University of Hertfordshire UH

UNIVERSITY OF HERTFORDSHIRE

School of Physics, Engineering and Computer Science

Course: MSc Artificial Intelligence and Robotics with Advanced Research

7COM1039 – Advanced Computer Science Masters Project

Date: 4th December 2023

Machine Learning Techniques for Online Payment System Fraud Detection

Name: Ranjith Maliga Guruprakash

Student ID: 20063331

Supervisor: Imran Khan

Abstract

Theft of credit cards is a problem that continues to become worse in the current financial climate. The frequency of fraudulent activities has sharply increased in recent years, which has cost several enterprises, organisations, and governmental agencies a sizable sum of money. Because of the anticipated increase in numbers, several researchers in this field have focused on using cutting-edge machine learning techniques to early detect fraudulent practices. The dataset is highly unbalanced, meaning that the majority samples (real cases) are more common than the minority samples (fraudulent cases), which makes it challenging to identify credit card fraud. The fraudulent behaviours typically vary for each attempt. The predictive model tends to favour class samples that represent the majority when dealing with input data that exhibits an extraordinarily skewed class distribution. This propensity frequently causes fraudulent transactions to be mistaken for real ones.

This study aims to identify fraudulent credit card transactions using machine learning algorithms and stop fraudsters from accessing victims' accounts without their consent. Due to the global increase in credit card fraud, measures should be taken to dissuade criminals. Setting a restriction on certain behaviours would benefit the clients since their money would be recovered and returned to their accounts, and they wouldn't be charged for goods or services they hadn't requested, which is the primary objective of the project. Five machine learning techniques—random forest, gradient boosting, ADAboost, MLP, and ANN—were used to identify fraudulent transactions.

Acknowledgements

I extend my deepest gratitude to those whose support and contributions have facilitated the successful completion of this research endeavour entitled “Identifying Fraudulent Transactions using Machine Learning Algorithms.”

I wish to express my sincere appreciation to Imran Khan for their invaluable guidance and mentorship. Their expertise and commitment to academic excellence have been instrumental in shaping the trajectory of this project.

I am grateful for the resources and facilities provided by the University of Hertfordshire, which have played a pivotal role in conducting comprehensive research and analysis.

The profound contributions of the broader research community in the domain of credit card fraud detection using machine learning techniques have significantly influenced the conceptualization and execution of this study.

In conclusion, this work stands as a testament to the collaborative efforts of all those acknowledged herein. Thank you for your indispensable roles in bringing this project to fruition.

Declaration

I, Ranjith Maliga Guruprakash, solemnly declare that the project titled "Identifying Fraudulent Credit Card Transactions using Machine Learning Algorithms" is an original and independent work conducted by myself. I assert that all information and findings presented in this project are the result of my research efforts.

I acknowledge that proper citations and references have been provided for all external sources used in this project. No part of this work has been previously submitted for any academic qualification, and it has not been concurrently submitted to any other institution.

I affirm that the content of this project is free from any form of plagiarism, and I understand the serious consequences associated with academic dishonesty. The intellectual contributions of others are appropriately credited through citation.

I express my sincere appreciation to Imran Khan for their unwavering guidance, mentorship, and valuable insights that significantly contributed to the successful completion of this project.

I understand the ethical standards expected in academic research and take full responsibility for the integrity of this work.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1 INTRODUCTION

The last several decades have seen an increase in the use of online payments. This is primarily due to how simple it is to transmit money from any place, while the epidemic has also greatly fueled an increase in e-payments. According to several surveys, e-commerce and online payments will gain prominence in the years to come. This surge in online payments has also raised the possibility of payment fraud. Given the rise in online payment fraud over the past few years, both customers and service providers must be informed about these scams. Users must make sure that the legal beneficiaries of their payments are receiving them; If they don't, they incur the possibility of having to file a fraud complaint, having their payment method frozen, and having their data shared with thieves, which occasionally leads to additional crimes. However, businesses must make sure their clients aren't paying these scammers with their money. Businesses could be forced to make payments to customers to maintain their business, which places pressure on them. Even though businesses have developed and implemented a large number of fraud detection programs, very few of them are efficient at detecting online payment fraud. Companies try their best to make the payment method as safe as possible, but occasionally criminals can get beyond security measures and carry out these online payment scams

E-commerce has advanced significantly since its start. The majority of organisations, businesses, and governmental bodies now use it as a crucial tool to boost their efficiency in international commerce. The simplicity of online credit card transactions is a major factor in e-commerce's growth [LBCS16]. Every time we discuss financial transactions, we also need to take financial fraud into account. A fraudster who intentionally deprives a victim of their right or who seeks financial advantage is committing financial fraud [AAO17]. Credit card transactions have been the most used payment method in recent years, which has caused a rapid increase in fraud activities.

The significant financial losses brought on by fraud are a severe problem that businesses and government institutions are dealing with. Global losses from credit card, debit card, and prepaid card fraud are estimated to have totalled $16.31 billion in 2015, according to the Nilson Report [nila]. Additionally, a recent study by The Nilson analysis [nila] found that the gross fraud loss increased by 4% from 2015 to $22.8 billion in 2018 and is expected to expand even further in the years to come.

1.1 Background

The body of research on corporate fraud spans several academic disciplines, and this work mainly focused on the detection models that have been studied in the accounting literature. Amiram, et al. (2018) provide a more thorough analysis of the literature in the disciplines of law, finance, and accounting. The Securities and Exchange Commission (SEC) took regulatory action as a result of this study, primarily through the Accounting & Auditing Enforcement Release (AAER), which focuses on the most serious forms of financial reporting breaches. The first multivariate model to use financial statement ratios to detect AAERs was the M-Score, created by Beneish in 1999. The M-Score is a useful resource since the data and analytics company AuditAnalytics focuses on providing services to the accounting sector. Notably, the M-Score is incorporated into the curriculum of the Chartered Financial Analyst (CFA), a key credential for individuals in the banking business. The F-Score was then developed, using a larger dataset of AAER patients, as described by Dechow et al. in 2011.

There are more possible dependent factors for financial misreporting than AAERs, most of which would not result in SEC action. For instance, shareholder lawsuits and financial restatements are two examples of these outcome factors. In addition to corporate fraud, there are several more reasons why shareholder lawsuits could be filed. Based on research by Kim & Skinner (2012) on shareholder litigation, the first multivariate prediction model was developed. Financial statements, the other possible dependent variable, include a broad variety of inaccuracies in financial reporting that are not always tied to fraud. The non-reliance financial restatement database from Audit Analytics is the one that is accessible for financial restatements. When applied to restatements in comparison to AAERs, the F-Score and the M-Score scored badly, according to Larcker & Zakolyukina's (2012) study of statements. Unreported data supports the finding that shareholder lawsuits and financial restatements were insufficient dependent variables for fraud detection, which is why this study chose to use the Accounting and Auditing Enforcement Releases (AAERs).

To create the M-Score using probit regression, Beneish first used a small sample of problematic financial statements that included AAERs. Later, starting in the early 1980s, Dechow et al. (2011) did a study on a noticeably bigger and more thorough database of AAERs. They created a detection model using logistic regression analysis and seven important criteria, all of which could be easily deduced from financial records. The F-Score was then developed, using a larger dataset of AAER patients, as described by Dechow et al. in 2011. The authors kindly granted

me access to utilise this database for research purposes in this dissertation and currently support it. The USC Marshall School of Business offers access to the AAER database (Dechow, et al. 2011). For instance, Cecchini et al. (2010) created a customised financial kernel using a support vector machine and financial statement data. Perols (2011) investigated the efficacy of several statistical and machine learning models in separate research. Early literature on advanced machine learning tools also included these works. These investigations, however, used matched samples. When applied to actual world prevalence (e.g., 1:200), conclusions drawn from matched samples (e.g., 50:50) might differ dramatically. Beaver noted this problem of bankruptcy in the past (Beaver 1966). Studying unusual events with machine learning may have the drawback that the machines may be challenging to train. Random undersampling techniques for the training data were investigated by Perols et al. (2017), who demonstrated that they increased model efficacy. In reality, balancing the training data by randomly over or under-sampling is normal practice in machine learning. So that inferences would still be valid, take note that out-of-sample test sets are unaltered. RUSBoost, a boosting model with random undersampling, was implemented by Bao et al. (2020) utilising sample data with actual uncommon prevalence rates. In contrast to the M-Score or the F-Score, one novel aspect of their work was the use of raw financial statement variables rather than financial ratios. With this strategy, risk ratings might be generated more easily and directly using information from financial reports without the need for further transformations. Since machine learning investigated nonlinear routes to create predictions, interpretability suffered as a result. They cited a substantial improvement over the F-Score of 70% in their article. I looked into it more when the Journal of Accounting study required that the source code for their published study be made available, which led me to write a critique that was recently featured in Econ Journal Watch. This critique was presented in the dissertation's subsequent chapter. Benford's law, which is based on the distribution of the initial digits and transcends traditional machine learning, was introduced by Amiram et al. in 2015. The authors were the first to use Benford's law to detect AAERs, and the benchmarking research used their summary measure. They were the first to apply Benford's law to this particular scenario, although it has long been a component of fraud investigators' toolkits outside of corporate fraud detection.

Prediction modelling was not the only field of research that looked at how fraud is found. According to Dyck, Morse, and Zingales (2010), most fraud is often discovered through other channels, such as investigative journalism or the findings of criminal investigations. Fraud detection supposedly "takes a village." Several outside parties, including staff members, media

representatives, and business experts, participated in discussions about fraud detection in this area from a variety of perspectives. As an example, one viewpoint sometimes referred to as the legal position, asserts that auditors and securities regulators are in charge of fraud detection, as described by Coffee in 1986. However, from a financial perspective, as stated by Dyck et al. in 2010, it is recommended that to complete the time-consuming activities involved in fraud detection, debt and equity holders work together with their analysts and auditor agents. However, Dyck, Morse, and Zingales' research eventually revealed that employees, other industry regulators, and the media played crucial roles, accounting for the majority of fraud detection, while auditors and the SEC only made up 10% and 7% of the detection, respectively.

The question of whether the thematic content of financial statement disclosures influences the likelihood of purposeful misreporting, as described by Brown et al. in 2020, has recently been explored using textual analysis. These results showed an improvement, especially in the top 1% of the probability distribution, even if they did not significantly outperform those in the Bao et al. research. Notably, the same journal issue from March 2020 had both of these studies.

If sophisticated data mining techniques are successfully used on easily accessible raw financial data, Bao and his coauthors ask, does the value of textual data stay intact? This is an interesting subject for future scholars to consider. The regularly employed Dechow et al. ratio-based logistic regression model, they claim (Bao et al., 2020), significantly underestimates the usefulness of financial data in the context of fraud prediction. They also emphasise the relevance of their findings.

The data is being used for a variety of studies while maintaining privacy. According to Kalbande et al. (2021), one of the tests involved the use of blockchain technology and machine learning methods. The use of blockchain technology, however, might be beneficial in preserving data privacy, but we cannot overlook the fact that it is a decentralised solution and comes with certain disadvantages, such as scalability concerns and high energy consumption. Thennakoon et al. (2019) created a supervised machine learning approach utilising blockchain technology. The author used Ethereum to put blockchain technology into practice. In the study, 300,000 accounts were utilised, and the results were contrasted with some machine learning methods. Studies that used the federated learning and gossip learning paradigms were also carried out. According to Kolodiziev et al. (2020), gossip learning is ineffective because it lacks a centralised management system. The federated learning approach, often known as the F.L., was thought to be more effective and performed better due to its semi-decentralized character.

According to Jain et al. (2020), Cash Out and transfers when money is transferred to a merchant before being transmitted to users or rarely, inadvertently, to fraudsters, are the two transfers where scams are most frequent. The initial transfer entails the transfer of money from one user, a fraudster, or a consumer to another.

The majority of scams occur on the second transfer. Yee et al. (2018) employed accuracy, precision, and specificity criteria to rate the performance of each machine learning algorithm in their evaluation of multiple algorithms for the detection of credit card fraud. The goal of this research is to offer a model that employs the supervised Random Forest algorithm to more accurately detect credit card payment fraud. The data warehouse, the API module, and the fraud detection models are the three main components of the fraud detection system studied by Thennakoon et al. (2019). Each of these components had a simultaneous function in our investigation. The API Module is required to transfer real-time transactions between the data warehouse, GUI, and fraud-detection model.

1.2 Problem Statement

The issue at stake is the growing possibility of fraud in online payment systems, which poses significant financial hazards to both consumers and companies. The difficulty is in developing and putting into practice an advanced machine learning system that can quickly and accurately identify fraudulent transactions while minimising false positives and negatives. This necessitates the creation of cutting-edge feature engineering approaches, data preparation techniques, and the choice and improvement of machine learning algorithms. The system must also be built to manage large transaction volumes and change with fraud tendencies as they emerge. This project aims to create a strong and reliable defence against online payment system fraud, maintaining the security and confidence of digital financial transactions. Its effectiveness will be evaluated based on accuracy, recall, and F1-score metrics.

1.3 Research Questions

The research questions are as below:

1) Which of the selected machine learning models is most effective at identifying fraudulent activity in online payment systems?

2) When it comes to detecting fraudulent transactions in online payment systems, how do the performance results of the selected machine learning models compare to those of the models from earlier research, such as KNN and Naive Bayes?

1.4 Research Aim

This study aims to improve the efficiency of fraud detection in online payment systems by selecting and using the most accurate and useful machine learning model(s) from the list of models that includes Random Forest, Gradient Boosting, AdaBoost, MLP, and ANN. To build more reliable and effective fraud detection solutions in the area of online payment security, the study aims to not only evaluate model performance but also take into account additional criteria for real-world deployment.

1.5 Research Objective

The main objective of this study's research is to evaluate and compare the effectiveness of several machine learning models in the context of identifying fraud in online payment systems, including Random Forest, Gradient Boosting, AdaBoost, MLP, and ANN. The main goal is to thoroughly assess these models' skills, with an emphasis on determining how accurate they are at spotting fraudulent transactions. This requires a thorough examination of the advantages and disadvantages of each model, including how well they can reduce false positives and false negatives. The study also seeks to clarify variables like dataset features and parameter settings that affect model performance. Without specifically addressing their actual deployment, the study hopes to achieve these goals and offer insightful information on the efficacy of various machine learning algorithms for online payment fraud detection.

CHAPTER 2 LITERATURE REVIEW

2.1 Introduction

The simplicity of payments has greatly improved with the advent of internet payment systems. However, it also led to a rise in payment fraud. Anyone utilising any payment method, especially when using a credit card, is susceptible to online payment fraud (Bin Sulaiman *et al*., 2022). To prevent customers from being charged for products or services that they never purchased, credit card issuers must detect online payment fraud. Online payment systems have emerged as the backbone of international trade in today's interconnected digital world, offering simplicity and effectiveness for activities ranging from purchasing goods to bill payments. This convenience is accompanied by a sizable challenge including the growing danger of fraud within e-commerce platforms. Technology advancements have opened up new opportunities for hackers to exploit flaws and carry out sophisticated fraud schemes, necessitating the creation and implementation of advanced machine-learning techniques for effective payment system fraud detection (Lainjo, 2020). While still somewhat successful, conventional rule-based systems find it difficult to keep up with the fraudsters' continuously changing strategies. Machine learning techniques conducted centre stages and have the potential to improve fraud detection through flexible and data-driven approaches (Strielkowski *et al*., 2023). The concept of fraud detection in online payments using machine learning techniques will be covered in this paper and relevant research papers and literature will be reviewed to achieve a proper insight into the topic.

2.2 Concept of Online Payments Fraud Detection Using Machine Learning Techniques

Because more and more businesses are using credit cards, in addition to the number of consumers putting a halt to financial transactions, there has been a sharp rise in fraud cases according to the research conducted by Alenzi and Aljehane, (2020). Handling outliers, unbalanced, and noisy data has made this issue more apparent. Artificial intelligence-based fraud detection is suggested in this paper. To create the classifier in the proposed system that would stop credit card transaction fraud, logistic regression is used. An additional step called pre-processing is utilised to manage unclean data plus guarantee a higher level of accuracy in detection. During the stage of pre-processing, the data is cleansed utilising 2 unique major techniques: the **“mean-based technique”** and the **“clustering-based method”**. The suggested classifier exhibits a better accuracy, sensitivity, and error rate when it corresponds to 2 widely used classifiers: the **“voting classifier”** and the **“support vector machine classifier”**.

There is a markedly higher risk of fraud connected with credit card transactions because of recent advancements in **"electronic commerce systems"** and **"communication technology"**, which have made credit cards the most widely used payment mechanism for both offline and online purchases according to the research conducted by Taha and Malebary, (2020). Every year, companies and individuals lose a lot of money due to fraudulent credit card transactions, and scammers are often trying to find unique methods to do these transactions using technology. Utilising electronic payments more often is now significantly impacted by the identification of fraudulent activities. As such, methods for identifying fraud in credit card transactions should be both efficient and effective. By utilising an **"optimised light gradient boosting machine (OLightGBM)"**, this research suggests a clever method for identifying fraud in credit card transactions. A creative integration of a Bayesian-based hyperparameter optimisation approach was used to adjust the parameters of a "Light Gradient Boosting Machine (LightGBM)". Two "real-world public credit card transaction datasets" that included both valid and fraudulent transactions were used in our tests. These tests were designed to show how well our suggested "OLightGBM" works in spotting fraudulent activity in credit card transactions. When evaluated across the two datasets, our suggested strategy surpassed previous approaches in terms of accuracy (98.40%), precision (97.34%), and the "Area Under the Receiver Operating Characteristic Curve (AUC)".

2.3 Review of Existing Literature

2.3.1 Credit Card Fraud Trends and Machine Learning Solutions:

The study paper by Khatri *et al*., (2020), stated that Given the current situation with the economy, credit card use has become more common. With the use of these cards, users may make large purchases without necessarily carrying a lot of currency. Cashless transactions have been revolutionised, and they have made it simple for clients to make any form of payment. Although very useful, this technological method of payment entails a unique set of risks that can result in data breaches and fraudulent transactions (Demertzis *et al*., 2020). Inappropriate use of this data breach could endanger the individual in question and generate risks. Similar to an increase in customers, fraudulent use of credit cards is also on the rise. Credit card information can be illegally accessed and employed for fraudulent transactions. The issue can be remedied through the application of specific machine learning algorithms which gather data and use it for analysis.

According to Dornadula *et al*., (2019), Targets for payment fraud are straightforward and practical to approach. Online fraud is becoming more prevalent now that there are more choices for online payment on online retailing and other websites. Due to a corresponding rise in incidents of fraud, investigators are now using a variety of machine-learning algorithms to identify and look into online transaction fraud. The study's principal objective is to create and put into use a special fraud identification algorithm for streamed financial information to analyse and extract behavioural patterns from past customer transaction data. wherein cardholders fall into categories based on the total amount of money they spend on all of their transactions. The purchasing habits of each group can then be obtained separately according to the window sliding strategy, which is used to aggregate the transactions made by cardholders from distinct groups. As a result, numerous classifiers are taught to distinct groups. Then, one of the best strategies to spot fraud is to choose the classification algorithm with the greatest evaluation score. The problem of idea drift is subsequently dealt with via a feedback mechanism. To create this report, the team of investigators used the "European Credit Card Fraud" collection.

2.3.2 Fraudulent Activity Identification using Artificial Neural Networks:

The critical analysis by Asha *et al*., (2021), demonstrated that Credit card theft is a common occurrence because credit cards are used for the majority of purchases. Technology development and the rise in online sales, which have increased fraudulent activities and caused significant financial losses, are to blame for this trend. Therefore, effective means for mitigating the amount that is lost are required. Additionally, con artists use fraudulent SMS and calls, phishing, impersonating, and various additional techniques to steal the user's credit card information. Several machine learning methods, such as "Support Vector Machines" (SVM), "K-nearest Neighbours (KNN)", and "Artificial Neural Networks (ANN)", are used in this study to attempt to predict the possibility of fraud. It carried out the separation of the successfully used conventional deep learning and machine learning algorithms used to discriminate between fraudulent and lawful transactions.

The suggested method for detecting fraudulent activities in credit card transactions makes use of an "Artificial Neural Network" (Berhane *et al*., 2023). Performance is evaluated, and dependability is calculated, based on the prediction. Additionally, a predictive model for identifying credit card fraud is constructed using classification approaches like "Support Vector Machines" and "K-Nearest Neighbours." Artificial neural networks forecast more accurately

than systems created with "support vector machines" and "k-nearest neighbour" algorithms, according to a research investigation of the performance of the investigation's three algorithms. 30 of the 31 characteristics in the dataset used in the experiment contain information on a person's name, age, account information, and other comparable subjects. The ultimate result of the transaction is provided by the final attribute and can either be 0 or 1.

2.3.3 Machine Learning for Online Payment Fraud Detection:

According to Adepoju *et al*., (2019), Credit card fraud is a serious and growing problem in the modern world due to the growth of e-commerce and online payments. Through theft of identification and monetary losses, such illicit acts have an opportunity to have an enormous international effect on millions of individuals. Criminal activity is posing a greater threat to the financial system, with far-reaching consequences (Cao *et al*., 2019). The data set measuring technique, the selection of variables and the verification algorithms utilised have a significant impact on the effectiveness of identifying fraudulent transactions in credit card purchases. The detection of online payment fraud seemed to have relied heavily on information extraction.

The use of "Support Vector Machine," "Naive Bayes," "Logistic Regression," and "K-Nearest Neighbour" algorithms on highly distorted credit card fraud data is examined in this study. In the assessment, the applications of these methodologies' accuracy, sensitivity, precision, and specificity are examined. The findings show that the best accuracy attained by the classifiers, supported, respectively, by "Logistic Regression," "Naive Bayes," "K-Nearest Neighbour," and "Support Vector Machines," is 99.77%, 95.98%, 96.91%, and 97.53%.

The study paper by Trivedi *et al*., (2020), stated that Since the advent of modern technology developments and the highways of contemporary communications, fraudulent use of credit cards has dramatically increased. Financial analysis's primary focus on the underlying economic effects seems to be on spotting transactions that include credit card fraud. For both the individual and the financial institution, credit card fraud often results in annual losses of millions of dollars. Scammers are constantly seeking new guidelines and unethical ways to conduct their business. Therefore, it has become essential to use technological advances for fraud protection to shield financial institutions and other financial businesses from losses. The research study provides a machine learning-based approach with a feedback mechanism for identifying credit card fraud.

Its feedback strategy helps the classifier's detection to be improved cost-effectiveness. After

that, the performance of several techniques using slightly skewed credit card fraud data sets was studied. These approaches included **"Random Forest", "Tree Classification Techniques", "Artificial Neural Networks", "Support Vector Machines", "Naive Bayes", "Logistic Regression"** and **"Gradient Boosting Classifier"** algorithms. These data sets include credit card transaction data collected from 284,807 European account holders' purchases. Similarities exist between raw materials, including pre-processed items and these processes. For evaluating how effective specific techniques are, performance assessment measures such as the terms precision, recall, F1-score, accuracy and FPR percentage are utilised.

2.3.4 Deep Learning Approaches in Financial Fraud Detection:

According to Alghofaili *et al*., (2020), A growing number of businesses including the financial one, are providing their services online as internet usage rises tremendously. Financial fraud continues to be a major problem as it extends globally and increases in both number and diversity, resulting in enormous financial losses. Commercial systems for identifying fraud should be on the lookout for threats like unauthorised access and unanticipated attacks (Ravipati and Abualkibash, 2019). This issue has been thoroughly studied utilising data mining as well as machine learning approaches during the last few years. The aforementioned techniques still need to be improved to handle large amounts of data, compute quickly, and identify fresh attack patterns.

Therefore, the use of technology for the detection of financial wrongdoing is encouraged by a "Deep learning-based approach" that is based on "Long Short-Term Memory" (LSTM). This technology, which is specifically made for managing enormous datasets, attempts to improve the effectiveness and precision of existing fraud detection techniques. The proposed model is evaluated using an actual dataset of credit card frauds, and the results are contrasted with those of a deep learning model already in use called the Auto-encoder framework and other machine learning techniques (Singh *et al*., 2022). The trial results demonstrated the LSTM's perfect performance, achieving 99.95% dependability in less than a minute.

Numerous organisations, notably those in the financial industry, have integrated online services as a result of the Internet's usage growing rapidly. According to Chen et al. (2021), this rise in online financial activity has also significantly increased financial fraud throughout the world, causing huge losses. The use of data mining and machine learning techniques has recently increased in response to these problems. To strengthen the efficacy of these tactics, more

development is still required in some areas, such as broad data analytics, computing speed, and the detection of previously undetected attack patterns.

The **"Deep Convolution Neural Network" (DCNN)** based fraudulent activity identification approach is proposed in this study using a deep learning algorithm. In situations where there is a lot of data to analyse, this DCNN method can increase detection accuracy (Mehbodniya *et al*., 2021). The performance of the suggested model is tested to that of additional models based on deep learning, auto-encoder models and current machine learning models using a real-time dataset on fraudulent usage of credit cards. The recommended model has an accuracy for detection of 99% over some time equal to 45 seconds, as shown by the experimental results. Real-time data integration allows for the immediate detection of suspicious activity, while ensemble techniques, which combine many models, improve overall accuracy. The new study focuses on multi-class classification for diverse fraud types, even though binary classification (legitimate vs. fraudulent) is the standard. Deep learning techniques with promise include recurrent and convolutional neural networks. As fraud trends change, it is obvious that there are problems with imbalanced data and concept drift, which necessitate continual model adaptation. The literature provides an in-depth analysis of machine learning methods for identifying online payment fraud, highlighting their benefits, shortcomings, and potential future study areas.

2.3.5 Challenges and Solutions in Fraud Detection:

According to Itoo *et al*., (2021), Financial fraud is a concern that is becoming more urgent and has detrimental effects on the economy, collaborative institutions and government. Because of the development of Internet technology, payments made with credit cards are growing more quickly which results in a significant reliance on the internet. The usage of credit cards has increased along with technological advancements which have made fraud rates a burden for the economy (Wang *et al*., 2019). As additional safety precautions are being added to credit card transactions, fraudsters have developed new patterns or missed opportunities to track the transactions. Because of this, the conduct of both transactions that are legitimate and fraudulent is always improving. Additionally, it makes it difficult to predict fraudulent transactions due to the extremely unbalanced characteristics of credit card data. To get better outcomes, uneven or unbalanced data is beforehand processed employing the re-sampling (over-sampling or under-sampling) technique. The literature on "Machine Learning Techniques for Online Payment System Fraud Detection" analyzes the use of several machine learning techniques to improve

the precision of fraud detection in online payment systems in great detail. Researchers have examined supervised algorithms including decision trees, support vector machines, and neural networks utilizing historical data to construct prediction models for detecting fraudulent transactions. Unsupervised techniques, such as clustering and anomaly detection, have revealed transaction data's underlying patterns. For improved model performance, the significance of feature engineering—which takes transaction characteristics and user behaviour into account—is emphasized.

According to Shukur and Kurnaz, (2019), participating in online transactions quickly creates fictitious situations everywhere and results in significant losses for both personal and financial businesses. While there are many illegal actions taking place in the commercial sector, online clients are particularly concerned about fraudulent e-card operations, which are among the most prevalent. To verify the patterns and traits of suspicious and non-suspicious transactions backed by normalised and anomaly knowledge, data processing techniques were applied. Yet, victimisation classifiers employed **"machine learning (ML)"** techniques to automatically determine which transactions were suspicious and which weren't. The main topic of this study is supervised learning for categorization according to Fiore *et al*., (2019). Compared to the results obtained before preprocessing the dataset, all of the classifiers attained above 95.0% accuracy when the dataset was normalised and **"Principal Element Analysis"** was used.

2.3.6 Current Trends in Fraud Detection Techniques:

According to Sadgali *et al*., (2019), in the financial industry, financial fraud is becoming a more significant concern with dire repercussions. Financial organisations must thus constantly enhance their fraud detection systems. Machine learning and data mining approaches have been employed in multiple research in recent years to address this issue. In addition to detection and prevention methods including regression, clustering, and classification that have been suggested in the literature, we present a state-of-the-art on a variety of fraud strategies in this work. Finding the strategies and approaches that provide the best outcomes that have been refined to date is the goal of this research.

According to Kute *et al*., (2021), for many years, money laundering has been a huge global concern that poses a significant risk to both the economy and society. Although the government, financial institutions, and regulators are all working together to combat it, the report nonetheless highlights the billions of dollars that the authorities have fined. Financial

institutions can now provide a better client experience through multi-channel interactions thanks to high-speed internet connections, which have caused an exponential surge in transaction volume and opened up new channels for money laundering for scammers (Baesens *et al*., 2021). Research on **"Deep Learning (DL)"** approaches is restricted, mostly because of the lack of model interpretability and explainability of the judgements taken. However, the literature demonstrates the use of statistical methods, data mining, and **"Machine Learning (ML)"** techniques for money laundering detection.

2.3.7 Blockchain-based Cryptocurrency Systems and Anomaly Detection:

According to Sayadi *et al*., (2019), today's positive perception of this technology has led to a rise in the popularity of electronic transactions via **"blockchain-based cryptocurrency systems"**. Notwithstanding its positive image, these coins carry significant dangers and abnormalities. The researchers provide a novel model in this study for electronic transaction anomaly detection over Bitcoin. Both the **"One-Class Support Vector Machines (OCSVM)"** technique for outlier detection and the **"K-Means algorithm"** for grouping comparable outliers with similar types of anomalies are machine learning algorithms that we employed in our proposal. Accuracy performance results were high, indicating that our effort was assessed through the generation of detection findings.

The analysis of the literature on "Machine Learning Techniques for Online Payment System Fraud Detection" reveals a significant body of work emphasizing the efficiency of machine learning in detecting fraudulent acts in online payment systems. According to Habeeb *et al*., (2019), real-time anomaly detection and categorization algorithms are essential. Lopez-Garcia *et al*., (2019) recommendation for handling imbalanced datasets is to use ensemble classifiers. As demonstrated by Chen and Lai, (2021), convolutional neural networks in particular are efficient in identifying transaction patterns.

2.3.8 Hybrid Approaches and Future Directions in Fraud Detection:

The currently published literature on "Machine Learning Techniques for Online Payment System Fraud Detection" examines the application of several machine learning algorithms to enhance the accuracy and efficacy of fraud detection in online payment systems. Researchers have delved into the use of supervised learning techniques, including decision trees, support vector machines, and neural networks, to construct prediction models that identify fraudulent transactions by looking at historical data trends. The relevance of feature engineering is

emphasized by Zebari *et al*., (2020), while Zhou, (2020, September) propose a hybrid approach that blends machine learning with rule-based approaches.

2.3.9 State-of-the-Art in Fraud Detection Literature:

Lund et al. investigated explainable AI in 2020 to increase decision-making transparency. Madabushi *et al*., (2020) provide methods like oversampling and cost-sensitive learning to address the problem of imbalanced data. Mazza *et al*., (2019, June) discover that more recent algorithms are more effective in identifying patterns when compared to older ones. Unsupervised learning techniques like clustering and anomaly detection have also been developed to uncover previously unnoticed patterns and abnormalities in transaction data. To enhance model performance, the literature highlights the relevance of feature engineering, which entails collecting and processing important data including transaction amount, location, and user behaviour. To address the dynamic nature of fraud, studies have examined the integration of real-time data streams into the detection process, providing for the quick identification of suspicious behaviours.

The research highlights the value of ensemble approaches, which mix numerous models to produce better detection accuracy. While the bulk of studies concentrate on categorizing transactions as either genuine or fraudulent on a binary basis, newer research also addresses multi-class classification to distinguish between distinct forms of fraud. Convolutional and recurrent neural networks are two examples of deep learning approaches that have been examined in the context of fraud detection and have shown promising results. The research does, however, address the problems with unbalanced datasets and idea drift, where fraud patterns evolve and require ongoing model adaption. The available literature gives a thorough review of the many machine-learning techniques used for online payment system fraud detection, highlighting their advantages, drawbacks, and prospective directions for further study.

2.4 Related Work

The research papers listed in Table 1 below provide a comprehensive overview of the various approaches and techniques used in detecting credit card fraud using machine learning and artificial intelligence. Khatri, Arora, and Agrawal (2020) delve into supervised learning algorithms to differentiate between legitimate and fraudulent transactions, while Dornadula and Geetha (2019) develop a unique algorithm using streaming transaction data to identify behavioural patterns indicative of fraud. Asha and KR (2021) explore the use of SVM, KNN,

and ANN in predicting payment fraud, emphasizing the versatility of machine learning techniques. In a similar vein, Adepoju, Wosowei, and Jaiman (2019) evaluate multiple fraud detection methods, focusing on their sensitivity, accuracy, precision, and specificity. Trivedi, Simaiya, Lilhore, and Sharma (2020) investigate various methods using slightly distorted datasets, assessing crucial metrics like recall, precision, F1-score, and the false positive rate (FPR) proportion.

Table 1: Comparison of the Literature

Author	**Name of the paper**	**Comments**
1. Khatri, Arora, and Agrawal., 2020 2.Dornadula and Geetha,2019	Credit Card Fraud Trends and ML Solutions	The study contrasts supervised learning algorithms for legitimate and fraudulent transactions
1. Asha and KR., 2021. 2. Berhane.et.al,2023	Fraudulent Activity Identification using ANN	The paper employs SVM, KNN, and ANN for predicting payment fraud.
1. Adepoju *et al*., 2019 2. Trivedi, Simaiya, Lilhore, and Sharma., 2020.	Machine Learning for Online Fraud Detection	The study explores methods, assessing recall, precision, F1-score, efficiency, and FPR.
1. Alghofaili, Albattah, and Rassam., 2020. 2. Chen and Lai, 2021	Deep Learning Approaches in Financial Fraud Detection	This paper Enhances precision, and speed in data with deep learning, specifically LSTM.
1. Itoo, Meenakshi and Singh, 2021. 2. Shukur and	Challenges and Solutions in Fraud Detection	The study applies Naïve Bayes, logistic regression, and K-nearest neighbour algorithms.

Kurnaz,2019		
1. Sadgali, Sael, and Benabbou, 2019. 2. Kute, Pradhan, Shukla, and Alamri, 2021.	Current Trends in Fraud Detection Techniques.	Positive view fuels blockchain transactions; risks and abnormalities accompany popularity.
1. Sayadi, Rejeb, and Choukair, 2019 2. Habeeb et al., 2019.	Blockchain-Based Cryptocurrency and anomaly detection	In our study, OCSVM and K-Means detect outliers and group anomalies.
1. Zhou,2020 2. Zebari et al., 2020	Hybrid Approaches and Future Directions in Fraud Detection	Explores ML to boost fraud detection in online payments, using various techniques.
1. Mazza et al., 2019 2 Lund et al., 2020	State-of-the-Art in Fraud Detection Literature	This paper is used to Enhance transparency; it addresses imbalanced data.

Continuing this trend, Alghofaili, Albattah, and Rassam (2020) suggest a deep learning-based approach using Long Short-Term Memory (LSTM) to enhance identification precision in large datasets. Chen and Lai (2021) propose a Deep Convolution Neural Network (DCNN) model that achieved a 99% detection accuracy on a real-time credit card fraud dataset. Itoo, Meenakshi, and Singh (2021) compare logistic regression, Naïve Bayes, and K-nearest neighbour algorithms, while Alenzi and Aljehane (2020) focus on logistic regression for fraud detection in credit cards. Taha and Malebary (2020) optimize a light gradient boosting machine (LightGBM) for credit card fraud detection, and Shukur and Kurnaz (2019) highlight the prevalence of fraudulent e-card operations in online transactions. The studies by Fiore, De Santis, Perla, Zanetti, and Palmieri (2019), Sadgali, Sael, and Benabbou (2019), Kute, Pradhan, Shukla, and Alamri (2021), and Sayadi, Rejeb, and Choukair (2019) further enrich this body of work by exploring various aspects of fraud detection, from generative adversarial networks

and anomaly detection to the challenges posed by the rise of electronic transactions and blockchain-based cryptocurrency systems.

CHAPTER 3 METHODOLOGY

3.1 Introduction

The approach used in our work to improve fraud detection in online payment systems using machine learning techniques is covered in detail in this chapter. Beginning with a description of the dataset utilised for model training and assessment, we lay out the methodical methodology taken to fulfil our research goals. We next go into depth about the data's pretreatment methods, which included feature engineering and data separation. After that, we go into choosing and setting up machine learning algorithms and give the assessment measures for gauging model performance. This chapter acts as a thorough explanation of the research techniques used, assuring objectivity and rigour in the conduct of our study.

3.2 Dataset

In this study, I have taken this dataset from Kaggle and the link is https://www.kaggle.com/datasets/ealaxi/paysim1. There are 11 columns and 6362620 rows are present in the dataset. There are no null values present in the dataset. The attributes are step, type, amount, nameOrig, oldbalanceOrg, newbalanceOrig, nameDest, oldbalanceDest, newbalanceDest, isFraud and isFlaggedFraud.

3.3 Data Pre-processing

Pre-processing the data is essential for machine learning. This aspect must be taken into account in the model we are employing, and it must also be compared to earlier models we have created. When cleaning up raw datasets, pre-processing techniques are widely utilised. I used pre-processing techniques to remove extra data during the training phase, which will enhance the functionality of the system. Engineering features for our implementation were quite easy.

3.4 Exploratory Data Analysis:

The exploratory data analysis (EDA) step of our study is crucial because it allows us to carefully assess and comprehend the properties of our dataset. The effectiveness of our machine learning models for detecting online payment fraud is eventually improved by EDA, which offers insightful information about the distribution of the data, the correlations between variables, and subsequent data preparation and feature engineering decisions.

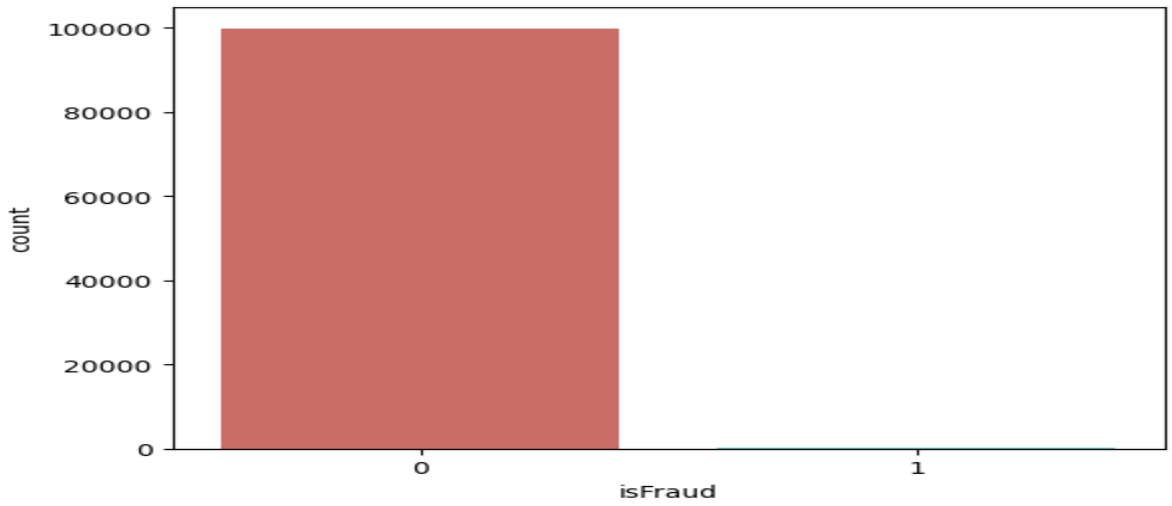

Figure 3.1: Countplot for isFraud

In the above figure here count plot is plotted for isFraud here for 0 I get the highest count as compared to 1, here data is not balanced.

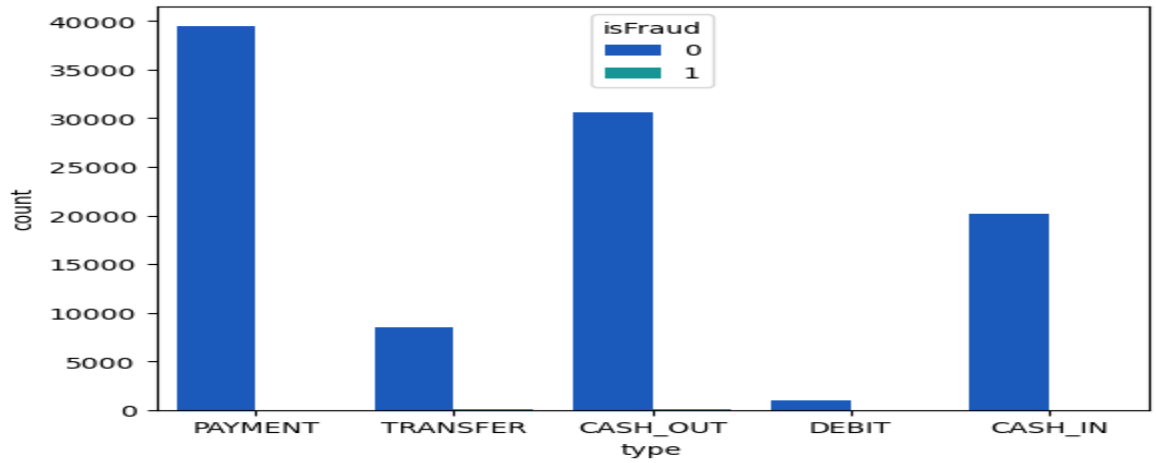

Figure 3.2: Countplot for Type with IsFraud

In the above image, the count plot is shown for the type with IsFraud; the blue and other colours denote IsFraud 0 and 1, respectively. I receive the greatest count for the Payment type here among all types, with Isfraud 0 having the highest count in comparison to Isfraud 1.

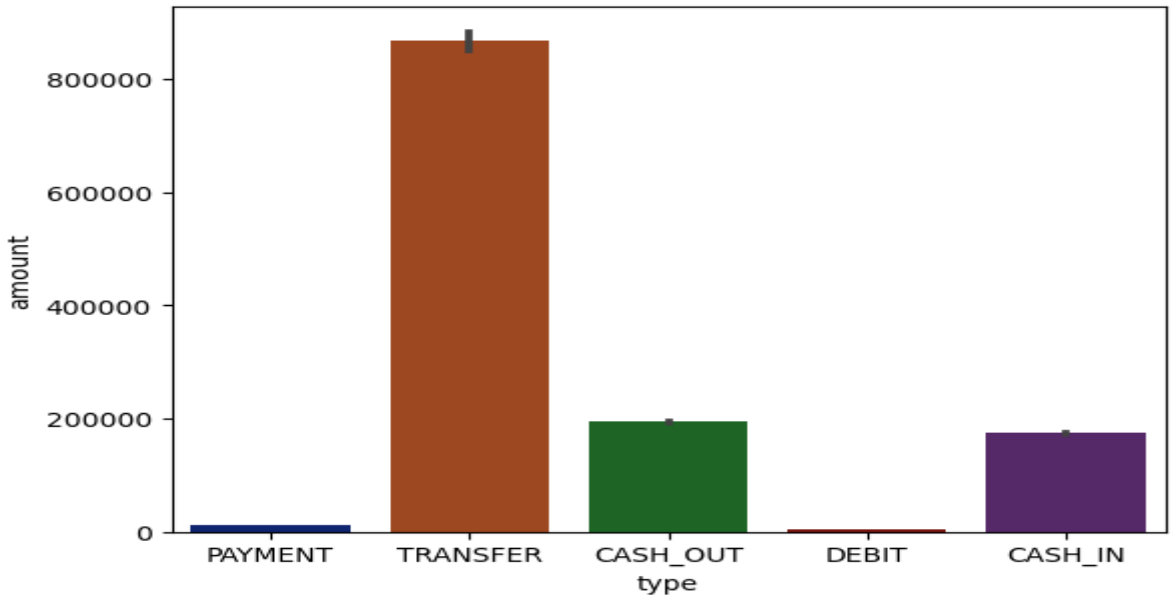

Figure 3.3: Barplot for type and amount

A barplot showing the distribution of transaction kinds (such as "transfer," "debit," and others) and associated transaction amounts is shown in the figure. Especially noteworthy is that the "transfer" transaction type has the highest frequency, indicating that it is the most typical transaction type in the dataset. The "debit" transaction type, on the other hand, is linked to the lowest average transaction amount, indicating that, generally speaking, debit transactions entail lower monetary values when compared to other transaction kinds. This visualisation offers a useful first look at the dataset's structure, assisting in the identification of common transaction types and their corresponding financial patterns, which may be crucial in financial analysis and decision-making settings.

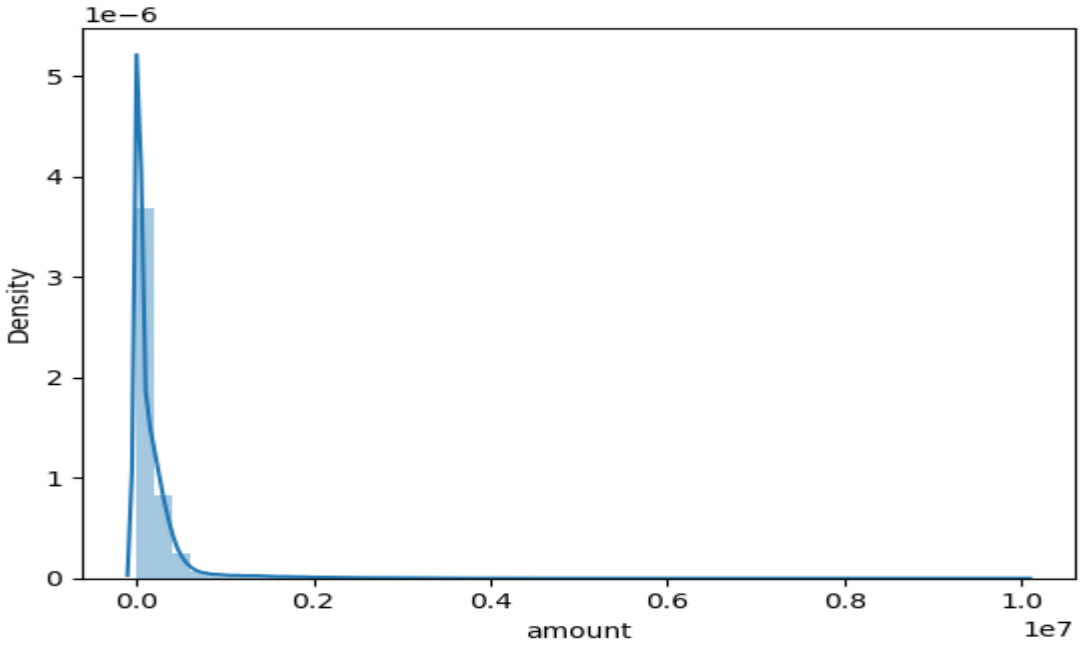

Figure 3.4: Distplot for an amount

The distribution of a continuous variable, in this example the transaction amounts, is frequently represented by this kind of figure. The distribution's form, any peaks or modes, as well as the spread and skewness of the 'amount' data, would all be depicted in the ensuing graphic. Understanding the major patterns and variability within the transaction amount data in your fraud detection analysis may be a beneficial tool.

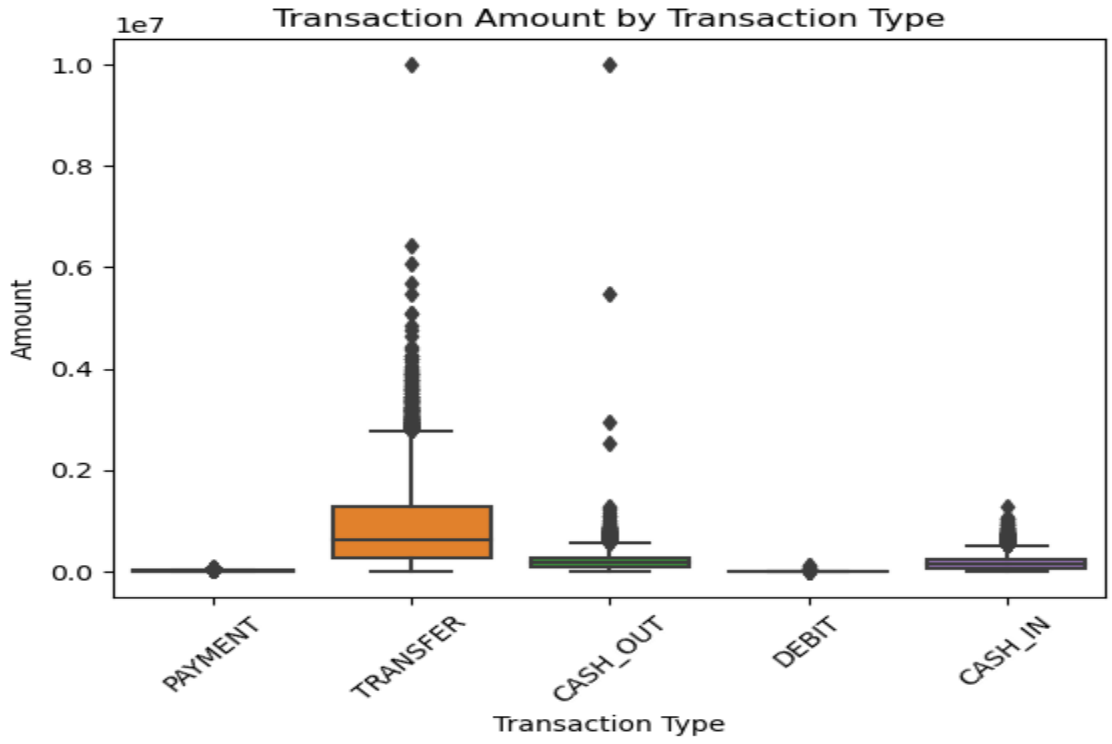

Figure 3.5: Boxplot for Amount and Type

A horizontal line inside a rectangular box that represents the interquartile range (IQR) of the data in a boxplot designates the median value. The "whiskers" that protrude from the box are the values that fall between the minimum and highest values within a given range (usually 1.5 times the IQR). Any data points that are outside of this range and are shown independently as points are considered outliers. This kind of visualisation can highlight possible outliers or changes in the spread and central tendency of the data across various transaction kinds and aid in understanding the distribution of transaction amounts for each transaction type.

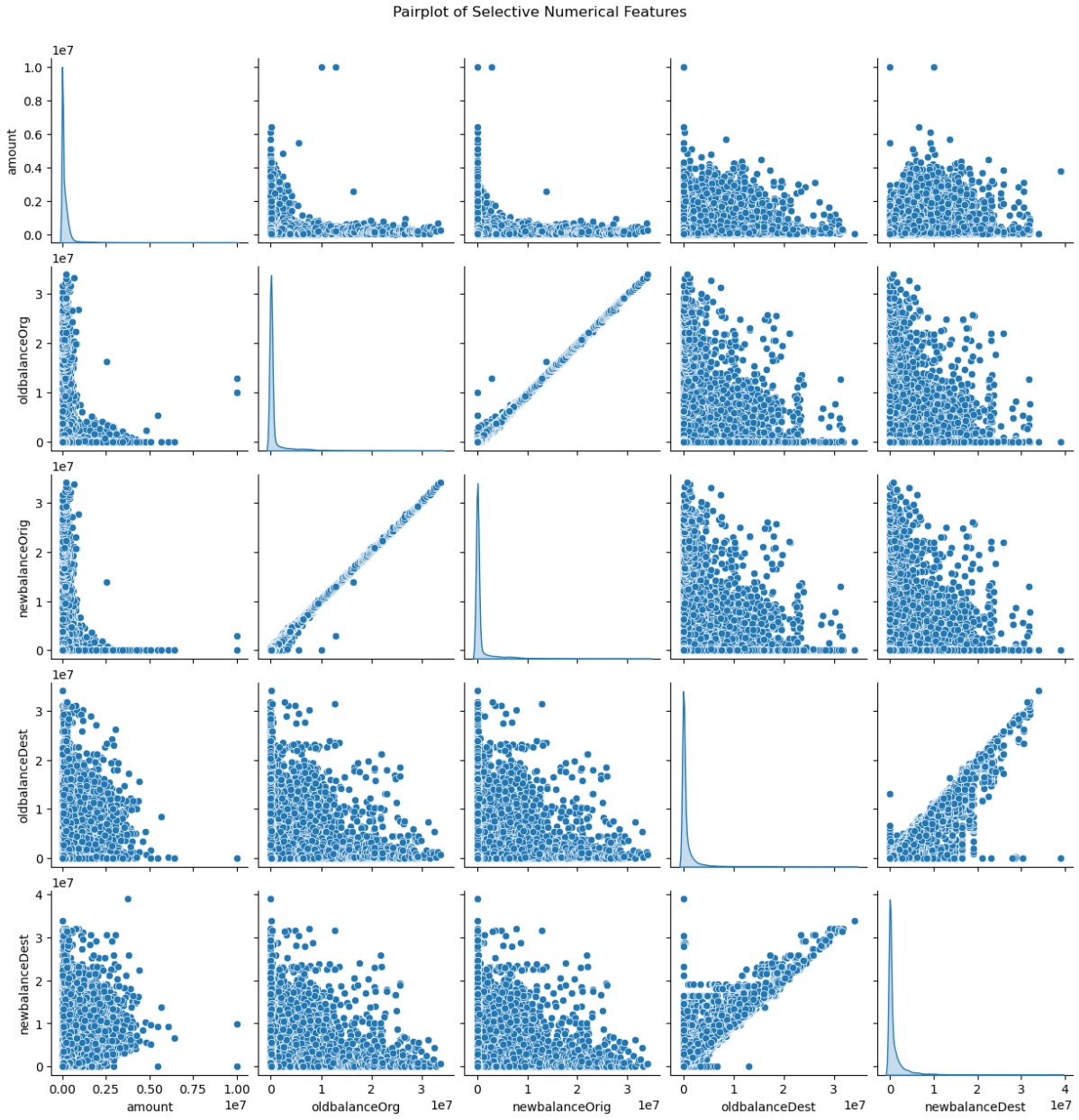

Figure 3.6: Pairplot for Dataset

In this pair plot, the diagonal elements display scatterplots to show the relationships and correlations between these numerical features, while the off-diagonal elements display kernel density estimate (KDE) plots to represent the estimated probability density for each feature.

A pair plot is an effective tool for understanding how several numerical variables interact with one another in a dataset. They aid in the discovery of possible trends, correlations, and distributions across variables, which helps comprehend the data and guides additional analysis or modelling choices in our fraud detection project.

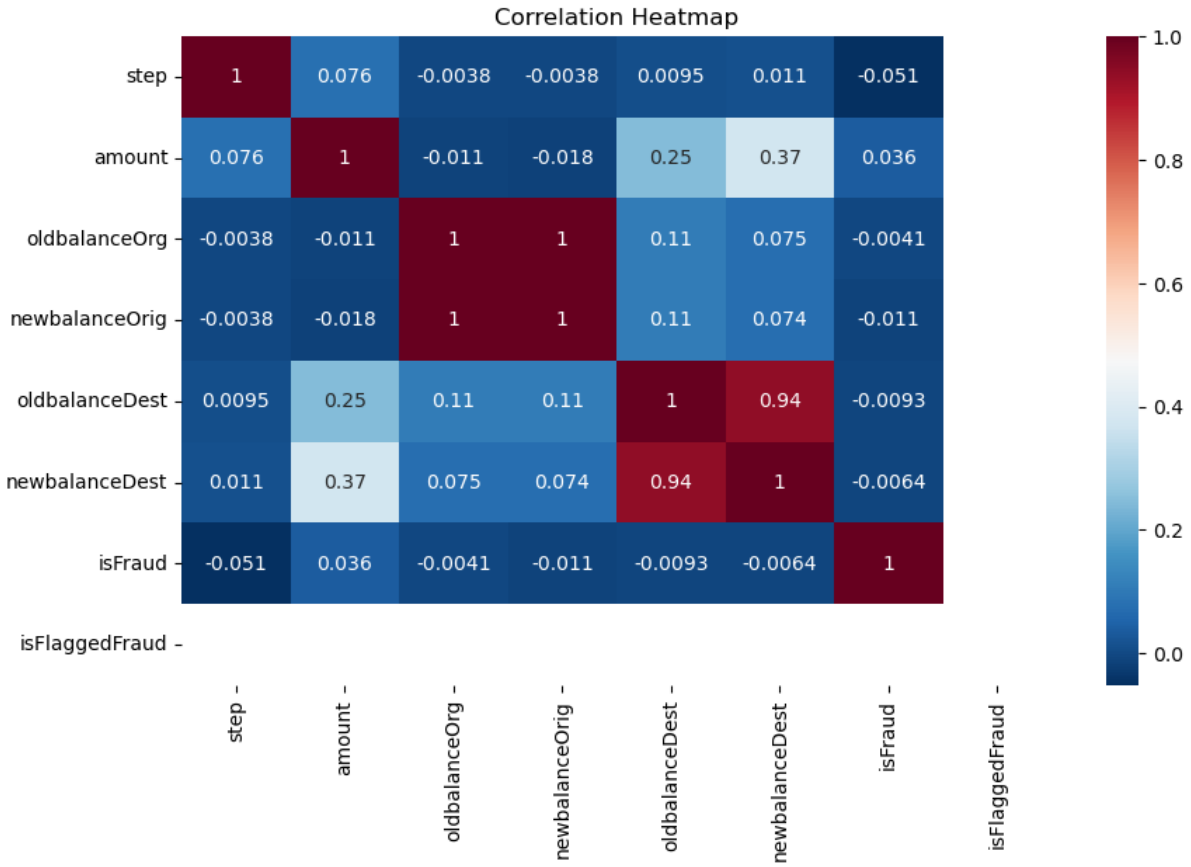

Figure 3.7: Correlation Heatmap

These coefficients are represented as a heat map to show the strength of the correlations among various parameters. The best qualities for the creation of machine learning models may be found with the help of this visualisation. The correlation matrix is converted into a colour-coded representation via the heat map. The correlation matrix of numerical variables in a dataset is represented visually by a correlation heatmap. The intensity and direction of the correlations between the pairs of variables are represented by colours. Each heatmap cell shows the correlation between two variables, with positive correlations commonly represented by warmer colours and negative correlations by colder hues. We may easily find patterns and

relationships between variables with the use of the heatmap. Strong correlations between two variables might either imply that when one increases, the other tends to increase as well, or that when one grows, the other tends to decline. Weak or almost zero correlations between variables imply a tenuous or nonexistent linear link.

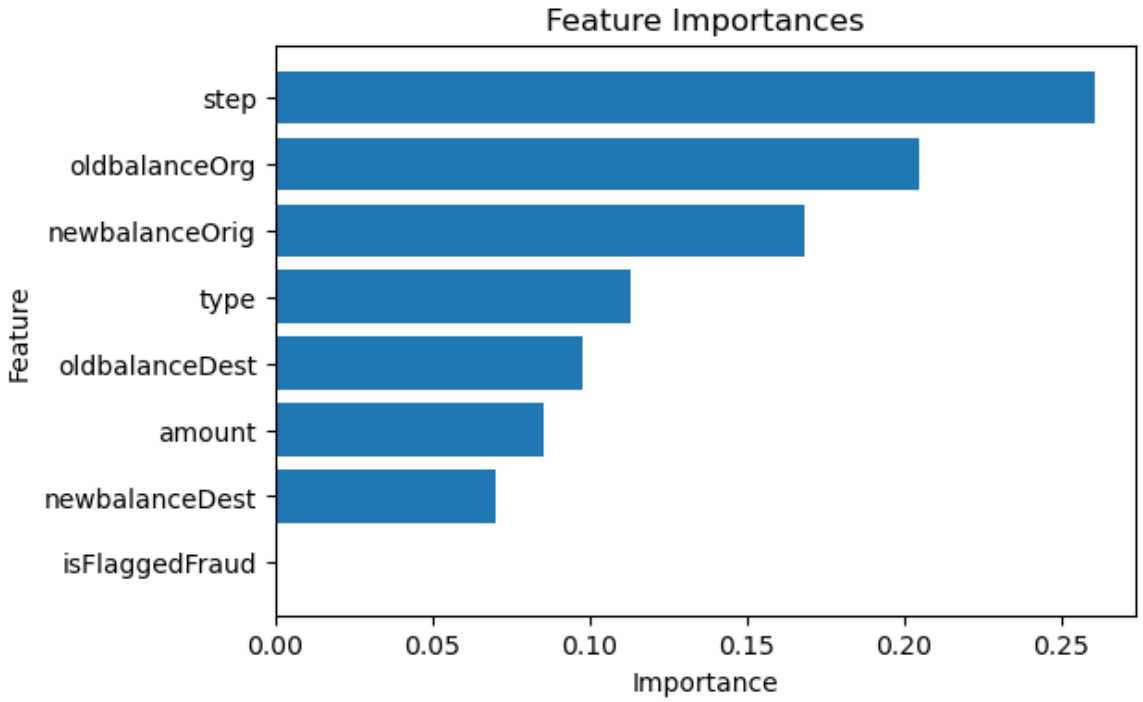

Figure 3.8: Feature Importance

The predictive performance of the machine learning model is assessed using the feature importance analysis, which quantifies the relevance of each feature. The findings show that the step characteristic has the most significance and considerably enhances the model's predictions. Then come "oldbalanceOrg" and "newbalanceOrig," which are equally important in the decision-making process of the model. The 'type' of transaction is somewhat significant, which implies that the kind of transaction may have an impact on the results of fraud detection. 'OldbalanceDest' and 'amount' contribute to a lesser extent, although 'newbalanceDest' has a lower significance value. It's interesting that 'isFlaggedFraud' is deemed to be of minimal value, indicating that it might not have a substantial influence on the model's predictions of fraud detection. For improved fraud detection, these insights can guide feature selection and model optimisation efforts.

3.4 Classification

To classify the specified characteristics as either fraud or non-fraud, classification methods are utilised. In my work, I classified things with the strategy below:

3.4.1 Gradient Boosting

An effective ensemble approach called gradient boosting turns poor learners become strong ones. The main goal is to reduce the mean square error or cross-entropy of the preceding model's loss function. Each succeeding model is trained using gradient descent to do this. We determine the gradient of the loss function concerning the forecasts produced by the current ensemble in each iteration. The gradient is then decreased by training a new weak model. The ensemble is then updated with the new model's predictions, and the cycle is repeated until a predetermined stopping condition is satisfied.

3.4.2 Adaboost

The ensemble learning method AdaBoost, short for Adaptive Boosting, is used in machine learning for classification and regression issues. AdaBoost's primary principle is to iteratively train a weak classifier on a training dataset, with each subsequent classifier assigning greater weight to the misclassified data points. Combining all of the weak classifiers used for training with the weights assigned to the models based on their accuracy results in the final AdaBoost model. The model with the lowest accuracy is given a lower weight, and the weakest model with the best accuracy is given the highest weight.

3.4.3 Random Forest

Machine learning techniques like Random Forest are highly advised since they involve no modelling or data preparation and often produce accurate results. Random forests are built on the decision trees explained in the preceding section. To be more precise, decision tree collections known as Random Forests produce more precise forecasts. Because it primarily consists of a group of decision trees, it is referred to as a "forest." The basic idea is to construct several decision trees from various independent subsets of the dataset. It is decided which n variables, randomly selected from the feature set at each node, should be divided the best.

3.4.4 Multi-Layer Perceptron

A neural network with numerous linked layers called a multi-layer perceptron, or MLP for short, is capable of efficiently converting input data from one dimension to the required dimension. This neural network architecture is distinguished by its various layers, and the connections between the neurons within these layers allow some of their outputs to function as inputs, resulting in a complicated neural network. The Scikit Learn library has a class called

MLP Classifier that may be used to train a multi-layer perceptron (MLP) neural network for classification problems. An MLP is a particular kind of feedforward neural network made up of several layers of neurons coupled to one another. For specifying the network architecture, training the model, and assessing its performance, the MLP Classifier class offers several choices. It may be applied to a variety of classification tasks, such as the categorization of time series, text, and images.

3.4.5 Artificial Neural Network

The phrase "artificial neural network" refers to a particular field of artificial intelligence (AI) that is strongly influenced by the complex structure and operation of the human brain. Artificial neural networks were created as painstakingly designed computer simulations to closely resemble the organic neural networks inherent to the complex architecture of the human brain. These artificial neural networks are essentially made up of synthetic neurons, also known as nodes or units, which have been painstakingly joined in a way resembling the complex network of real neurons present in the brain.

The main goal of these networks is to imitate the fundamental rules dictating how real neurons transfer signals and process information in the human brain using a computational approach. Artificial neural networks have been specifically designed to execute a wide range of activities and handle enormous quantities of information with amazing efficiency by precisely simulating this complex brain connection and information processing. Essentially, these networks are a significant advancement in the field of artificial intelligence since they are a potent tool for resolving difficult issues and improving our comprehension of various cognitive and computational processes.

3.5 Overall workflow

Creating a machine learning-based solution for online payment system fraud detection is the project's overall workflow. Data collection and preparation, such as feature engineering and data segmentation, are the first steps. On the preprocessed data, several machine learning algorithms are taught. The effectiveness of the model is then assessed using measures including accuracy, precision, recall, and F1-score. The best machine learning model is chosen using the information gleaned through exploratory data analysis and correlation analysis.

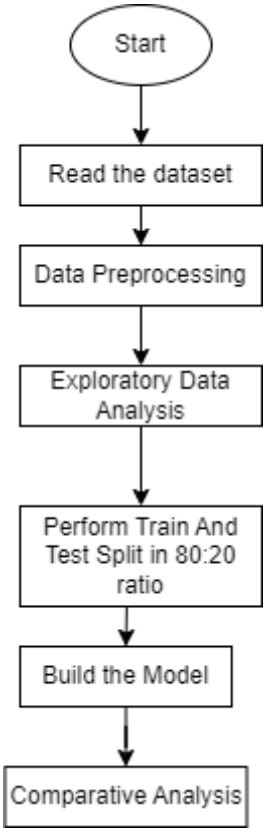

Figure 3.9: Overall workflow

(Source: Author's Creation)

3.6 Summary

This study's methodology for detecting fraud in online payment systems uses a systematic approach. It starts with data collecting that includes transactional information. Later data preparation methods are used, such as feature engineering and data splitting. Then, a variety of machine learning algorithms are trained and evaluated for performance using accepted measures like accuracy, precision, recall, and F1-score, including Random Forest, Gradient Boosting, AdaBoost, MLP, and ANN. Insights gained from exploratory data analysis and correlation analysis serve as the basis for these evaluations. These observations are taken into account while choosing the best machine-learning model. Following thorough testing, error analysis, and model interpretability and computational efficiency concerns.

CHAPTER 4 RESULTS

Synthetic Financial Datasets play a critical role in the development and evaluation of online fraud detection systems. In my study, I utilised a dataset that was divided into the categories of fraud and non-fraud, and I used the random forest, decision tree, and gradient boosting algorithms to evaluate how well my suggested technique worked. To evaluate the effects of my suggested improvements, I examined performance indicators including Accuracy, Confusion Matrix, Precision, Recall, and F1 Score. I was able to measure performance measures like accuracy and precision by removing these variables from my code, which allowed me to assess how well my suggested fixes worked.

This chapter provides the result of an analysis of the machine learning methods that were employed. The following results are from several machine learning models:

Precision, Recall, F1 score, Confusion Matrix and Accuracy of the models:

After creating the dataset, we went ahead and used it to train the models. Careful analysis of each model's performance produced results for each approach. For each model, we thoroughly evaluated important parameters such as Accuracy, Precision, Recall, F1-score, and the Confusion Matrix. We were able to identify the model that had the greatest degree of performance in fraud detection because of this thorough study.

4.1 Results for Random Forest

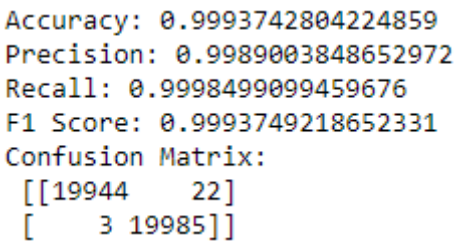

Figure 4.1: Result for Random Forest

In the above figure, here for random forest, I get 0.99 accuracy, 0.99 precision, recall and f1 score.

4.2 Results for Gradient Boosting

```
Accuracy: 0.9887620763878461
Precision: 0.9824682700380266
Recall: 0.9952971783069842
F1 Score: 0.9888411163854165
Confusion Matrix:
 [[19611   355]
 [   94 19894]]
```

Figure 4.2: Result of Gradient Boosting

In the above figure for the gradient boosting model, I get the accuracy, precision and f1 score of 0.98 and recall is 0.99.

4.3 Results for Adaboost

```
Accuracy: 0.9660859988987336
Precision: 0.9567135643904113
Recall: 0.9763858314988993
F1 Score: 0.9664496001188502
Confusion Matrix:
 [[19083   883]
 [  472 19516]]
```

Figure 4.3: Result for Adaboost

In the above figure for adaboost, accuracy and f1 score is 0.96, precision is 0.95 and recall is 0.97.

4.4 Results for MLP

```
Accuracy: 0.9831306001902188
Precision: 0.9849352214522447
Recall: 0.9812887732639584
F1 Score: 0.9831086161094682
Confusion Matrix:
 [[19666   300]
 [  374 19614]]
```

Figure 4.4: Result for MLP

In the above figure for multi-layer perception accuracy, precision, recall and f1 score is 0.98.

4.5 Results for ANN

```
Accuracy: 0.9599289182559944
Precision: 0.9598819468760943
Recall: 0.9600260156093656
F1 Score: 0.9599539758373146
Confusion Matrix:
 [[19164   802]
 [  799 19189]]
```

Figure 4.5: Result For ANN

In the above figure, for artificial neural network accuracy, precision and f1 score is 0.959 and recall is 0.96.

After evaluating all machine learning algorithms in the aforementioned picture, I found that random forest has the best accuracy in comparison to other algorithms.

CHAPTER 5 FINDINGS

The results of our investigation will be covered in detail in this chapter, with an emphasis on the findings of our research. We will carefully assess how these findings square with the original study aims and hypotheses that guided our inquiry.

5.1 Random Forest

The Random Forest Classifier's findings for detecting fraud in online payment systems are quite encouraging. The algorithm is extraordinarily good at properly categorizing transactions as either fraudulent or real, as seen by the accuracy score of almost 99.94%. The model's capacity to minimise false positives, which is essential in preventing legal transactions from being mistakenly reported as fraudulent, is shown in the accuracy score of around 99.89%. The model's ability to identify virtually all real fraudulent transactions while minimizing false negatives is demonstrated by the recall score of roughly 99.99%. Precision and recall are balanced by the F1 Score, which is roughly 99.94%. The model performs admirably, with a small percentage of misclassifications, as shown by the confusion matrix. 3 transactions were anticipated to be fraudulent but turned out to be fraudulent, compared to 22 transactions that were expected to be fraudulent but weren't.

5.2 Gradient Boosting

The Gradient Boosting Classifier performed well in the job of detecting fraud in an online payment system, obtaining an accuracy of 98.88%. This shows that the majority of transactions were correctly categorised by the model. The model's ability to avoid wrongly classifying valid transactions as fraudulent is demonstrated by the precision score of 98.25%, which denotes a remarkably low rate of false positives. Furthermore, the model successfully detected a substantial fraction of real fraudulent transactions, minimising false negatives, as shown by the high recall score of 99.53%. With an F1 score of 98.88%, the accuracy and recall are well-balanced. Although there are occasional misclassifications, as shown by the confusion matrix, the model performs well overall, helping to increase the security of online payment systems. 355 transactions were anticipated to be fraudulent but turned out to be fraudulent, compared to 94 transactions that were expected to be fraudulent but weren't.

5.3 Adaboost

With an accuracy of 96.61%, the AdaBoost Classifier has demonstrated outstanding performance in the area of online payment system fraud detection. This indicates that a sizable

number of the transactions were correctly categorised by the model. The model is effective at minimising the misclassification of genuine transactions as fraudulent, as indicated by the accuracy score of 95.67%, which also implies a reasonably low number of false positives. The recall score of 97.64% further indicates that the model successfully detected the bulk of real fraudulent transactions, hence lowering the percentage of false negatives. At 96.64%, the F1 score exhibits a balanced performance in terms of recall and precision. Although the confusion matrix reveals certain misclassifications, overall, the AdaBoost Classifier helps to improve the safety of online payment systems. 883 transactions were anticipated to be fraudulent but turned out to be fraudulent, compared to 472 transactions that were expected to be fraudulent but weren't.

5.4 MLP

With an accuracy of 98.31%, the MLP (Multi-Layer Perceptron) Classifier has shown remarkable performance in the area of online payment system fraud detection. This demonstrates that a sizable number of the transactions were correctly categorised by the model. With an accuracy score of 98.49%, the model significantly reduces the misclassification of genuine transactions as fraudulent, indicating a low percentage of false positives. Furthermore, the model appears to detect the bulk of real fraudulent transactions, minimising the number of false negatives, as indicated by the high recall score of 98.13%. A balanced performance in terms of recall and precision can be seen in the F1 score, which is 98.31%. The confusion matrix shows occasional misclassifications, but generally, the MLP Classifier helps to increase the security of online payment systems. The number of transactions that were fraudulent but were expected to be non-fraudulent is 300, compared to the 374 transactions that were fraudulent but were expected to be non-fraudulent.

5.5 ANN

The Artificial Neural Network (ANN) has shown strong performance in the context of detecting fraud in online payment systems, with an accuracy of 95.99%. This suggests that a sizable number of the transactions were correctly categorised by the model. With an accuracy score of 95.99%, the model appears to efficiently reduce the misclassification of normal transactions as fraudulent. This is indicated by the low number of false positives. Additionally, the model's high recall score of 96.00% shows that it correctly classifies the majority of real fraudulent transactions, lowering the rate of false negatives. A balanced performance in terms of recall and precision is shown by the F1 score, which is 95.99%. The confusion matrix shows

some misclassifications, but overall, the ANN makes a positive contribution to improving the security of online payment systems. 802 transactions were fraudulent but were expected to be non-fraudulent, compared to 799 transactions that were fraudulent but were expected to be non-fraudulent.

Based on a comparison of every machine learning algorithm, it is shown that random forest obtains the maximum accuracy in comparison to other algorithms.

CHAPTER 6 EVALUATION AND CONCLUSION

The identification of fraudulent online transactions is one of the biggest problems facing modern banking and the Internet world. In this work, we developed some machine learning models and rigorously evaluated them across numerous datasets in light of the size and volume of data at our disposal. We made comparisons against a large, independent dataset to evaluate the models' real-time performance. We used the Synthetic Minority Oversampling Technique (SMOTE) to rectify the imbalance in the dataset.

In this study article, we presented the idea of online payment fraud detection. Online payment fraud has been highlighted as one of the major frauds in recent decades. It was discovered that feature selection methods are crucial and may be used to reduce the false positive rate. To determine if a certain transaction is fraudulent or not, we deployed some machine learning techniques, including Adaboost, Random Forest, Gradient Boosting, MLP, and ANN. If a particular transaction is fraudulent or not, a competent fraud detection system should be able to predict it with accuracy.

6.1 Limitations of the Study

Although our study is thorough, it does have some limitations. To begin with, despite the vast datasets utilised, they may not have comprehensively captured the dynamic and ever-changing landscape of online fraud. This absence of coverage may have led to the omission of certain fraudulent behaviours from the present study. Furthermore, it should be noted that although our machine-learning models demonstrated efficacy, their applicability to datasets or real-life situations beyond the scope of our testing environment may be limited. Another difficulty that arises is the issue of overfitting, which occurs when models exhibit remarkable performance on our datasets but fail to provide comparable outcomes in practical applications.

To mitigate the issue of imbalanced datasets, the Synthetic Minority Oversampling Technique (SMOTE) could not provide an accurate representation of the minority class, which might result in predictions that are skewed. Additionally, the emphasis on certain machine learning models may have inadvertently disregarded alternative methodologies that may have been equally efficacious.

6.2 Conclusion

Our study emphasised the usage of multiple machine-learning models to improve fraud detection in online payment systems. In this important domain, we investigated the

effectiveness of Random Forest, Gradient Boosting, AdaBoost, MLP, and ANN. The outcomes demonstrated that Random Forest demonstrated remarkable accuracy, precision, recall, and F1-score, making it a potential option for online payment fraud detection. AdaBoost and ANN produced decent results, while Gradient Boosting and MLP revealed equally impressive performance.

6.3 Discussion

Our results highlight the significance of choosing a machine learning model that is suitable and specifically matched to the needs of online payment fraud detection. In terms of precision, recall, and computing efficiency, each model had particular benefits and drawbacks. When organizations deploy fraud detection technologies, these insights can help them make wise judgements.

The impact of transaction-related features affecting model predictions was further underlined by feature importance analysis. The total efficacy of fraud detection systems is increased by understanding feature significance, which helps with feature selection and optimization.

Although the findings of our study were encouraging, it's vital to recognize the dynamic nature of fraud practices and the requirement for ongoing model monitoring and modifications. Further investigation into ensemble approaches, which combine the advantages of many models to provide even better accuracy and resilience, is also something we advise.

The insights obtained from our study are crucial for organizations looking to implement fraud detection systems. They provide a foundation for understanding which models might be most effective for their specific needs. Additionally, our research highlights the dynamic nature of online fraud, underscoring the need for continuous monitoring and updating of the models to keep pace with evolving fraud tactics.

The comparative performance of different models also opens up discussions about the best practices in model selection and implementation in the field of fraud detection. Our research contributes to the broader efforts to enhance security in digital payment ecosystems and provides a valuable reference for future studies in this domain.

Future Work

Future research on fraud analysis will monitor the system live and make performance assessments of the system in real-time by contrasting the new fraud rates with the manual

structure used prior to the smart blacklist system. Applying deep learning techniques following the results of performance measurement and new data size by evaluating the presence of new variables by new frauds will result in the calculation of the number of frauds missed in the online structure and the number of users labelled as fraudulent even though they are not fraudulent, and the outputs will then be compared.

REFERENCES

Adepoju, O., Wosowei, J. and Jaiman, H., 2019, October. Comparative evaluation of credit card fraud detection using machine learning techniques. In 2019 Global Conference for Advancement in Technology (GCAT) (pp. 1-6). IEEE.

Alenzi, H.Z. and Aljehane, N.O., 2020. Fraud detection in credit cards using logistic regression. International Journal of Advanced Computer Science and Applications, 11(12).

Alghofaili, Y., Albattah, A. and Rassam, M.A., 2020. A financial fraud detection model based on LSTM deep learning technique. Journal of Applied Security Research, 15(4), pp.498-516.

Asha, R.B. and KR, S.K., 2021. Credit card fraud detection using artificial neural network. Global Transitions Proceedings, 2(1), pp.35-41.

Baesens, B., Höppner, S. and Verdonck, T., 2021. Data engineering for fraud detection. Decision Support Systems, 150, p.113492.

Berhane, T., Melese, T., Walelign, A. and Mohammed, A., 2023. A Hybrid Convolutional Neural Network and Support Vector Machine-Based Credit Card Fraud Detection Model. Mathematical Problems in Engineering, 2023.

Bin Sulaiman, R., Schetinin, V. and Sant, P., 2022. Review of machine learning approach on credit card fraud detection. Human-Centric Intelligent Systems, 2(1-2), pp.55-68.

Cao, S., Yang, X., Chen, C., Zhou, J., Li, X. and Qi, Y., 2019. Titant: Online real-time transaction fraud detection in Ant Financial. arXiv preprint arXiv:1906.07407.

Chen, J.I.Z. and Lai, K.L., 2021. Deep convolution neural network model for credit card fraud detection and alert. Journal of Artificial Intelligence and Capsule Networks, 3(2), pp.101-112.

Chen, J.I.Z. and Lai, K.L., 2021. Deep convolution neural network model for credit card fraud detection and alert. Journal of Artificial Intelligence and Capsule Networks, 3(2), pp.101-112.

Demertzis, K., Iliadis, L., Tziritas, N. and Kikiras, P., 2020. Anomaly detection via blockchain deep learning smart contracts in industry 4.0. Neural Computing and Applications, 32, pp.17361-17378.

Dornadula, V.N. and Geetha, S., 2019. Credit card fraud detection using machine learning algorithms. Procedia computer science, 165, pp.631-641.

Fiore, U., De Santis, A., Perla, F., Zanetti, P. and Palmieri, F., 2019. Using generative adversarial networks for improving classification effectiveness in credit card fraud detection. Information Sciences, 479, pp.448-455.

Habeeb, R.A.A., Nasaruddin, F., Gani, A., Hashem, I.A.T., Ahmed, E. and Imran, M., 2019. Real-time big data processing for anomaly detection: A survey. International Journal of Information Management, 45, pp.289-307.

Khatri, S., Arora, A. and Agrawal, A.P., 2020, January. Supervised machine learning algorithms for credit card fraud detection: a comparison. In 2020 10th international conference on cloud computing, data science & engineering (confluence) (pp. 680-683). IEEE.

Kute, D.V., Pradhan, B., Shukla, N. and Alamri, A., 2021. Deep learning and explainable artificial intelligence techniques applied for detecting money laundering–a critical review. IEEE Access, 9, pp.82300-82317.

Lainjo, B., 2020. Network security and its implications on program management. International Journal of Safety and Security Engineering, 10(6), pp.739-746.

Lopez-Garcia, P., Masegosa, A.D., Osaba, E., Onieva, E. and Perallos, A., 2019. Ensemble classification for imbalanced data based on feature space partitioning and hybrid metaheuristics. Applied Intelligence, 49(8), pp.2807-2822.

Madabushi, H.T., Kochkina, E. and Castelle, M., 2020. Cost-sensitive BERT for generalisable sentence classification with imbalanced data. arXiv preprint arXiv:2003.11563.

Mazza, M., Cresci, S., Avvenuti, M., Quattrociocchi, W. and Tesconi, M., 2019, June. Rtbust: Exploiting temporal patterns for botnet detection on Twitter. In Proceedings of the 10th ACM conference on web science (pp. 183-192).

Mehbodniya, A., Alam, I., Pande, S., Netware, R., Rane, K.P., Shabaz, M. and Madhavan, M.V., 2021. Financial fraud detection in healthcare using machine learning and deep learning techniques. Security and Communication Networks, 2021, pp.1-8.

Ravipati, R.D. and Abualkibash, M., 2019. Intrusion detection system classification using different machine learning algorithms on KDD-99 and NSL-KDD datasets review paper. International Journal of Computer Science & Information Technology (IJCSIT) Vol, 11.

Sadgali, I., Sael, N. and Benabbou, F., 2019. Performance of machine learning techniques in the detection of financial frauds. Procedia computer science, 148, pp.45-54.

Sayadi, S., Rejeb, S.B. and Choukair, Z., 2019, June. Anomaly detection model over blockchain electronic transactions. In 2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC) (pp. 895-900). IEEE.

Shukur, H.A. and Kurnaz, S., 2019. Credit card fraud detection using machine learning methodology. International Journal of Computer Science and Mobile Computing, 8(3), pp.257-260.

Singh, A., Ranjan, R.K. and Tiwari, A., 2022. Credit card fraud detection under extreme imbalanced data: a comparative study of data-level algorithms. Journal of Experimental & Theoretical Artificial Intelligence, 34(4), pp.571-598.

Strielkowski, W., Vlasov, A., Selivanov, K., Muraviev, K. and Shakhnov, V., 2023. Prospects and Challenges of the Machine Learning and Data-Driven Methods for the Predictive Analysis of Power Systems: A Review. Energies, 16(10), p.4025.

Taha, A.A. and Malebary, S.J., 2020. An intelligent approach to credit card fraud detection using an optimized light gradient boosting machine. IEEE Access, 8, pp.25579-25587.

Trivedi, N.K., Simaiya, S., Lilhore, U.K. and Sharma, S.K., 2020. An efficient credit card fraud detection model based on machine learning methods. International Journal of Advanced Science and Technology, 29(5), pp.3414-3424.

Wang, D., Lin, J., Cui, P., Jia, Q., Wang, Z., Fang, Y., Yu, Q., Zhou, J., Yang, S. and Qi, Y., 2019, November. A semi-supervised graph attentive network for financial fraud detection. In 2019 IEEE International Conference on Data Mining (ICDM) (pp. 598-607). IEEE.

Zebari, R., Abdulazeez, A., Zeebaree, D., Zebari, D. and Saeed, J., 2020. A comprehensive review of dimensionality reduction techniques for feature selection and feature extraction. Journal of Applied Science and Technology Trends, 1(2), pp.56-70.

Zhou, C., 2020, September. A hybrid approach for coronary artery anatomical labelling in cardiac CT angiography. In Journal of Physics: Conference Series (Vol. 1642, No. 1, p. 012020). IOP Publishing.

APPENDICES

Code:

```
#Import all needed libraries
import numpy as np
import pandas as pd
import tensorflow as tf
import seaborn as sns
import matplotlib.pyplot as plt
from sklearn.model_selection import train_test_split
from sklearn.preprocessing import LabelEncoder
from imblearn.over_sampling import SMOTE
from sklearn.preprocessing import StandardScaler
from sklearn.ensemble import RandomForestClassifier, GradientBoostingClassifier, AdaBoostClassifier
from sklearn.neural_network import MLPClassifier
from sklearn.metrics import accuracy_score, precision_score, recall_score, f1_score, confusion_matrix
import warnings
warnings.filterwarnings('ignore')
```

```
#Read the dataset
df_fd = pd.read_csv("PS_20174392719_1491204439457_log.csv", nrows=100000)
df_fd.head()
```

```
#Checking the columns name
df_fd.info()
```

```
#Shape of dataset
df_fd.shape
```

```
#Statistical description
df_fd.describe()
```

```
#Drop the unwanted columns
df_fd.drop(['nameOrig','nameDest'],axis=1,inplace=True)
```

```
#Label Encoder
la=LabelEncoder()
df_fd['type']=la.fit_transform(df_fd['type'])
```

```
#Separate the dependent and independent variables
X=df_fd.drop('isFraud',axis=1)
y=df_fd['isFraud']
```

```
# Apply SMOTE for Handling Imbalanced Data
smote = SMOTE(random_state=42)
X_resampled, y_resampled = smote.fit_resample(X, y)
```

```
# Standard Scaling
scaler = StandardScaler()
X_scaled = scaler.fit_transform(X_resampled)
```

```
# Splitting the Data into Training and Testing Sets
X_train, X_test, y_train, y_test = train_test_split(X_scaled, y_resampled, test_size=0.2, random_state=42)
```

```
# Random Forest Classifier
rf_classifier = RandomForestClassifier(random_state=42)
rf_classifier.fit(X_train, y_train)
y_pred_rf = rf_classifier.predict(X_test)
```

```
# Print the results
print("Random Forest Classifier:")
print("Accuracy:", accuracy_score(y_test, y_pred_rf))
print("Precision:", precision_score(y_test, y_pred_rf))
print("Recall:", recall_score(y_test, y_pred_rf))
print("F1 Score:", f1_score(y_test, y_pred_rf))
print("Confusion Matrix:\n", confusion_matrix(y_test, y_pred_rf))
```

```
# Gradient Boosting Classifier
gb_classifier = GradientBoostingClassifier(random_state=42)
gb_classifier.fit(X_train, y_train)
y_pred_gb = gb_classifier.predict(X_test)
```

```
#Print the results
print("Gradient Boosting Classifier:")
print("Accuracy:", accuracy_score(y_test, y_pred_gb))
print("Precision:", precision_score(y_test, y_pred_gb))
print("Recall:", recall_score(y_test, y_pred_gb))
print("F1 Score:", f1_score(y_test, y_pred_gb))
print("Confusion Matrix:\n", confusion_matrix(y_test, y_pred_gb))
```

```
# AdaBoost Classifier
ada_classifier = AdaBoostClassifier(random_state=42)
ada_classifier.fit(X_train, y_train)
y_pred_ada = ada_classifier.predict(X_test)
```

```
#Print the Results
print("AdaBoost Classifier:")
print("Accuracy:", accuracy_score(y_test, y_pred_ada))
print("Precision:", precision_score(y_test, y_pred_ada))
print("Recall:", recall_score(y_test, y_pred_ada))
print("F1 Score:", f1_score(y_test, y_pred_ada))
print("Confusion Matrix:\n", confusion_matrix(y_test, y_pred_ada))
```

```
# MLP Classifier
mlp_classifier = MLPClassifier(random_state=42)
mlp_classifier.fit(X_train, y_train)
y_pred_mlp = mlp_classifier.predict(X_test)
```

```
#Print the Results
print("MLP Classifier:")
print("Accuracy:", accuracy_score(y_test, y_pred_mlp))
print("Precision:", precision_score(y_test, y_pred_mlp))
print("Recall:", recall_score(y_test, y_pred_mlp))
print("F1 Score:", f1_score(y_test, y_pred_mlp))
print("Confusion Matrix:\n", confusion_matrix(y_test, y_pred_mlp))
```

```
#ANN
ann = tf.keras.models.Sequential()
ann.add(tf.keras.layers.Dense(units=6, activation='relu'))
ann.add(tf.keras.layers.Dense(units=6, activation='relu'))
ann.add(tf.keras.layers.Dense(units=1, activation='sigmoid'))
ann.compile(optimizer = 'adam', loss = 'binary_crossentropy', metrics = ['accuracy'])
ann.fit(X_train, y_train, batch_size = 32, epochs = 10)
```

```
y_pred = ann.predict(X_test)
y_pred_ann = (y_pred > 0.5)
```

```
1249/1249 [==============================] - 5s 4ms/step
```

```
#Print the result
print("ANN:")
print("Accuracy:", accuracy_score(y_test, y_pred_ann))
print("Precision:", precision_score(y_test, y_pred_ann))
print("Recall:", recall_score(y_test, y_pred_ann))
print("F1 Score:", f1_score(y_test, y_pred_ann))
print("Confusion Matrix:\n", confusion_matrix(y_test, y_pred_ann))
```