balanced performance of precision and recall in single metric form These findings highlight the strength of Logistic Regression model in detecting fraud, and how it can be a useful detector to catch fraudulent activities while providing decent precision-recall tradeoff.

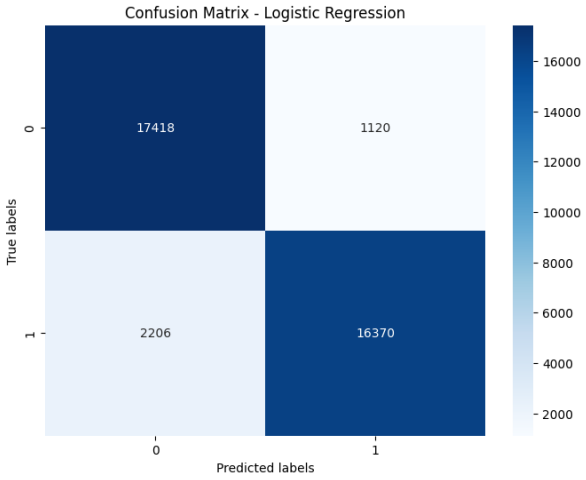


Figure 4.3: Confusion Matrix of Logistic Regression

4.3.4 Result of Random Forest Classifier

The Random Forest model gets an accuracy of 96.87% — which is excellent performance in the case of credit card fraud detection. I think this high accuracy shows a lot, the model could be very useful if it has that much capability to classify fraudulent and non-fraudulent transactions. This high precision score of 96.88% indicated that our model had a low rate of false positives and as such was able to identify legitimate fraudulent transactions with not much error). The recall, likewise at 96.87%, suggests that the model can detect almost all true fraudulent transactions. This balance can be evidenced by the F1 Score of 96.87%, which combines precision and recall, giving one succinct measure of how well it classifies this dataset in general.

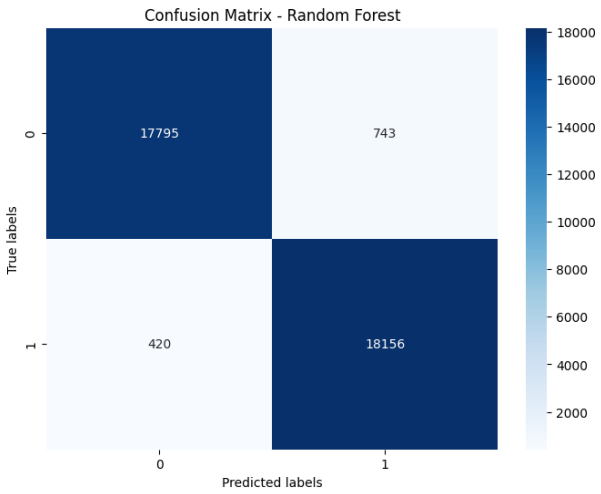


Figure 4.4: Confusion Matrix of Random Forest Classifier

Concluding Remarks: Despite the predictive power of each model, Random Forest proved to be more consistent and robust when it comes to fraud detection over time-principal changes making it a great candidate for deployment in practice.

4.3.5 Result of K-Nearest Neighbors

The K-Nearest Neighbors (KNN) model exhibits strong performance in credit card fraud detection with an accuracy of 96.29%. This high level of accuracy signifies the model's capability to correctly classify a substantial proportion of both fraudulent and non-fraudulent transactions. The precision of 96.29% indicates that KNN effectively minimizes false positives, ensuring that most of the predicted fraudulent transactions are indeed fraudulent. The recall score of 96.29% reflects the model's effectiveness in identifying a significant proportion of actual fraudulent transactions.

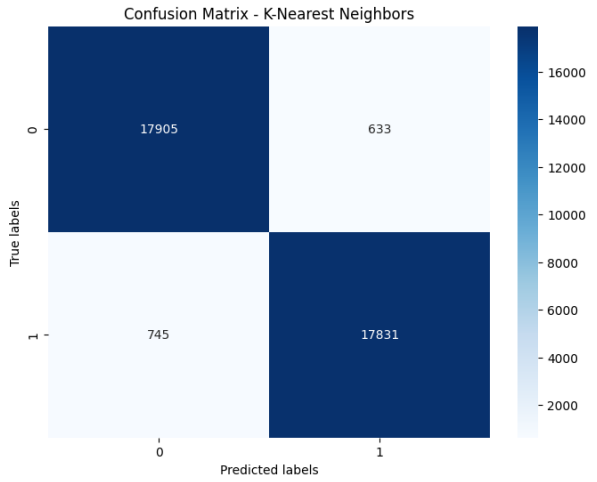


Figure 4.5: Confusion Matrix of K-Nearest Neighbors

With an F1 Score of 96.29%, KNN demonstrates a well-balanced performance, integrating both precision and recall. This makes KNN a reliable and effective model for credit card fraud detection, with consistent results across key performance metrics.

Chapter 5
Conclusion and Future Work

5.1 Conclusion

So, to summarize the comparison of a bunch of machine learning models for credit card fraud detection; we can say lots of things are there but some key insights were given through this analysis at last. The best performing methods were the Extra Trees and Random Forest models, both managing an accuracy of 96.87% along with well-balanced precision, recall and F1 measure scores. They have also proven to provide enhanced performances heuristically and in perspective of their distribution over the imbalanced nature of fraud detection features as these ensemble methods are high on accuracy with balanced metrics, indeed! The accuracy of the SVM model was 94.32%, and it performed quite well, but with slightly worse results in comparison to our ensemble methods. The logistic regression gave 91.04% accuracy which is better than the Manh-AKF due to its simplicity and interpretability, but it has lower power for capturing complex patterns compared with more complicated models when set up correctly along the PIPE Workflow (see Table I). Ensure that the ensemble methods met or exceeded performance by experimenting with other aspects, like the K-Nearest Neighbors model has 96.29%, also it demonstrated balanced metrics close to those yielded from ensemble ways. Concerning the detection of fraudulent transactions, these results indicate that Extra Trees and Random Forest in combination with KNN provide more stable solutions which are also among the most accurate ones showing a better chance to be an effective resource for credit card fraud detection systems running in real environments.

5.2 Future Work

Several possibilities may be explored to improve model performance and generalization in future research on the credit card fraud detection problem. For instance, the incorporation of more sophisticated deep learning methods (e.g., neural networks and ensemble models) that capture inflated patterns among transaction data — which are subject to many machine-learning-use cases; it might provide a better detection. Further, including a richer array of transaction types

and fraud scenarios in the dataset can help to ensure that models are generalizable, as well as offer more opportunities for models trained on synthetic data through generative model training. Employing more recent algorithms along with widespread techniques like anomaly detection and ensemble learning can help control imbalanced data, as well as the ever-changing fraud types. Additionally, the introduction of real-time processing capabilities and richer feature engineering techniques may provide us with more accurate fraud detection promptly. As such, addressing privacy and data protection compliance (especially in light of regulations like the GDPR) when AI models are deployed into production is crucial. Investigating these avenues will allow future work to move beyond the present findings, resulting in better-understood and more sophisticated fraud detection systems.

References

[1]. "Credit Card Fraud - Consumer Action" (PDF). Consumer Action. Retrieved 28 November 2017.

[2]. "Official PCI Security Standards Council Site - Verify PCI Compliance, Download Data Security and Credit Card Security Standards". www.pcisecuritystandards.org. Retrieved 1 October 2021.

[3]. "FRAUD THE FACTS 2019 - The definitive overview of payment industry fraud" (PDF). UK Finance.

[4]. "Credit card fraud: the biggest card frauds in history". uSwitch. Retrieved 29 December 2019.

[5]. "Preventing payment fraud | Barclaycard Business". www.barclaycard.co.uk. Retrieved 29 December 2019.

[6]. Irby, LaToya. "9 Ways to Keep Credit Card Fraud From Happening to You". The Balance. Archived from the original on 30 November 2020. Retrieved 29 December 2019.

[7]. "Court filings double estimate of TJX breach". 2007.

[8]. A. Mishra, C. Ghorpade, “Credit Card Fraud Detection on the SkewedData Using Various Classification and Ensemble Techniques” 2018IEEE International Students' Conference on Electrical, Electronics andComputer Science (SCEECS) pp. 1-5. IEEE

[9]. S. V. S. S. Lakshmi, S. D. Kavilla “Machine Learning For Credit Card Fraud Detection System”, unpublished

[10]. N. Malini, Dr. M. Pushpa, “Analysis on Credit Card Fraud Identification Techniques based on KNN and Outlier Detection“, Advances in Electrical, Electronics, Information, Communication and BioInformatics (AEEICB), 2017 Third International Conference on pp. 255-258. IEEE

[11]. Mrs. C. Navamani, M. Phil, S. Krishnan, “Credit Card Nearest NeighborBased Outlier Detection Techniques”

[12]. J. O. Awoyemi, A. O. Adentumbi, S. A. Oluwadare, “Credit card frauddetection usingMachine Learning Techniques: A ComparativeAnalysis”, Computing Networking and Informatics (ICCNI), 2017International Conference on pp. 1-9. IEEE

[13]. Z. Kazemi, H. Zarrabi, “Using deep networks for fraud detection in thecredit card transactions”, Knowledge-Based Engineering and Innovation(KBEI), 2017 IEEE 4th International Conference on pp. 630-633. IEEE.

[14]. S. Dhankhad, B. Far, E. A. Mohammed, “Supervised Machine LearningAlgorithms for Credit Card Fraudulent Transaction Detection: AComparative Study”, 2018 IEEE International Conference onInformation Reuse and Integration (IRI) pp. 122-125. IEEE.

[15]. C. Wang, Y. Wang, Z. Ye, L. Yan, W. Cai, S. Pan, “Credit card frauddetection based on whale algorithm optimized BP neural network”, 201813th International Conference on Computer Science & Education(ICCSE) pp. 1-4. IEEE.

[16]. N. Kalaiselvi, S. Rajalakshmi, J. Padmavathi, “Credit card frauddetection using learning to rank approach”, 2018 Internat2018International Conference on Computation ofPower, Energy, Informationand Communication (ICCPEIC) ional conference on computation ofpower, energy, Information and Communication (ICCPEIC) pp. 191-196. IEEE

[17]. F. Ghobadi, M. Rohani, “Cost Sensitive Modeling of Credit Card Fraudusing Neural Network strategy”, 2016 Signal Processing and IntelligentSystems (ICSPIS), International Conference of pp. 1-5. IEEE.

[18]. A. Pumsirirat, L. Yan, “Credit Card Fraud Detection using DeepLearning based on Auto-Encoder and Restricted Boltzmann Machine”,2018 International journal of advanced computer science andapplications, 9(1), pp. 18-25

[19]. Learning – Towards Data Science. [online] Available at:https://towardsdatascience.com/deep-learning-vs-classical-machinelearning-9a42c6d48aa [Accessed 19 Jan. 2019].

Nazia Project-Credit Card Fraud Detection-v2

ORIGINALITY REPORT

14%	10%	7%	6%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	dspace.daffodilvarsity.edu.bd:8080 Internet Source	2%
2	fastercapital.com Internet Source	1%
3	Submitted to Oxford Brookes University Student Paper	1%
4	Asma Cherif, Arwa Badhib, Heyfa Ammar, Suhair Alshehri, Manal Kalkatawi, Abdessamad Imine. "Credit card fraud detection in the era of disruptive technologies: A systematic review", Journal of King Saud University - Computer and Information Sciences, 2023 Publication	1%
5	assets-eu.researchsquare.com Internet Source	<1%
6	Submitted to University of Hertfordshire Student Paper	<1%
7	repository.aust.edu.ng Internet Source	<1%