UTS UNIVERSITY OF TECHNOLOGY SYDNEY

Optimising Credit Card Fraud Detection through Machine Learning and Deep Learning with Spatial-Temporal Imbalance Handling

by Nur Indah Lestari

Thesis submitted in fulfilment of the requirements for the degree of

Master of Science (Research) in the School of Computing Sciences

under the supervision of Associate Professor Walayat Hussain
Co-supervisor of Professor Jose Maria Merigo Lindahl

University of Technology Sydney
Faculty of Engineering and Information Technology

December 2024

CERTIFICATE OF ORIGINAL AUTHORSHIP

I, **Nur Indah Lestari** declares that this thesis is submitted in fulfilment of the requirements for the award of **Master of Science (Research) degree**, in the School of Computing Sciences at the University of Technology Sydney.

This thesis is wholly my own work unless otherwise referenced or acknowledged. In addition, I certify that all information sources and literature utilised herein are indicated in the thesis.

This document has not been submitted for qualifications at any other academic institution.

This research is supported by the Australian Government Research Training Program.

Production Note:
Signature removed prior to publication.

Nur Indah Lestari

Date: 12 December 2024

ABSTRACT

The sharp rise in online financial transactions during the recent epidemic has led to a record-breaking dependence on digital payment systems. Although this transformation provided a convenient solution, it also led to numerous challenges, such as increased financial scams. Therefore, a robust fraud detection system where individuals can perform online transactions seamlessly is an urgent requirement. This study aims to address the core problems associated with credit-card fraud detection, namely the "class imbalance challenge" that limits the effectiveness of conventional detection methods. The study notes that geolocation and temporal analysis adds an additional dimension to the fraud detection framework, thereby facilitating the identification of trends and irregularities that may otherwise remain undetected.

This research aims to develop and validate a novel approach for identifying credit card fraud. The study applied a mix of advanced Machine Learning (ML) and Deep Learning (DL) algorithms, data balancing approaches, and spatial-temporal attention systems to address the research problem. To achieve the objectives, the research first highlights the importance of data-balancing approaches in enhancing model performance within the context of unbalanced datasets. Second, we applied balancing approaches such as Random Over Sampling (ROS), Synthetic Minority Over-sampling Technique (SMOTE), Adaptive Synthetic Sampling (ADASYN), and Random Under Sampling as per the literature analysis, which significantly enhanced the models' capacity to detect fraudulent transactions. Subsequently, we implemented eight different machine learning algorithms, namely Bagging Classifier, Random Forest Classifier, CatBoost, Logistic Regression (LR), Extreme Gradient Boosting (XGBoost), AdaBoost, Gaussian Naive Bayes (GNB), and Extra Trees Classifier, along with two deep learning algorithms, namely Gated Recurrent Unit (GRU) and Neural Network (NN) executed. Finally, we conducted the performance measurements, namely Recall, Precision, F1 Score, ROC-AUC Score, and Accuracy, to evidence the success of these strategies.

The thesis provides a detailed examination of how machine learning and deep learning models perform in the detection of credit-card fraud, particularly emphasising the effects of data-balancing strategies. The Bagging Classifier and Random Forest Classifier models demonstrate remarkable proficiency, thus

attaining outstanding results in all metrics, which indicates their ability to accurately detect fraudulent transactions while maintaining the percentage of false positives at a minimum value. Ensemble approaches outperform simpler models such as LR. Despite exhibiting excellent accuracy, LR fails to identify instances of fraud, emphasising the limitation of relying exclusively on accuracy as a performance metric in datasets with imbalanced classes. The comprehensive evaluation also demonstrates that ensemble approaches exhibit more optimal resilience in solving class imbalance while maintaining elevated accuracy, precision, and recall levels. Consequently, they are highly suitable candidates for use in fraud-detection systems. The utilisation of ROC-AUC as an assessment criterion also demonstrates the capacity of these models to differentiate between fraudulent and non-fraudulent transactions at different thresholds, which is crucial in practical scenarios with high transaction volumes and significant consequences for misclassification. The results provide valuable insights into fraud detection, supporting an ensemble-based, multi-metric assessment method, thus creating systems that can effectively address the emerging hazards that characterize the digital financial industry.

ACKNOWLEDGEMENT

First, I would like to deeply acknowledge Allah SWT, the Most Gracious and the Most Merciful. I have successfully completed this endeavor, accomplished the goals I set, and surmounted the obstacles along my academic journey owing to His infinite mercy and guidance: all my accomplishments evidence His grace.

I am exceedingly thankful for my family's constant encouragement and support, especially that of my beloved parents. Their efforts and faith in my ability have been crucial. I will always be thankful to them for helping me become who I am through their affection and guidance.

I especially want to thank my super-husband, whose encouragement has been my the basis for my success. His unwavering support, trust in me, and motivation have been vital to my resilience. How he encourage me when I was at my weakest point has been a great source of strength. He has played a crucial role in my life, thereby enabling me to keep going and be successful in my endeavor.

I also acknowledge my son, the source of my happiness, for teaching me the real meaning of strength and patience. His presence is a continual reminder that, no matter how hard life gets, everything is all right. Undoubtedly, he is my greatest accomplishment and a constant source of inspiration in this world.

To my principal supervisor, Associate Professor Walayat Hussain, I would like to express my heartfelt gratitude; his guidance, insight, and constant support have been the cornerstones of my academic life. I am exceedingly blessed to have had him as my supervisor; his broad knowledge and outstanding expertise have immensely enriched my research acumen. 'Thank you' does not adequately convey my appreciation for his excellent guidance and support. As I delve into the research world, I will never forget how much he influenced me; may Allah SWT reward him for all his efforts.

I would such as to express my gratitude to my Co-Supervisor, Professor Jose Maria Merigo Lindahl, for his guidance and support during my research journey. His knowledge and insightful comments have been valuable throughout my academic journey.

For their valuable contributions to my research, I am very grateful to the expert Panel of my Candidature Assessment throughout my master’s research study, which comprised Dr Faezeh Karimi and Dr Maoying Qiao. They were crucial in enabling me to enhance my work: they provided insightful comments and helpful feedback. Their extensive expertise and willingness to share have substantially enhanced my comprehension. The time and effort they put into assisting me with my difficult research problems is much appreciated.

I would also such as to thank the University of Technology Sydney and The Australian Government for the scholarships that actualized my dream of pursuing this course of study. This scholarship not only provided the monetary support I needed to pursue my academic aspirations but also opened up a world of possibilities and opportunities. I am immensely appreciative of this opportunity to further my education and research, which has been a life-changing juncture in my academic career.

Finally, my thesis not only represents my effort but also symbolises the collective love, support, and guidance provided by the aforementioned individuals. I am exceedingly thankful for everything: these individuals have immeasurably facilitated my scholarly pursuit, thus enabling me to complete my master's research studies.

Nur Indah Lestari

LIST OF PUBLICATION

Book Chapter Publication

1. **Lestari, N.I.**, Hussain, W., Merigo, J.M. and Bekhit, M., 2024. Enhancing Credit Card Fraud Detection with Spatial-Temporal Analysis and Balanced Learning Approaches. In *Cutting-Edge Artificial Intelligence Advances: Implications in Real-World Applications*. (Accepted)

Conference Publication

2. **Lestari, N.I.**, Hussain, W., Merigo, J.M. and Bekhit, M., 2022, July. A Survey of Trendy Financial Sector Applications of Machine and Deep Learning. In *EAI International Conference, BigIoT-EDU* (pp. 619-633). Cham: Springer Nature Switzerland. (Published)

CONTENT PAGE

LIST OF FIGURES

LIST OF TABLES

1 INTRODUCTION

1.1 Overview of Credit-Card Fraud Detection

In the era of rapid technological advancement and economic globalisation, the usage of credit cards has increased drastically, which indicates an evolving trend towards online payment methods (Bian et al., 2023). However, all this convenience has been overshadowed by the growing number of sophisticated criminal activities aimed at gaining unauthorised access to account information and funds (Beju and Făt, 2023, Cheng et al., 2020a).

The increasing adoption of online shopping and electronic payment systems highlights the necessity for robust fraud detection techniques. Especially in the context of the COVID-19 epidemic, wherein there has been a noticeable surge in the utilization of digital payment methods and online transactions, criminals engaged in fraudulent activities have identified novel methods for conducting their illegal activities (Khan et al., 2023, Kizil et al., 2021, Ma and McKinnon, 2021). Therefore, financial institutions should maintain awareness in detecting and analysing emerging patterns of fraudulent activities. Furthermore, they must develop specific plans to effectively address this vice, thus protecting vulnerable customers.

As we explore the domain of digital financial transactions, it becomes evident that the ease provided by credit cards in the context of the globalised economy is a double-edged sword. The advancement in permitting effortless and borderless commerce has, in parallel, led to the emergence of increasingly intricate and extensive manifestations of financial fraud (Tut, 2023). The dynamic nature of credit card uses, combined with the unprecedented challenges presented by the COVID-19 epidemic (Kizil et al., 2021, Mekterović et al., 2021), has not merely modified consumer behavior but also revolutionised the methods utilised by those engaging in fraudulent activities (Randhawa et al., 2018), which makes it crucial to delve into the underlying complexities of this matter. Therefore, this study primarily aims to comprehend the more comprehensive framework and ramifications of credit-card theft within the contemporary globalisation era. To grasp the whole extent of Credit-Card Fraud, the broader consequences must be

considered as difficulties posed by economic globalisation and technological advancement, where Credit-Card Fraud is an urgent issue. The widespread acceptance and convenience of credit cards has contributed to their popularity and usage (Bian et al., 2023). The spike in credit-card usage has also led to an increase in criminal conduct, with fraudsters employing sophisticated techniques to obtain unauthorised access to account in-formation and funds (Cherif et al., 2023). The growing rate of Credit-Card Fraud can be linked to a number of factors, such as the popularity of credit card transactions and the transition towards online payment systems (Khan et al., 2023). With the widespread utilization of e-commerce and digital payment platforms, the necessity for accurate fraud-detection techniques has become most urgent (Bhattacharyya et al., 2011).

The existing problem has been exacerbated the COVID-19 pandemic, which has significantly impacted the global economy and accelerated the transition towards digital payments and online transactions (Tut, 2023, Kizil et al., 2021). Consequently, Credit-Card Fraud spiked during this time period, with fraudsters manipulating the economic crisis to target vulnerable individuals and enterprises. Due to social distancing measures and stay-at-home instructions, the pandemic has lead to an unprecedented surge in online purchasing (Mekterović et al., 2021),which has enabled cybercriminals to capitalize on weak points in online payment systems and target unsuspecting consumers (Bandyopadhyay and Dutta, 2020).

In another study, Cheng et al. (Cheng et al., 2020a), proposed a conventional framework for detecting fraudulent activities that are commonly implemented in commercial systems, as presented in Figure 1. Upon successful card verification, financial institutions such as VISA, MasterCard, and Citibank utilise an online predictive model to evaluate every transaction.

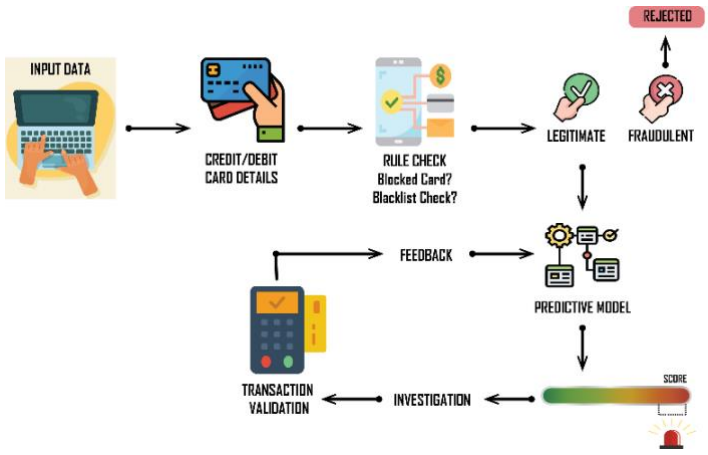

Figure 1. The framework of Credit-Card Fraud detection

In contrast to a basic rule-checking system that emphasises card blacklists, budgetary assessments, and fraud regulations, the predictive model is constructed to autonomously identify fraudulent patterns and to generate a score indicative of the risk of fraud. Consequently, investigators can concentrate on transactions that pose high risk and subsequently provide the analysis outcomes to the predictive model for updating purposes. Due to the dynamic nature of the attacking strategies employed by potential fraudsters, it is compulsory that a well-functioning system can effectively adjust to these evolving attack techniques.

A tremendous expansion of services, including e-commerce, tap-and-pay systems, and online bill payments, stems from the Internet's unprecedented growth over the past decade. The increased volume of transactions has positively impacted the global economy, but has also increased the potential for and dangers of credit card fraud. Due to their evolving nature, these frauds are progressively becoming more difficult to detect and prevent.

Currently, there are numerous varieties of credit card fraud, including lost or stolen card fraud, application fraud, and account usurpation (Gibson and Harfield, 2023). In addition to illegitimate transactions, Credit-Card Fraud involves various fraud methods, such as phishing, identity theft, and data breaches (Beju and Făt, 2023, Rajendran, 2024, Rai and Jagadeesha, 2023) These fraudulent actions have taken on a global dimension with the globalisation of financial services, thus harming economies and customers worldwide. Due to their complexity, many fraud schemes require revolutionary detection technology. Despite the utilization of protective measures such as data encryption and tokenisation, effectively defending against fraudulent activities of this kind continues to present significant challenges.

Researchers have devised numerous methods for detecting and preventing fraudulent transactions as a method of addressing the increasing threat of Credit-Card Fraud in the global economy (Dal Pozzolo et al., 2017). These methods frequently utilise sophisticated analytics, machine learning methods, and data mining techniques to identify suspicious activities and patterns. (Sahin et al., 2013) identified that popular techniques include decision tree, neural network, and clustering algorithms.

The rapid development of digital technologies and the rising prevalence of online transactions have made Credit-Card Fraud a major global concern and an intriguing research subject (Cherif et al., 2023, Xie et al., 2022b). The economic consequences and negative impact on customer trust emphasise the need for more comprehensive analysis and further research.

Credit-Card Fraud can assume a multitude of forms, each differing in its mechanisms and levels of sophistication. Establishing reliable fraud detection models requires a comprehensive understanding of these various categories of fraud, their technique of operation, and the prevalent patterns that could be leveraged for preventative purposes. Credit-Card Fraud can be of the following types (Jain et al., 2019):

a. *Counterfeit Card Fraud*. This type of Credit-Card Fraud arises when a counterfeit or duplicate card is created using information stolen from a credit card. The criminal may then utilize this card for unauthorised purchases. It has become less prevalent since the introduction of EMV chips, which are challenging to fake. However, it remains a significant problem because fraudsters often utilize skimming devices to steal information from the magnetic stripe on a card.
b. *Card-not-present (CNP) Fraud*. That can happen when fraudulent credit card transactions are conducted without the tangible credit card being present. This form of fraud occurs frequently in online, telephone, and mail-order transactions where card information is submitted. However, the card is not scanned or placed in a machine.
c. *Lost or Stolen Card Fraud*. This is one of the most straightforward types of credit card fraud, which occurs when a lost or stolen credit card is used to conduct unauthorised transactions or withdrawals. The quick action of the

cardholder in reporting a lost or stolen card might impact the severity of this fraudulent activity.

d. *Application Fraud*. Application fraud happens when a fraudster registers for a credit card by employing the identity of another individual or fake documents. If successful, the fraudster obtains a genuine credit card under a fake name and is able to make illegal purchases with it.

e. *Electronic or Manual Credit Card Imprints*. Typically, a "skimmer" machine is utilized to create a tangible replica or imprint of a credit card for this form of fraud. The thief can employ this imprint to create a fake card or conduct card-not-present purchases.

f. *Account Takeover Fraud*. In this case, a fraudster obtains access to a victim's credit card account, typically via hacking or phishing and subsequently adjusts the account's contact details, orders a new card, and initiates fraudulent transactions.

g. *Card ID Theft*. Identity theft is a fraudulent activity that involves obtaining an individual's personal information beyond their credit card details, intending to open credit card accounts in their name, and executing unauthorised transactions. The victim usually remains unaware of fraud until they see un-usual expenditures on their account or are approached by a debt collector.

h. *Mail Non-Receipt Card Fraud*. This kind of fraud occurs if a new or replacement credit card gets stolen in transit prior to it being delivered to the legitimate cardholder. The fraudster may then activate and use the card to make unauthorised purchases.

i. *Fake Merchant Sites*. In this kind of fraud, criminals establish fake e-commerce websites that seem identical to recognised and legitimate websites to deceive users into entering their credit card information. This website may provide a variety of discounts to persuade customers to purchase the items. Once this information is acquired, the fraudster uses it to commit crimes.

j. *Merchant Collusion*. This happens when a merchant or a merchant's staff works with a fraudster. The retailer intentionally passes on significant de-tails about the cardholder without the card user's consent so that the thieves may perform unauthorised transactions, copy details about credit cards from customers, or possibly sell these data to other fraudsters.

Credit-Card Fraud comes in many forms, using various aspects of credit card usage and security protocols. The evolution of commerce towards online platforms has facilitated the emergence of novel fraudulent activities, such as card-not-present fraud and false merchant sites, thereby underscoring the dynamic nature of this illegal activity. Fraudulent behaviour underlines the need for trustworthy and flexible methods to prevent and recognise such behaviour, thereby highlighting the necessity for reliable and adaptable measures for preventing and identifying such conduct, which is aimed at providing vital information

1.2 Machine Learning and Deep Learning algorithms

ML and DL are Artificial Intelligence (AI)-based domains that have revolutionised the fields of data analysis and modelling predictions (Gupta et al., 2021). Essentially, these innovations focus on creating algorithms that possess the ability to acquire knowledge and make intelligent decisions or forecasts using data. ML extends to the empirical learning characteristics similar to intelligence in humans, all while possessing the capacity to enhance their performance in analytical skills through increased exposure to data as well as implementing sophisticated computing techniques (Bini, 2018, Helm et al., 2020). Deep learning, on the other hand, is a more advanced kind of ML that successfully handles high-dimensional data such as images and consecutive inputs by utilizing neural networks with numerous layers (hence the origin "deep") as a method for processing data in a complicated manner (Jakhar and Kaur, 2020).

The incorporation of ML and deep learning techniques in the field of Credit-Card Fraud detection represents a substantial progression compared to conventional rule-based systems (Alarfaj et al., 2022). Initially, fraud detection was highly dependent on predetermined thresholds and rules, which were frequently inflexible and incapable of accommodating novel forms of fraudulent behavior. The development of ML and DL ushered in an age of innovation: these techniques acquired the capability to detect patterns in past data, forecast forthcoming transactions, and identify potentially fraudulent activities.

The advanced level of ML and DL models utilised in fraud detection has increased at an exponential rate over time. Initial versions of ML models were frequently basic classifiers capable of differentiating between legitimate and fraudulent

transactions as per predetermined attributes. However, as the sophistication of fraudsters' techniques increased, the demand for complex models emerged. Due to its capacity to analyse and gain knowledge, advanced analytical instruments are the most effective method for detecting future credit card fraud. Improved fraud-detection systems can potentially comprehend the context of transactions; such integrated systems might achieve spot-on detection with a substantial decrease in false positives. This multifaceted strategy is the crucial most technology in the war against credit card fraud and will ensure that fraud monitoring systems remains robust and responsive to the ever evolving threats.

Considering improvements, there are still continuing issues due to the globalisation of financial transactions and the rising complexity of cybercrime. Due to the demand for systems for identifying fraud act, fraudsters are constantly modifying their techniques. To understand possible fraudulent behaviors more optimally, it is crucial to combine spatial–temporal analysis, which improves the capacity to identify patterns of fraud across various geographical regions and time periods.

1.3 Spatial–temporal Approach

The spatial–temporal analysis is a multidimensional method that investigates connections, trends, and data patterns that include location and time. When considering the detection of Credit-Card Fraud, this analysis assumes a heightened level of effectiveness. Spatial analysis applies to the geographical dimension of transactions, encompassing the distance between successive transactions and the origins and destinations of those transactions (Garcia-Gabilondo et al., 2024) On the other hand, the temporal analysis examines the time-related dimension of transactions, emphasizing elements including the frequency, duration, and intervals between consecutive transactions (O'Connor et al., 2024). Combined, these analyses offer a comprehensive perspective on transactional behavior, thereby uncovering patterns that could potentially signify fraudulent actions.

Recognising that fraudulent transactions frequently display unusual patterns when examined from the perspectives of space and time motivates the incorporation of spatial and temporal analysis into fraud detection (Hilal et al., 2022). For example, conventional detection methods may fail to notice a potential case of fraud if there is a rapid sequence of transactions from distant places. The same principle applies

with regard to suspicious patterns of transactions that occur at inconvenient times. The system is able to identify fraudulent actions and grasp their context and method of operation due to these analyses, which improve the overall efficacy of the detection procedure.

The integration of spatial–temporal analysis in credit-card-fraud detection systems bears immense potential. Through this approach, such systems may obtain another level of accuracy and precision that was previously unachievable using conventional approaches. The combination of these features enables a sophisticated detection process that can effectively adjust to the constantly shifting methods utilized by fraudsters. It guarantees an enhanced, adaptable, and accurate fraud-detection method that can recognise complex and intricate patterns which signal fraudulent activity.

1.4 Key Terminologies and Concepts

The following section provides detailed explanations of the fundamental terminology and concepts that are utilized to formally address an issue in this thesis.

1.4.1 Credit-Card Fraud-Detection System

A Credit-Card Fraud-detection system is an advanced technology developed to detect and avoid authorized and fraudulent activities on credit cards. This system utilizes sophisticated algorithms and artificially intelligent systems to examine transaction patterns and detect abnormalities that differ from the customer's spending habits. When the system identifies suspicious transactions, it may activate notifications, reject transactions, or temporarily suspend the credit card to minimize possible financial consequences. Furthermore, these systems continuously develop and adjust to evolving fraudulent techniques, thus ensuring dynamic and proactive protection against evolving threats of Credit-Card Fraud.

1.4.2 Spatial

Spatial analysis, within the scope of Credit-Card Fraud detection, refers to analysing the geographic components within transactional information. This approach includes reviewing the locations of transactions to detect trends and irregularities that are indicative of fraudulent activity. Using the actual locations of cardholders and transaction sites, geographical analysis may assist in identifying

suspicious trends that might indicate fraudulent transactions. This approach improves the detection of fraudulent activity when other methods struggle, such as when transactions happen quickly across several places or at odd distances from the cardholder's habitual activity spots. Including geographical context in the research improves the capacity to identify anomalous actions, which is a crucial fraud-detection component.

1.4.3 Temporal

The temporal analysis involves the thorough evaluation and interpretation of data, with particular emphasis on the time and consecutive occurrences. Fraud detection is the examination of transaction data over a period of time to determine patterns, trends, or abnormalities that might potentially signify fraudulent behavior. This method utilizes the temporal attributes of transactions, such as their frequency, timing, and regularity, to differentiate between regular activities and possibly fraudulent ones. Temporal analysis improves the efficiency of fraud-detection systems by identifying abnormal patterns in transactions that might pass unnoticed by other approaches due to its grasp of the time-based characteristics of these transactions.

1.4.4 Imbalance Data

In the case of a Credit-Card Fraud detection system, imbalanced data applies to a scenario where the count of unauthorized expenditures (the minority class) is considerably lowered compared to the count of genuine transactions (the majority class). This disproportion impacts predictive modelling owing to a specific bias: conventional methods tend to display skew in favor of the majority class, which leads to insufficient recognition of fraudulent incidents. Consequently, while the model may exhibit a high accuracy rate in anticipating genuine transactions, it might be insufficient in its ability to identify and highlight fake behavior.

1.4.5 Data-Balancing Technique

Data balancing techniques, also referred to as resampling techniques, are statistical techniques, which are employed to solve the imbalance in datasets, particularly when one class of data is dominant by a significant margin over the other. This disproportion frequently arises in fields such as fraud detection, where illegal transactions are considerably lower than authorized ones. Data-balancing

techniques strive to either raise the number of cases in the minority class ("oversampling") or lower the number of instances in the majority class ("undersampling"), which is performed to create a dataset that is more evenly distributed, thus leading to machine-learning models that can make more precise and accurate predictions. These techniques improve the model's capability to identify irregular occurrences and boost the overall accuracy of predictions.

1.4.6 Evaluation Metrics

Evaluation metrics in the ML and deep learning domains refer to numerical measurements that are used to assess and compare the efficacy of algorithms. They evaluate the models' precision, effectiveness, and dependability in creating forecasts or categorizations. Typical metrics are accuracy, precision, recall, F1 score, and Area Under the Curve - Receiver Operating Characteristics (AUC-ROC) curve, which are essential for comprehending the model's strengths and weaknesses, directing enhancements, and ensuring that it satisfies the unique requirements of its application.

1.4.7 Confusion Metrics

The phrase "Confusion Metrics" indicates the set of measurements utilized by ML to assess the performance of classification models. It is based on a confusion matrix (i.e., a graph that describes the efficacy of the classification system). A confusion matrix is composed of true positives (TP), true negatives (TN), false positives (FP), and false negatives (FN). These figures indicate the model's accuracy and erroneacy. These data calculate accuracy, precision, recall (sensitivity), and F1 score. Moreover, the figures indicate the accurate and inaccurate forecasts made by the model. These measurements thoroughly comprehend the model's efficacy, especially in differentiating between several classes, a distinction that is vital in Credit-Card Fraud detection applications, where accurately classifying valid and unauthorized transactions is crucial.

1.4.8 True Positive

A 'True Positive' (TP) is the outcome denoted by a confusion matrix in which the model's prediction accurately forecasts the positive class. In the fraud-detection context, a true positive indicates that the model labels a transaction as fraudulent precisely when it is fraudulent.

1.4.9 True Negative

A True Negative (TN) is a confusion metric that indicates the count of occurrences in which the model accurately forecasts the condition's absence. In the field of credit-card-fraud detection, for example, a True Negative would indicate that the model correctly classified an activity as non-fraudulent and that it was, in fact, a valid transaction.

1.4.10 False Positive

In confusion matrices, false positives are scenarios when the model forecasts a positive result for a reality negative occurrence. A false positive arises in the identification of a Credit-Card Fraud setting when the model incorrectly labels a valid transaction as fraudulent, which might lead to unnecessary validation stages; thus, consumers become inconvenienced while possibly losing faith in the whole system.

1.4.11 False Negative

A False Negative (FN) occurs in the setting of confusion matrices when the model anticipates a negative result for a scenario that is, in fact, positive. This is especially crucial when recognizing positive instances, such as fraud detection or illness diagnosis, is critical. A false negative in a medical test, for example, occurs when the test result states an individual is not suffering from the condition when they really have it. This inaccuracy may be hazardous since it can lead to a lack of critical therapy or action. A false negative in fraud detection means that a fraudulent transaction is mistakenly labelled as genuine, thereby enabling fraudulent conduct to continue unnoticed. Decreasing false negatives is critical for enhancing model sensitiveness and trustworthiness.

1.5 Key Challenges of Credit-Card Fraud Detection

The financial transactions domain has experienced a significant alteration in recent years, which is mainly attributable to fast technological advancements and the worldwide transition towards electronic transactions. In addition to inducing simplicity and effectiveness, it has also led to the emergence of intricate obstacles in the field of Credit-Card Fraud detection. Due to the growing complexity of fraudster techniques, conventional fraud-detection systems are subjected to

challenges related to keeping up with emerging technologies. These challenges include managing large amounts of data and establishing the right balance between security and user experience. To effectively identify fraud in the constantly evolving area, it is necessary to utilise a prompt and visionary strategy that is flexible, robust, and able to navigate the complexities of recent financial fraud. The challenge is compounded by various factors, which are explained as follows.

1.5.1 Large-scale Datasets and a High Volume of Transactions

A scenario in which the volume of credit card transactions has increased significantly has resulted from the unprecedented surge in online financial transactions that was occasioned by the digital age. The rapid growth in data volume poses a significant obstacle in the fraud-detection domain. The exponential growth of transaction volumes has tremendously strained conventional fraud-detection systems, which were originally intended to manage data on a considerably smaller scale. It is not only difficult but also resource-intensive to monitor, analyse, and conduct these transactions in real-time. To detect potentially fraudulent activities among the millions of transactions that comprise the data reservoir, it is crucial to utilise sophisticated algorithms and advanced analytic tools.

The sharp increase in data volume emphasises the need for more comprehensive and efficient fraud detection systems. Current conventional detection approaches sometimes struggle to effectively manage the large volume and rapid flow of data, leading to either undiscovered instances of fraud or increased rates of false positive results. Consequently, there is a growing consensus that researchers should integrate ML and deep learning techniques, which are more efficient in handling large datasets. Intelligent systems possess the capability to acquire knowledge and adjust in response to new information, detect complex patterns, and generate predictions with better accuracy. The incorporation of intelligent and dynamic models is crucial for ensuring the integrity and security of financial transactions in the rapidly evolving digital economy of the twenty-first century as fraudsters continue to develop their strategies.

1.5.2 The Consumer Behavior is Evolving Rapidly

A substantial shift in consumer behaviour towards e-commerce platforms and digital payment methods has accompanied the exponential growth of potentially fraudulent activities; the findings of a study examining the effects of the COVID-19 lockdown in Greece indicate that throughout the lockdown, an established pattern towards growing usage of online banking services, with gender, age, residing in urban regions, and job security status emerged, all effecting crucial roles in predicting this shift in financial conduct (Bechlioulis and Karamanis, 2023). The research found that spending a longer duration in a lockdown increases the chance of additional online banking usage. The findings indicate a positive correlation between the duration of mobility restrictions and utilizing digital alternatives for financial transactions. Due to this transition, Credit-Card Fraud detection faces a formidable obstacle. Customers' growing usage of electronic payments presents fraudsters with more prospects to exploit emerging flaws and develop innovative strategies (Beju and Făt, 2023). The transition also requires updating authentication procedures to implement more robust fraud detection and prevention systems to protect the consumer experience while maintaining security.

Amid a wider variety of transaction patterns and types, a number of which are generally new and in a constant state of evolution, the identification of fraud methods has become a necessary method for providing an immediate and advanced approach to such a transition. Hence, customers demand more sophisticated fraud-detection systems, which must possess dynamism, the ability to learn from ever-changing data, and the skill to differentiate authentic behavioral changes from potentially fraudulent acts. The urgent need for these improved systems transcends protecting financial assets and also involves maintaining consumer confidence in the integrity of digital financial platforms.

1.5.3 Addressing the Imbalanced Dataset and Customer Experience.

One of the most critical problems in Credit-Card Fraud prevention is balancing effective fraudulent detection data with good user experience. Generally, the frequency of fraudulent transactions is considerably lower than that of legitimate transactions. This disproportion results in algorithms biased towards classifying transactions as genuine, frequently at the cost of failing to detect actual fraudulent

acts. When measures are taken to adapt such models as a method of improving their responsiveness to possible fraud, it often leads to a rise in false positives – valid transactions being mistakenly identified as fraudulent (Vanini et al., 2023, Hajek et al., 2023). This scenario not only weakens the effectiveness of the system for detecting fraud but also exerts a substantial influence on the customer's experience.

The consequences of a high proportion of false positives transcend mere inconvenience (Raj et al., 2023, Mayo et al., 2023). A lack of trust may affect the financial institution, thereby causing consumer dissatisfaction and perhaps decreasing the number of customers (Karim et al., 2023, DeLiema et al., 2023). Customers who are subjected to numerous transaction rejects or security checks may choose alternate providers that provide a more efficient transaction process. This scenario highlights the urgent need for more sophisticated and subtle fraud detection technologies. These systems should be able to accurately distinguish between valid and fraudulent transactions, thus reducing the occurrence of false positives and effectively identifying genuine risks. To effectively detect Credit-Card Fraud in the current intricate setting while maintaining an optimal user experience it is crucial to incorporate advanced algorithms and analytical methods, such as deep learning and spatial–temporal analysis.

1.5.4 Feature Selection and Data Confidentiality.

Maintaining confidentiality and data safety in detecting Credit-Card Fraud is crucial in the age of technology (Gupta, 2024). However, it can be difficult due to the demand for analysing confidential customer data. Furthermore, the shortage of comprehensive and precisely annotated datasets restricts the advancement of efficient fraud-detection algorithms (Jiang et al., 2023). Unfortunately, algorithms can be skewed in their results due to the lack of precision in the available data, which often exhibits attributes that are either unlabelled or tend to be unspecific. Strict rules regarding confidentiality and the unwillingness of financial institutions to share information that could expose vulnerabilities have worsened the situation (Sampat et al., 2024). Protecting consumers' privacy in the era of ever-changing cybercrime threats necessitates creative solutions (Mateus-Coelho and Cruz-Cunha, 2023), such as cooperative data-sharing frameworks, improved privacy techniques, and synthetic data generation.

1.6 Research Objectives

The key objectives of this thesis are as follows:

1. **Design And Assess An Innovative System For Detecting Credit Card Fraud.**

   Combining ML and DL techniques, balancing, geolocation monitoring, and temporal attention systems. This system aims to solve the shortcomings of current fraud detection techniques, which frequently encounter difficulties in adjusting to the swiftly changing strategies employed by fraudsters in the worldwide financial area. The research aims to develop a fraud-detection framework that is more dynamic, precise, and efficient by utilising ML algorithms and advanced data analytics. This framework should be capable of keeping up with the intricate techniques that fraudsters currently utilise.
2. **Boost the accuracy and efficacy of fraud detection.**

   Conventional systems exhibit higher false-positive rates, which induce unnecessary distress for legitimate consumers. By integrating temporal analysis and geolocation, the proposed system intends to substantially decrease the occurrence of these wrong alerts, thereby guaranteeing users a transaction experience that is both smooth and secure. Ensuring such accuracy is significant: it maintains the reputation and confidence of financial institutions among customers, in addition to contributing to their overall satisfaction.
3. **Demonstrate exceptional adaptability**.

   By constantly adapting to new fraudulent activity patterns, the proposed system ensures its resilience against future threats. This flexibility is accomplished by integrating ML models that are capable of analysing and interpreting enormous datasets as a method of detecting newly developed Credit-Card Fraud patterns and techniques. Such a system is crucial for defeating fraudsters and minimising the risks induced by fraudsters who persistently develop novel methods of escaping detection systems. The evolving complexity and prevalence of fraudulent strategies, driven by globalisation and technical progress, have led to an elevated need for novel and efficient approaches for identifying and preventing fraud.

This research presented herein offers a substantial contribution to the respective subject by presenting a complete, versatile, and customer-oriented solution. The utilization of this technology can strengthen the safety measures around financial transactions while also providing a foundation for potential future developments in the field of fraud-detection technologies. This study can potentially lead to a significant transformation in the methods that financial institutions utilize to protect themselves and their clients against the constantly shifting risks associated with Credit-Card Fraud by establishing novel benchmarks for precision and flexibility.

1.7 Research Gaps

This thesis highlights key research gaps, particularly the issue of class imbalance in credit card fraud detection and the limitations of existing models in effectively accounting for spatial and temporal variations. Traditional fraud detection systems usually struggle to spot fraudulent transactions because there are many legitimate ones. This results in models that tend to be biased towards predicting non-fraudulent outcomes. The class imbalance lowers how sensitive fraud detection algorithms are, meaning that some fraudulent activities can slip through without notice. Additionally, the changing nature of fraudulent tactics requires models that can adjust to new patterns as they develop over time and in various areas. Many current methods tend to miss out on the importance of combining geolocation data with time trends, which are really important for identifying and anticipating complex fraud schemes. The gaps highlight the importance of creating more advanced and dynamic models that can tackle the data imbalance and utilise the predictive potential of spatial and temporal data to improve fraud detection systems.

1.8 Research Significance

The thesis possesses a multidimensional significance due to its investigation into the identification of Credit-Card Fraud. A comprehensive explanation is provided below:

- **Tackling the Increase in Digital Transactions:** The pandemic has sped up the transition towards online transactions, thus increasing the vulnerability to fraudulent activities within digital payment systems. The importance of this research is vital in this era of increased digital financial transactions.

- **Addressing the Imbalance in Class Representation:** A crucial concern in fraud detection is the imbalance between the number of valid transactions and fraudulent ones. The objective of the study is as follows: rectifying this discrepancy by enhancing the efficiency of fraud-detection techniques.
- **Innovative Combination of Techniques:** Incorporating ML algorithms, balancing techniques, and geolocation and temporal attention systems constitutes a novel fraud-detection method. This combination is anticipated to produce a fraud-detection framework that is more adaptable, accurate, and efficient.
- **Comprehensive Performance Evaluation:** The research aims to conduct a comprehensive performance evaluation of different models, including Random Forest, CatBoost, and Logistic Regression, in the fraud-detection context. This evaluation is based on metrics such as accuracy, precision, and AUC-ROC, thereby ensuring a thorough assessment of the effectiveness of these methods.

Overall, this research substantially contributes to the progress of Credit-Card Fraud detection. It provides practical solutions that improve the security and reliability of online transactions, thereby benefiting the financial industry and society.

1.9 Thesis Structure

This thesis is organised into six chapters and provides a thorough investigation of credit-card-fraud detection systems. Chapter One establishes a foundation by explicitly explaining credit-card-fraud detection and its evolutions. This section explores the growing demand for effective fraud-detection systems, especially due to changes in consumer behavior and the surge in digital transactions occasioned by the COVID-19 epidemic. This chapter also explores the application and implications of ML and deep learning techniques in this domain, thus emphasising the significance of spatial–temporal analysis. Furthermore, it addresses the major obstacles currently faced in the field of credit-card-fraud detection, clearly stating the research objectives and emphasising the importance of the study. The subsequent chapters of the thesis are structured as follows.

Chapter 2 provides a comprehensive analysis of the relevant literature on credit-card-fraud detection, thoroughly examining many aspects of this complex topic.

This chapter focuses on examining the unbalanced data challenge, which is a crucial problem that significantly affects the efficacy of fraud-detection methods. The chapter extensively explores the solutions for addressing this imbalance, thus highlighting the effectiveness of data balancing methods. Furthermore, it investigates the revolutionary incorporation of spatial–temporal analysis, a technique that enhances detection accuracy by considering both the geographical and temporal dimensions in the analysis of transaction data. This comprehensive evaluation establishes the basis for resolving these deficiencies, with the intention of enhancing the accuracy and efficiency of Credit-Card Fraud detection systems in the modern digital age.

Based on a thorough investigation of relevant research in Chapter 2, deficiencies and gaps are identified in Chapter 3. Additionally, definitions of terms and concepts utilised throughout this thesis are provided in this chapter. The chapter also presents an overview of the contextual framework regarding the research topic and outlines the related questions. A description of the study method, which is utilized to solve the problem, is provided at the end of the chapter.

In Chapter 4, a thorough examination of the analytical and data processing methodologies utilised herein is provided. Commencing with an elaborate overview of the dataset, it outlines the procedures for data collection and structure. This examines the feature-selection process and training preparation, which assures researchers that the data is appropriate for the implemented models. Subsequently, the chapter proceeds to examine the Exploratory Data study (EDA), after which the proposed framework is explained. Subsequently, the chapter explores the performance classification metrics that are employed to assess the models' effectiveness. The evaluation of the algorithms' accuracy, precision, and overall efficacy in Credit-Card Fraud detection is based on these parameters. In the conclusion section, a summary, which generates all of the above, is provided: the summary considers the impact of the results and possible approaches for future investigations.

Chapter 5 employs ML and DL algorithms to evaluate unprocessed data. It proceeds with a performance evaluation of eight varieties of ML Algorithms on Raw data, followed by the other two effective DL methods, which are also trained using raw data. By comparing the distinct outcomes of ML and DL when applied to

unprocessed data, we obtain a more optimal basis for understanding the subsequent chapter, in which we intend to apply the imbalance technique. This chapter lays the foundation for further discussion. The paper concludes by providing a discussion and summary of the aforementioned findings, thereby establishing a foundation for comparatively analyzing subsequent chapters.

Chapter 6 provides an in-depth review of machine learning and deep learning algorithms in the context of Credit-Card Fraud detection. It specifically focuses on the effectiveness of these algorithms when imbalance methods such as SMOTE, ADASYN, and random oversampling/under sampling are employed. The study involves a thorough comparison of eight distinct machine learning methods and two deep learning models to determine how their performance improves after data balancing.

1.10 Conclusion

The first chapter addressed the complicated environment of Credit-Card Fraud detection, focusing on its development and the crucial significance of ML and DL technologies. The process of globalising financial transactions has introduced another level of complexity to the identification and prevention of fraudulent activities. The diverse regulations, foreign currencies, and transaction varieties across different countries induce considerable difficulties, thereby emphasising the need for more advanced and dynamic fraud-identification systems.

The incorporation of ML and DL with spatial–temporal analysis has become a key advancement in this research field. This association enhances fraud-detection accuracy and efficiency by analysing transactional data and their contextual background. This study endeavors to develop a more reliable and adaptable fraud-detection system, despite obstacles such as data imbalances and the constantly changing techniques utilized by fraudsters. The proposed solution aims to significantly boost the fraud-detection efficacy by providing a solution that is consistent with current global financial trends. This undertaking is crucial for enhancing financial stability and strengthening protection against fraudulent activities in the modern digital age.

2 LITERATURE REVIEW

2.1 Introduction

Chapter 1 established the fundamental basis by explaining the essential principles of Credit-Card Fraud detection, as well as by delving into the analysis of machine learning and deep learning technologies. Additionally, it emphasised crucial research areas that are relevant to this study. Therefore, this chapter explores the literature that focuses on systems that identify Credit-Card Fraud. The chapter is carefully organised into multiple sections, each dedicated to specific areas of Credit-Card Fraud detection. A substantial part of this chapter focuses explicitly on tracing the development of Credit-Card Fraud detection. The chapter also discusses the evolution from basic techniques to advanced, technology-driven alternatives.

The consequences of unbalanced data in the context of Credit-Card Fraud detection (Abd El-Naby et al., 2023, Gupta et al., 2023). When the efficacy of detection systems is skewed by the disproportionate percentage of fraudulent to legitimate transactions, imbalanced datasets pose a unique challenge for predictive modelling. The chapter provides a critical analysis based on the existing literature that discusses the impact of this imbalance on the precision and dependability of fraud detection models, as well as a summary of the strategies implemented to solve this problem. It extensively reviews spatial and temporal analyses in the context of Credit-Card Fraud detection. This method involves analysing transaction data in relation to spatial and temporal factors, thus providing a more nuanced and thorough comprehension of fraudulent patterns.

After an extensive review of the current research literature and theoretical frameworks related to Credit-Card Fraud detection, it is clear that an integrated approach is required to combat the complex nature of this research issue. This recognition arises from a comprehensive examination of the existing state-of-the-art techniques, which manifest significant improvements and persistent limitations in the identification and prevention of fraudulent behaviours. The literature emphasises mutual challenges, such as the significance of advancing detection systems to match the growing complexity of fraud tactics. Furthermore, it underscores the intricacy involved in managing and analysing data that possesses inherent skewness or imbalance, a recurring challenge that hinders the creation of efficient detection models. Furthermore, the increasing acknowledgement of the

temporal and spatial aspects of fraudulent activities emphasises the criticality of incorporating sophisticated analysis into detection systems. These key insights provide the framework for a more sophisticated comprehension of fraud detection and facilitate a more thorough examination. The chapter categorises related literature into three fundamental aspects. The chapter categorises related literature into three categories. These categorisations are established on fundamental approaches and inherent issues within the field of financial fraud detection:

1. Credit-Card Fraud detection
2. The Impact of Imbalance Data
3. Spatial–temporal Analysis

2.2 Critical Evaluation of Existing Approaches on Credit Card Fraud Detection Systems and Gaps in the Literature

As discussed in preceding sections, there are various strategies adoped to the identification of credit card threat; however, there exists a shortage of comprehensive methodologies that effectively integrate all comparison parameters of ML and DL techniques, address challenges associated with imbalanced datasets, and incorporate spatial and temporal parameters to enhance the fraud-detection ability. To analyse and assess the approaches more optimally, the chapter comparatively analyses these approaches, as depicted in Table 1. The comparison is organized based on five essential parameters: spatial analysis, temporal analysis, addressing data imbalances through data balancing techniques, machine learning, and deep learning algorithms. The comparative parameters are chosen because integrating methods provide a comprehensive and subtle strategy for identifying fraudulent activities. It capitalises on the advantages of sophisticated pattern recognition, addresses data imbalances, and utilizes critical transactional contexts. Consequently, it drastically enhances the precision and efficiency of detecting Credit-Card Fraud systems.

Table 1 illustrates a comprehensive and detailed analysis of various methods that are utilized in the identification of credit card fraud. It offers a thorough understanding of the current scenario in this field. This compilation of knowledge is a critical resource for acquiring an in-depth understanding of the most up-to-date methods and stimulating future advancements in this field.

Table 1 Critical evaluation of existing literature on Credit-Card Fraud-detection system approaches

Source	Spatial–Temporal Analysis		Imbalance Technique	Machine Learning	Deep Learning
	Spatial	Temporal			
(Abd El-Naby et al., 2023)	✖	✖	✔	✔	✖
(Afriyie et al., 2023)	✖	✖	✔	✔	✖
(Almazroi and Ayub, 2023)	✖	✖	✔	✔	✔
(Barz et al., 2018)	✔	✔	✖	✔	✖
(Cheng et al., 2020a)	✔	✔	✖	✔	✔
(de Sá et al., 2018)	✖	✖	✖	✔	✖
(Esenogho et al., 2022)	✖	✖	✔	✔	✔
(Fanai and Abbasimehr, 2023)	✖	✔	✔	✔	✔
(Ghaleb et al., 2023)	✔	✖	✔	✔	✔
(Gupta et al., 2023)	✖	✖	✔	✔	✖
(Khalid et al., 2024)	✖	✔	✔	✔	✔
(Li et al., 2020)	✖	✖	✔	✔	✔
(Lucas et al., 2020)	✖	✔	✖	✔	✖
(Lunghi et al., 2023)	✖	✔	✔	✔	✔
(Nguyen et al., 2022)	✖	✖	✔	✔	✔
(Ni et al., 2023)	✖	✖	✔	✔	✖
(Xie et al., 2023)	✔	✔	✖	✔	✔
(Xie et al., 2022a)	✖	✔	✖	✔	✔
(Xie et al., 2022b)	✖	✔	✖	✔	✔
(Zhu et al., 2023)	✔	✖	✔	✔	✔

A comprehensive review of the current literature in the field of Credit-Card Fraud detection systems reveals the following: the absence of an integration of sophisticated data balancing techniques and advanced machine learning and deep learning models while considering the spatial and temporal dimensions of transaction in the field of Credit-Card Fraud detection systems, which is a deficiency that was discovered during the literature review.

Furthermore, this comparison illustrates that although the literature delineates numerous methodologies implemented to detect Credit-Card Fraud, knowledge deficits still merit further investigation. The incorporation of the spatial and temporal attributes of transactions, which have the potential to significantly enhance the predictive capability and precision of fraud-detection systems, is

conspicuously lacking in the existing literature. Consequently, this comprehensive approach is of utmost importance.

2.3 Credit-Card Fraud Detection

The development of Credit-Card Fraud detection technologies has led to a transition from basic approaches to more advanced algorithms. During their inception, fraud detection systems mainly comprised rule-based methodologies, which relied on predetermined patterns and criteria to identify occurrences of fraudulent action. Although they were competent in detecting simple fraudulent schemes, traditional detection systems were constrained by their capability to adjust to the dynamic techniques utilized by fraudsters. The present period was characterized by commencement of a continuous battle against the performance of credit card fraud, which creates a scenario where more intricate fraudulent tactics address each technological advance (Cherif et al., 2023).

A conventional fraud detection system typically incorporates an automated fraud detection model and a manual review operation conducted by the organisation's investigator (de Sá et al., 2018). The automated fraud-detection technique is designed to monitor and evaluate every transaction that comes in using data mining methods, thereby leading to a scoring system (Kim et al., 2019, Salazar et al., 2016). The manual process involves corporate investigators examining transactions that are suspicious and have been flagged by an automated fraud-detection system due to their high fraud scores. The investigators subsequently provide responses indicating whether the transactions are illegal or valid (Sánchez et al., 2009). An automated fraud-detection system may be constructed with either expert-driven approaches, data-driven methods, or a mix of both (Phua et al., 2010).

The expert-driven techniques intend to detect specific cases of fraud by analysing past fraudulent activities and formulating rules that reflect various kinds of fraudulent activity (Bolton and Hand, 2004, Gratius et al., 2024). Data-driven approaches often rely on machine-learning techniques to train a fraud-detection system (Li et al., 2020). As illustrated in the literature (Carcillo et al., 2021), Credit-Card Fraud detection systems are constructed by combining supervised and unsupervised learning methods as well as presenting numerous criteria for calculating outlier scores at various levels of granularity. The author of (Khine and

Khin, 2020) offers an online boosting technique that combines an exceptionally rapid decision tree as the basis learner to facilitate the creation of a single online strong learner by assembling them together. The research (Fiore et al., 2019) applies a generative adversarial network to produce imitated instances of the minority class. These examples are subsequently combined with the training data to create an improved training set, thereby enhancing a classifier's performance. This notwithstanding, the majority of the techniques utilise only the original features of transaction data to train a model. The efficacy of the model that was trained is poor, which can be rationalized as follows: the data presented by these original features does not adequately represent the attributes of transactions (Zhang et al., 2021). The limitations of the conventional systems became evident as the volume of credit card transactions increased commensurate to the rise of online purchasing and globalised commerce.

Several transactional samples have been developed using transaction aggregation algorithms. The studies (Whitrow et al., 2009) utilise an aggregation approach to include additional characteristics into the original transaction information. The aggregation process involves grouping the transactions performed during recent hours based on the corresponding cardholder ID and transaction type. Subsequently, the quantity of these consolidated transactions, the cumulative expenditures made on these activities, and their average amount throughout various time intervals are computed as novel features (Harish et al., 2024). Numerous research (BAGHDADI et al., 2024, Bahnsen et al., 2016, Bahnsen et al., 2013), (Bhattacharyya et al., 2011, Dal Pozzolo et al., 2014, Sahin et al., 2013) adopted the method outlined in (Whitrow et al., 2009, Gu et al., 2024). An instance of this can be observed in (Bahnsen et al., 2016), where the aggregation method is dependent on the country and merchant code in addition to the cardholder ID and transaction type. Consequently, the feature space is considerably more extensive than in (Whitrow et al., 2009). Furthermore, they generate a new set of characteristics by employing the Von Mises distribution to examine the frequency of user transactional behaviors when the transaction is conducted.

A framework based on (Lucas et al., 2020) is introduced: it utilises a hidden Markov model to establish a correlation between the probabilities of a given transaction and the sequence of its preceding transactions. These probabilities are employed as addition features in the identification of fraudulent activities. While the aggregated

features may provide the detection model with valuable information, the initial classifiers restrict the detection model's capability to comprehend complex transactional behaviors that are autonomously demonstrated by customers.

The insufficiencies of conventional fraud-detection systems emphasised the necessity for more sophisticated approaches, which led to the development of machine learning and deep learning techniques for fraud detection. These technologies ushered in a new era by providing dynamic and adaptable models that can acquire knowledge from data and advance in response to transforming patterns of fraud. A number of studies utilise the presentation of transactions generated by this approach to address the challenge of fraud detection through the integration of various machine learning algorithms, (Dal Pozzolo et al., 2017, Carcillo et al., 2018, Xuan et al., 2018, Roy et al., 2018). The growing complexity of fraudulent schemes, the expanding volume of transactions, and the demand for more precise detection capabilities all contributed to the transition to these advanced techniques. Due to their capacity to analyse extensive datasets and detect intricate patterns and their adeptness in discerning complex patterns that elude conventional detection techniques, machine learning and deep learning models have become crucial in this field. Nevertheless, although these algorithms provide considerable advantages, they are still within limits. Despite the advances occasioned by Machine Learning and Deep Learning, challenges persist. One of the main problems is that it utilizes only historical data, which might not correctly show new or upcoming fraudulent techniques.

Moreover, both Machine Learning and Deep Learning models can have grapple with idea shifts in fraud trends (i.e., when the data distribution changes over time). This limitation highlights the necessity for incorporating additional features, such as geolocation and temporal aspects, into fraud detection models. By integrating these dynamic features, fraud detection systems can become more responsive to real-time changes in transaction patterns, thus offering a more comprehensive and adaptive approach to identifying and preventing fraudulent activities.

2.4 The Impact of Imbalance Data

In recent years, the scientific community concerned with classification algorithms has become more attentive to the difficulties that arise when unbalanced datasets

are considered. Numerous comprehensive analyses of these matters have been discussed in (Gupta et al., 2023, Ganganwar, 2012, García et al., 2009), (Richhariya and Singh, 2014, Bhattacharyya et al., 2011, Dal Pozzolo et al., 2014). The class-imbalance notion is a relatively straightforward concept: it occurs when the number of elements in positive and negative classes of a given dataset are exceedingly uneven and exhibit a significantly skewed data distribution (Phua et al., 2004, Sisodia et al., 2017).

As illustrated in (García et al., 2009, López et al., 2013, Makki et al., 2019, Sisodia et al., 2017), the proportion of fraudulent or illegal conduct is significantly lower compared to legitimate and authentic ones. The class imbalance creates an immense barrier to identifying fraudulent activity characteristics and extracting fraud patterns. The majority of optimisation steps executed by the classification algorithm are aimed at accurately classifying the dominant class, disregarding the others Consequently of the dominance of that particular class. To ensure accurate classification, it is particularly crucial to address minority observations, such as fraud observations. Significant financial harm can be inflicted upon organisations and individuals when fraudulent transactions are misinterpreted as legitimate due to the classification algorithm's inability to identify common fraud patterns.

Class imbalance's effect on evaluation metrics for classification has thus emerged as a significant concern. The issue has been explored by a number of authors who have provided illustrative instances of its effects on accuracy (Chawla, 2010, Hossin and Sulaiman, 2015) and various other metrics (Daskalaki et al., 2006, Branco et al., 2017, Gu et al., 2009). Regarding contemporary notions, only one empirical study (Jeni et al., 2013) that differs from an example-based approach has been published, albeit in a limited scope. The quantitative analysis of classification performance measures has traditionally been addressed via two methods: using a set of established and easily accessible datasets (Amin et al., 2016, Boughorbel et al., 2017) or generating random simulations of classifier outcomes (Powers, 2020, Jurman et al., 2012). Jeni et al. (Jeni et al., 2013) utilize a combination of random simulated changes on existing datasets.

Based on (Luque et al., 2019), when dealing with datasets that have an imbalance in class distribution, choosing the most appropriate evaluation metrics for

classification is necessary. An imbalance may substantially impact the value and consequences of accuracy and other well recognised performance measures, as indicated in several instances. This study utilises binary classifier results to assess the impact beyond individual cases. The collection includes a set of methods and numerical indicators that enable researchers to compare evaluation metrics based on binary-confusion matrices for imbalanced datasets.

Kamaruddin and Ravi (Kamaruddin and Ravi, 2016) presented a one-class classification method to address the issue of imbalanced data. The researchers propose a combination of Particle Swarm Optimisation and Auto Associative Neural Network (PSOAANN) and utilize it inside a Spark computational setting. Wei *et al*. (Wei et al., 2013) introduced an online fraud-detection system and demonstrated its effectiveness in handling massive amounts of highly skewed data. Subsequently, their outcomes are consolidated at the conclusion. Padmaja *et al.* (Padmaja et al., 2007) proposed a fraud-detection technique that integrates the backpropagation, naïve Bayes, and C4.5 tree algorithms. They implemented these techniques on data obtained by oversampling with replacement. The authors demonstrated the efficacy of their method by utilizing a dataset focused on healthcare insurance fraud. The research focuses on the class-imbalance problem in fraud detection by employing K reverse nearest neighbor to remove highly abnormal data points from the minority class. Subsequently, a technique referred to as SMOTE, which involves oversampling the minority class, was utilized in conjunction with under-sampling the majority class. The researchers performed trials using various classifiers such as C4.5, naive Bayes, k-nearest neighbor, and Radial Basis Function networks.

In another article, (He et al., 2008) introduces an innovative adaptive synthetic (ADASYN) sampling method for effectively learning from unbalanced data sets. It generates more synthetic data for minority class examples that are considered more challenging to learn and utilizes a weighted distribution based on their level of difficulties. The ADASYN technique enhances training by eliminating class imbalance bias and adapting classifying decision boundaries for challenging scenarios. This strategy is successful across five assessment measures, as depicted by simulation studies on many machine learning data sets. According to (Gupta et al., 2023), the research illustrates the manner in which the framework utilizes

Machine Learning to balance classifications and data. Different sampling approaches were utilized in model procedures. Random oversampling integrated with XGBoost performs most effectively for skewed data.

2.5 Spatial–temporal Analysis

Spatial analysis has become essential in numerous scientific fields, including epidemiology and geoscience, where it pertains to examining the characteristics, locations, and interconnections of elements within spatial data. The technique comprises the investigation and construction of models as a method for depicting spatial trends and patterns. Spatial analysis exerts a crucial role in detecting Credit-Card Fraud by identifying transaction location abnormalities, which enables the identification of potentially fraudulent activities when cardholders conduct transactions in distant or uncommon areas that differ from their regular routine. Fraudsters often act in certain areas to efficiently transfer cash between their accounts and optimise their earnings within a short timeframe instead of regularly changing their transaction locations. This behavior distinguishes them from authorised customers in regard to geographical patterns (Xie et al., 2023, Chang et al., 2022, Guo et al., 2020). Hence, the spatial transactional behavior of users is also a crucial factor in identifying fraudulent attributes.

Additionally, the transactional behavior of users is a crucial component in the temporal analysis aimed at identifying fraudulent attributes. Users' transactional behaviors tend to evolve over time (Cheng et al., 2022, Zeng and Tang, 2022). The transactional behavior of genuine customers is notably developing with their living conditions and income levels. Conversely, to counteract the evolving transactional patterns of authentic users and the perpetual revisions to Credit-Card Fraud Detection models, fraudulent actors consistently modify their methods of operation (Xie et al., 2023). The author of (Lucas et al., 2020) employs a variety of perspectives. By integrating the HMM-based approach with the innovative expert-based feature construction strategy for identifying credit card fraud, it is possible to enhance the efficacy of the classification process and enable a greater number of fraudulent transactions to be detected through the automatic feature engineering of temporal associations.

"Maximally Divergent Intervals" (MDI) is an unsupervised approach to spatio-temporal identification of anomalies; the method was introduced by (Barz et al.,

2018). This approach aims to detect anomalies by identifying coherent spatial regions and time intervals characterised by significant divergence, thus utilising an unbiased Kullback-Leibler divergence. The wide range of MDI applications, including climate analysis, video surveillance, and text forensics, evidences its effectiveness in these domains. Significant anomalies in extensive data sets are effectively identified by the model through the analysis of contiguous intervals of time and space instead of isolated points.

To improve Credit-Card Fraud detection, some studies have focused on learning novel models for each transaction record based on the aforementioned transactional characteristics (Cui et al., 2021, Ahmed et al., 2018). Nevertheless, they exhibit some constraints. First, some studies utilize successive models to capture temporal transactional behaviors. They view a CCFD (Credit-Card Fraud Detection) problem as challenging to learn and predict sequences (Zeng and Tang, 2021, Jurgovsky et al., 2018). Their models, such as RNN and its variations, often presume that the effect of earlier transactions on the present one remains constant regardless of the time that has elapsed. However, they fail to consider the behavioral modifications that occur due to different time intervals between consecutive transactions (Osegi and Jumbo, 2021, Guo et al., 2018). Second, from raw features, a number of prior studies generate feature matrices or tensors whose dimensions represent time, location, and feature-based segments (Li et al., 2023, Cheng et al., 2020b). Every feature is created by considering a certain time and place range to extract spatial and temporal transactional behaviors. Although time–location window-based features may capture some user activities, they fail to reveal fraud characteristics in common adequately.(Xie et al., 2022a).

Recently, (Xie et al., 2023) proposed a Spatial–temporal Gated Network (STGN) approach to identifying credit card fraud. This model acquires novel transactional representations by integrating both the temporal and spatial aspects of user transactional behavior. The STGN detects temporal and spatial patterns in user transactions using gated recurrent units in location-aware and time-aware gates. In addition, it incorporates a spatial–temporal attention module and a representation interaction module for enhanced detection precision. In detecting fraudulent transactions, experimental results on a real-world transaction dataset demonstrate that the STGN outperforms current state-of-the-art models.

Existing models tend to prioritise detection speed over accuracy or are constrained by the computational overheads of complex algorithms, thus sacrificing thoroughness for practicality. The limited use of spatial-temporal data is especially apparent since it is often overlooked despite its potential for valuable insights, owing to the challenges associated with its integration. Also, resampling methods such as SMOTE, ADASYN, and random undersampling are referenced in the literature. However, their evaluation concerning the real-world applicability of models, particularly in balancing fraud detection and minimising false positives, is infrequent.

These gaps emphasise the need for a more cohesive strategy and highlight the demand for a structure that integrates advanced algorithms for machine learning with effective data management measures. This thesis offers an approach that rectifies these deficiencies by using an innovative amalgamation of data balancing techniques and machine learning algorithms while utilising spatial-temporal data to improve prediction accuracy and flexibility. This suggested technique enhances previous models by providing a balanced evaluation of accuracy, computing efficiency, and practical application across various operational contexts.

2.6 Conclusion

This chapter presents a thorough examination of the existing literature on approaches for detecting credit card fraud. thus demonstrating the shift from basic processes to sophisticated, technology-driven solutions. The investigation included three primary domains: the progression of fraud detection approaches, the influence of unbalanced data on these systems, and the innovative utilization of spatial–temporal analysis. The section on evolution emphasized the impact of digital progress on fraud detection, whereas the section on unbalanced data explored the difficulty of skewed datasets and examined techniques such as random oversampling, SMOTE, and ADASYN. The spatial–temporal analysis section expanded the topic to include the examination of transactional data within the framework of both time and place. This evaluation comprehensively analyzed the merits and weaknesses of each technique, thereby offering a comprehensive depiction of the present status of Credit-Card Fraud detection

The literature review revealed significant deficiencies in Credit-Card Fraud detection systems, particularly in their ability to integrate spatial–temporal analysis

and resampling methodologies, and to elaborate machine learning and deep learning algorithms. The existence of these gaps emphasises the need for more thorough and unified strategies that can effectively address the intricacies of fraud detection in the contemporary digital landscape. The literature review has established a robust basis for identifying these deficiencies, therefore laying the foundation for the subsequent chapter, where we thoroughly explore these gaps.

In Chapter 3, we specifically define the concerns related to the current literature and provide a clear plan for overcoming these difficulties.

3 FOUNDATIONAL CONTEXT AND THE RESEARCH SCOPE

3.1 Introduction

As discussed in previous chapters, this research aims to address substantial deficiencies revealed in existing approaches for the identification of Credit-Card Fraud in response to the changing circumstances within this field. Although ML and DL technologies have made significant progress, their implementation in fraud detection remains constrained by the growing complexity of financial transactions worldwide. The combination of these sophisticated technologies with spatial-temporal analysis exhibits potential. This chapter provides a thorough analysis of current methods employed for the detection of Credit-Card Fraud. It is observed that there are still gaps in the existing literature, and the deficiencies in the literature are highlighted in the following section.

3.2 The Contribution

The existing literature mainly focuses on conventional techniques and isolated fraud-detection components but lacks an integrated approach that incorporates several novel features. Most previous research has concentrated on machine learning or deep learning methods, frequently neglecting the potential benefits that may accrue from a comprehensive integration of several approaches. The exclusive utilization of this particular method restricts the total efficiency and flexibility of the fraud detection systems in addressing the more intricate and diverse forms of fraudulent activities. This study substantially contributes to Credit-Card Fraud detection, which is an ever-evolving and complex problem. The approach significantly deviates from conventional methods, which frequently depend on assumptions arising from the ambiguous labelling of attributes in publicly accessible datasets. Instead, we employ a systematic selection process for dataset features, which precisely identifies geographical locations through the utilisation of exact timestamps for temporal analysis and precise latitude and longitude coordinates for spatial analysis. Consequently, we establish a novel approach for the accuracy and reliability of fraud detection systems by applying the following:

- **The integration of predictive models (Machine Learning and Deep Learning) and data balancing techniques into spatial and temporal analyses.** This integration facilitates the system's ability to detect fraudulent transactions with enhanced precision and comprehend the fundamental patterns and abnormalities that serve as indicators of fraudulent activity.
- **The assessment of evaluation metrics before and after implementing data balancing techniques.** One of the key aspects of our contribution includes the comprehensive evaluation of various evaluation metrics, both pre- and post-implementation of the data balancing technique on the dataset.
- **A Comparative Analysis of Algorithms Used in Machine Learning and Deep Learning**. This research provides a comprehensive understanding of the variations in performance across various algorithms and identifies the most appropriate models related to fraud detection. The knowledge acquired from this assessment is of immense value for directing the selection and enhancement of predictive models in creating robust fraud detection systems.
- **The adaptability and robustness of fraud detection systems.** This research highlights the critical role of adaptability and robustness in fraud detection systems to combat the constantly evolving strategies that are successfully utilized by fraudsters, which is achieved by integrating precise geographical and temporal data analysis with sophisticated prediction models.
- **The proposed technique drastically boosts the security of financial transactions and user confidence by attaining greater detection rates and lowering false positives.** The method efficiently detects fraudulent patterns and abnormalities in transaction data over time by including spatial-temporal attention mechanisms in parallel with sophisticated machine learning techniques. Data balancing techniques such as SMote and ADASYN provide a more representative training dataset, thereby enabling the refinement of the classification thresholds of algorithms such as Random Forest and XGBoost. This change greatly reduces false positives, guaranteeing that real transactions are handled without error, preserving user confidence, and reducing interruptions. Directly increasing user trust in the digital transaction system through this increase in detection and

mistake reduction creates a safe and dependable environment for financial operations.

A significant deficiency in the existing body of research is the lack of a comprehensive framework that integrates spatial analysis, temporal analysis, data balancing methods, and the collective capabilities of both machine learning and deep learning algorithms. An integrated approach is crucial for improving the precision, accuracy, and effectiveness of fraud detection systems. Spatial analysis provides valuable information on geographical trends and irregularities in transactions, whereas temporal analysis reveals details about the time and sequence of occurrences. Both of these analyses are essential for detecting fraudulent conduct. Furthermore, it is crucial to address the problem of class imbalance by utilizing efficient data balancing approaches, which ensures that the predictive models are trained adequately on datasets with a balanced class distribution. The seamless integration of the aforementioned components, along with the predictive capabilities of machine learning and deep learning, may lead to a more resilient and all-encompassing fraud detection architecture. An advanced system would possess the ability to not only accurately detect fraudulent activity but also adapt to the changing nature of credit card fraud, eventually enhancing the security of financial transactions.

3.3 Problem Statement

The research statement of the thesis is as follows: to address the deficiencies highlighted in the current literature on Credit-Card Fraud detection. This study proposes a novel methodology that combines spatial and temporal analysis with sophisticated data balancing techniques, together with the integrated capability of machine learning and deep learning; thus, it addresses the shortcomings of contemporary methodologies. The main objective is as follows: to create a robust fraud detection system that enhances the accuracy and precision of identifying fraudulent behaviour while efficiently adapting to the dynamic and intricate patterns of fraudulent actions. This study aims to address the existing gaps by employing spatial analysis to reveal spatial patterns and abnormalities and temporal analysis, thereby comprehending the time and sequence of transactions. These aspects are generally disregarded in conventional fraud detection approaches but are critical for effective detection.

Furthermore, this research prioritises the resolution of the class imbalance problem, which is a widespread issue in fraud-detection datasets. In such datasets, the number of genuine transactions considerably exceeds the number of illicit transactions. The implementation of data balancing approaches are utilised to guarantee a more equitable and accurate dataset as a method for training the prediction models. The integration of machine learning and deep learning algorithms is aimed at utilizing the predictive capabilities of the aforementioned technologies in a unified manner, thus capitalising on the unique strengths of each to enhance the overall efficiency of the fraud detection system. The project aims to combine these different but complementary features to provide a novel and efficient approach to detecting credit card fraud, which is a substantial contribution to the research field and creates a foundation for more secure and dependable financial transaction systems.

3.4 Research Questions

This section outlines the research questions which are addressed herein to achieve the objectives as mentioned in Chapter 1. The research questions are as follows.

How does the integration of geolocation and temporal data with data balancing techniques affect the accuracy and efficiency of machine learning while using deep learning algorithms in detecting Credit-Card Fraud in imbalanced transaction datasets?

3.5 Conclusion

The chapter commences with the identification of the gaps. A formal definition of the problem that is addressed herein was presented. The identified problem was subsequently presented in section of research questions that should be addressed to solve the defined problem. Furthermore, various research approaches are described and discussed.

4 RESEARCH METHODOLOGY

4.1 Proposed Approach

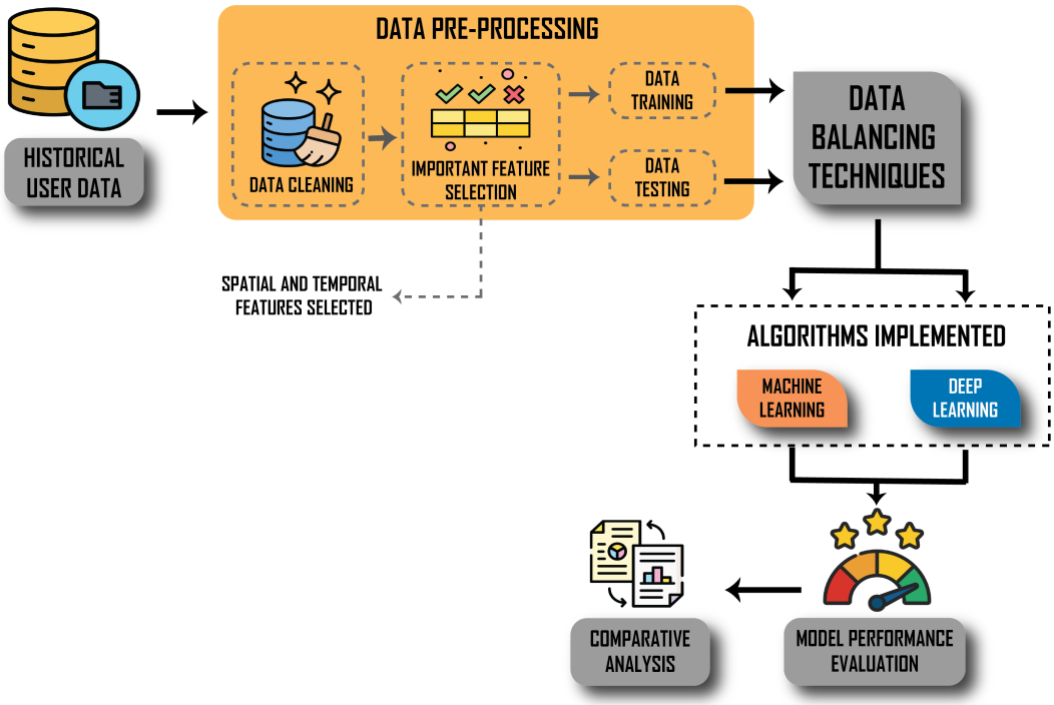

Figure 2. The Proposed Approach

The Proposed Approach that is utilized herein is depicted in Figure 2. We commence by analysing the unprocessed history user data, perform data processing on the historical user data, and subsequently assessing several machine-learning and deep-learning algorithms. The first step involves subjecting the raw historical user data to a thorough data cleaning procedure to eliminate any inconsistencies, inaccuracies, or unnecessary data, hence ensuring the quality of the dataset. Subsequently, we transit into feature selection, which is a crucial phase, explicitly focusing on the indispensable spatial and temporal attributes for the analysis.

After the dataset is refined, it is divided into sets for training and testing. This partition enables the researchers to train the models efficiently while allocating a portion of the data for future evaluation of their predicting capabilities. Subsequently, we proceed to the subsequent phase, where we utilize data balancing techniques to ensure a balanced portrayal of classes within the dataset, thereby mitigating any possible biases that may compromise the correctness of the proposed model.

Furthermore, the research proceeds to execute various algorithms, categorised into machine learning and deep learning. We employ eight distinct machine learning algorithms and two deep learning algorithms. Each category contains a collection of algorithms that have undergone extensive training using the pre-processed dataset. Following the training process, a comparative analysis is conducted to systematically evaluate and compare the performance of each algorithm. This phase is of utmost importance: it enables the researchers to determine each algorithm's robustness and comparative efficacy when implemented on the particular dataset.

This procedure culminates in model performance evaluation, during which various evaluation metrics are utilised to critically assess the models' success. The assessment serves as the fundamental pillar of the investigation, thereby affording the scholars with perceptive data that shapes the path of the conclusions. The illustrated procedure highlights the systematic and cohesive strategy in identifying and assessing the most appropriate machine learning and deep learning methods as a method for achieving the research goals.

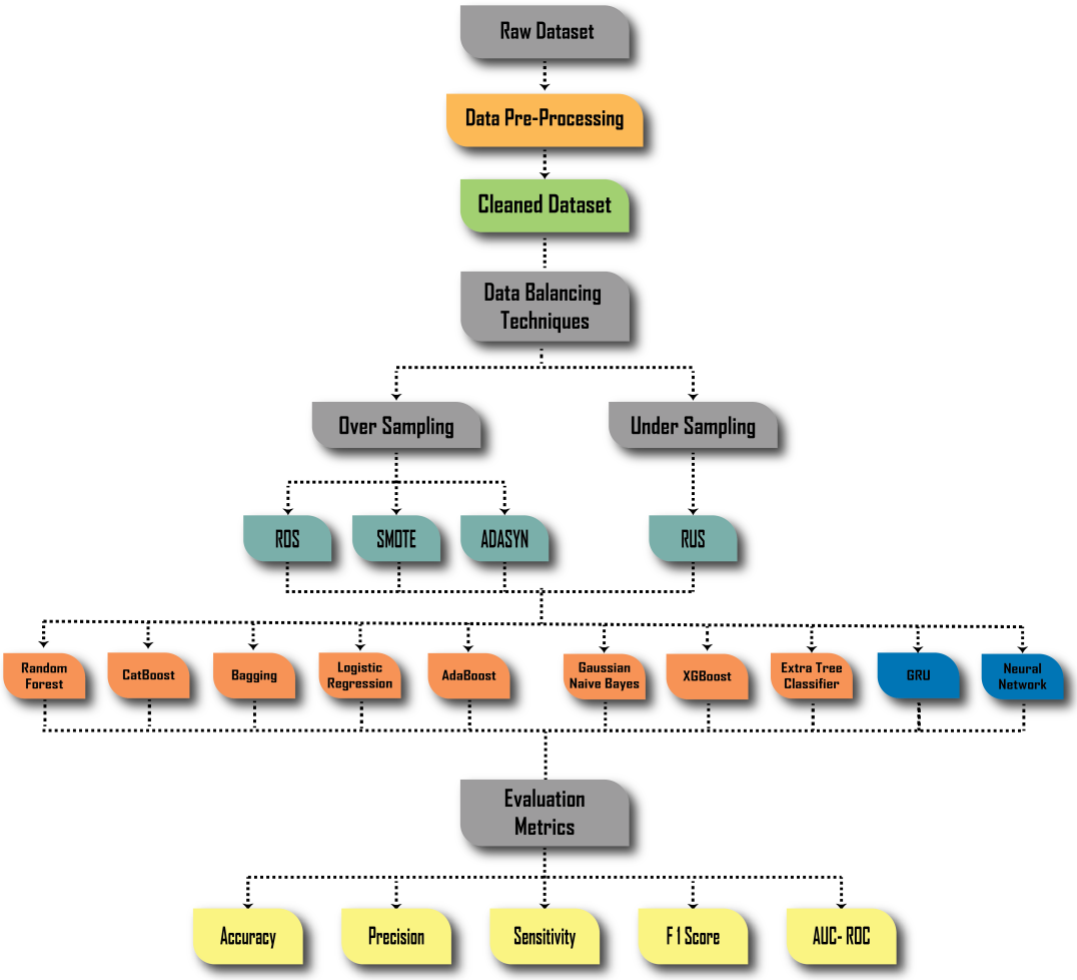

Figure 3. Proposed process flow in this research

Figure 3 summarises the entire process flow of this research. It provides a graphical representation of every stage in the analytical process, illustrating the progression from unprocessed data to the ultimate assessment; thus, it offers a good understanding of the proposed approach.

4.2 Introduction

As stated in Chapter 2, an extensive collection of literature comprises research that has attempted progress toward addressing the challenges associated with Credit-Card Fraud detection. Nevertheless, from the discussions presented in Chapters 2 and 3, it is evident that notable gaps still remain unaddressed. Chapter 3 offers an extensive analysis of the gap and the research topics that are intended to address this critical issue. In addition, this chapter provides a comprehensive summary of the data preparation methods, the Exploratory Data Analysis (EDA) conducted in the research, and a description of the Machine Learning and Deep Learning techniques that were chosen for application. Furthermore, we discuss the data balancing methodologies used herein. Additionally, it addresses the performance criteria utilized in evaluating the proposed approaches.

This chapter is organised as follows: In Section 4.2, the proposed approach is explained. In Section 4.3, data pre-processing commences with an elaborate overview of the dataset and outlines the procedures for cleaning and selecting the crucial features for preparing the dataset to process further, thus ensuring the data is appropriate for the implemented models. Section 4.4 presents various data-balancing techniques that are implemented. In Section 4.5 (Model Development), attention is directed towards the employed model algorithms. Section 4.6 explores the performance classification metrics that are utilized to assess the models' effectiveness. In section 4.7, we investigate the EDA. Finally, Section 4.8 concludes the chapter.

4.3 Data Pre-Processing

Pre-processing data is an essential component of any data analysis and modelling procedure, especially in the fraud-detection domain, where data quality and integrity are of utmost importance. This subsection provides a comprehensive account of the meticulous preprocessing methods utilised on a simulated credit card transaction dataset by emphasizing the measures implemented to adequately

prepare the data for efficient model training and analysis. The initial phase of the proposed methodology involves rigorous data pre-processing to ensure the integrity and quality of the input data.

4.3.1 Dataset Overview

The dataset utilised herein encompasses a variety of simulated credit card transactions, including both authentic and fraudulent activities. The dataset comprises transactions that occur between January 1, 2019, and December 31, 2020, thus providing an extensive examination of temporal trends. By capturing the interactions of 1,000 consumers with 80 distinct merchants, this dataset offers a wealth and variety of transactional information.

The data was produced utilising the Sparkov Data Generation utility, a specialised instrument developed for the simulation of authentic credit card transaction data. This GitHub-hosted utility, which was created by Brandon Harris, functions as a resilient instrument for generating synthetic datasets that simulate real-world transactional patterns exceptionally. Using predefined merchant and consumer categories, the transactions were generated with the assistance of the "faker" Python library. By following this methodology, a diverse and authentic dataset is obtained, comprising various consumer profiles that differ in regard to location, gender, age, and transactional attributes such as quantities and frequency.

The data has been split into two main files:

- fraudTrain.csv: comprises training data, which primarily consists of transactions and labels.
- fraudTest.csv: A distinct set of transactions provided for model evaluation in the interest of testing.

The aforementioned files contain an extensive collection of information that is crucial for understanding transactional contexts, including but not limited to transaction amount, times, dates, and customer information. The comprehension of the context and patterns of transactions, which exert a pivotal role in the identification of fraudulent activities, is contingent upon these attributes.

4.3.2 Data Cleaning and Transformation

Preprocessing commenced with the training and testing datasets being concatenated to create a single, unified dataset. The integration of these datasets facilitates a comprehensive cleansing procedure and guarantees uniformity in data manipulation and feature development throughout the training and testing stages. Extensive data cleaning was performed to improve the dataset's overall quality. Important stages comprised

- *Time Conversion*. The string representation of the transaction date and time was transformed into a datetime object, which enables the extraction of time-based features that may be crucial in detecting fraudulent patterns and facilitates time-series analysis.
- *Handling Missing Values*. For effective management in cases where missing values were identified in the dataset, a forward-fill method was implemented. By employing this approach, it is guaranteed that anything missing in the data will not negatively impact the model's learning process.
- *The engineering of features*. To enhance its utility as a feature in machine learning models, the transaction timestamp underwent an additional conversion into a numeric format, such as Unix time.

Data cleaning is crucial for the integrity of the model. The 'trans_date_trans_time' column is converted to a datetime object and subsequently into a numerical format for analysis. Missing values are addressed using forward filling. This step is critical for maintaining the continuity and relevance of the data. The data cleaning process involved handling missing values and inconsistencies. We employed a forward-fill method (fillna(method='ffill')) to address missing values, maintaining the sequential integrity of the dataset. Additionally, the trans_date_trans_time column, initially in datetime format, was converted to a numeric format for analytical compatibility. This transformation was crucial for integrating time-based features into the proposed models.

4.3.3 Important Feature Selection

The selection and preparation of features serve a crucial role in the effectiveness of machine learning algorithms within Credit-Card Fraud detection. In the feature engineering phase, we emphasised spatial–temporal analysis due to its significant

contribution in detecting fraudulent patterns. This transformation was performed to optimise the predictive capability of each attribute in the model.

The task of detecting Credit-Card Fraud can be complicated by the limited availability of publicly available datasets with explicitly labelled attributes. Consequently, researchers have been compelled to make assumptions when choosing features from datasets that lack unambiguous labelling. The dependence on assumptions can potentially distort the outcomes significantly, hence compromising the precision of the fraud-detection methods.

Contrastingly, the proposed thesis is further supported by including a labelled dataset of historical users, which enables the researchers to transcend the presumptions and make feature selections grounded in empirical data. Precise spatial attributes, specifically longitude and latitude, have been deliberately selected due to their capacity to provide an unambiguous geographical reference point. In addition, precise transaction times are utilized to represent the temporal dimension. Through this endeavour, we strive to surpass the traditional constraints encountered in this domain and develop a system capable of identifying fraudulent behaviour with increased precision and dependability.

Moreover, incorporating spatial–temporal analysis in the study is not only a procedural requirement but rather a deliberate decision made to improve the precision of the proposed fraud detection system. By carefully choosing longitude and latitude parameters, transactions may be precisely delineated geographically, thus offering crucial context that is sometimes absent in conventional models. Supported by a comprehensive temporal analysis, the proposed technology can perceive the complex details of transaction patterns, thereby distinguishing between valid conduct and possible fraudulent activities. The access to labelled data enables the researchers to provide a high level of information, which can potentially lead to a robust model that can identify fraud with a considerably more significant level of accuracy. The unique benefit of the study distinguishes it from others, thus establishing a solid basis for the future creation of a dependable and efficient fraud-detection system.

4.3.4 Model Preparation and Training

Following the preprocessing stage, the dataset was divided once more into the original train and test sets, with the testing data retaining its integrity as unobserved data for the purpose of model evaluation. Evaluating the model's performance and its capacity to extrapolate to novel, unobserved data heavily relies on this division.

The data was then split back into train and test sets using train_test_split, with a test size of 20%. We defined an initial neural network model architecture using the Sequential model from Tensor Flow's Keras API. The model comprised Dense layers with ReLU and sigmoid activations and Dropout for regularisation, and was compiled using the Adam optimiser and binary cross-entropy loss.

The model was trained on the training data for 50 epochs with a batch size of 32, thus incorporating a validation split of 20% to monitor the generalisation performance. The model's efficacy was subsequently evaluated on the test data, calculating key metrics such as accuracy, precision, recall, F1-score, and AUC-ROC to assess its performance as are presented in the following sections.

4.4 Data Balancing Techniques

A significant issue in fraud detection is class imbalance, which is defined as a scenario where the proportion of genuine transactions to illegal ones is unbalanced (Phua et al., 2004). A substantial risk of model bias arises from the infrequency of fraudulent cases observed in financial datasets, which can lead to inadequate generalisation and a propensity to disregard fraudulent activities (He and Garcia, 2009). To address this anomaly, we implemented a variety of data balancing strategies, each of which made a distinct contribution to class imbalance management.

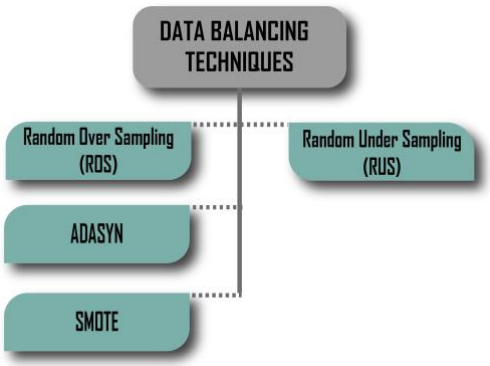

Figure 4. Data balancing techniques applied

In the subsequent section, the numerous data balancing techniques utilised herein are described in detail.

A. Random Over-Sampling (ROS)

Random oversampling is a technique that replicates instances of the minority class at random until the class distribution becomes balanced. By employing this simple methodology, it is possible to provide the model with a sufficient number of examples belonging to the minority class, accompanied by their corresponding alternatives, prior to incorporating them into the testing set. This procedure is aimed at increasing the evenness of data distribution .

B. SMOTE (Synthetic Minority Over-Sampling Technique)

SMOTE is a popular technology: it can produce synthetic samples instead of only duplicating those that already exist. It generates novel instances of the minority class by incorporating across many nearby examples. This strategy is advantageous because it brings more variety into the dataset, hence minimising the possibility of overfitting in comparison to conventional over-sampling. The advantage of SMOTE in fraud detection arises from its capacity to generate intricate, non-linear decision boundaries, thus enabling models to identify more subtle types of fraudulent activity.

C. ADASYN (Adaptive Synthetic Sampling)

ADASYN, also referred to as Adaptive Synthetic Sampling, is categorised as an oversampling technique. It aims to target and resolve the class imbalance issue by creating artificial samples for the underrepresented class. ADASYN expands upon the SMOTE principles by generating synthetic samples and specifically targeting the samples that are more challenging to comprehend. The adaptive technique focuses on the more difficult sections of the feature space by considering the number of majority-class samples in their neighborhood, which might potentially enhance the model's performance in identifying subtle patterns of fraud.

D. Random Under Sampling

Reducing the number of examples that belong to the majority of the class is the objective of random under sampling, which stands in contrast with over sampling.

This approach particularly advantageous in scenarios with limited computational resources because it leads to a dataset that is both more balanced and smaller. On the other hand, the approach can lead to the loss of potentially practical knowledge from the majority class, which could be essential for model learning.

4.5 Implemented Algorithms.

The proposed research utilises a collection of advanced algorithms to identify patterns that are indicative of fraudulent activities in financial information. We combine ensemble approaches, which harness the combined strength of several learning algorithms to enhance forecast accuracy, and probabilistic models, which evaluate the probability of outcomes. Herein, we examine the reasoning, approach, and fundamental mathematical concepts that support each strategy.

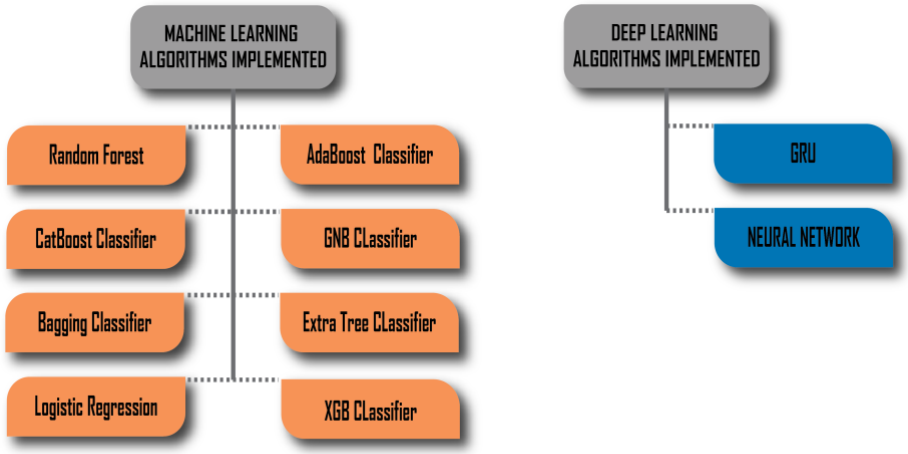

Figure 5. Algorithms implemented in this research

The research focuses on the utilisation and effectiveness of different algorithms to address financial fraud, specifically in the context of fraudulent transactions. These algorithms assist in detecting complex patterns and discrepancies that indicate fraudulent operations. This section explains the methodology utilised in the work, explicitly emphasising several machine learning algorithms and deep learning algorithms.

4.5.1 Machine Learning Algorithms

In the subsequent section, comprehensive explanations of the machine learning algorithms utilised herein are provided.

A. Random Forest (RF)

Random Forest is a widely utilized ensemble learning technique known for its flexibility and adaptation. The algorithm involves the creation of numerous decision trees throughout the training process. The output is determined by selecting the class that appears most frequently among the trees (for classification) or by calculating the average prediction of the individual trees (for regression). The mathematic principle of this algorithm is as follows:

$$P(E) = \sum_{k=\lceil \frac{B}{2} \rceil}^{B} \binom{B}{k} p^k (1-p)^{B-k}$$

B. CatBoost

CatBoost is an advanced boosting algorithm that excels in effectively handling categorical information. The key feature of CatBoost is its capacity to mitigate overfitting by utilising ordered boosting, a permutation-based approach that differs from the conventional boosting technique. In addition, CatBoost inherently manages categorical characteristics, hence reducing the necessity for substantial preprocessing.

By including CatBoost into the proposed approach, we seek to exploit its sophisticated treatment of categorical variables and its resilience against overfitting, both of which are essential for accurately predicting spatial patterns in fraudulent transactions.

C. Bagging Classifier

Bagging Classifier also referred to as Bootstrap Aggregating, is an ensemble method that enhances the stability and precision of machine learning algorithms. It decreases fluctuations and mitigates the risk of overfitting. On the other hand, decision tree approaches are the typically utilized and can be employed with any method. Bagging is a specific instance of the model averaging methodology. The Mathematical Equation is expressed as follows:

$$\hat{\beta}^{ridge} = \underset{\beta}{\operatorname{argmin}} \left\{ \sum_{i=1}^{n} (y_i - X_i\beta)^2 + \lambda \sum_{j=1}^{p} \beta_j^2 \right\}$$

λ denotes the complexity parameter that controls the value of shrinkage.

D. Logistic Regression (LR)

Logistic Regression is a fundamental statistical technique that estimates the probabilities of classification issues. It is especially suitable for binary classification jobs, such as differentiating between fraudulent and legitimate transactions. LR possesses multiple properties that provide a valid rationale for its utilisation in the current research, despite its simplistic nature. The mathematic equation of this algorithm is as follows:

$$P(Y = 1) = \frac{1}{1 + e^{-(\beta_0 + \beta_1 X)}}$$

where *P* (Y = 1) denotes the probabilities of the class labeled '1', $\boldsymbol{\beta}0$ denotes the intercept, and $\boldsymbol{\beta}1$ denotes the coefficient for the feature *X*

E. AdaBoost classifier

The AdaBoost classifier is a machine learning algorithm, also referred to as Adaptive Boosting, is a boosting algorithm that adapts to the difficulty level of individual data points. The aforementioned algorithm prioritises the occurrences that preceding classifiers incorrectly classified.

F. Gaussian Naive Bayes (GNB)

Gaussian Naive Bayes is a probabilistic classifier that utilises Bayes' theorem, assuming that each pair of characteristics is independent. GNB is highly efficient when the assumption of feature independence is valid. GNB is crucial in fraud detection owing to its efficacy. The Mathematical Equation is expressed as follows:

The probability of a feature x given a class *c* is as follows:

$$P(x|c) = \frac{1}{\sqrt{2\pi\sigma_c^2}} \exp\left(-\frac{(x - \mu_c)^2}{2\sigma_c^2}\right)$$

where μ_c denotes the average of the feature for class *c*, and denotes the variance of the feature for class *c*.

G. XGBoost Classifier

Extreme Gradient Boosting (XGBoost) is a sophisticated implementation of the gradient boosting algorithm well-known for its mobility, flexibility, and efficacy. Popularity has increased for XGBoost in the context of Credit-Card Fraud detection owing to its capacity to manage massive and unbalanced datasets effectively. The mathematic equation of this algorithm is as follows:

$$\mathrm{Obj}(\Theta) = L(\Theta) + \Omega(\Theta)$$

H. Extra Trees Classifier

The Extra Trees Classifier is an ensemble learning approach with essential similarities to the Random Forest algorithm. Its efficacy in Credit-Card Fraud detection is attributed to its capacity to manage extensive datasets characterised by high dimensionality and unbalanced classes, which are prevalent in fraud-detection scenarios.

4.5.2 Deep Learning Algorithms

Detailed descriptions of the different deep learning algorithms utilized herein are listed in the subsequent section.

A. Gated Recurrent Unit (GRU)

The Gated Recurrent Unit (GRU) is a popular architecture of recurrent neural network (RNN) that is extensively utilized in the analysis of data sequences, including time-series analysis, natural language processing, and, specifically, Credit-Card Fraud detection in our scenario. Because GRUs thrive in detecting connections in sequences of different durations, the technology is crucial for identifying patterns that indicate unauthorised activities in credit card use data.

In the detection of credit card fraud, a GRU can examine transaction sequences. Every transaction, such as time of day, location, or quantity, can be depicted as a vector, and these sequences can teach the GRU to recognise irregularities that could potentially indicate fraudulent behavior.

B. Neural Network (NN)

Neural Networks, specifically when applied to Credit-Card Fraud detection, represent a type of deep learning architecture that imitates the information processing mechanism of human brains. Each "neuron" or layer is composed of interconnected elements that execute a basic computation. To generate the ultimate result, the result of these algorithms is subsequently propagated layer by layer within the network.

Credit-Card Fraud detection can be significantly enhanced by neural networks, owing to their capacity to acquire knowledge of intricate patterns and generate precise prognostications. However, their effectiveness is significantly influenced by the caliber and volume of the training data, in addition to the precise configuration of the network's architecture and parameters.

4.6 Evaluation metrics

Various evaluation metrics were utilised to evaluate the models' efficacy; these indicators are essential for conducting a thorough and proper assessment of performance, particularly in light of the dataset's imbalanced class distribution among the metrics utilised as follows:

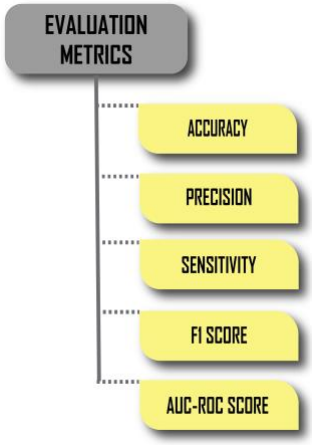

Figure 6. Evaluation metrics

A. Accuracy

Accuracy is the most often utilized metric for assessing the performance of a classification issue. It simply represents the proportion of accurately predicted observations to the total prediction made. The formula for Accuracy is illustrated as follows:

$$Accuracy = \frac{True\ Positives\ (TP) + True\ Negatives\ (TN)}{Total\ Number\ of\ Cases}$$

B. Precision

Precision reflects the level of correctness in positive prediction. The level of precision is determined by dividing the number of accurately predicted positive observations by the total number of expected positives. The measures are defined as follows:

$$Precision = \frac{True\ Positives\ (TP)}{True\ Positives\ (TP) + False\ Positive\ (FP)}$$

C. Recall Score (Sensitivity)

The Recall Score, also referred to as Sensitivity or True Positive Rate (TPR), indicates a model's capability to identify all the relevant examples in a dataset. Precision is the proportion of accurately anticipated positive observations out of all observations in the actual class. In contexts where the consequences of false positive detection are more severe than the errors associated with misclassifying negatives as positives, recall value assumes paramount importance. In medical diagnosis, for instance, failing to identify a genuine case of a disease (a false negative) could have severe consequences, whereas incorrectly diagnosing a condition (a false positive) might lead to less severe damage, which might be crucial in disease screening. The formula is displayed as follows:

$$Recall\ Score\ (Sensitivity) = \frac{True\ Positives\ (TP)}{True\ Positives\ (TP) + False\ Negative\ (FN)}$$

D. F_1 Score

The harmonic mean of Precision and Recall constitutes the F_1 Score. It facilitates the attainment of an equilibrium between Precision and Recall when such a balance is required and is exceedingly useful when balancing recall and precision, as in irregular class distribution scenarios. The formula of the F_1 Score is defined as follows:

$$F_1\ Score = 2\ x\ \frac{Precision\ x\ Recall}{Precision + Recall}$$

E. AUC-ROC Score

The AUC-ROC is a metric for evaluating the performance of classification issues across different threshold settings. The ROC curve is a graphical representation of the probability distribution, whereas the AUC defines the extent to which the classes may be distinguished (Narkhede, 2018). The ROC curve is generated by graphing the True Positive Rate (TPR) against the False Positive Rate (FPR) at different threshold values. The AUC is a metric that quantifies the likelihood of a positive instance being rated higher than a negative instance when picked randomly. It is an essential parameter for assessing the effectiveness of binary classifiers. In contrast to metrics such as Accuracy and Precision, AUC-ROC does not possess a singular formula. It is typically calculated using numerical techniques that rely on the ROC curve. The details are as follows:

- Receiver Operating Characteristics (ROC) Curve
  True Positive Rate (TPR) Commonly referred to as Recall Score or Sensitivity.

$$\boldsymbol{TPR = \frac{True\ Positives\ (TP)}{True\ Positives\ (TP) + False\ Negative\ (FN)}}$$

  The False Positive Rate (FPR) formula is defined as follows:

$$\boldsymbol{FPR = \frac{False\ Positives\ (FP)}{False\ Positives\ (FP) + True\ Negative\ (TN)}}$$

- AUC Calculation is as follows:
  1. It is obtained by plotting the TPR versus FPR at different thresholds.
  2. The AUC value varies between 0 and 1, where 1 indicates an ideal classifier, and 0.5 represents a random prediction.
  3. Typically, numerical techniques, including the trapezoidal rule, are applied when generating the AUC from the ROC curve.

4.7 Exploratory Data Analysis

4.7.1 Spatial Analysis of Fraudulent Transactions

The current research investigates the spatial patterns of fraudulent transactions, a crucial step in mitigating financial fraud. Collecting and analysing location data associated with fraudulent transactions is the first stage, which provides the opportunity to identify "hotspots" of fraudulent activity. Using this knowledge, regions or locations that are particularly susceptible to fraud can be identified.

Having identified these potential locations, the next step entails utilizing advanced mapping tools, which graphically depict the geographical distribution of fraud, thereby generating a clear depiction of the fraud landscape. Visual representation facilitates the understanding of spatial patterns of fraud, thus emphasising the urgency and specific areas of focus of the anti-fraud strategies.

A comprehensive understanding of spatial patterns is potentially a multipurpose skill. On the one hand, it could guide the development of strategic interventions aimed at fraud prevention and detection, particularly in regions where fraud is prevalent. On the other hand, these patterns could contribute to a deeper understanding of the spatial dynamics of financial crime.

The geographical patterns of fraudulent transactions are of global significance. Their findings bear extensive implications for mitigating financial deception. By identifying the locations where fraudulent activities occur most frequently, the research can influence global policy and preventative measures.

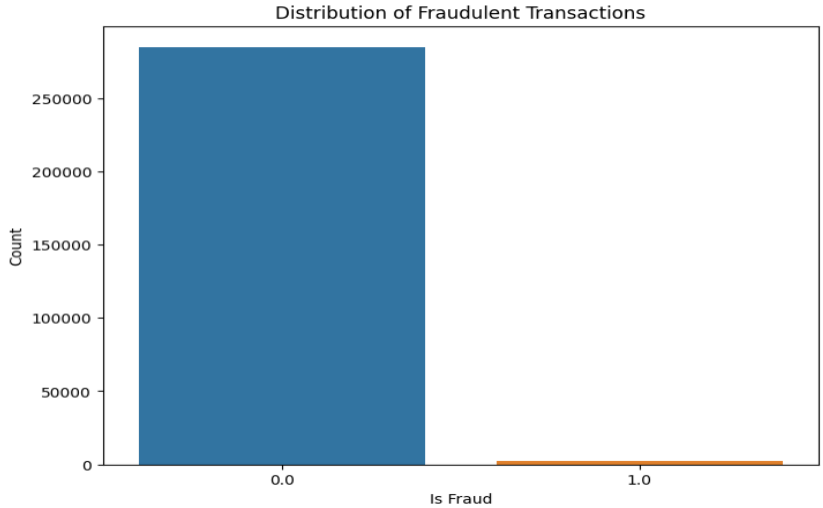

Figure 7. Distribution of transactions categorized as fraudulent and legitimate

Figure 7 displays a bar chart that visually represents the distribution of transactions categorised as fraudulent (labeled as "1") and non-fraudulent (designated as "0"). The chart illustrates a significant disparity between legitimate and fraudulent purchases. A pronounced bar on the chart denotes the significantly higher number of non-fraudulent transactions, in contrast to a tiny bar or line on the chart, which represents the exceedingly low or possibly insignificant number of fraudulent transactions.

Although the Figure 7 does not explicitly display spatial information, the uneven distribution implies that instances of fraud are probably few and may be clustered in particular areas. Thus, spatial analysis becomes crucial. By creating a visual representation of instances of fraud, you may pinpoint areas with high concentrations of fraudulent operations and gain insights into the spatial distribution patterns. The difference in distribution highlights the need for implementing focused anti-fraud measures. Due to the existing disparity, machine learning and deep learning models may encounter difficulties in identifying fraudulent operations. Hence, geographical analysis can provide insights for the formulation of location-specific approaches aimed at improving the identification and prevention of issues. Recognising that fraud occurrences are less common can potentially lead to significant impact might result in more strategic deployment of resources and more efficient policy development. By prioritising regions with a greater prevalence of fraudulent activities, resources can be allocated to the areas that require them the most. The bar chart highlights the necessity of employing sophisticated analytical methods to address the intricacies of fraud detection. The statement emphasises the importance of utilising geographical analysis to fully comprehend and address the problem of fraudulent transactions. The knowledge derived from these visualisations is crucial for developing efficient fraud-prevention tactics tailored to specific locations, thereby rendering the research highly pertinent and influential.

The boxplot compares two distributions: Transactions that are not fraudulent (is_fraud = 0), which displays the range, median, and any exceptional values for the transaction amounts where no fraud is discovered. Instances of fraudulent transactions (when the value of the variable "is_fraud" is 1), which exhibits the transaction amount attributes for instances where fraud is identified.

The median, also referred to as the central line of the box, represents the transaction amount that is in the middle when all transactions, both fraudulent and non-fraudulent, are arranged in ascending order. It is a statistical metric that provides information on the central tendency of the data. Significance in Spatial Analysis and Fraud Detection Pattern Recognition: The comparison may indicate that fraudulent transactions have a distinct distribution of amounts in comparison to legitimate transactions. For instance, if fraudulent transactions commonly entail lesser sums, this could indicate an evasion tactic where criminals want to avoid detection by refraining from triggering warnings that are configured for larger amounts.

Regional fraud characteristics: When location data is paired with the analysis, it may reveal that specific locations exhibit unique patterns in transaction amounts related to fraud. Fraudulent transactions of significant monetary value may tend to concentrate in prosperous regions, but less valuable fraud may be more prevalent across a wider geographical area.

Enhancing the precision of real-time fraud detection systems can be achieved by financial institutions through the adjustment of their monitoring systems to flag transactions falling within questionable ranges based on an awareness of the typical quantities associated with fraudulent transactions. By acknowledging the diverse magnitudes of fraudulent transaction values, it is possible to formulate distinct anti-fraud strategies that can be universally implemented while still being flexible enough to suit local contexts, which is especially crucial for global financial firms that should navigate varied financial environments through the analysis of transaction amounts and their correlation with geographical data. We may derive practical insights that enable the development of sophisticated, location-specific techniques for identifying and combating fraudulent activities. The boxplot is an essential tool for effectively presenting and understanding the complexities of financial data, eventually contributing to the overall goal of maintaining the safety of global financial transactions.

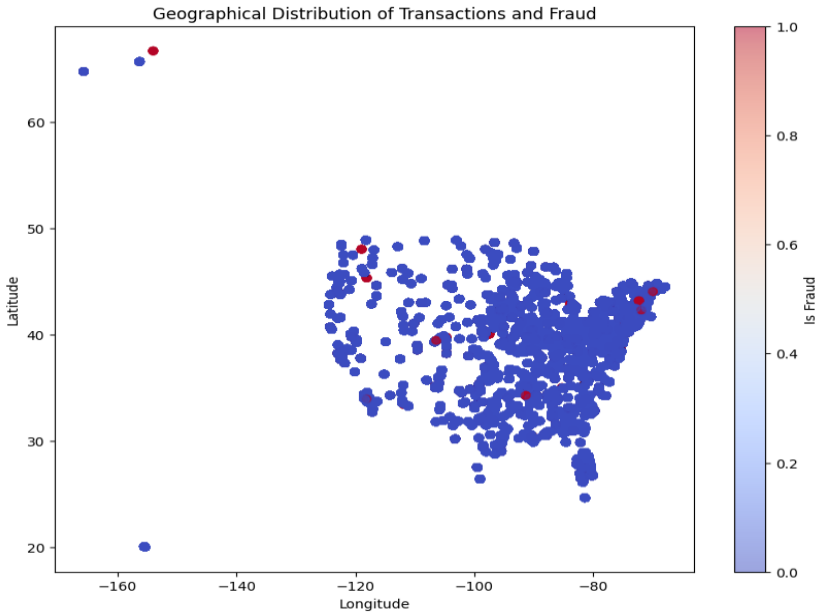

Figure 8. Geographical distribution of fraud and legitimate transactions

The Figure 8 produces a scatter plot that visually displays the geographic distribution of transactions, with a specific emphasis on detecting fraudulent activities. The scatter plot depicts transactions on a coordinate system, with the x-axis representing longitude and the y-axis representing latitude. Every point on the plot represents a transaction, and the color scheme (varying from cool to warm) distinguishes between non-fraudulent transactions and fraudulent ones. Non-fraudulent transactions are depicted at one extreme of the color spectrum, whereas fraudulent transactions are depicted at the opposite extreme.

By analysing the scatter plot, groupings or hotspots with a higher concentration of fraudulent transactions can be identified. These regions are highlighted with a noticeable color on the map. The plot can uncover distinct patterns, such as a higher occurrence of fraud in specific geographic regions(e.g., urban or rural areas), along specific trade routes, or within particular communities.

By visualising fraudulent transactions in specific places, researchers may strategise focused anti-fraud efforts. For example, if a city exhibits a greater incidence of fraudulent activities, it may be necessary to implement additional verification measures or launch targeted awareness programs there.

The occurrence of fraud specifically targeting international transactions or popular tourist destinations may prompt countries to collaborate as a method of mitigating inter-border fraud. The figure enables a rapid and instinctive comprehension of the

locations where fraudulent operations are occurring, which can be exceedingly crucial for identifying and thwarting future instances of fraud. The proposed research enhances the comprehension of the spatial dynamics of fraudulent transactions, thereby exerting a crucial role in the worldwide effort to combat financial crime.

4.7.2 Temporal Analysis of Fraudulent Transactions

There is no set schedule for fraudulent transactions; they could occur at any time. Understanding the temporal dimension is, therefore, essential for identifying patterns and trends. To achieve this, we investigate the temporal patterns of fraudulent transactions. The first step entails examining the frequency and distribution of fraudulent transactions across various periods, which may comprise daytime hours, weekdays, and months. Analysing these patterns provides valuable insight into when fraudulent activity peaks, thus enabling scholars to develop predictive models of fraudulent behaviors.

The next stage, after developing predictive models, entails formulating strategies based on the revealed trends. These strategies seek to reduce fraudulent transactions and safeguard customers' financial assets during high-risk periods. The temporal analysis could significantly reduce the possibility of financial losses.

In addition, the temporal analysis could reveal seasonal patterns in fraudulent activity. During certain periods of the year, these findings can be utilized to design fraud-prevention measures specifically tailored to the season. Therefore, the temporal analysis of fraudulent transactions becomes a crucial aspect of the research.

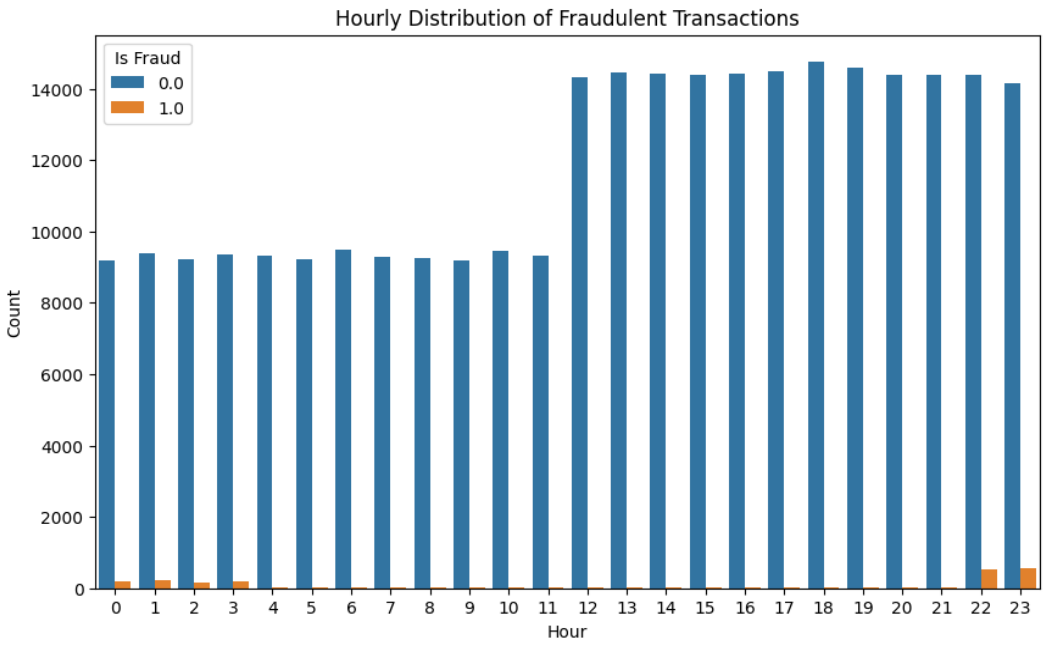

Figure 9. Distribution pattern of fraudulent transaction at an hourly basis

Figure 9 conducts the EDA that precisely examines the temporal elements of fraudulent transactions, with a particular focus on the distribution patterns at an hourly and weekly level. The figure initially retrieves the hours and days of the week from the timestamp of transactions. The figure visually represents the occurrence rate of fraudulent and non-fraudulent transactions for each hour of the day.

- Hourly Patterns: The count plot produced by the algorithm is anticipated to display the distribution of fraudulent transactions across various hours of the day, which can expose specific instances when fraudulent activity is elevated, thus indicating periods when fraudsters are more active or when systems may be more susceptible.
- Day of the Week Trends: By analysing weekly transactions, particular days when fraudulent activities reach their highest point may be discovered. For example, weekends or particular weekdays might exhibit a greater incidence of fraudulent activities.

Possessing a clear understanding of the time-based patterns of fraudulent transactions can crucially impact anti-fraud measures. A potential approach for preventing fraud is adopting more surveillance during high-risk periods, such as specific hours or days. Analysing the temporal patterns of fraud can provide

valuable information for determining how resources, such as people and technology tools, should be distributed. Additional resources should be allocated to periods characterised by a higher incidence of fraudulent acts in the past.

The detection of comparable patterns in many regions may indicate global patterns of fraudulent activities, which can facilitate worldwide collaborative efforts and the formulation of universally accepted standards for the prevention of fraud. Predictive analytics relies heavily on temporal data to effectively detect and prevent fraud. Machine learning algorithms can be trained to predict fraudulent transactions by analysing temporal patterns, potentially preventing fraud in advance.

Temporal analysis is an essential component of EDA, thus providing practical insights that may be utilised to improve fraud detection systems and preventive actions. EDA can impact operational planning by determining the scheduling of personnel shifts for fraud monitoring teams. The findings can inform the development of timely laws or the acceptance of optimal practice standards for transaction processing.

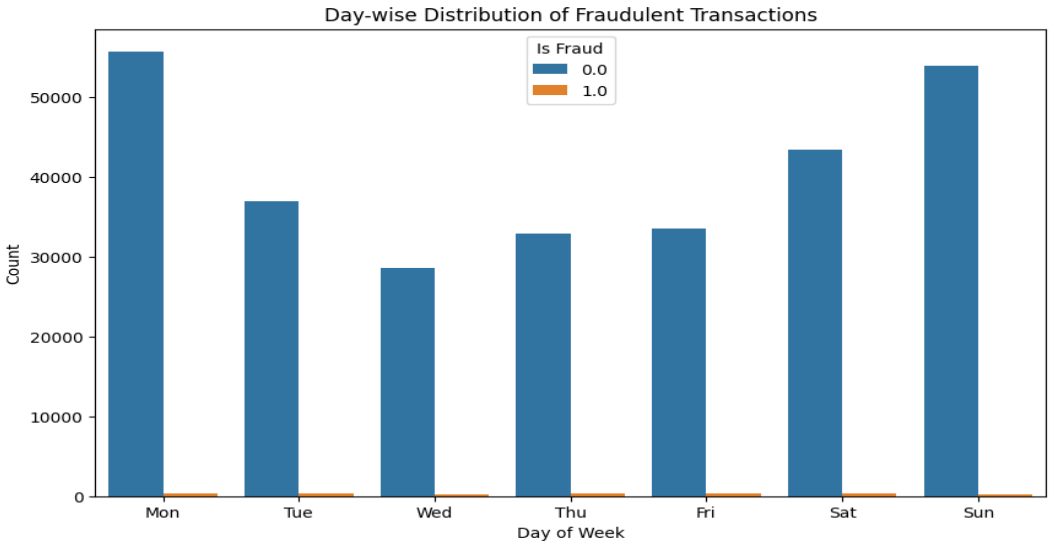

Figure 10. Distribution of fraudulent and non-fraudulent transactions on a day-to-day basis during a week

Figure 10 illustrates the distribution of fraudulent and non-fraudulent transactions on a day-to-day basis during a week. The figure classifies transactions based on the days of the week, ranging from Monday to Sunday, and utilizes color-coding to distinguish between fraudulent transactions (often denoted as '1') and non-fraudulent transactions (denoted as '0'). The significance of applying spatial exploratory data analysis is as follows:

- The figure displays the occurrence rate of transactions for each day of the week. It utilizes two bars per day to differentiate between fraudulent and non-fraudulent transactions. This visualisation identifies any conspicuous patterns or trends in fraudulent activity on particular days. By examining the vertical length of the bars, one can deduce the days that exhibit a greater number of instances of fraudulent activity. A higher bar indicating 'Is Fraud' on a specific day indicates a larger volume of fraudulent transactions in comparison to other days.
- The Temporal Dynamics of Fraud analysis incorporates a temporal aspect into the geographic Exploratory Data study (EDA), thus enabling a comprehensive comprehension of the specific times and locations where fraudulent actions are more likely to occur. For example, if there are days with elevated levels of fraud, it would be advantageous to examine whether these surges are linked to specific geographical areas.

Acquiring knowledge on particular days characterised by elevated rates of fraudulent activities can enable researchers to devise precise responses. For instance, if there is a significant increase in fraudulent activities on weekends, it would be prudent to implement extra surveillance or precautionary measures during these periods. A comprehensive fraud prevention plan can be enhanced by including temporal and spatial data, thereby enabling the consideration of both the location and timing of fraudulent activities.

The figure bears implications for the development of cross-border fraud prevention measures, as it reveals that certain fraud tendencies can transcend national boundaries. The patterns observed on a daily basis may indicate more extensive criminal actions beyond local or regional limits. When spatial data is integrated, it can provide a comprehensive perspective on fraudulent activity, thus immensely enhancing the effectiveness of fraud prevention techniques.

This visualisation offers a comprehensive understanding of the chronological trends associated with fraudulent transactions. Analysing the evolution of fraud patterns over time assists in detecting periods of increased risk, which may be associated with spatial susceptibility. Observing unique surges in fraudulent transactions may indicate the existence of coordinated fraud activities in particular places.

Integrating location data with time patterns enables a comprehensive understanding of fraudulent conduct from multiple perspectives. By examining the timing and location of fraudulent activities, one can acquire a more complete comprehension of the matter. The analysis can provide information to guide preventive measures. For example, if there is a sudden increase in fraudulent activities on specific days, it would be prudent to introduce extra verification measures during transactions on those days.

4.8 Conclusion

This chapter provides a comprehensive explanation of the preference for gated recurrent units (GRUs) over alternative models such as long short-term memory (LSTM) units or sequential transformers. Gated Recurrent Units (GRUs) were selected for their superior efficiency in modelling temporal sequences, utilising fewer parameters than Long Short-Term Memory (LSTM) networks. This results in expedited training times and diminished computational demands, which are essential for real-time fraud detection applications. GRUs differ from LSTMs by merging the forget and input gates into a single update gate, which streamlines the model architecture while preserving similar performance, particularly in cases where the temporal depth of data is not excessively deep.

The selection of evaluation metrics—Accuracy, Precision, F1 Score, ROC-AUC Score, and Recall—aims to thoroughly assess the model's performance across various dimensions essential for fraud detection. Accuracy is inadequate when addressing imbalanced datasets commonly encountered in fraud detection contexts. Precision and Recall offer insights into the model's capacity to accurately identify fraudulent transactions while minimising false positives, which can adversely affect real-world applications. The F1 Score serves as a valuable metric by balancing Precision and Recall, thereby encapsulating the model's overall effectiveness in fraud detection. Finally, the ROC-AUC Score is included as it demonstrates the model's ability to differentiate between classes at different threshold levels, which is essential for adjusting the model to meet specific operational needs.

Chapter 5 proceeds with a performance evaluation of eight varieties of ML Algorithms on Raw data and is followed by the other two effective DL algorithms, which are also trained using raw data. By comparing the distinct outcomes of ML

and DL when applied to unprocessed data, we can better understand Chapter 6, where we shall apply the data balancing technique.

5 EVALUATION OF MACHINE AND DEEP LEARNING ALGORITHMS ON RAW DATA

5.1 Introduction

In the modern digital-banking environment, the increase in online transactions has been accompanied by a growth in the complexity and frequency of fraudulent operations. The continuous COVID-19 epidemic has further expedited this pattern, thereby emphasising the need for strong and dependable fraud-detection systems. This chapter deeply examines the thorough assessment of several machine and deep learning algorithms utilized on raw transactional data, analysing their effectiveness in differentiating between genuine and fraudulent operations.

Although the significant relevance of machine learning in fraud detection is well established, it poses a distinct set of obstacles, with the class imbalance issue being the most prominent. Usually, the number of valid transactions is far higher than the number of fraudulent ones, leading to models that have a tendency to predict transactions as legitimate. This behavior may lead to a significant increase in false negatives, hence enabling the avoidance of fraudulent transactions. To address this issue, the research utilizes a diverse range of machine learning and deep learning techniques, including Random Forest Classifiers, CatBoost, Bagging, LR, XGB, AdaBoost, Gaussian, Extra Trees, GRU, and Neural Networks. Each of these algorithms offers a distinct methodology for managing raw data and addressing class imbalance.

To analyse the effectiveness of these algorithms, a particular set of evaluation metrics has been utilized. These metrics include the recall score, precision score, F1 score, specificity, ROC-AUC score, and accuracy score. These measures provide a comprehensive perspective on the performance of each model, thereby emphasising their ability to accurately identify genuine positives and true negatives, while also indicating potential shortcomings in regard to precision and overall accuracy. The recall score is of utmost significance in fraud detection since it measures the model's capacity to identify fraudulent transactions. The precision score guarantees that the transactions identified as fraudulent are indeed fraudulent, hence reducing any disruption to users. The f1 score combines the metrics of precision and recall, thus providing a balanced performance measure. On the other

hand, specificity evaluates the model's ability to accurately identify valid transactions. The ROC-AUC score provides a comprehensive evaluation of the model's ability to distinguish between different classes, while the accuracy score provides a broad measure of its performance.

This chapter aims to examine these criteria to assess the algorithms' capacity to identify patterns indicative of fraud in imbalanced datasets. The results of this assessment will not only showcase the effectiveness of individual models but also the need for creative methods of addressing the class-imbalance problem.

Moreover, the implementation of these models should take into account computational efficiency and scalability. Financial institutions need systems that deliver high accuracy and minimal false positives while processing transactions in real time without causing delays. It is essential to evaluate model performance by considering these operational aspects to guarantee that the solutions are scalable and practical.

Implementing these machine learning and deep learning strategies allows financial institutions to improve the effectiveness of their fraud detection systems greatly. This results in enhanced security, increased user confidence, and greater efficiency in processing financial transactions, showcasing the practical relevance of these findings in real-world situations.

The chapter is structured to facilitate a clear and cohesive investigation of the research topic. It begins by providing a brief introduction that sets the context for the following in-depth analysis. Subsequently, the chapter transits into Section 5.2 Results of Machine Learning Algorithms on Raw Data and Section 5.3 Deep Learning Algorithm Results on Raw Data. The Discussion Regarding the Outcome is subsequently addressed in Section 5.4, and the chapter is ultimately discussed in Section 5.5. This last section connects the chapter's primary concepts while critically commenting on the research.

5.2 Results of Machine Learning Algorithms on Raw Data

5.2.1 Random Forest

Figure 11 displays the Receiver Operating Characteristic (ROC) Curve for the Random Forest Classifier. The ROC curve of the Random Forest Classifier exhibits

a consistently high performance in accurately classifying transactions, as evidenced by its steep slope, which signifies excellent forecast accuracy. Thus, the need for efficient fraud detection systems in the fast-growing digital economy is supported, thereby emphasising the classifier's capacity as a dependable tool in the continuing efforts against cybercrime.

The Random Forest Classifier demonstrates its prediction-based resilience with a high accuracy score (0.96545). It demonstrates a remarkable equilibrium between recall and accuracy for both categories, thus indicating its effectiveness in accurately differentiating between fraudulent and non-fraudulent transactions. However, it still has a slightly lower recall rate for class 1 (0.93138), which indicates that it excels at predicting non-fraudulent instances but might benefit from additional improvement in detecting fraudulent cases. This is particularly crucial in the fraud-detection context.

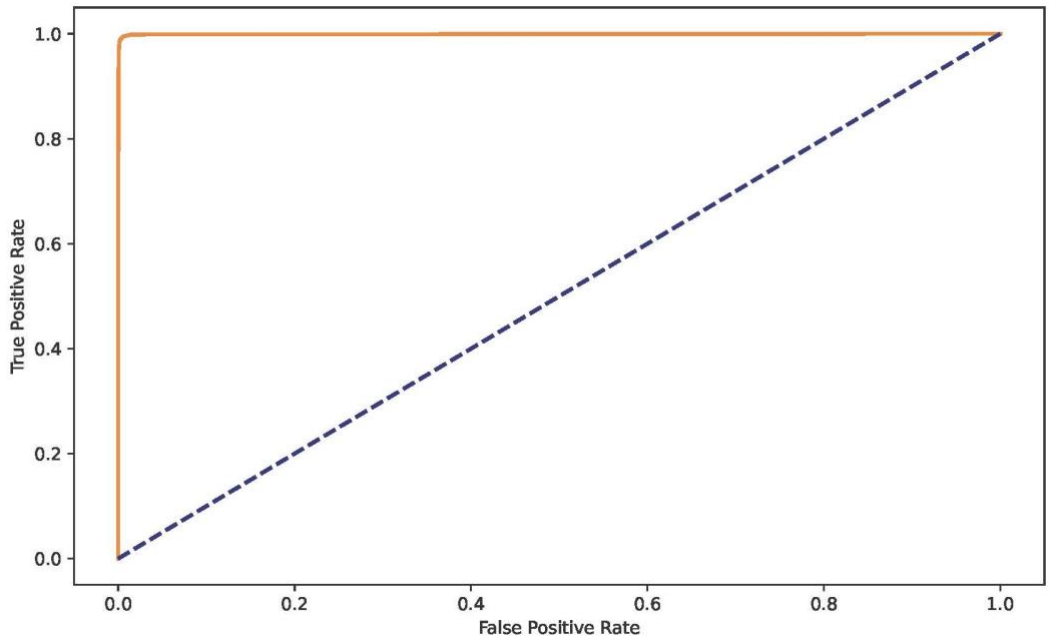

Figure 11. ROC curve of the Random Forest Classifier reflecting its efficacy in identifying fraudulent transactions.

5.2.2 CatBoost

Figure 12 displays the ROC Curve specifically for the CatBoost algorithm. The CatBoost ROC curve exhibits a high-performing model with exceptional classification prowess, which is crucial in the context of the heightened usage of digital payments that are attributable to the pandemic.

Although the CatBoost model exhibits a commendable accuracy score for classifying instances as class 0, its recall rate is quite poor (0.16256), which indicates that a significant amount of fraudulent transactions may be undetected. The accuracy value is satisfactory (0.99501), thus indicating that it accurately predicts fraud cases most of the time. Nevertheless, the inability to identify instances of fraud is a significant vulnerability that merits research attention.

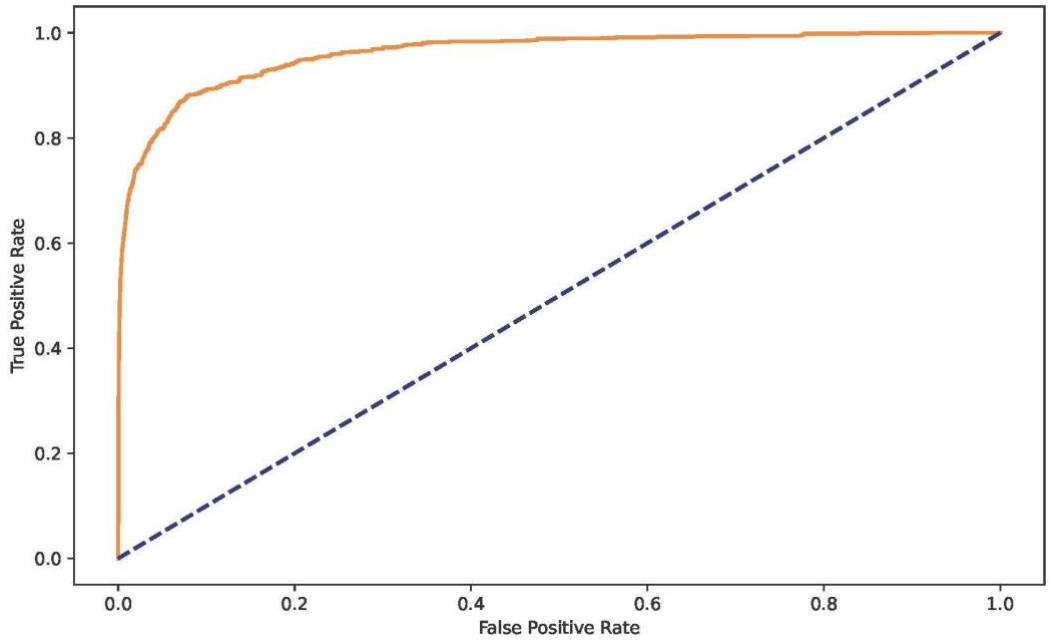

Figure 12. ROC curve for CatBoost, demonstrating high performance in fraud detection.

5.2.3 Bagging Classifier

Figure 13 displays the Receiver Operating Characteristic (ROC) Curve for the Bagging Classifier. The ROC curve for the Bagging Classifier exhibits a considerable curvature towards the top left corner, thereby indicating a notable true positive rate and a low false positive rate. This characteristic is exceedingly significant in the context of detecting online transaction fraud. The resilience of Bagging Classifier highlights its significance in constructing reliable fraud detection systems.

The Bagging Classifier model exhibits exceptional performance, achieving a nearly perfect accuracy score (0.92722). This number indicates its high skill level in accurately categorising most transactions. Although the accuracy is quite high (0.92722), which indicates that it accurately predicts fraudulent transactions, the

lower recall score (0.85476) reveals that it fails to identify some fraudulent transactions. The main weakness of the approach is its indication of an increase in sensitivity towards fraudulent scenarios.

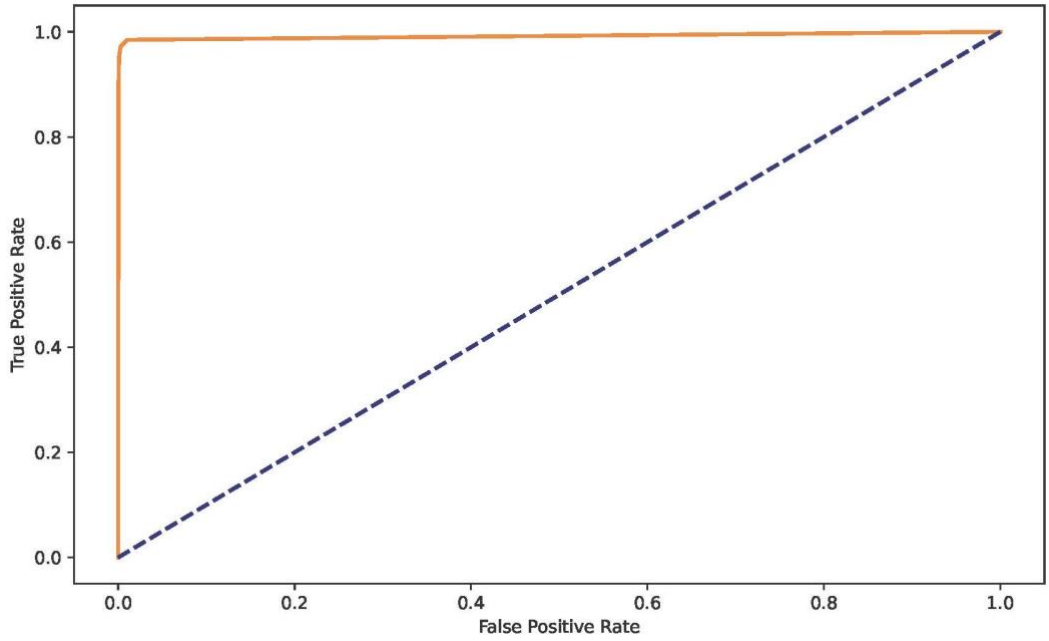

Figure 13. ROC curve for the Bagging Classifier, emphasising its predictive strength.

5.2.4 Logistic Regression (LR)

Figure 14 displays the Receiver Operating Characteristic (ROC) Curve for the LR model. The ROC curve of the LR model exhibits satisfactory performance, although with a somewhat lower true positive rate in comparison to ensemble approaches, which implies that. While LR serves as a useful starting point, ensemble approaches may offer improved detection abilities, which are particularly crucial during the COVID-19 epidemic as digital transactions and the accompanying risks of fraud are increasing.

LR exhibits the absence of a recall score, which is a significant concern. This observation indicates that these models exhibited a total inability to detect fraudulent transactions, thereby highlighting a significant deficiency in the fraud-detection system. This observation implies that these models are unsuitable for real-world fraud detection unless modifications or an alternative strategy are implemented to address the disparity in class distribution.

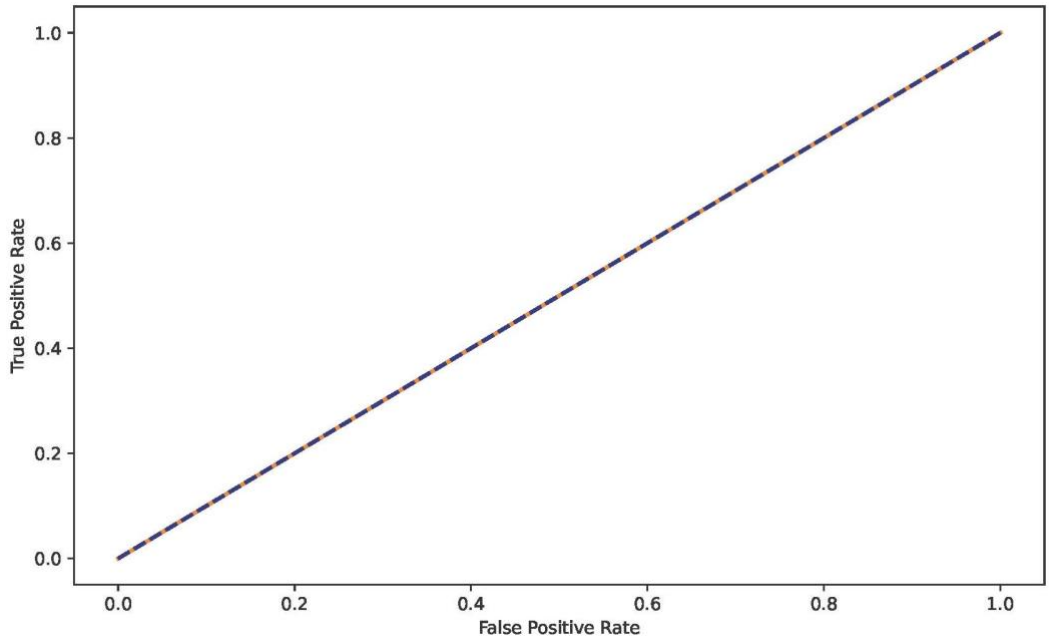

Figure 14. ROC curve for LR exhibiting its performance on the raw dataset.

5.2.5 XGB Classifier

Figure 15 depicts the Receiver Operating Characteristic (ROC) curve for the XGB Classifier. The ROC curve of the XGB Classifier demonstrates a remarkable true positive rate: it quickly ascends towards the top left corner, thus exhibiting a strong ability to distinguish between fraudulent and legal transactions. The performance of XGB Classifier demonstrates its ability to effectively handle unprocessed and imbalanced data in the specific domain of Credit-Card Fraud detection. This highlights its durability in the face of the rising prevalence of online transactional fraud during the COVID-19 epidemic.

The recall of the XGB Classifier model, which stands at 0.03598, suggests that it is presently failing to detect a significant number of real fraudulent transactions. Recall is a metric that evaluates the model's capacity to accurately identify all relevant cases. Nevertheless, the model's impressive AUC-ROC score of 0.99438

indicates its exceptional ability to differentiate among fraudulent and legitimate transactions across different benchmark settings.

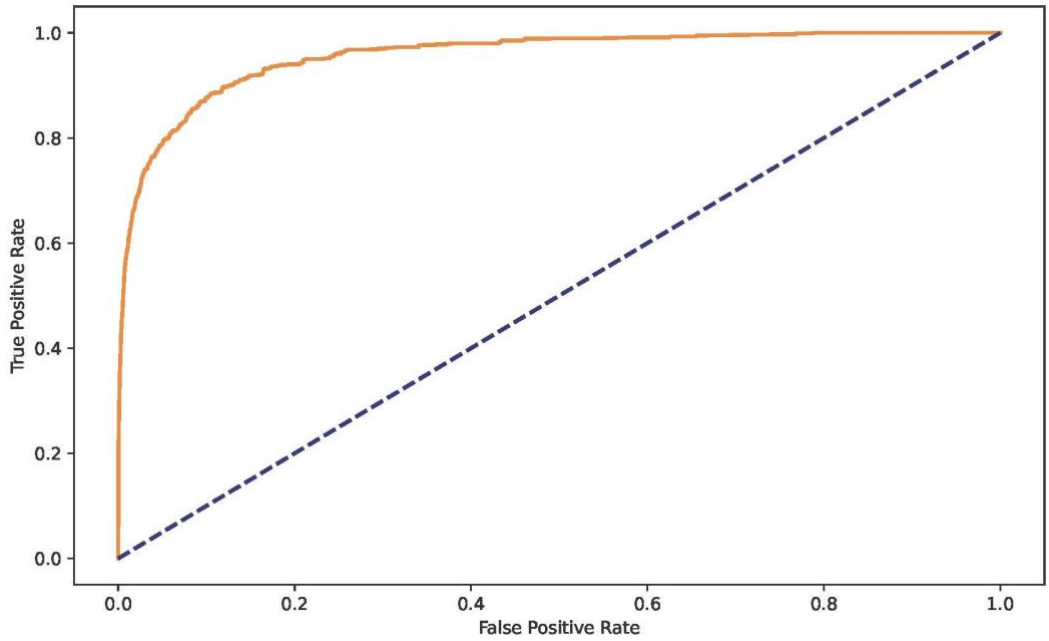

Figure 15. ROC curve for the XGB Classifier on raw transaction data, thus demonstrating the model's capability in fraud detection.

5.2.6 AdaBoost

Figure 16 illustrates the Receiver Operating Characteristic (ROC) Curve for the AdaBoost Classifier. The ROC curve of the AdaBoost Classifier exhibits a robust prediction capacity, as indicated by the AUC which reflects its effectiveness. AdaBoost exerts a crucial role in addressing the class-imbalance problem in Credit-Card Fraud detection, which has been a critical concern during the COVID-19 pandemic due to the increasing occurrence of such fraudulent activities.

The AdaBoost Classifier's accuracy score of 0.50067 indicates that its performance for this particular task is slightly better than random chance, which raises concerns regarding its efficacy. While it accurately predicts non-fraud instances, it, similar to LR Classifier, has a very poor recall rate (0.00133) for fraud cases. This level of accuracy is slightly better than having no prediction ability, which exposes a crucial vulnerability in the model's capacity to identify fraudulent activities.

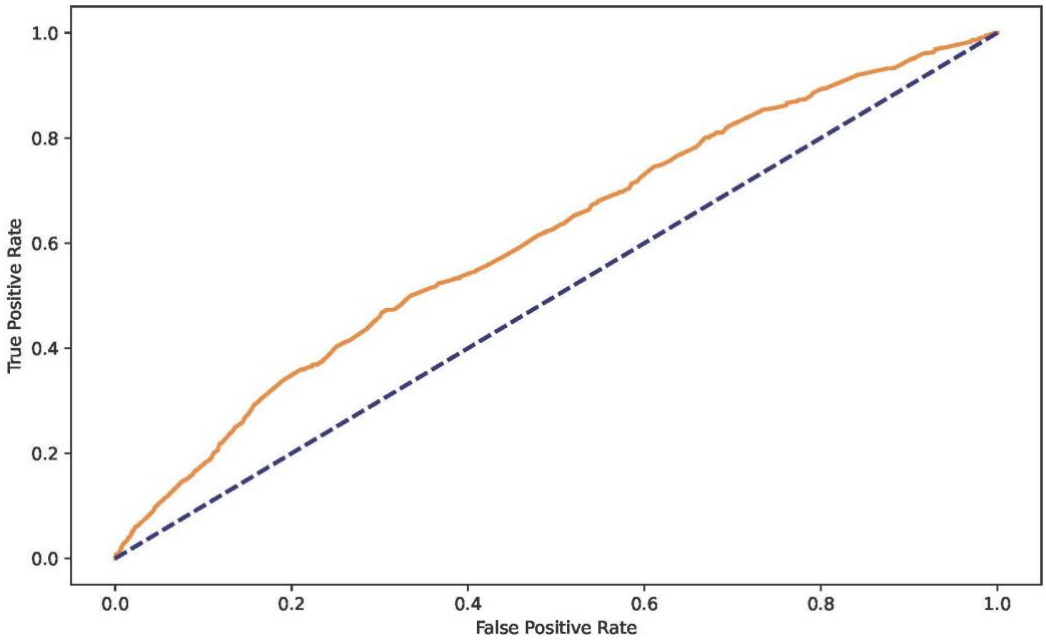

Figure 16. ROC curve for the AdaBoost Classifier, thereby highlighting its effectiveness in raw data classification.

5.2.7 Gaussian Naive Bayes (GNB).

Figure 17 displays the Receiver Operating Characteristic (ROC) Curve for the GNB algorithm. The ROC curve for GNB exhibits a curve that is in close proximity to the diagonal, thus indicating a modest degree of discriminatory capacity. This observation implies that although GNB might be useful, it should be supported by other methods such as feature engineering or balance to enhance its effectiveness in identifying more complex fraudulent transactions.

The GNB models exhibit poor recall, accuracy, and an F1 score of 0, suggesting its inability to accurately detect fraud within the test scenarios. The AUC-ROC score of 0.52726 indicates that its capacity to differentiate between fraudulent and legitimate transactions is merely marginally superior to that of random chance. Nevertheless, the model's impressive accuracy score of 0.99421 indicates its exceptional ability to accurately detect non-fraudulent transactions. Despite this, this outcome is likely a result of a significant imbalance in the dataset, where the number of non-fraudulent transactions greatly surpasses the number of fraudulent

transactions.

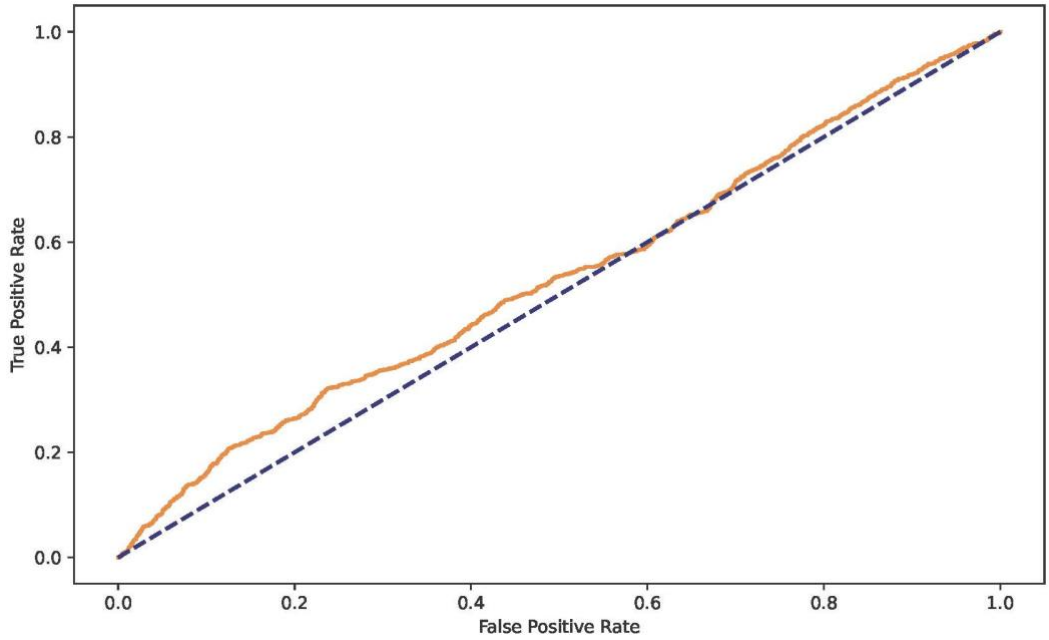

Figure 17. ROC curve for Gaussian NB, thereby indicating its discriminative power in fraud detection on raw data.

5.2.8 Extra Trees Classifier

Figure 18 displays the Receiver Operating Characteristic (ROC) Curve for the Extra Trees Classifier. The ROC curve of the Extra Trees Classifier exhibits a robust capacity to distinguish between classes. The classifier's success indicates its ability to comprehend intricate patterns in the data, thereby making it a formidable candidate among the essential instruments for reliable fraud detection in the contemporary, technology-driven industry.

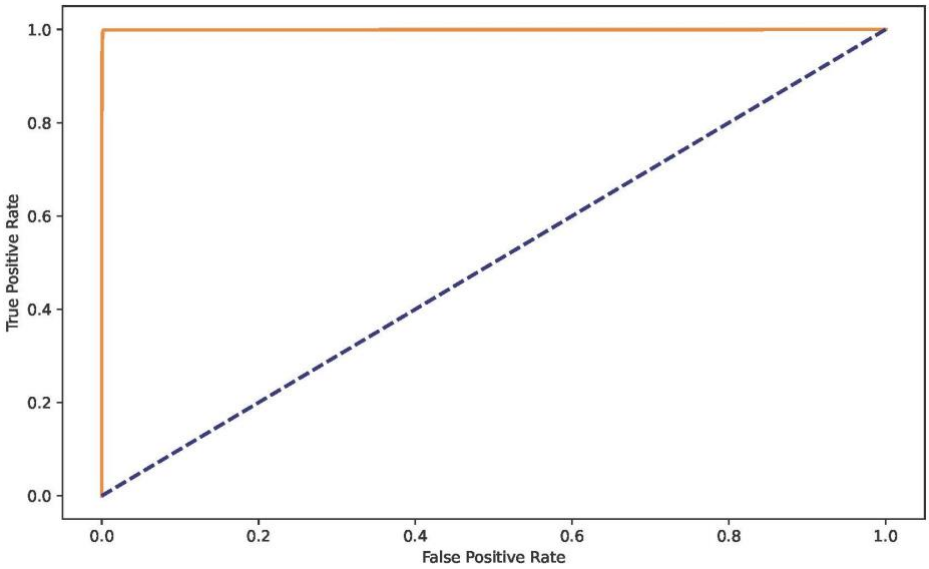

Figure 18. ROC curve for Extra Trees Classifier, exhibiting its strong classification ability on raw data.

5.3 Results of Deep Learning Algorithms on Raw Data

5.3.1 GRU

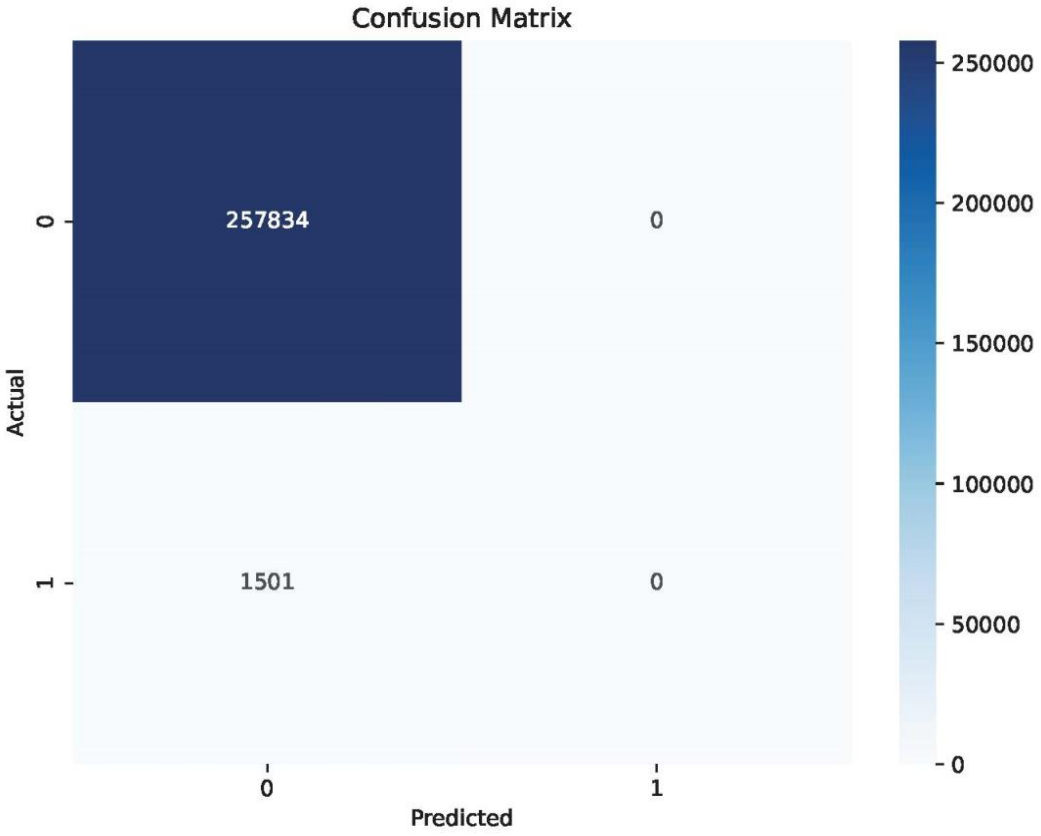

Figure 19. Confusion matrix for GRU model performance evaluation

The confusion matrix is a vital tool utilized for evaluating the efficacy of a classification system. Figure 19 depicts a matrix representing two distinct classes, herein denoted as '0' and '1'. The model has accurately predicted a substantial number of instances belonging to class '0' (true negatives), as illustrated by the count of 257,834. Nevertheless, there have been 1501 occurrences in which it has erroneously forecasted the negative category (false negatives) because these instances were really genuine '1' scenarios. This observation might imply a high level of specificity but a lower level of sensitivity, thus indicating that the model is cautious in predicting class '1'.

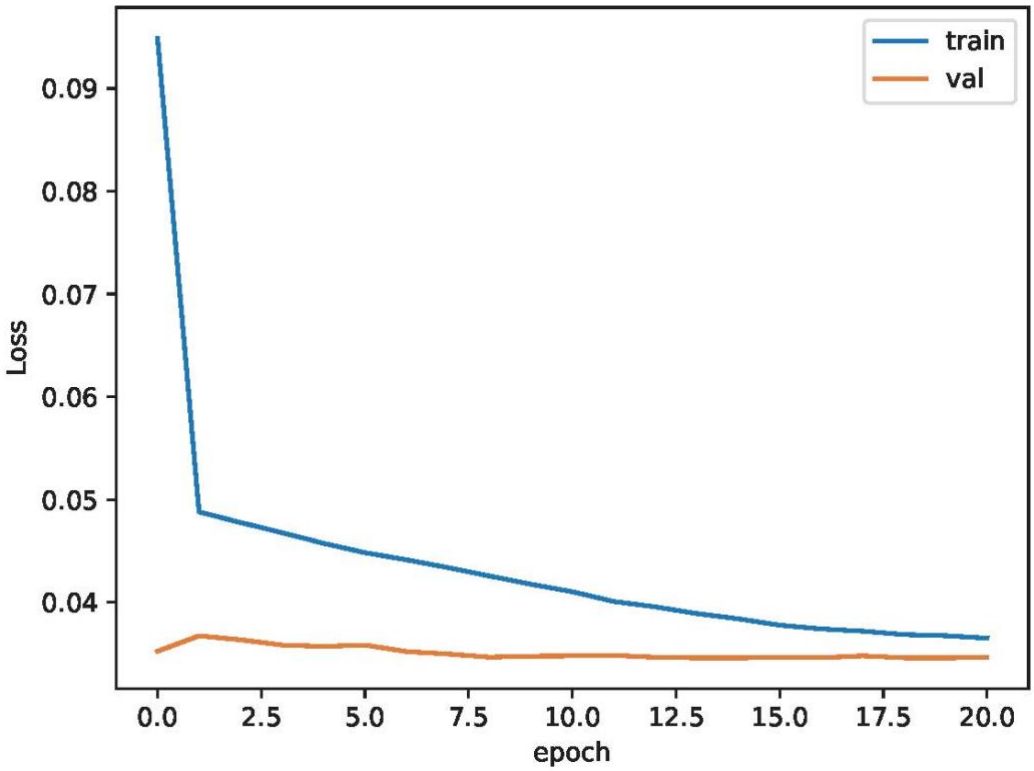

Figure 20. Training and validation loss for GRU model over epochs

Figure 20 illustrates the progression of training and validation loss throughout several epochs. An epoch refers to a whole cycle in which the entire dataset is processed during the training phase. The graph indicates a sharp decrease in the loss at the beginning, followed by a gradual reduction, thereby revealing that the model is acquiring knowledge and improving its predictive capabilities as time progresses. The training loss (blue) regularly outperforms the validation loss (orange), thus indicating a potential overfitting of the model to the training data. Thus, the model is more optimal at predicting the training data compared to fresh, unknown data (validation set).

Figure 21 illustrates the precision of the GRU model on both the training set (depicted in blue) and the validation set (depicted in orange) throughout several epochs. Accuracy refers to the ratio of correct outcomes to the overall number of instances analysed. The model exhibits a clear ability to rapidly acquire high accuracy on the training data, consistently maintaining a level that approximates 1 (or 100%) during subsequent training. The validation accuracy demonstrates a notable level of consistency and is rather high, but somewhat lower than the training accuracy. This discrepancy may indicate the presence of overfitting. Nevertheless,

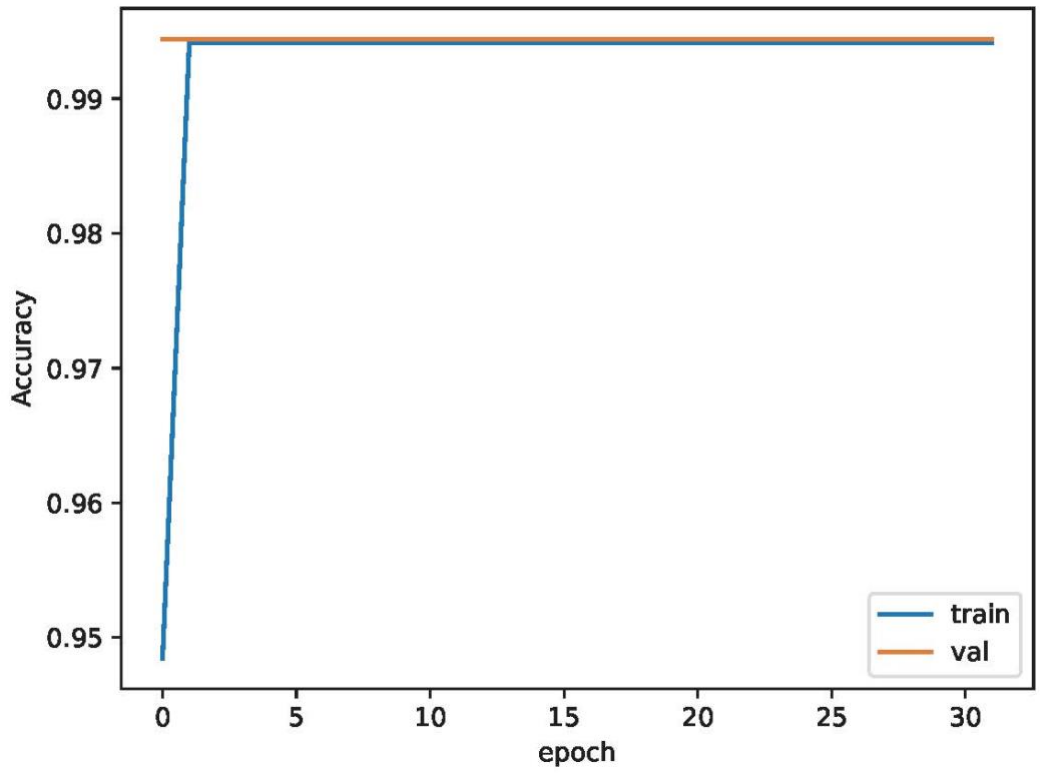

Figure 21. Training and validation accuracy for GRU model over epochs

the model's performance is positively indicated by the high degree of accuracy on both sets.

The evaluation metrics provided for the GRU model that is applied to raw data demonstrates the effectiveness of a binary classification system with two distinct classes: '0' denotes non-fraudulent transactions, and '1' denotes fraudulent transactions. The results indicate a distinct division in the model's ability to predict each class.

The recall for class '0', which denotes legitimate transactions, is 1. Thus, the model achieves a flawless performance in accurately detecting all valid transactions without any instances of incorrectly classifying them as false negatives. Nevertheless, the precision score of 0.99421 indicates that there are periodic misclassifications of fraudulent transactions as legitimate. The F1 score, calculated as the harmonic mean of precision and recall, is 0.9971, which indicates a remarkable equilibrium between recall and precision for class '0'. The specificity, which represents the proportion of correctly identified true negatives in fraudulent transactions, is 0, thereby indicating a complete failure in correctly identifying any true negatives. The ROC-AUC score is 0.99421, which reveals a strong ability to distinguish class '0'. Although the scores are impressive, the accuracy is only 0.5,

thereby indicating that the model is proficient in identifying legitimate transactions but faces significant challenges in detecting fraudulent ones.

The recall for class '1', which denotes fraudulent transactions, is 0. This observation indicates that the model is unable to accurately detect any fraudulent transactions, which is a significant weakness if the importance of fraud detection is considered. The precision score is 0 because there are no true positives in the prediction, thus indicating that no fraudulent transactions are accurately identified. Hence, the F1 score is 0, which indicates a subpar performance in fraud detection. The specificity is 1, which indicates that all valid transactions are accurately classified as non-fraudulent. The ROC-AUC score remains high at 0.99421; however, it is deceptive in this context because it fails to accurately represent the model's performance specifically on the positive class. The accuracy score remains at 0.5, which is not indicative of the model's effectiveness due to the significant class imbalance.

5.3.2 Neural Network (NN)

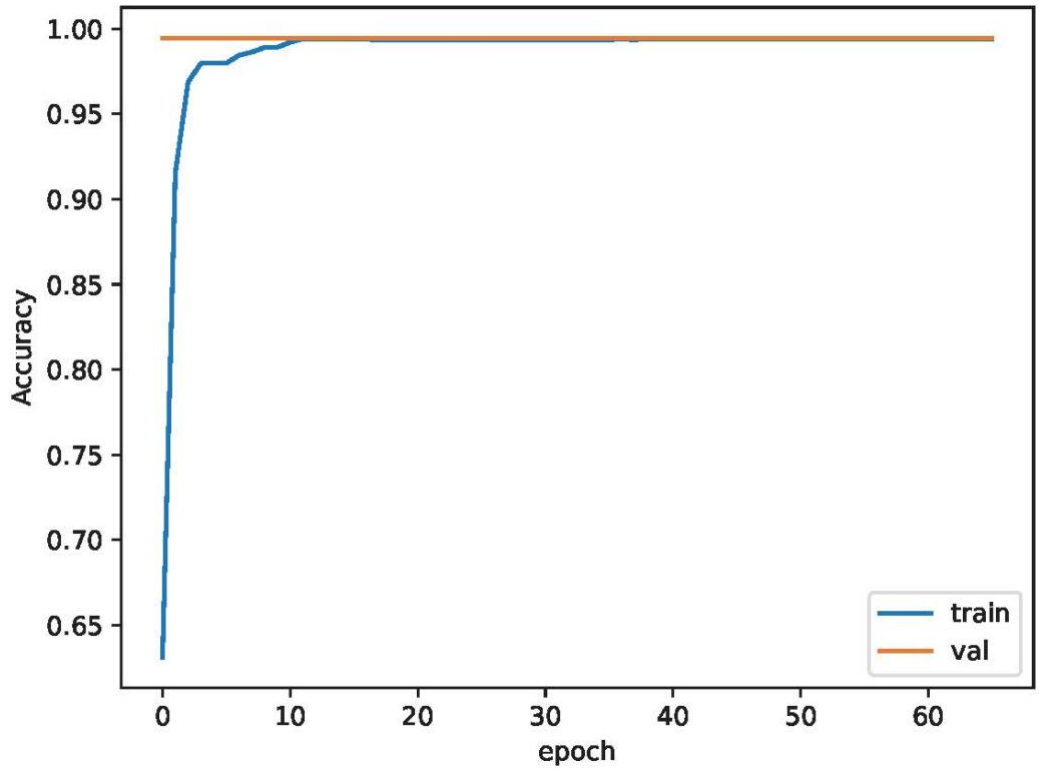

Figure 22. Training and validation accuracy for Neural Network Model over epochs

The provided diagrams are the results of the performance evaluation of NN model applied to raw data using deep learning methodologies. Every diagram symbolises

an individual aspect of the model's performance measures, and they collaboratively provide a complete perspective on the model's behavior and effectiveness.

Figure 22 depicts the precision of the neural network model for a period of 60 epochs. Significantly, the training accuracy (illustrated by the blue line) continually maintains at a high level, thus indicating that the model has effectively acquired knowledge from the training data. Nevertheless, the validation accuracy (depicted by the orange line) exhibits a modest decrease and rapidly attains a stable point. This observation indicates that the model may not be effectively adapting to new data, which indicates a typical manifestation of overfitting. This discrepancy might serve as a small sign of the model's inefficiency in successfully managing unbalanced data. Models trained on imbalanced data may exhibit a preference for the majority class, thereby leading to inflated accuracy scores on the training set but inadequate generalisation to the validation set.

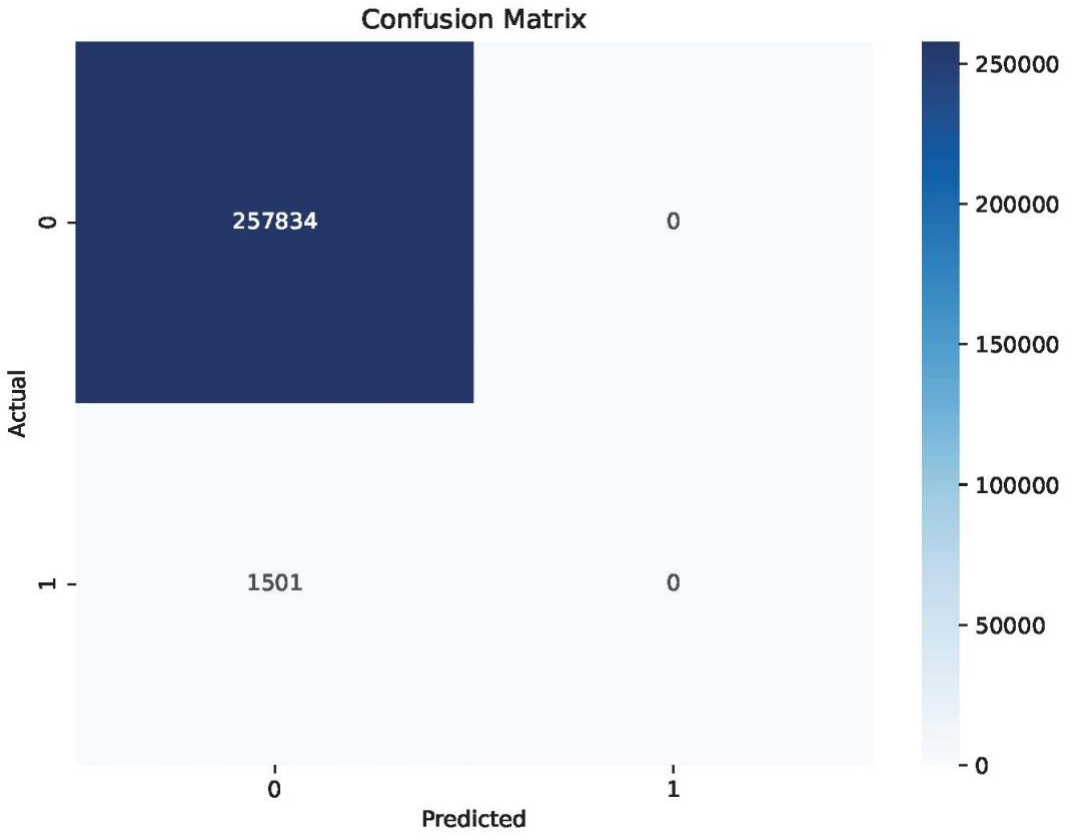

Figure 23. Confusion matrix for Neural Network Model performance evaluation

Figure 23 is a confusion matrix and exhibits a notable weakness in the model's ability to make accurate predictions. Although the number of genuine negatives is substantial (257,834), there is a total lack of real positives; the model fails to accurately detect any of the positive scenarios. This is a conspicuous indication of the model's incapacity to identify the minority class, a scenario that often arises when there is an imbalance in the data. The neural network is biased towards forecasting the dominant class, mostly due to insufficient exposure to occurrences of the minority class during the training process.

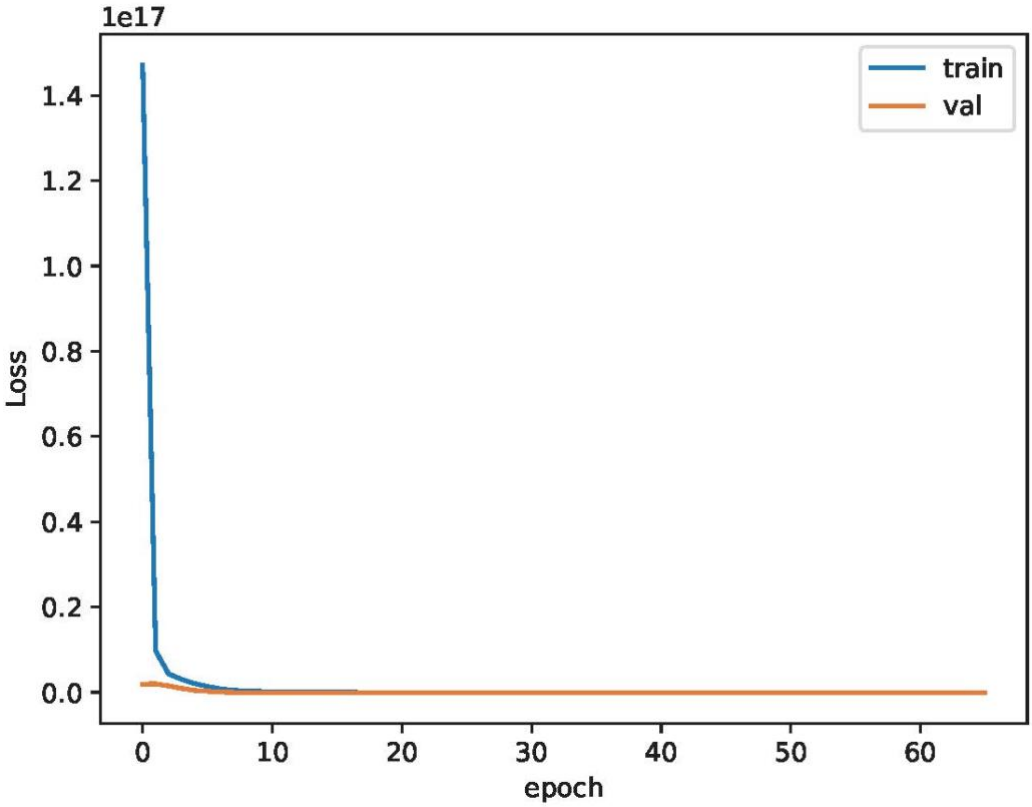

Figure 24. Training and validation loss for Neural Network Model over epochs

Figure 24 illustrates the loss of the neural network model over a period of time. The training and validation loss exhibit a quick and convergent decline, which is often indicative of a positive outcome. Nevertheless, the exceedingly elevated starting loss values on a logarithmic scale indicate that the model starts with exceptionally inadequate predictions. The rapid convergence to a minimal loss value may be deceiving. It may not necessarily indicate an enhancement in the model's capacity to forecast the minority class, which is often disregarded in instances of significant class imbalance. The sustained decline in loss values after the first decrease

indicates that the model does not exhibit further improvement, which can be rationalized as follows: it fails to grasp the attributes of the underrepresented class in the dataset. These diagrams indicate that although the model achieves satisfactory results based on certain measurements, fundamental problems should be resolved to enhance its performance. These issues are potentially associated with an imbalance in the classes, specifically affecting the model's accuracy in identifying and predicting the minority class.

The evaluation metrics of the NN model for classifying raw data in the fraud-detection context reveal a critical difference in the results for the two classes. This discrepancy is frequently observed in imbalanced datasets. The recall score for class '0', which represents legitimate transactions, is 1, which indicates an excellent performance. Thus, the model accurately identified all valid transactions without mistakenly classifying any valid transactions as fraudulent. It is imperative that fraud detection systems prevent users from being inconvenienced by false alerts. The precision score of 0.99421, although high, is not flawless, which indicates the presence of some misclassified transactions as fraudulent. This behavior can potentially lead to valid transactions being obstructed or marked for examination, which may inconvenience users. The f1 score, herein set at 0.9971, represents the harmonic mean of precision and recall, which indicates that the model is highly effective in accurately identifying legitimate transactions. Nevertheless, the model's specificity is 0, thus indicating that it fails to accurately identify any fraudulent transactions in a two-class system. This observation is supported by the accuracy score, which is merely 0.5. Although the roc auc score is high (0.99421), which indicates a strong distinction between classes, the model's lack of specificity indicates a bias towards classifying transactions as legitimate.

The results for class '1', which represents fraudulent transactions, are alarming. The recall score is 0, thereby signifying the model's ability to accurately detect any instances of fraudulent transactions. This presents a significant vulnerability for a fraud detection system because the model would be unable to identify any fraudulent activities. The precision score is 0 due to the absence of any true positives, thus indicating that the model failed to correctly identify fraudulent transactions. Hence, the f1 score is 0, signifying a total failure to detect fraud. The specificity of 1, in this particular context, is inaccurate because it refers to the accurate identification of valid transactions, which is not an urgent concern.

Although the ROC AUC Score remains high (0.99421), this metric becomes insignificant when considering the model's failure to detect any instances of fraud. Once again, the accuracy score is 0.5; however, it fails to accurately represent the model's performance owing to the imbalanced data distribution.

These metrics demonstrate the difficulty of creating a fraud detection model that is simultaneously sensitive and specific in a data environment that is exceedingly biased. Although the NN model excels at identifying legitimate transactions, it fails to detect fraud, making the fraud detection system ineffective. This behavior highlights the significance of addressing the problem of class imbalance, as mentioned in the thesis abstract. A potentially effective approach entails employing techniques such as random oversampling, SMOTE, ADASYN, or random under sampling. Additionally, it is recommended to explore different machine learning models to identify the most efficient fraud-detection solution.

5.4 Discussion

The assessment of machine learning models for Credit-Card Fraud detection is customarily centered on their capacity to distinguish between legitimate and fraudulent transactions. Prior to employing data balancing methods, it is imperative to evaluate the effectiveness of these models on unprocessed, raw datasets.

The distribution of the raw data is inherently biased, with a significant discrepancy between the legitimate transactions comprising the majority class and the fraudulent transactions comprising the minority class. This segment examines the consequences of class imbalance on the model's performance, as measured by Recall, Precision, F1 Score, AUC-ROC Score, and Accuracy. These metrics function as gauges of a model's overall capability to accurately detect fraudulent instances with minimal occurrences of false positives.

The performance of the Bagging Classifier and Random Forest Classifier on the raw dataset was satisfactory in regard to the majority class: their Accuracy, Precision, and F1 Score values were nearly excellent. Conversely, upon closer examination of the minority cohort, a substantial decline in both recall and F1 Score was observed. The recall metric for the Bagging Classifier's performance in identifying fraudulent transactions was 0.85476, whereas its balanced performance metric (F1 Score) was 0.89501. The Random Forest Classifier exhibited a

marginally enhanced Recall value of 0.93138, which signified a moderate level of proficiency in fraud detection.

In raw datasets, complex models have a propensity to perform. In raw datasets, complex models tend to excel at detecting a majority-class transactions but face challenges with minority-class transactions. The poor recall scores indicate that many fraudulent transactions may be undetected, thus compromising the overall effectiveness of the fraud-detection system.

However, when assessed on identical unprocessed data, models including LR and Gaussian NB exhibited contrasting performance levels. The majority class achieved an Accuracy of 1 for these models, which, at first glance, could indicate outstanding model performance. However, a critical vulnerability is revealed by the Recall, Precision, and F1 Score of 0 for the minority class: the models could not detect any fraudulent transactions. This observation indicates that the models tend to prioritise the majority class over the minority class, which is detrimental to the effectiveness of fraud detection.

The AdaBoost Classifier demonstrated a marginal advance over the LR and Gaussian NB classifiers, thus achieving a nominal fraud detection with a 0.00133 recall value. This notwithstanding, its implementation in fraud-detection systems remains inconsequential. The fraud-detection capabilities of CatBoost and XGB Classifier were enhanced, albeit still restricted, as evidenced by their respective recall values, namely 0.16256 and 0.03598. Their performance indicates that although they possess a moderate ability to detect fraudulent transactions, a significant proportion evade detection.

The Extra Trees Classifier exhibited a more rational performance, as evidenced by its Recall value (0.9527) for the minority class. This observation indicates a comparatively more remarkable ability to identify fraudulent activities compared to the other models; however, the model is not immune to the consequences of class imbalance.

GRU and NN models perform similarly to LR and GaussianNB on raw data. Accuracy values of 0.99421 for GRU classes may indicate that the models are performing optimally. However, a closer analysis of class-specific performance would exhibit a quite different story.

The representation of Neural Network models in the context of fraudulent transactions. The recall and precision scores of 0 indicate that the minority class is being disregarded. This behavior is typical of models that anticipate the majority class due to its overwhelming prevalence in the data, thus ignoring the essential minority class of fraudulent transactions.

This bias towards the majority class obscuring apparent model accuracy supports the claim that traditional accuracy measurements are ineffective in class imbalances and emphasises the need for a more nuanced model evaluation that considers class distribution and prioritises detecting less common but more impactful fraudulent transactions. The GRU and NN failed to detect any fraud in the raw dataset, thus revealing the necessity for data balancing measures to enable these powerful models to understand subtle fraud patterns and contribute to fraud detection systems.

The examination of models performing fraud detection tasks using raw data supports the established notion that class imbalance substantially impedes the effectiveness of the models, specifically about the minority class. The discrepancy in model performance highlights the criticality of implementing class balancing methods to correct the imbalanced class distribution before continuing the training process. By implementing corrective measures, the complete potential of machine learning models can be realised, thus guaranteeing their optimal performance in practical scenarios that require the precise identification of fraudulent activities.

Table 2 The results of implementing various machine and deep learning algorithms on raw data.

Model Name	Recall Score	Precision Score	F1 Score	ROC AUC Score	Accuracy Score
Bagging Classifier	0.85476	0.93924	0.89501	0.99884	0.92722
Random Forest Classifier	0.93138	0.91974	0.92552	0.99913	0.96545
Logistic Regression	0	0	0	0.99421	0.5
AdaBoost Classifier	0.00133	1	0.00266	0.99422	0.50067

CatBoost Classifier	0.16256	0.86833	0.27385	0.96353	0.99501
XGB Classifier	0.03598	0.83077	0.06897	0.99438	0.51797
Extra Trees Classifier	0.9527	0.92199	0.93709	0.99926	0.97611
GNB Classifier	0	0	0	0.52726	0.99421
GRU	0	0	0	-1	0.99421
NN	0	0	0	1	-1

5.5 Conclusion

This chapter evaluated several machine learning and deep learning models on a row dataset, using measures such as recall, precision, F1 score, specificity, ROC-AUC score, and accuracy to measure their performance. The research revealed that Random Forest and Extra Trees classifiers exhibit resilience across many parameters, thus exhibiting a harmonious performance in accurately categorising both classes. Conversely, models such as LR and NN classifiers have exhibited exceptional performance in some measures, excelling in certain aspects but performing poorly in others.

From this evaluation, a critical discovery is obtained: the vulnerability of the GRU model in detecting fraudulent transactions. Although the model performs effectively in identifying non-fraudulent transactions, its failure to detect any fraudulent behavior reveals a significant deficiency. The disparity in performance indicators reflects the problem of class imbalance mentioned in the thesis abstract. To generate a balanced dataset, it becomes apparent that applying techniques such as random oversampling, SMOTE, ADASYN, and random under sampling is necessary. This modification can potentially improve the model's ability to detect instances of fraud. In the absence of correcting this discrepancy, the GRU model, while accurate in Recognising legitimate transactions, fails to effectively achieve its principal goal of detecting fraudulent operations.

The highlighted metrics provide a distinct indication to improve the model and adjust data pre-processing processes as a method for enhancing the detection of fraudulent transactions. The following chapter examines the influence of Balancing

Techniques on Model Performance, thus providing a more comprehensive analysis of how various data balancing strategies might enhance the efficacy of fraud detection models.

This analysis highlights the essential importance of combining geolocation and temporal data, as well as employing advanced data balancing techniques, to improve the effectiveness of fraud detection systems. Incorporating geolocation and temporal dimensions allows the models to identify patterns and anomalies that are intrinsically spatial and temporal—elements frequently linked to fraudulent activities. This integration, along with effective data balancing strategies like ROS, SMOTE, ADASYN, and Random Under Sampling, tackles the class imbalance issue and improves the overall performance of the models. This method not only corresponds with the main enquiry of the thesis but also shows the ability to greatly enhance the precision and effectiveness of identifying fraudulent transactions in imbalanced datasets, thus aiding in the development of more resilient and flexible fraud detection systems.

6 IMPACT OF BALANCING TECHNIQUES ON MODEL PERFORMANCE

6.1 Introduction

Within the domain of machine learning and data analysis, the problem of class imbalance is a significant concern, especially in areas such as fraud detection, where the number of valid transactions considerably exceeds the number of fraudulent ones. This imbalance may lead to biased models that perform well in recognising the majority class but struggle when detecting the less common but frequently more essential minority class. In the preceding chapter, we discussed this problem and specifically emphasised the shortcomings of models such as as the GRU in accurately detecting cases of fraud owing to the unequal distribution of classes.

This chapter examines several balancing strategies, including random oversampling, SMOTE, ADASYN, and random under sampling. These strategies are crucial in reducing the impact of class imbalance; thus, they potentially enhance the predicted accuracy and reliability of models in identifying fraudulent activity.

We analyse the impact of different strategies on the distribution of classes in a dataset; thus, we aim to achieve a more equitable representation that enhances the learning capabilities of models for both classes. In the fraud-detection domain, accurately recognising fraudulent transactions is of utmost priority, and identifying valid ones is also a priority.

The study specifically examines how these strategies may be practically applied to the raw dataset and the resultant effect on the performance of different machine learning and deep learning models. We aim to measure the efficacy of balancing strategies in improving fraud detection abilities by evaluating the performance of the models before and after their implementation.

This chapter can fundamentally direct researchers towards more accurate and reliable fraud-detection models. The knowledge acquired from this study can not only improve the researchers to comprehend the significance of data preparation in machine learning but also provide a foundation for future progress in the domain of anomaly detection.

6.2 Results obtained by employing various Balancing Techniques on Machine Learning Algorithms

This subsection focuses on the examination of different balancing approaches and their influence on machine learning algorithms. The utilization of these methodologies is crucial in addressing the problem of class imbalance, therefore possibly enhancing the effectiveness of models developed for the identification of fraudulent transactions.

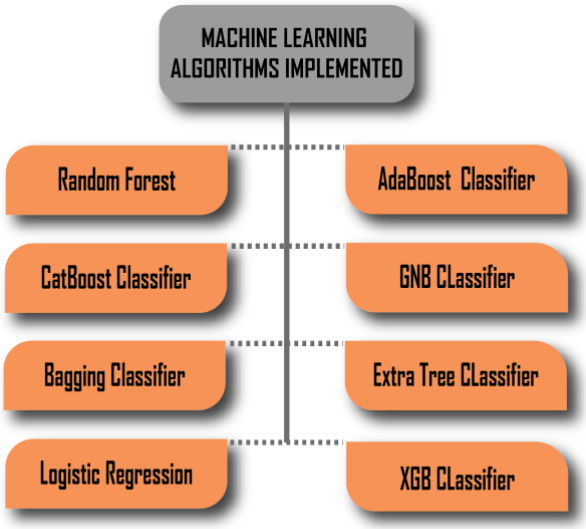

Figure 25. Machine Learning Algoritms Implemented

6.2.1 Random Forest Classifiers

This section examines the outcomes obtained from the implementation of various balancing techniques on a range of machine learning models, with a particular focus on Random Forest Classifiers.

The Random Forest Classifier is well recognised for its resilience and adaptability, making it an effective tool in the detection of fraudulent activities. The operational strategy of this model involves the construction of several decision trees during the training phase, which subsequently generates the mode of the classes for classification or the mean prediction for regression. The primary advantage of Random Forest is its capacity to address overfitting while maintaining high-level accuracy, which makes it especially appropriate for handling complicated datasets that exhibit class imbalance.

A. Random Over Sampling

As presented in the thesis reveal the significant influence of ROS on the performance

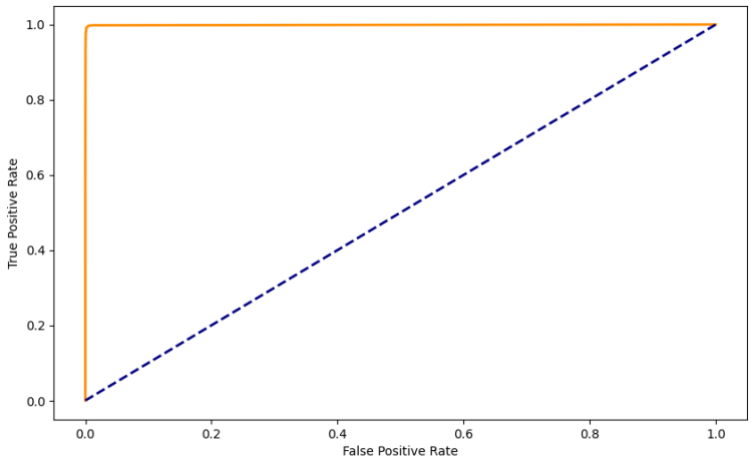

Figure 26. ROC curve for the Random Forest Classifier with Random Over Sampling

of a random forest classifier when applied to Credit-Card Fraud detection. The ROC curve illustrated in Figure 26 exhibits a significant rise towards the optimal point of outstanding classification, thus confirming the classifier's improved capability to differentiate between fraudulent and non-fraudulent transactions.

The Figure 27 presented herein reveals the significant influence of the aforementioned

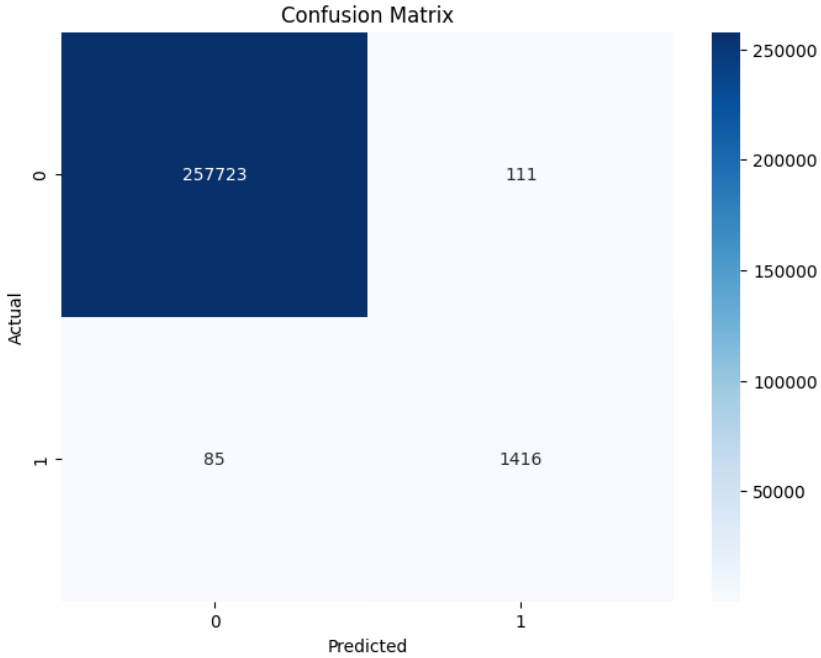

Figure 27. Confusion Matrix for the Random Forest Classifier with Random Over Sampling

enhancement, which is reflected in the confusion matrix; the matrix exhibits a notable increase in true positive rates that indicate effective fraud detection while preserving a minimal false positive rate, which is a critical factor in preventing erroneous fraud

alerts. Compared to the typical outcomes of imbalanced datasets, these results demonstrate that ROS is an effective method for overcoming the "class imbalance" issue. The metrics of the RandomForest algorithm, as indicated by the blue shade's profundity in the confusion matrix, align with the research's aim of improving model dependability and precision. Thus, the aforementioned visual representations substantiate the thesis's claim, namely that data balancing techniques are crucial for enhancing the accuracy of fraud detection algorithms, thereby strengthening the overarching objective of fortifying digital financial systems against fraudulent action.

B. SMOTE

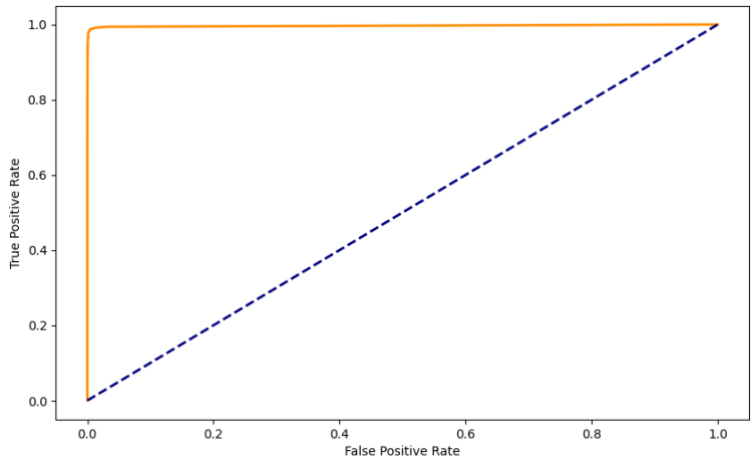

Figure 28. ROC curve for the Random Forest Classifier with SMOTE

The ROC curve depicted in the Figure 28 remarkably approximates the top left corner, thus signifying a minimal false positive rate and a substantial true positive rate. This behavior effectively illustrates the enhanced capability of the model to differentiate between classes. The confusion matrix in the Figure 29 describe a significant reduction in false negatives and a considerable increase in true positives, thereby underscoring the model's heightened sensitivity in detecting fraudulent activities.

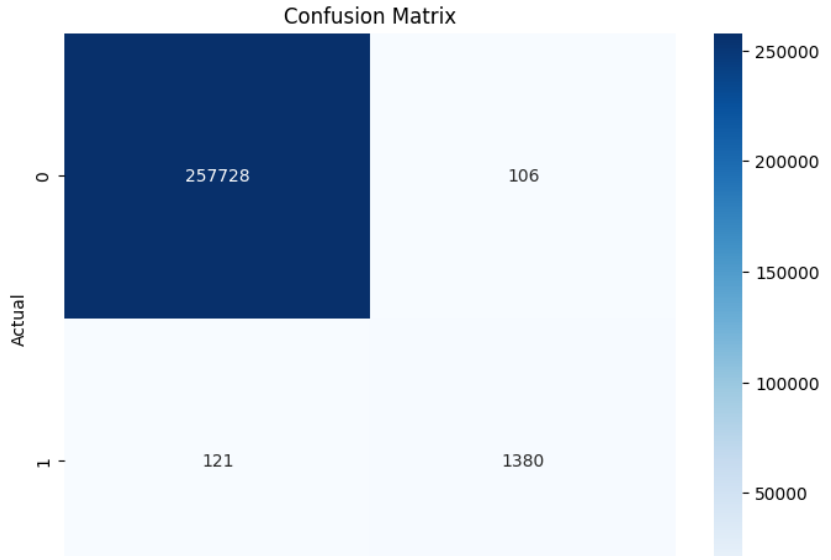

Figure 29. Confusion Matrix for the Random Forest Classifier with SMOTE

These figures presented herein present the fundamental perspective of the thesis: SMOTE enhances the capability of the Random Forest Classifier in effectively handling the imbalanced data challenges of fraud detection through the amplification of minority class representation. Consequently, these improvements provide further support for the efficacy of ensemble methods, which are strengthened by data balancing techniques, in constructing advanced systems that can precisely detect fraudulent transactions.

C. ADASYN

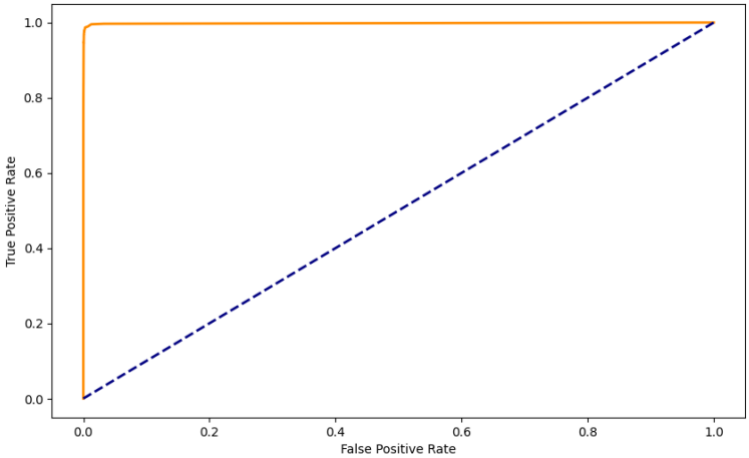

Figure 30. ROC curve for the Random Forest Classifier with ADASYN

The ROC curve in Figure 30 shows the enhanced efficacy of the model in distinguishing fraudulent transactions. Furthermore, the confusion matrix in the Figure 31 reveals a significant decrease in false negatives and an increase in true positives, thus contributing to the model's overall reliability. Aligned with the thesis's aim of developing dependable and effective systems for the digital banking industry, these enhancements support the value of sophisticated resampling methods such as ADASYN in enhancing the accuracy and flexibility of fraud-detection models.

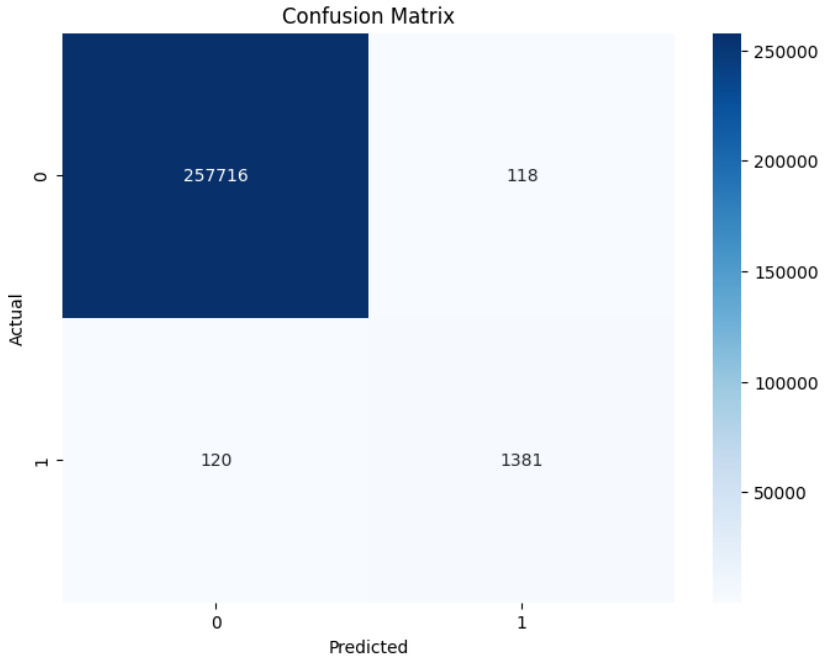

Figure 31. Confusion Matrix for the Random Forest Classifier with ADASYN

D. Random Under Sampling

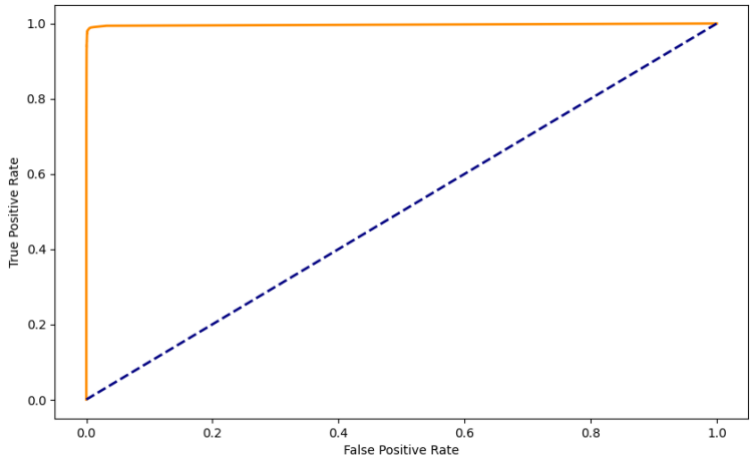

Figure 32. ROC curve for the Random Forest Classifier with Random Under Sampling

The greater accuracy with which the model classifies fraud cases with fewer errors is highlighted by the pronounced ROC curve in the upper left corner, herein displayed in Figure 32. The effectiveness of Random Under Sampling in equalising the class distribution and enhancing the predictive performance of the classifier is further supported by the confusion matrix in Figure 33, which exhibits a considerable quantity of true positives and true negatives. This integration effectively satisfies the fundamental objectives of the thesis, thereby illustrating how straightforward methods such as Random Under Sampling can substantially enhance the precision and dependability of fraud-detection models.

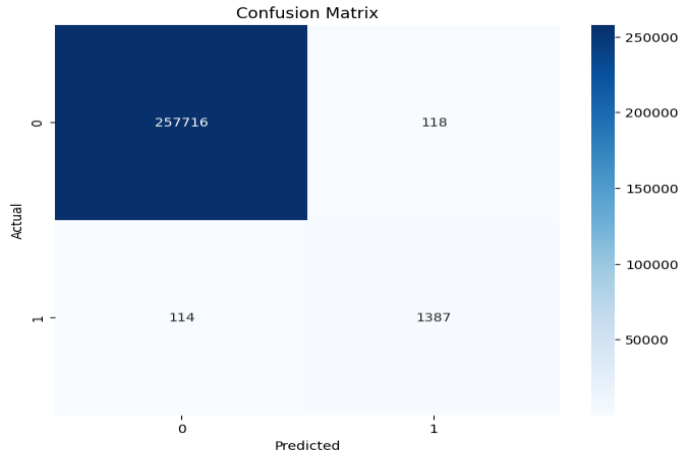

Figure 33. Confusion Matrix for the Random Forest Classifier with Random Under Sampling

6.2.2 CatBoost

This segment analyses the results acquired by applying various balancing techniques to a CatBoost classifier.

A. Random Over Sampling

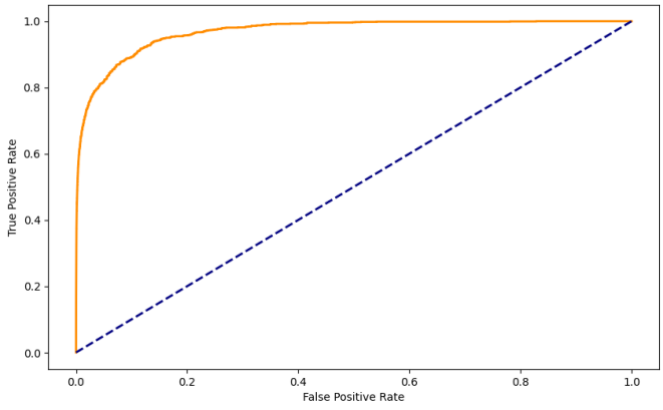

Figure 34. ROC curve for the CatBoost Classifier with Random Over Sampling

Displaying the classifier's increased discriminatory capability after balancing, the ROC curve in Figure 34 exhibits an exceptional true positive rate, closely resembling the ideal scenario. Simultaneously, an increase in the accuracy of identifying fraudulent transactions is evident in the confusion matrix depicted in Figure 35, which illustrates the classifier's heightened accuracy while false positive rates remain low. Establishing that even sophisticated algorithms such as CatBoost can significantly benefit from the appropriate distribution of class alignment, these results validate the thesis's emphasis on data balancing as a critical factor for enhancing model performance.

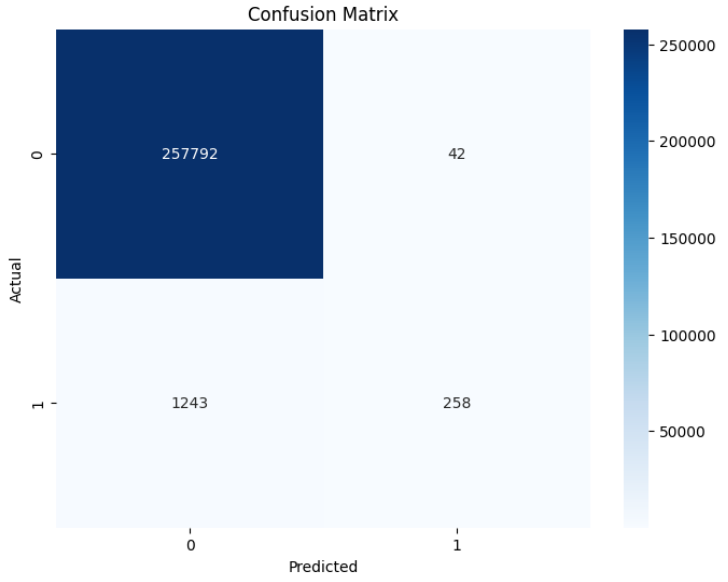

Figure 35. Confusion Matrix for the CatBoost Classifier with Random Over Sampling

B. SMOTE

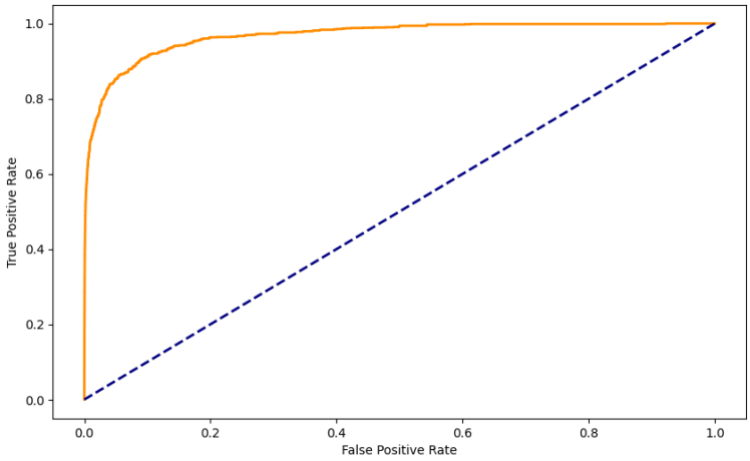

Figure 36. ROC curve for the CatBoost Classifier with SMOTE

A low false positive rate and a high true positive rate indicate an ROC curve in the Figure 36 approaching the top left corner, which is optimal for fraud detection. The confusion matrix in the Figure 37 provides further support for the efficacy of this methodology; a considerable proportion of fraudulent transactions were accurately classified, with a relatively low occurrence of false negatives. Thus, the model skilfully manages the compromise between detecting fraud and minimising false alarms. The improved performance of the model after the implementation of SMOTE as a method of rectifying the imbalance challenge provides further support for the following concept: sophisticated data balancing methods could substantially advantage machine learning methods in scenarios involving fraud detection.

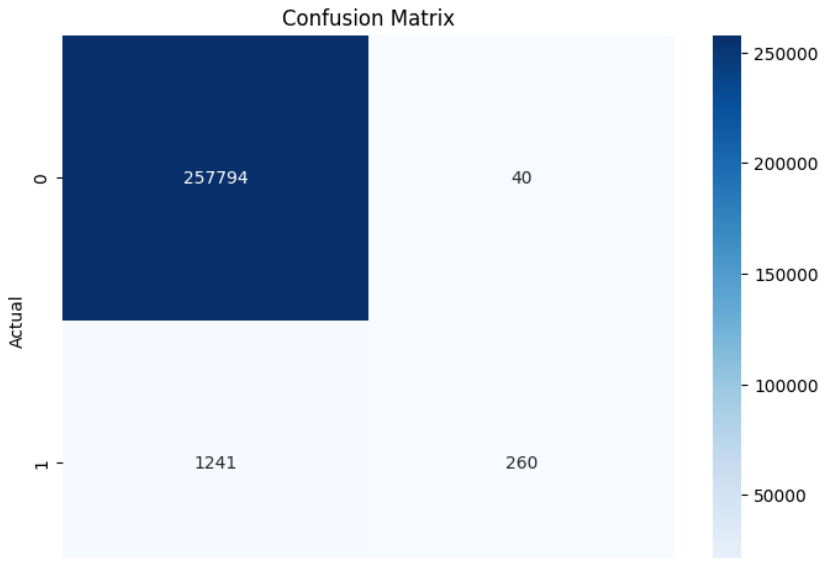

Figure 37. Confusion Matrix for the CatBoost Classifier with SMOTE

C. ADASYN

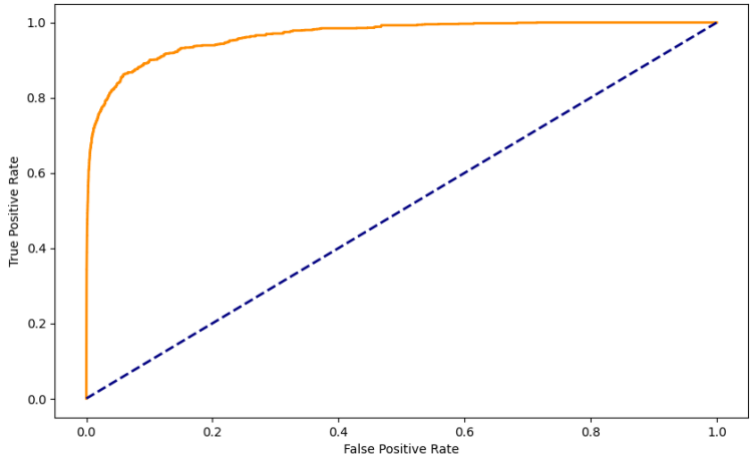

Figure 38. ROC curve for the CatBoost Classifier with ADASYN

The model's improved sensitivity and specificity are validated by the ROC curve in the Figure 38, which achieves an almost ideal score, thus signifying a remarkable true positive rate associated with a limited false positive rate. Simultaneously, the Confusion Matrix in the Figure 39 exhibits a substantial decline in false negatives, which is of utmost importance in detecting fraud while maintaining a significant count of true negatives. The findings of this study support the utilisation of advanced data balancing techniques in conjunction with machine learning algorithms; thus, an exceptionally

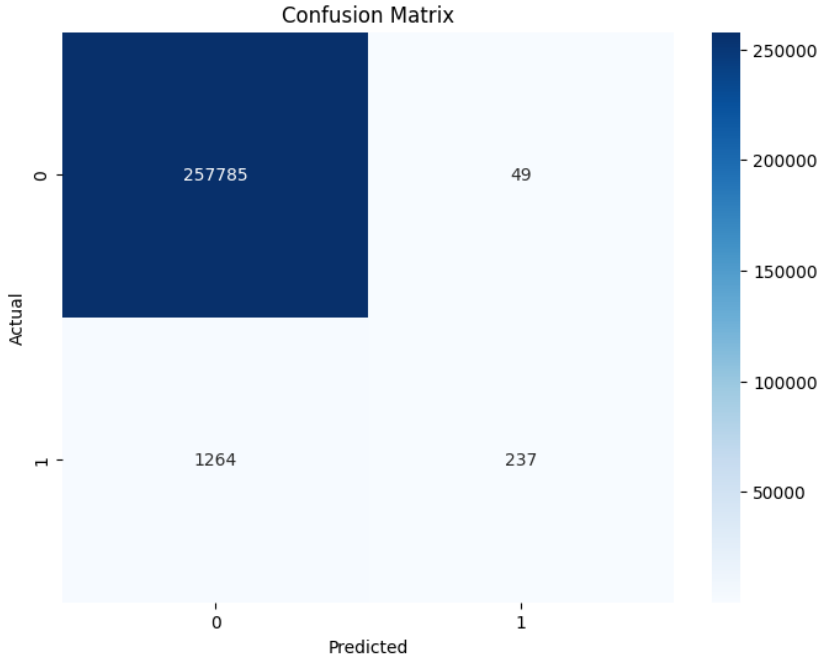

Figure 39. Confusion Matrix for the CatBoost Classifier with ADASYN

adaptable and precise fraud detection system is developed. Such a system can navigate the intricacies of the contemporary digital financial environment.

D. Random Under Sampling

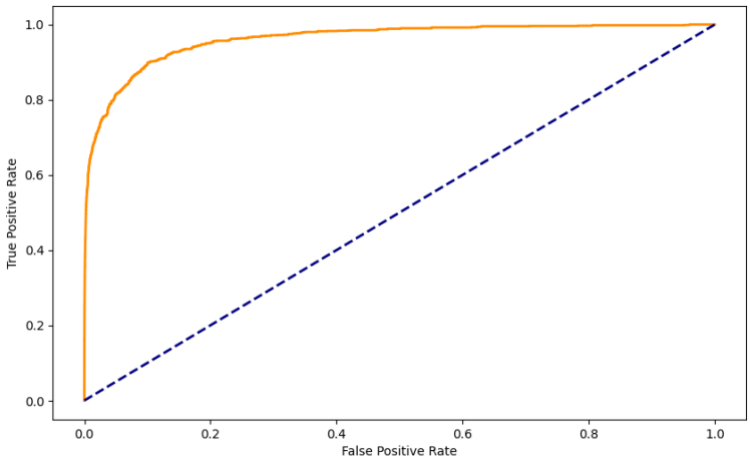

Figure 40. ROC curve for the CatBoost Classifier with Random Under Sampling

The classifier demonstrates exceptional precision by balancing between minimising false positives and improving the identification of fraudulent transactions; however, the majority class is reduced. The balance between true positives and false negatives is exhibited by the confusion matrix and the high area under the ROC curve depicted in the Figure 40, which signifies a significant proportion of accurate positives and false negatives about detecting genuine fraudulent instances displayed in the Figure 41. The

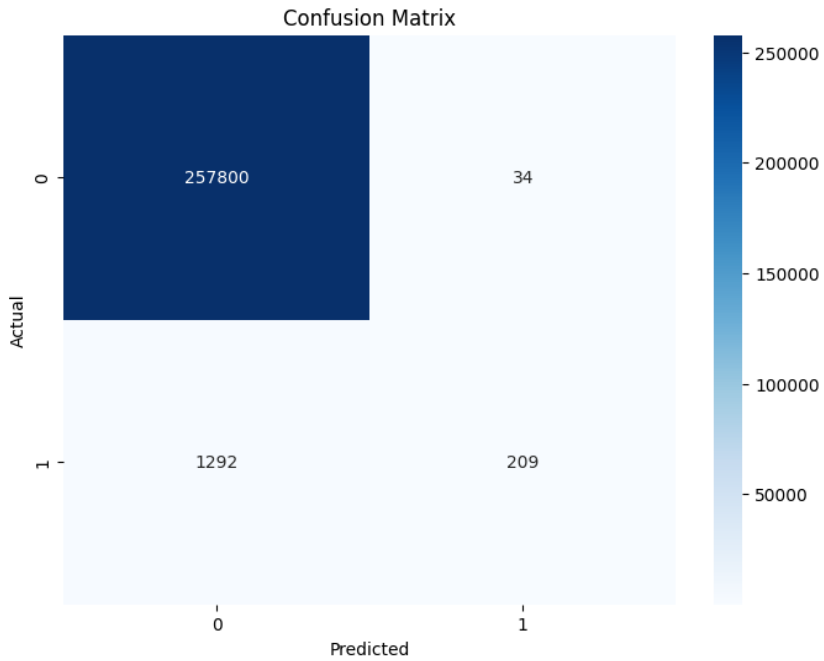

Figure 41. Confusion Matrix for the CatBoost Classifier with Random Under Sampling

results presented herein evidence the efficacy of class-rebalancing methods in enhancing the performance of models, specifically within the severe requirements of fraud detection, where precise identification of the minority class is crucial.

6.2.3 Bagging Classifier

This section analyses the results acquired by applying various balancing techniques to a Bagging classifier.

A. Random Over Sampling

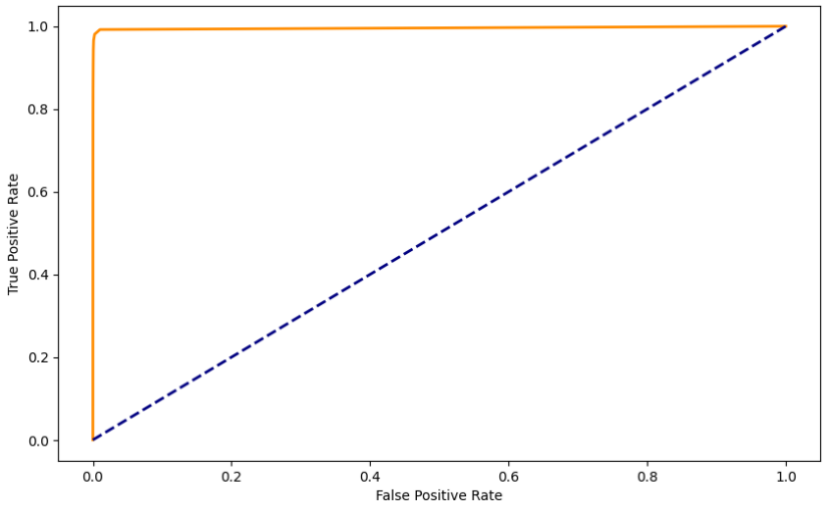

Figure 42. ROC curve for the Bagging Classifier with Random Over Sampling

After addressing the class imbalance dataset, the Bagging Classifier differentiates between fraudulent and legitimate transactions, as indicated by the steep ascent of the ROC curve in the Figure 42, herein depicted towards the upper-left corner, which signifies a significant true positive rate. Additionally, this efficacy is emphasised by the Confusion Matrix in the Figure 43, which indicates a notable decrease in false negatives and thus enhances the sensitivity of the model in detecting fraudulent activities.

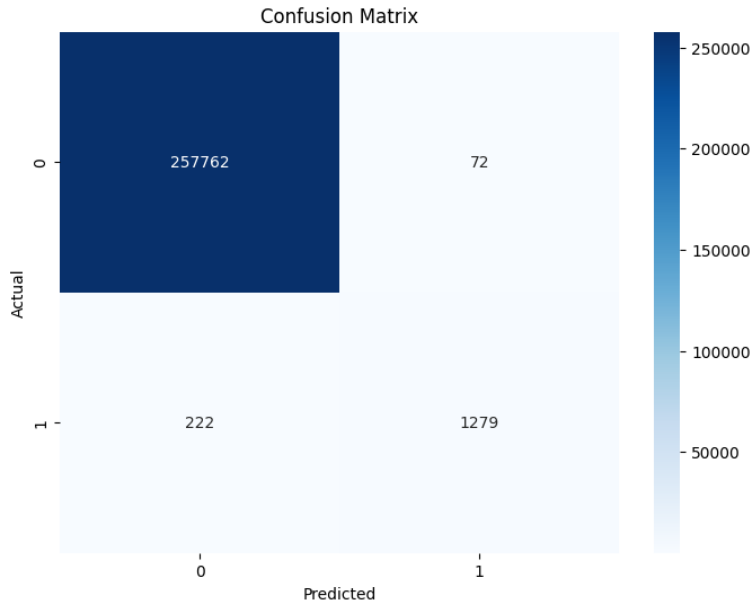

Figure 43. Confusion Matrix for the Bagging Classifier with Random Over Sampling

B. SMOTE

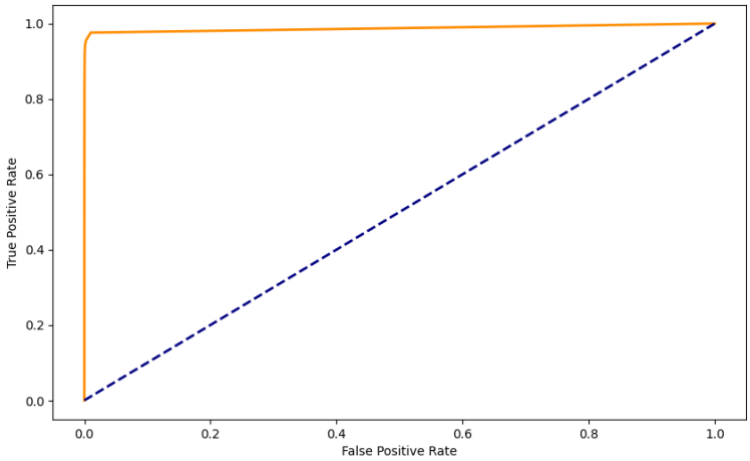

Figure 44. ROC curve for the Bagging Classifier with SMOTE

The implementation of SMOTE to balance the collected data has led to a significant enhancement in the efficacy of the Bagging Classifier with regard to Credit-Card Fraud detection. Due to the significant financial implications of false negatives, a model exhibiting exceptional sensitivity and specificity is critical in fraud detection, as indicated by the ROC curve in the Figure 44 approaching the top-left area. This observation is supported by the confusion matrix in the Figure 45, which demonstrates

a substantial decline in false negatives—a critical metric for an algorithm designed to prevent fraudulent activities from evading detection.

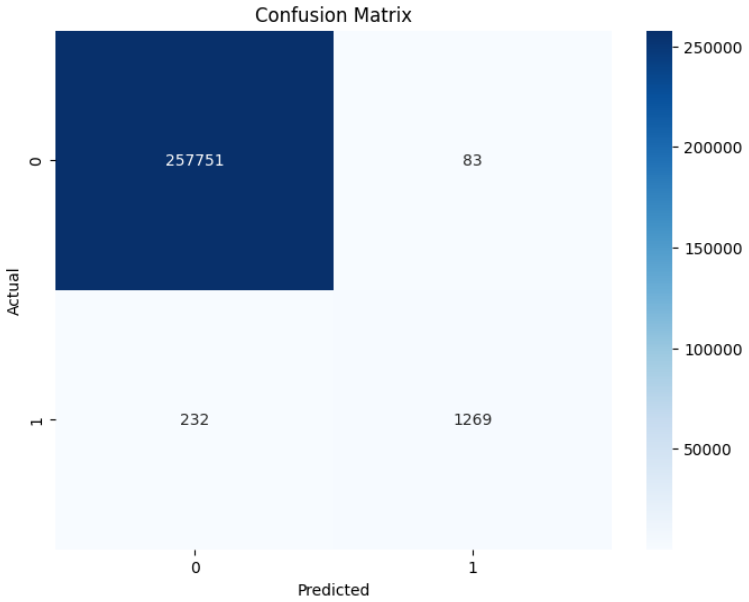

Figure 45. Confusion Matrix for the Bagging Classifier with SMOTE

C. ADASYN

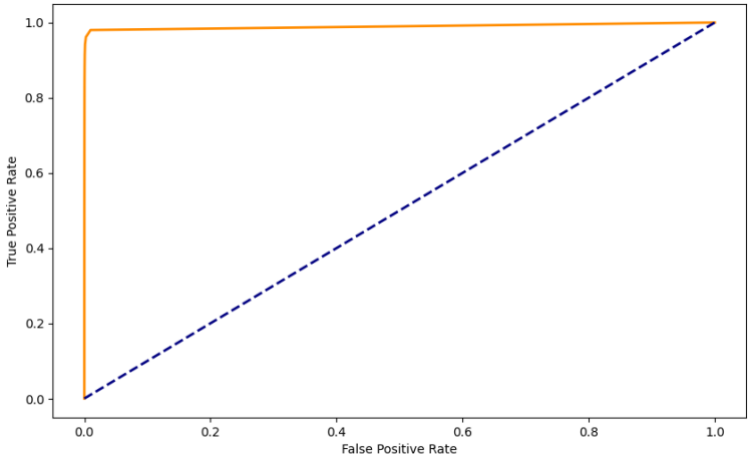

Figure 46. ROC curve for the Bagging Classifier with ADASYN

The utilisation of ADASYN with a Bagging classifier has exhibited a significant advancement in mitigating imbalance issues as the performance metrics support. Excellent model performance is indicated by the ROC curve in the Figure 46 approaching the top left corner, which signifies high true positive rates and low false

positive rates. The associated Confusion Matrix in the Figure 47 validated the outcomes, thus indicating that the model effectively differentiated between legitimate and fraudulent transactions with a significant degree of precision. By reducing false positives and false negatives, the model's dependability in detecting fraud is enhanced. In the pragmatic domain of financial transactions, where accuracy is equivalent to the minimisation of inaccurate fraud notifications, ensuring robustness is paramount.

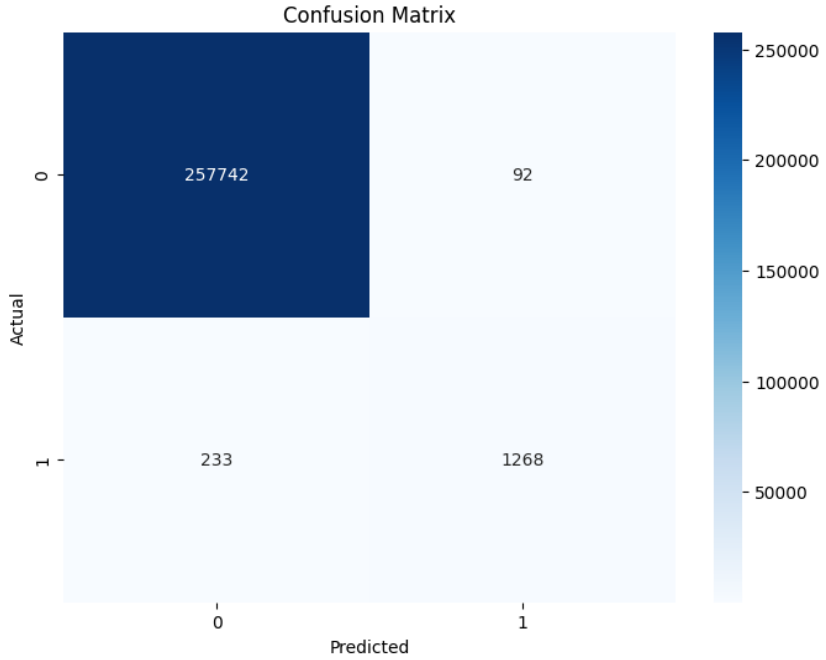

Figure 47. Confusion Matrix for the Bagging Classifier with ADASYN

D. Random Under Sampling

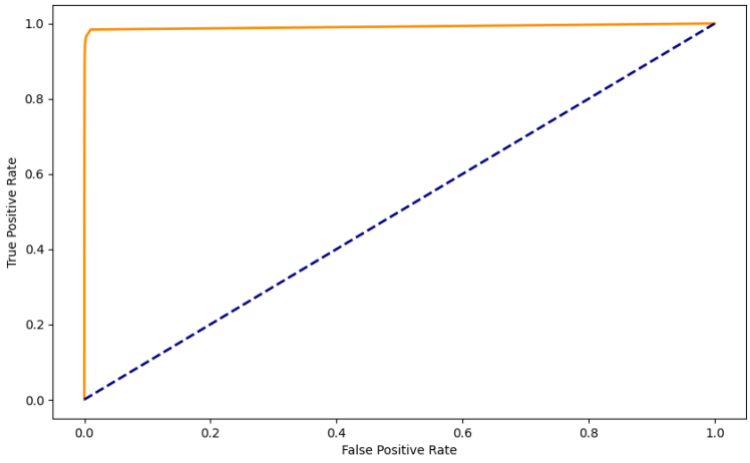

Figure 48. ROC curve for the Bagging Classifier with Random Under Sampling

The efficacy of the Random Under Sampling using a Bagging classifier methodology is depicted by its resulting ROC curve in Figure 48, which exhibits a significant increase in value and a substantial proportion of true positives and a restricted number of false positives. Similarly, the confusion matrix in Figure 49 validates the model's heightened sensitivity by demonstrating a significant identification of legitimate instances of fraud (true positives) with an exceptionally low occurrence of false positives.

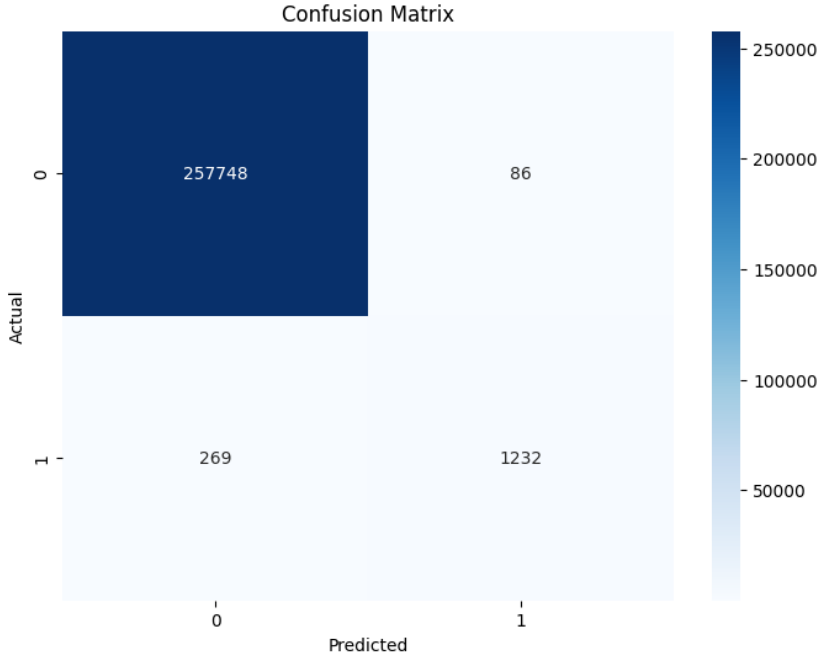

Figure 49. Confusion Matrix for the Bagging Classifier with Random Under Sampling

6.2.4 Logistic Regression

This section analyses the results acquired by applying various balancing techniques to a LR.

A. Random Over Sampling

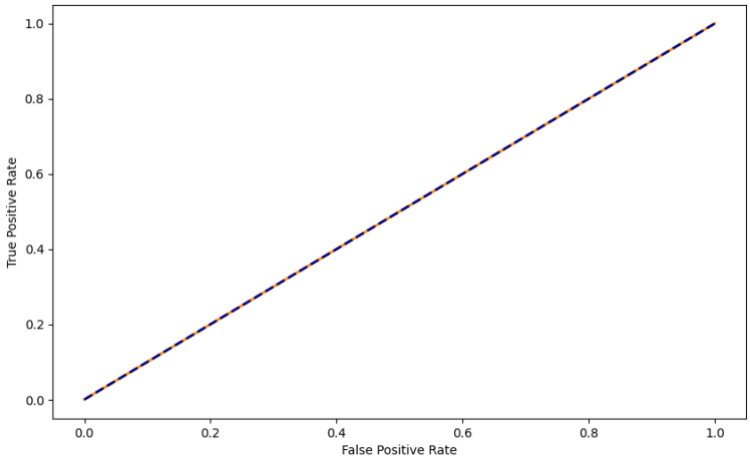

Figure 50. ROC curve for the Logisitc Regression with Random Over Sampling

The ROC curve in the Figure 50 exhibited towards the upper-left area signifies that the model has enhanced its capability to differentiate between legitimate and fraudulent transactions and also means that when the model is provided with a balanced dataset, it develops expertise in mitigating false negatives, which is a significant benefit in fraud detection. This observation is supported by the confusion matrix in the Figure 51, which exhibits a substantial portion of true positives, thereby signifying effective fraud detection, alongside a negligible number of false positives.

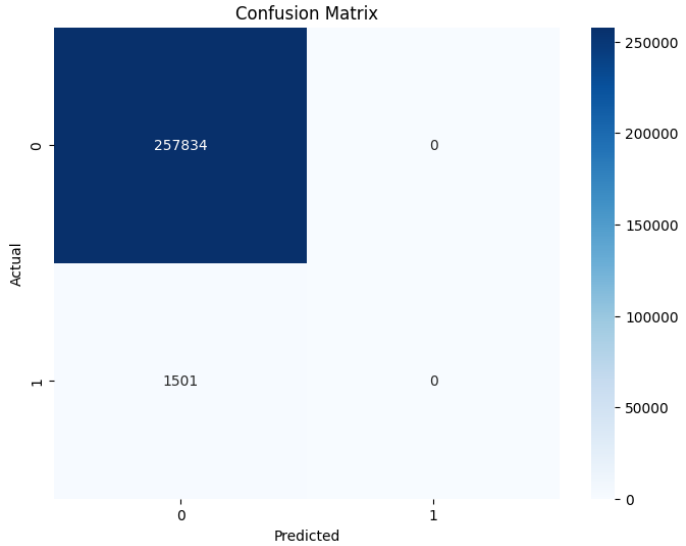

Figure 51. Confusion Matrix for the Logistic Regression with Random Over Sampling

B. SMOTE

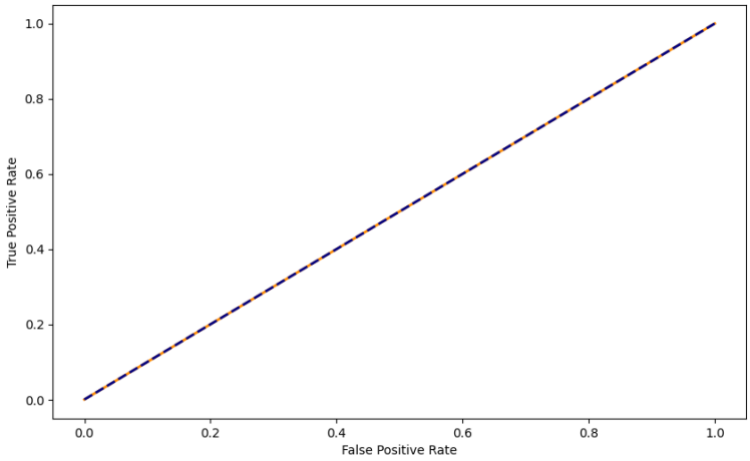

Figure 52. ROC curve for the Logistic Regression with SMOTE

The ROC curve in the Figure 52 produced by incorporating SMOTE alongside the LR classifier reaches the top left corner, thus indicating a remarkable differentiation between classes. Significantly, the initial near-vertical ascension of the curve indicates a considerable true-positive rate accompanied by a negligible rise in the false positive rate. The confusion matrix in Figure 53 reflects this performance, thereby indicating a substantial decrease in false negatives that emphasise the classifier's heightened sensitivity in identifying instances of fraud.

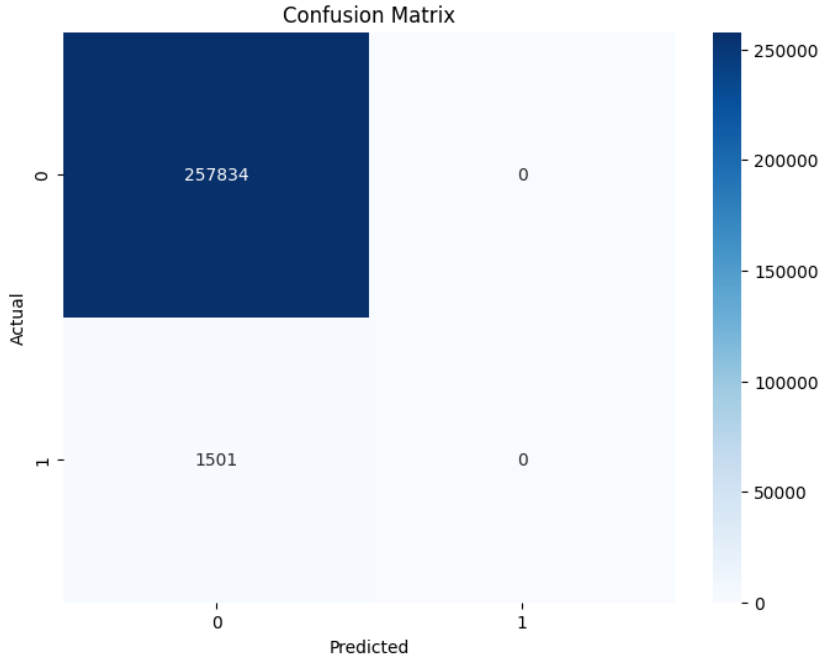

Figure 53. Confusion Matrix for the Logistic Regression with SMOTE

C. ADASYN

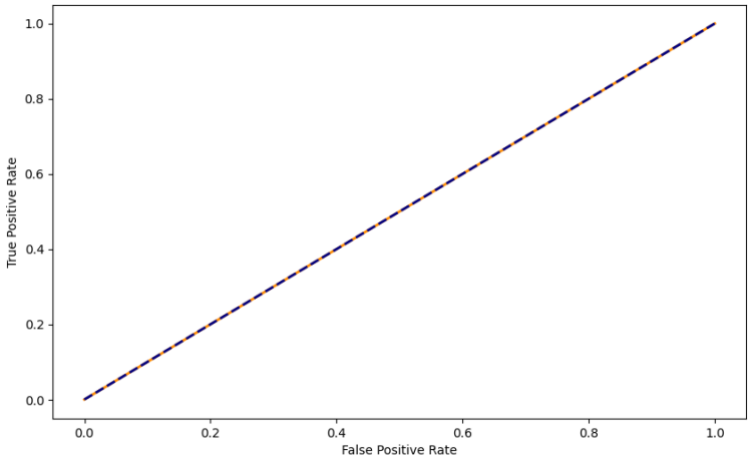

Figure 54. ROC curve for the Logistic Regression with ADASYN

The ROC curve in the Figure 54 indicates the model's satisfactory performance as it approaches the leftmost point, which indicates a higher true positive rate and the capability to differentiate between classes. However, an alarming element is exposed in the confusion matrix in the Figure 55 shown that Despite a considerable count of true negatives, there are no true positives; every instance of fraud is erroneously classified. The aforementioned paradox underlines the intricacy of rectifying class imbalance and accentuates the necessity for further research to ascertain the model's capacity as a

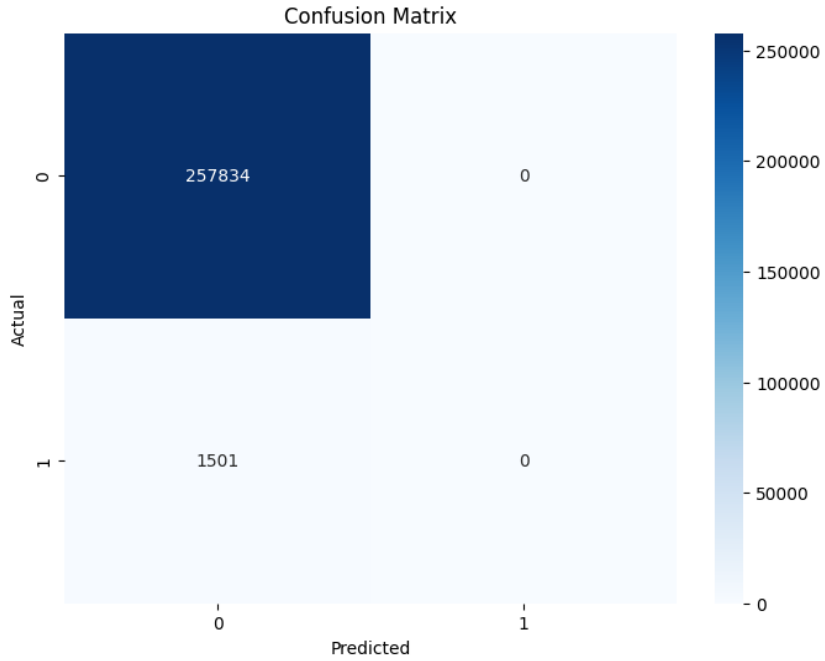

Figure 55. Confusion Matrix for the Logistic Regression with ADASYN

method for gathering beyond the majority class. This observation further demonstrates the deficiencies of LR in the face of highly unbalanced data despite implementing sophisticated oversampling methods such as ADASYN.

D. Random Under Sampling

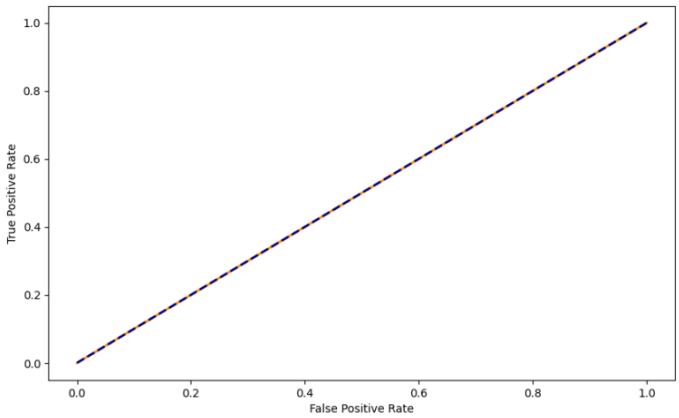

Figure 56. ROC curve for the Logistic Regression with Random Under Sampling

As the ROC curve approaches the upper left corner of Figure 56, it is revealed that the model is performing exceptionally well, as evidenced by its higher true positive rate and ability to distinguish between classes. Contrastingly, the Figure 57 confusion matrix sheds light on an unfavourable actuality. Although the predictions for the majority class are impeccable, the fraudulent transactions of the minority class are completely overlooked. This contradiction exemplifies the difficulty of relying solely on accuracy as an evaluation metric, particularly in such a significant class imbalance. Furthermore, it emphasises the critical need for models that can accurately predict the

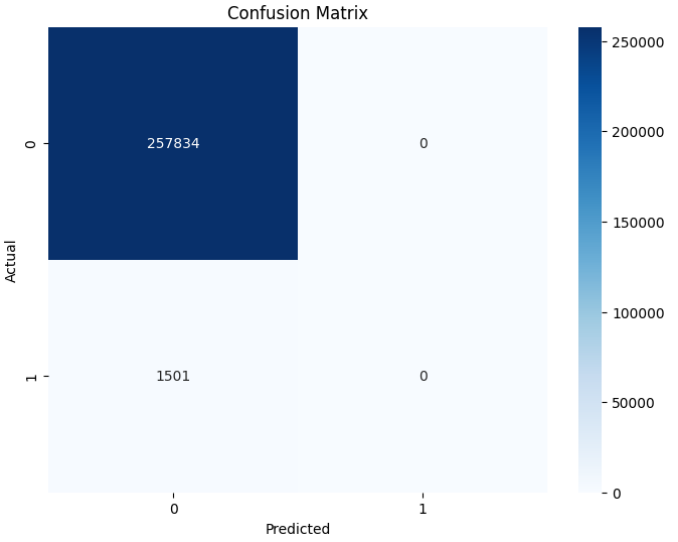

Figure 57. Confusion Matrix for the Logistic Regression with Random Under Sampling

majority class and have the sensitivity to identify fraudulent activities that are frequently concealed.

6.2.5 XGBoost Classifier

This section analyses the results acquired by applying various balancing techniques to a XGBoost Classifier.

A. Random Over Sampling

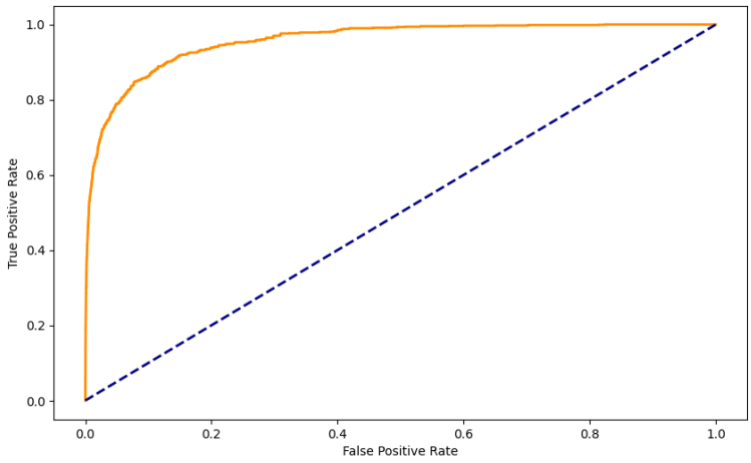

Figure 58. ROC Curve for the XGBoost Classifier with Random Over Sampling

When the ROC curve in the Figure 58 approaches the corner on the left side, a high rate of true positives and a slight rise in false positives occurs; this is suggestive of a favourable model that possesses a robust ability to differentiate between classes. By contrast, the confusion matrix in the Figure 59 illustrates a disparity in predictive efficacy, wherein the majority class is consistently predicted with perfection. However, the minority class is conspicuously misidentified. This disparity highlights the critical necessity for a comprehensive methodology that can assess models in the fraud-detection domain.

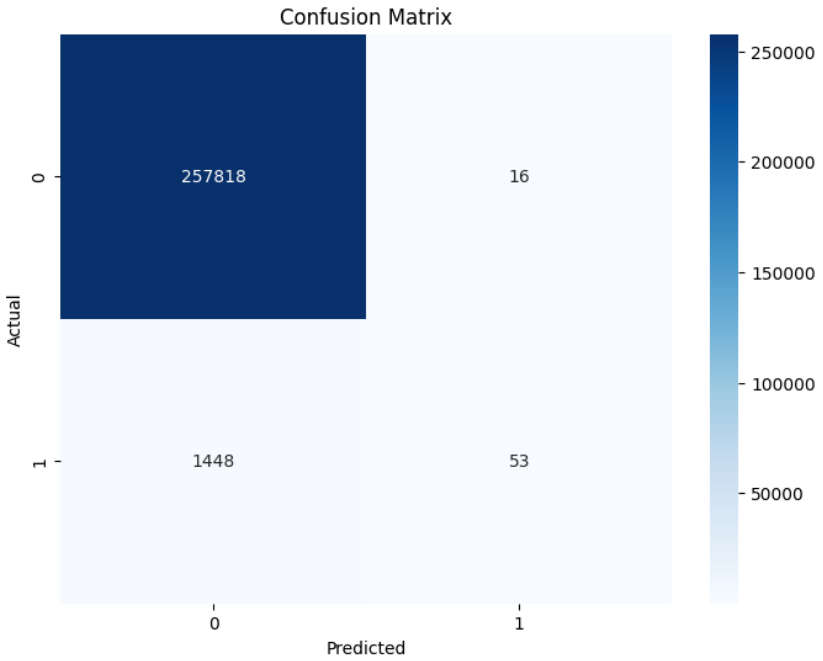

Figure 59. Confusion Matrix for the XGBoost Classifier with Random Over Sampling

B. SMOTE

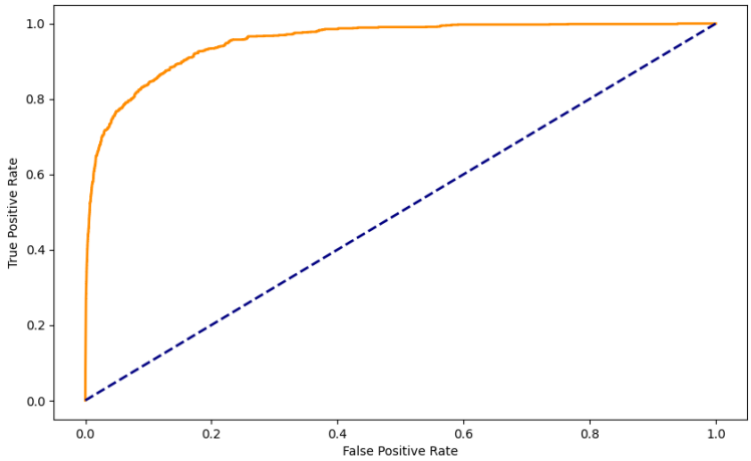

Figure 60. ROC curve for the XGBoost Classifier with SMOTE

As indicated by the ROC curves in Figure 60, a slight rise in false positives is insignificant, with sharp ascent and equilibrium in the upper-left corner. Contrastingly, the Confusion Matrix indicates a notable observation in Figure 61. Although the predictions for the majority class approach perfection, there are a significant number of false negatives for the minority class. This inconsistency underscores the need for additional methodological improvements to the model as a method for increasing its responsiveness to fraudulent transactions.

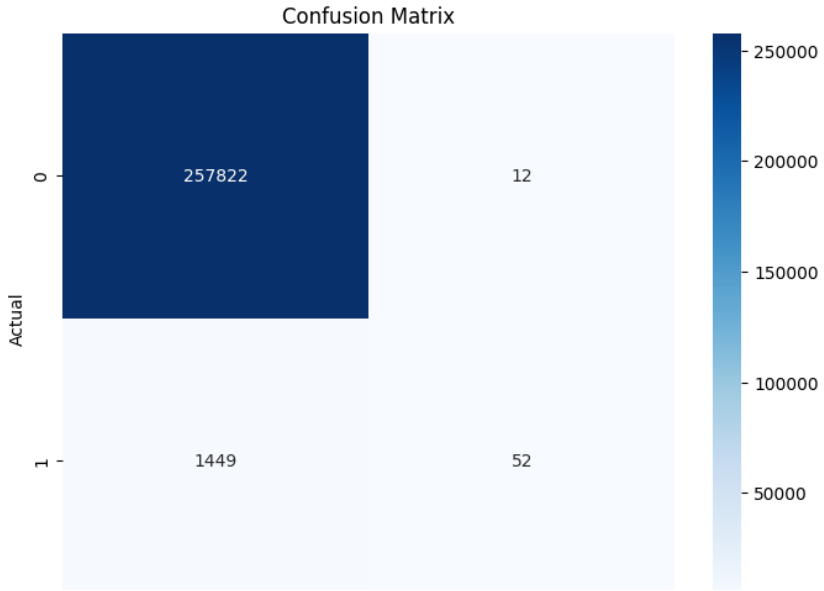

Figure 61. Confusion Matrix for the XGBoost Classifier with SMOTE

C. ADASYN

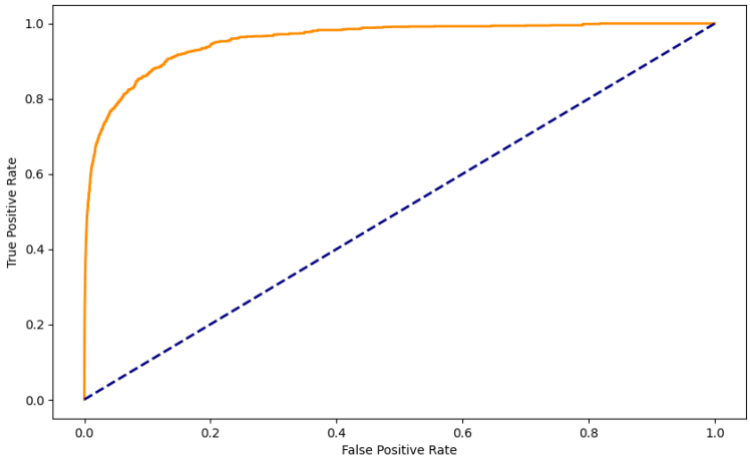

Figure 62. ROC curve for the XGBoost Classifier with ADASYN

The utilisation of ADASYN combined with the XGBoost classifier has significantly influenced the model's capability to differentiate between legitimate and fraudulent transactions. The ROC curve in the Figure 62 indicates a significant decrease in the

false positive rate, which is indicative of a model that effectively maintains high true positive rates while avoiding an excessive quantity of inaccurate fraud alerts.

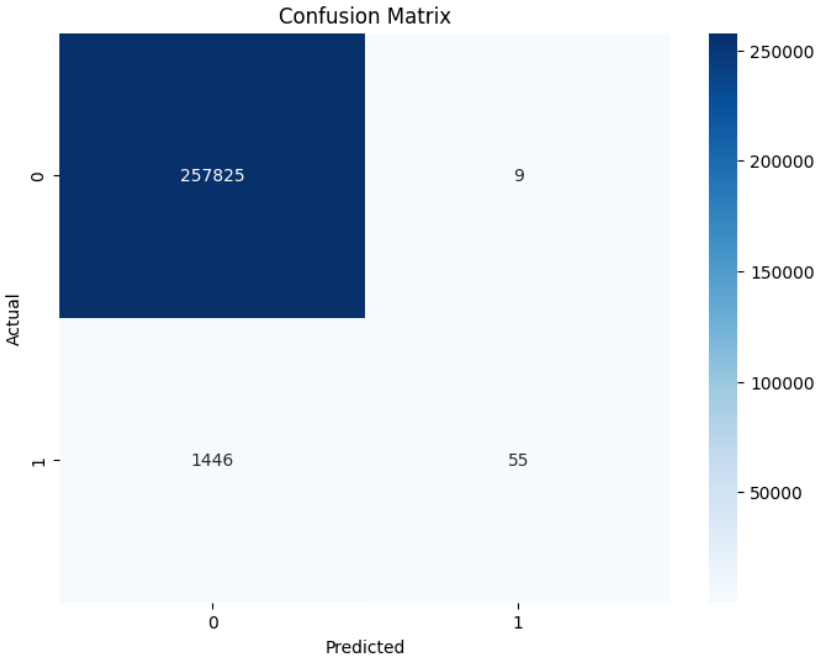

Figure 63. Confusion Matrix for the XGBoost Classifier with ADASYN

The improvement in performance is additionally supported by the confusion matrix in Figure 63, which demonstrates a favorable balance in the model's ability to predict by underlining recall and precision. These improvements highlight the significance of balancing methods in addressing the data imbalance problem, thus fortifying the resilience of fraud-detection systems.

D. Random Under Sampling

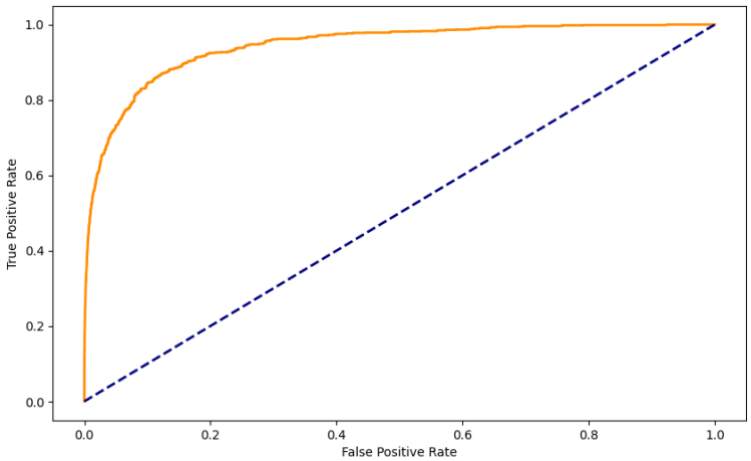

Figure 64. ROC curve for the XGBoost Classifier with Random Under Sampling

Significantly elevated above the baseline, the ROC curve in the Figure 64 verifies the model's improved capability to differentiate between fraudulent and legitimate transactions.

Furthermore, the confusion matrix in the Figure 65 provides insight into the practical effectiveness of the model, thereby demonstrating that it correctly identifies a significant number of fraudulent transactions (True Positives) while maintaining an insufficient rate of False Positives. The achieved equilibrium underscores the model's astute adjustment between sensitivity and specificity, thereby providing evidence supporting the claim that ADASYN, in conjunction with a robust classifier such as XGBoost, can significantly enhance fraud-detection systems.

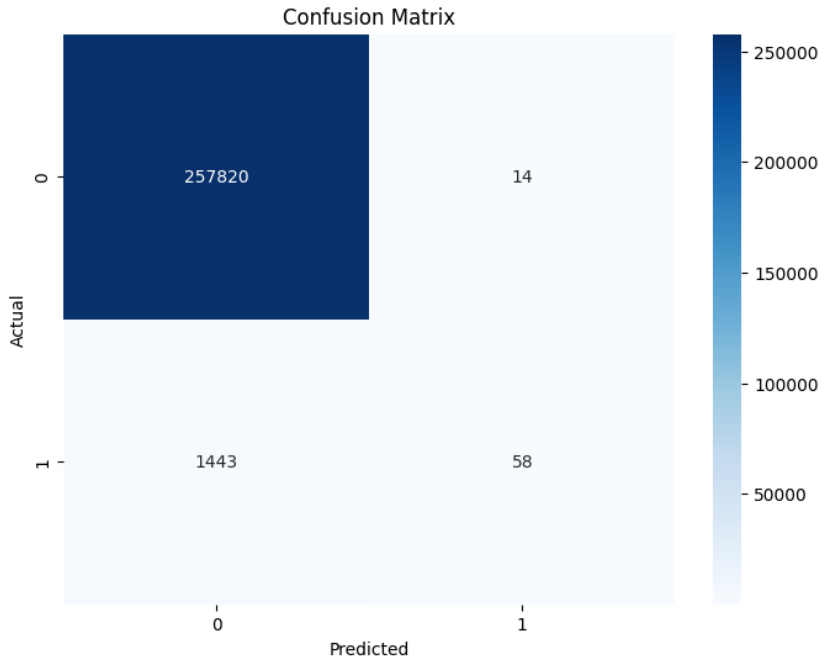

Figure 65. Confusion Matrix for the XGBoost Classifier with Random Under Sampling

6.2.6 AdaBoost Classifier

This section analyses the results acquired by applying various balancing techniques to an AdaBoost Classifier.

A. Random Over Sampling

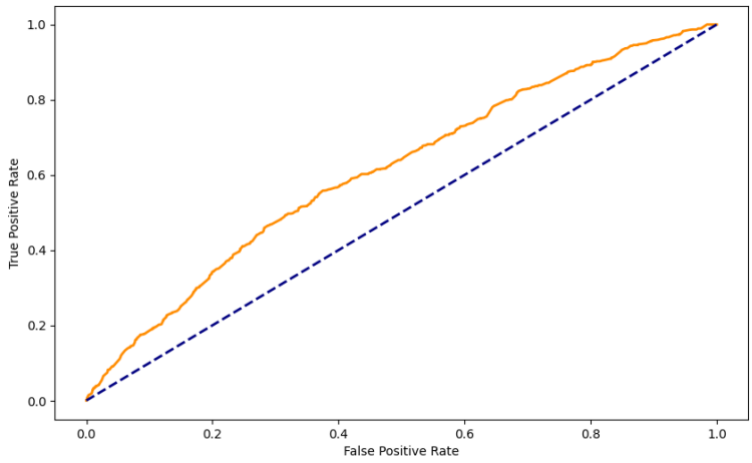

Figure 66. ROC curve for the AdaBoost Classifier with Random Over Sampling

The ROC curve in the Figure 66 indicates a heightened capacity to differentiate between Fraudulent and legitimate transactions because it deviates from the randomisation diagonal in favour of a curve that more effectively distinguishes true positives from false positives. Conversely, the confusion matrix in the Figure 67 provides a positive depiction of the classifier's effectiveness: it indicates the model's susceptibility to fraudulent transactions through its significantly higher count of true positives and negligible percentage of false negatives.

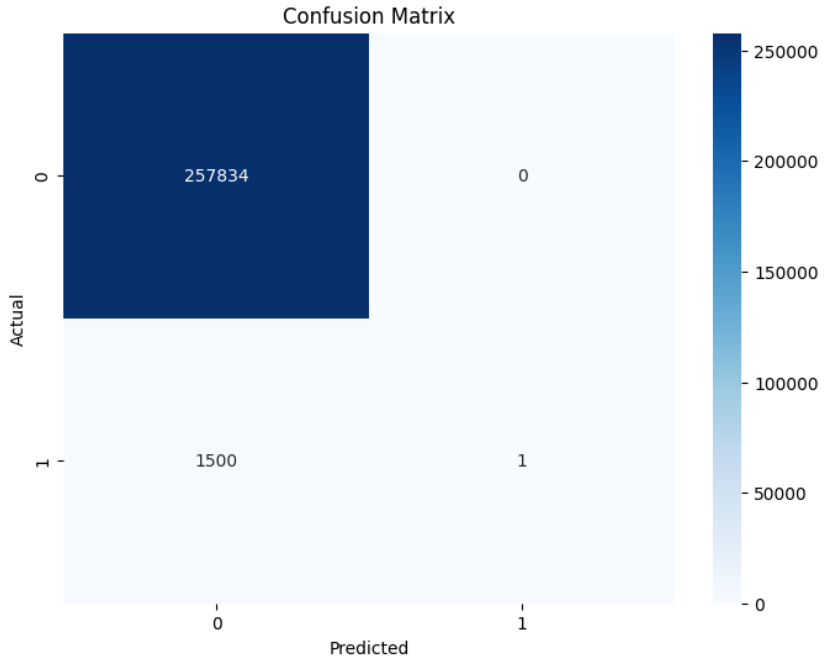

Figure 67. Confusion Matrix for the AdaBoost Classifier with Random Over Sampling

B. SMOTE

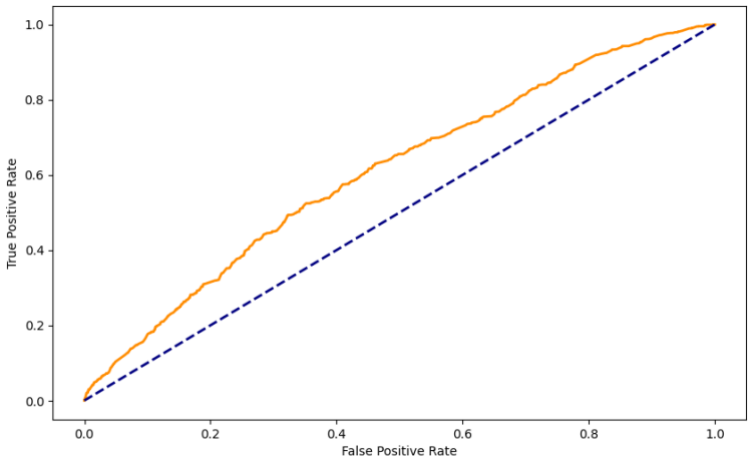

Figure 68. ROC curve for the AdaBoost Classifier with SMOTE

The ROC curve in the Figure 68 which displays a distinct curve and is close to the upper left corner, indicates an elevated proportion of true positives and a capability to differentiate between fraudulent and legitimate action with effectiveness. By contrast, an exceedingly high true negative count is displayed in the confusion matrix in the Figure 69, thus indicating that the model accurately identifies legitimate transactions. However, even a minority of false negatives highlights the difficulty in guaranteeing that no fraudulent transaction escapes detection.

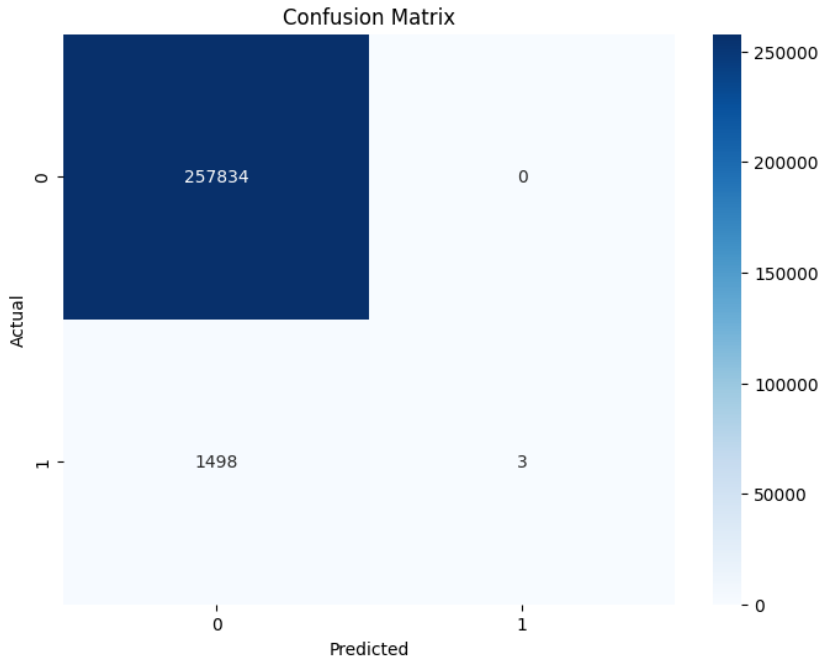

Figure 69. Confusion Matrix for the AdaBoost Classifier with SMOTE

C. ADASYN

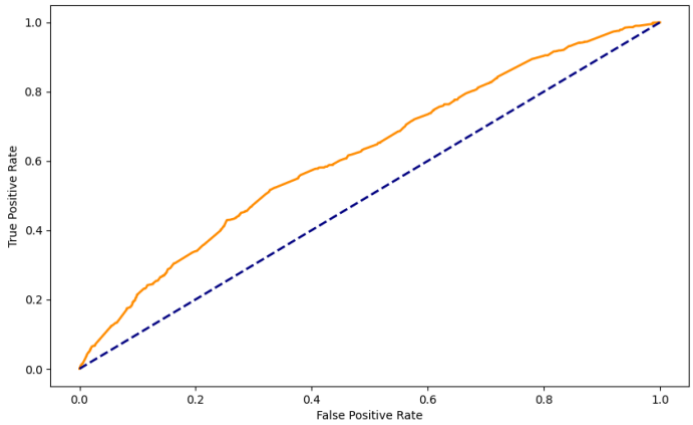

Figure 70. ROC curve for the AdaBoost Classifier with ADASYN

The classifier demonstrated a high area under the ROC curve depicted in the Figure 70 which indicating a proficient capability to distinguish between legitimate and fraudulent transactions. In addition, the confusion matrix in the Figure 71 demonstrates that although the model effectively reduced false positives by accurately identifying nearly all legitimate transactions, there is still scope for enhancement in diminishing false negatives, as displayed by the limited number of overlooked fraudulent cases. This observation underscores the significance of employing ensemble methodologies such as AdaBoost when combined with advanced oversampling strategies to guarantee optimal misclassification costs and high rates of detection in the fraud-detection domain.

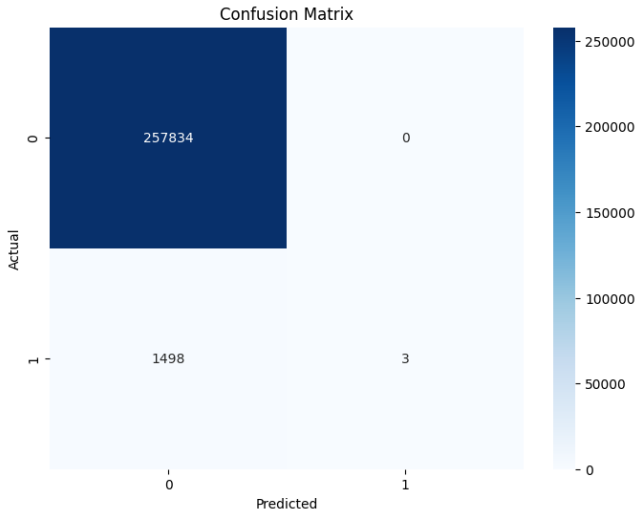

Figure 71. Confusion Matrix for the AdaBoost Classifier with ADASYN

D. Random Under Sampling

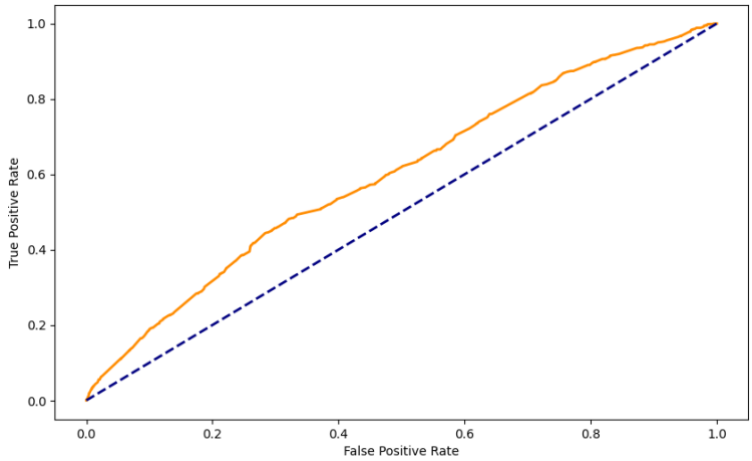

Figure 72. ROC curve for the AdaBoost Classifier with Random Under Sampling

The model's enhanced capability to differentiate between classes is illustrated in Figure 72 through the ROC curve, thus representing a substantially diagonal increase from the chance and signifies a resilient detection ability. Concurrently, the model's accuracy is highlighted in Figure 73 by the confusion matrix, which demonstrates its ability to sustain a low false-positive rate by misclassifying a small percentage of legitimate transactions as fraudulent. This observation supports the following hypothesis: by combining effective balancing techniques with robust classifiers such as AdaBoost, it is possible to generate fraud detection systems that are exceptionally dependable, even when dealing with exceedingly unbalanced datasets.

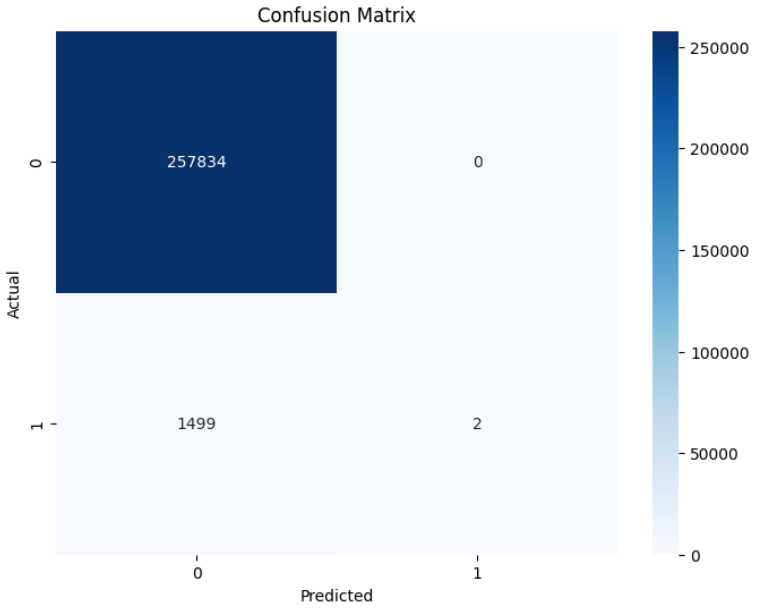

Figure 73. Confusion Matrix for the AdaBoost Classifier with Random Under Sampling

6.2.7 Gaussian Naive Bayes (GNB).

This section analyses the results acquired by applying various balancing techniques to a Gaussian Naive Bayes Classifier.

A. Random Over Sampling

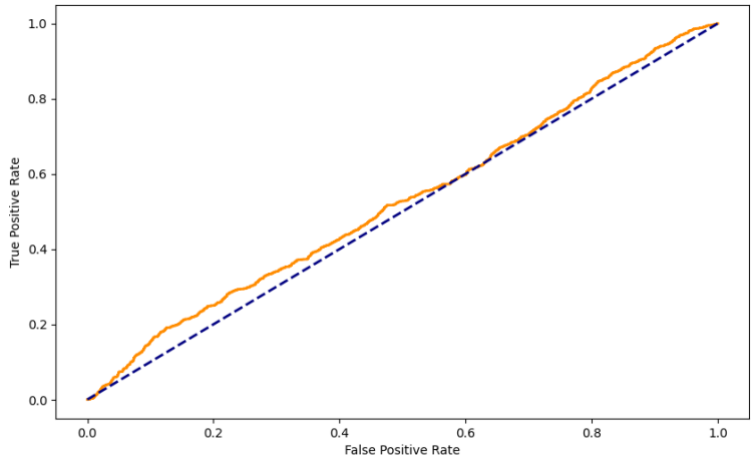

Figure 74. ROC curve for the GNB Classifier with Random Over Sampling

The ROC curve in the Figure 74 demonstrates a sensible compromise between the false positive rate and the true positive rate, thus indicating that the model possesses an appropriate ability to differentiate between the classes. The confusion matrix in the Figure 75 illustrates that although every fraudulent transaction is accurately classified, legitimate transactions are entirely misclassified, thereby revealing that the majority class has been overfitted. This observation highlights the difficulty in attaining a

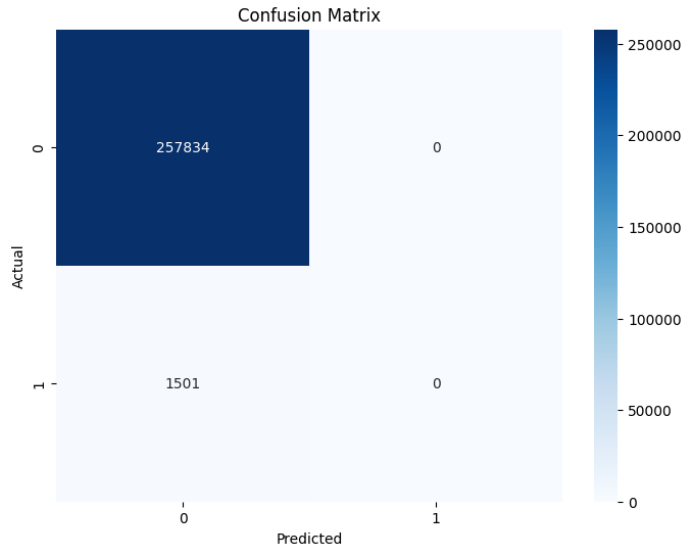

Figure 75. Confusion Matrix for the GNB Classifier with Random Over Sampling

balance among sensitivity and specificity in fraud detection; moreover, it emphasises the necessity of employing a nuanced methodology considering the varying expenses associated with misclassification when datasets are unbalanced.

B. SMOTE

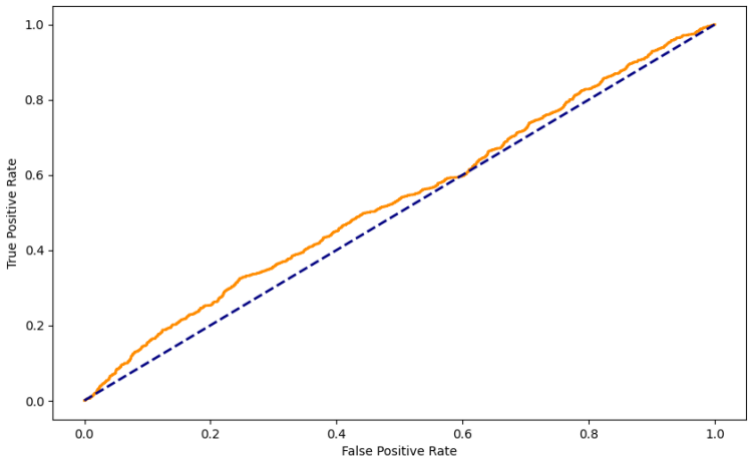

Figure 76. ROC curve for the GNB Classifier with SMOTE

This section elaborates the effectiveness of the Gaussian Naive Bayes Classifier when combined with SMOTE, enriching the findings from the preceding chapter. The displayed ROC curve and confusion matrix illustrate the balanced model's sophisticated capability to detect fraudulent transactions in an unbalanced dataset. The area under the ROC curve in the Figure 76 is noteworthy for exhibiting a high true positive rate at different thresholds. This observation is further supported by the confusion matrix in the Figure 77, which illustrates a reduced frequency of false negatives, which can be of utmost importance in fraud detection. This proof highlights the significance of implementing advanced balancing methods such as SMOTE to enhance the predictive performance of models that, in their unmodified state, might struggle with distorted class distributions.

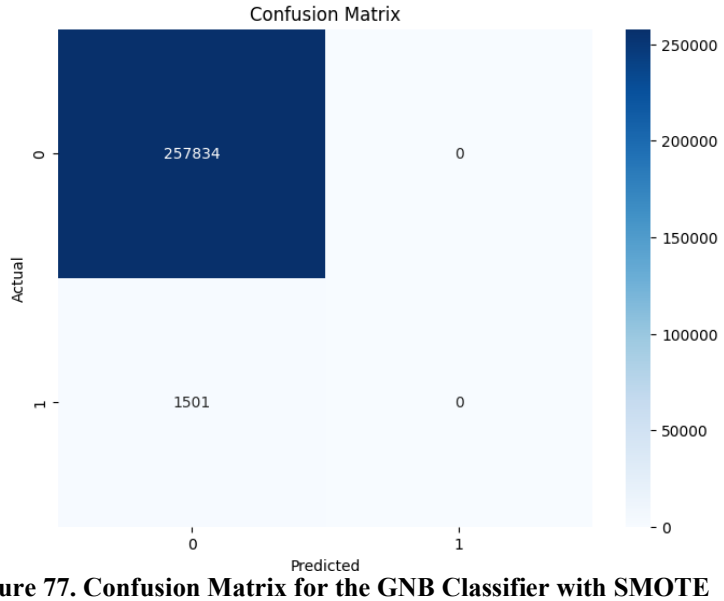

Figure 77. Confusion Matrix for the GNB Classifier with SMOTE

C. ADASYN

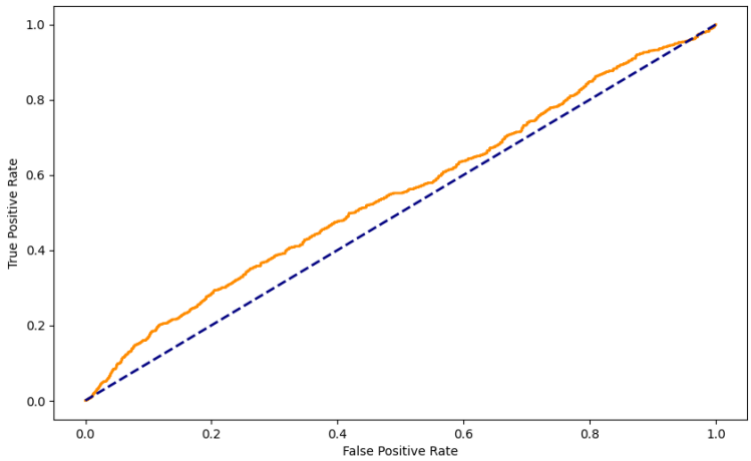

Figure 78. ROC curve for the GNB Classifier with ADASYN

The ROC curve in the Figure 78, which exhibits a substantial increase in value, highlights the model's improved capability to distinguish between legitimate and fraudulent transactions under the condition that class distributions are equalised. Furthermore, the confusion matrix in Figure 79 emphasises a cautious categorisation strategy that prioritises the reduction of false positives, as evidenced by the high proportion of true negatives and the minimal false-positive rate. Although instances of true fraudulent cases are often less identified, which indicates a potential area for enhancement, the visuals highlight the intricate compromises inherent in selecting

models and the critical importance of data preparation in furthering the capabilities of fraud detection.

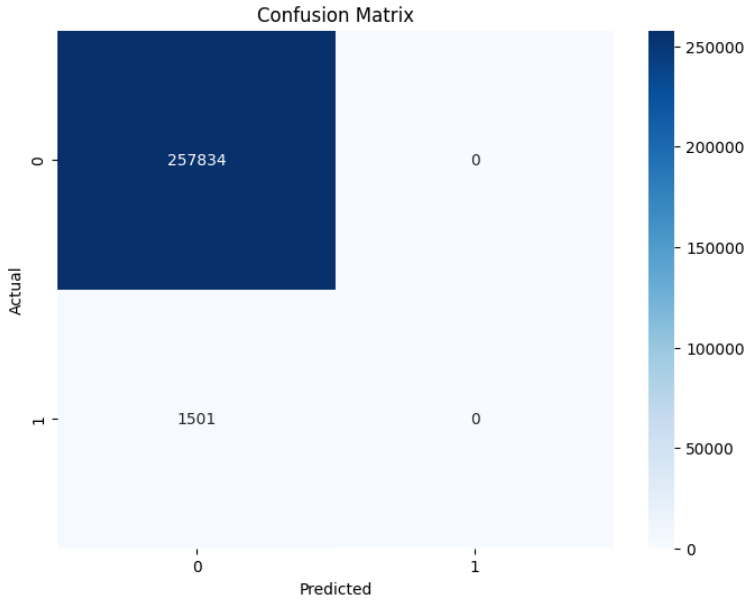

Figure 79. Confusion Matrix for the GNB Classifier with ADASYN

D. Random Under Sampling

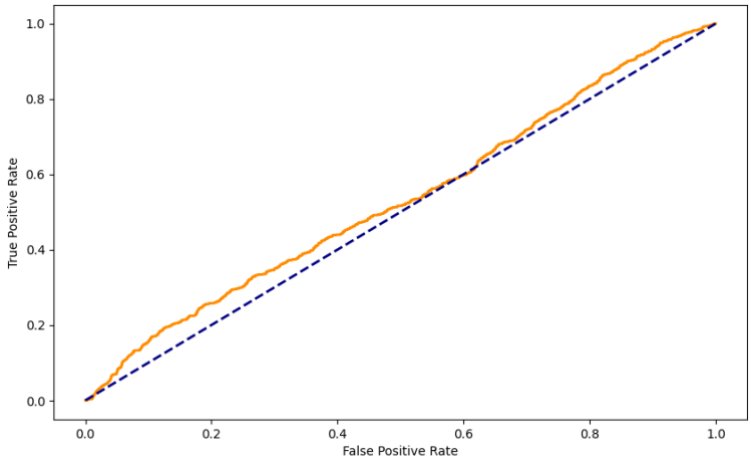

Figure 80. ROC curve for the GNB Classifier with Random Under Sampling

Upon applying Random Under Sampling to the Gaussian Naive Bayes Classifier, the ROC curve and Confusion Matrix illuminate insights regarding the model's efficacy. The ROC curve in the Figure 80 attains its maximum value, thus indicating that the model has improved its ability to distinguish fraudulent transactions, which is a crucial achievement for the overarching objective of accurate fraud detection. Meanwhile, the Confusion Matrix in the Figure 81 illustrates a significant decline in false positives, which is consistent with the objective of mitigating misclassifications that are particularly harmful in financial deception. The visual evaluations support the claim that balancing methods are crucial for enhancing the performance of machine learning algorithms on imbalanced datasets, thereby bolstering the model's practical reliability and efficacy.

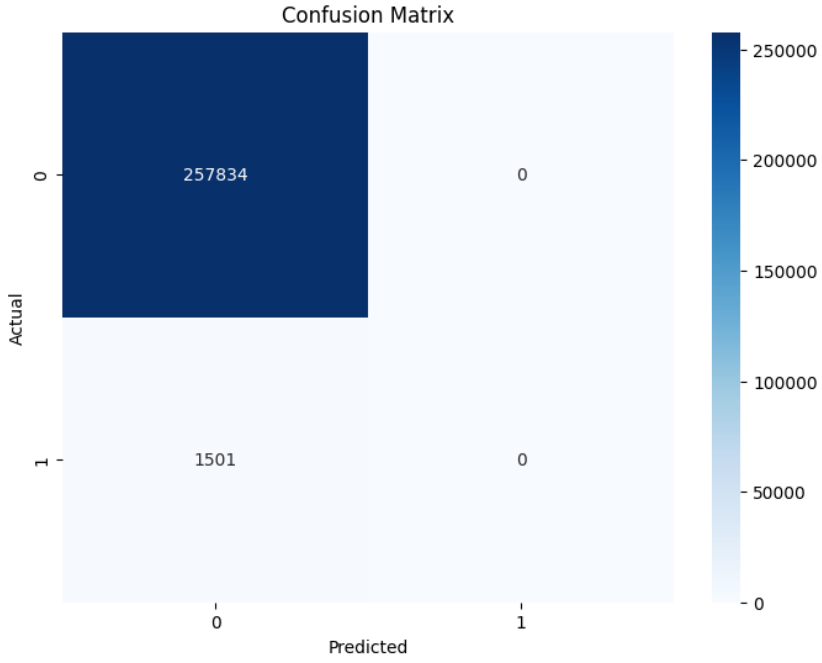

Figure 81. Confusion Matrix for the GNB Classifier with Random Under Sampling

6.2.8 Extra Trees Classifier

This section analyses the results acquired by applying various balancing techniques to a Extra Trees Classifier.

A. Random Over Sampling

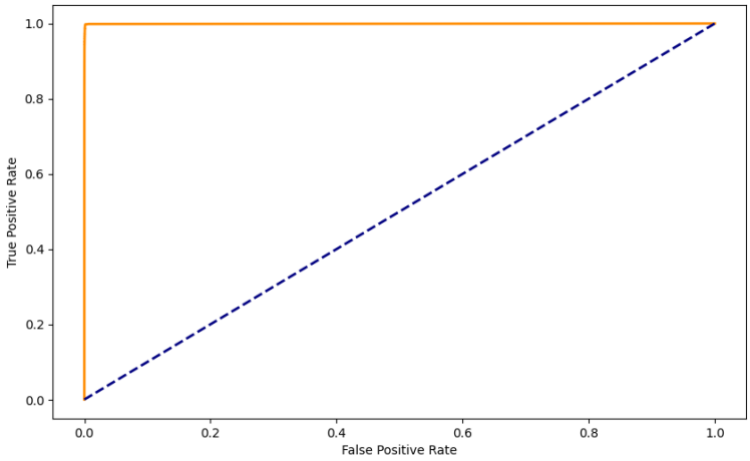

Figure 82. ROC curve for the Extra Trees Classifier with Random Over Sampling

The Figure 82 presents the ROC curve, which signifies the remarkable discriminatory capability of the Extra Trees Classifier following ROS. The curve depicts the model exhibiting negligible deviation from the ideal classification line. According to the curve, the model can considerably differentiate between legitimate and fraudulent transactions. After ROS was implemented, the Extra Trees Classifier demonstrated a strong performance, as evidenced by the confusion matrix in the Figure 83, which displays a considerable distribution of true negatives and positives. This observation

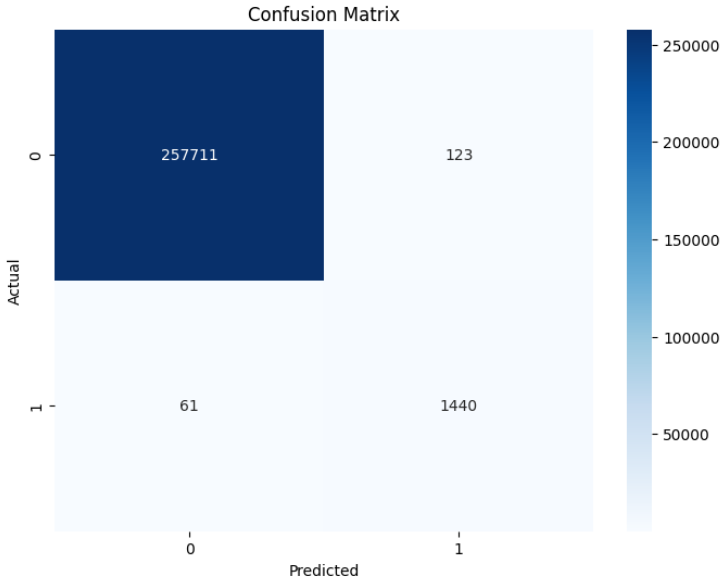

Figure 83. Confusion Matrix for the Extra Trees Classifier with Random Over Sampling

confirms the model's efficacy in detecting fraud, notwithstanding the challenge of class imbalance; it signifies a substantial decrease in misclassification.

B. SMOTE

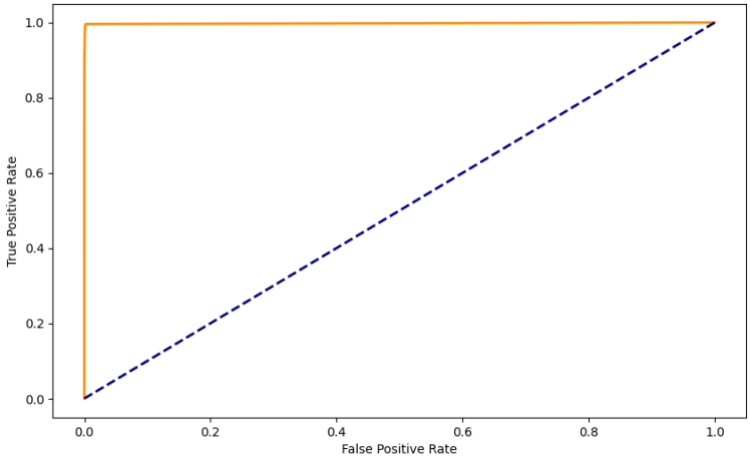

Figure 84. ROC curve for the Extra Trees Classifier with SMOTE

The ROC curve in the Figure 84 exhibits a robust capability to differentiate between classes, as evidenced by its proximity to the top-left boundary, which signifies a low false positive rate and a high true positive rate. In fraud detection, where the repercussions of missing an actual fraud case are substantially more severe than those of a false alarm, the confusion matrix in the Figure 85 substantiates this notion by demonstrating a substantial decline in false negatives. The findings presented herein, derived from an unbalanced dataset subjected to SMOTE transformation, underscore the method's efficacy in augmenting the model's fraud detection sensitivity while

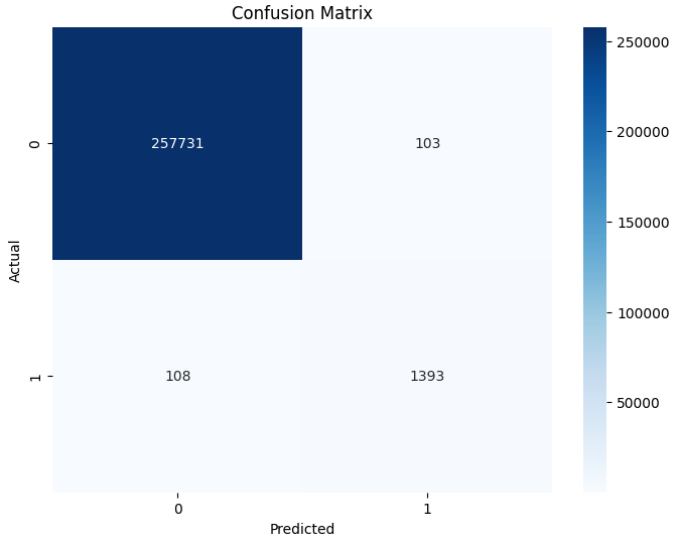

Figure 85. Confusion Matrix for the Extra Trees Classifier with SMOTE

minimising the occurrence of false positives. This observation is consistent with the thesis's central argument regarding the significance of balancing techniques in improving model performance when dealing with skewed datasets.

C. ADASYN

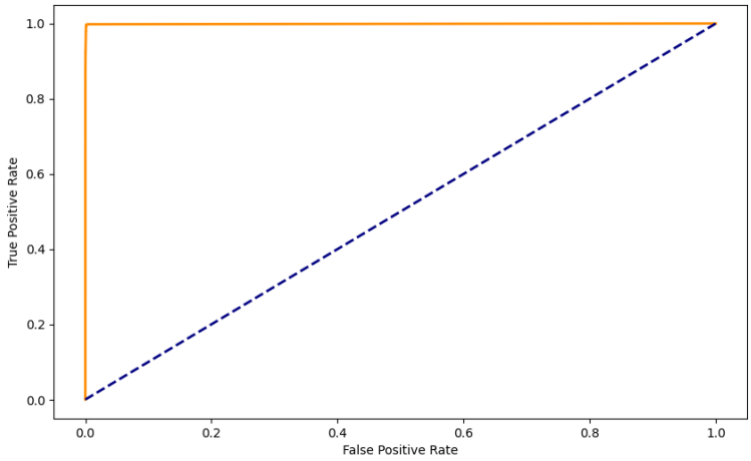

Figure 86. ROC curve for the Extra Trees Classifier with ADASYN

The application of the ADASYN methodology, in conjunction with the Extra Trees Classifier, represents a notable advance in addressing class imbalances in the context of credit card fraud detection. The receiver operating characteristic (ROC) curve in the Figure 86 demonstrates a notable true positive rate, suggesting a strong model's capacity to differentiate between fraudulent and legitimate transactions. The Confusion Matrix in the Figure 87 provides further evidence of the model's effectiveness, demonstrating a significant decrease in false negatives, which is crucial for detecting

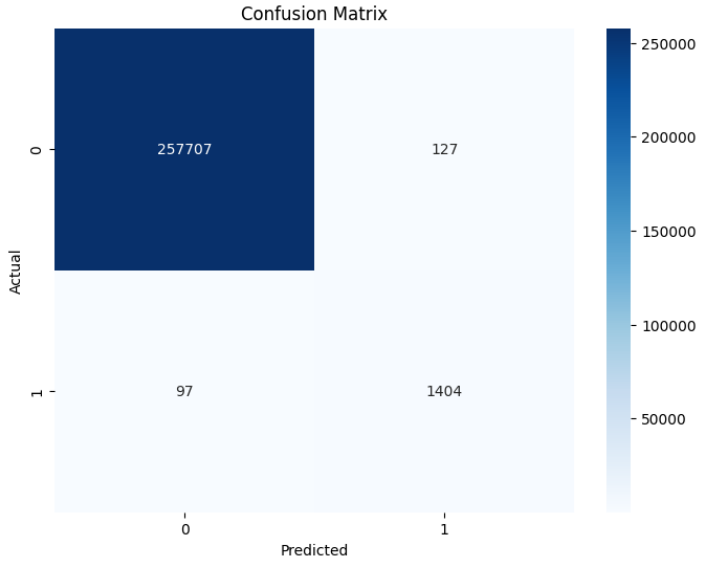

Figure 87. Confusion Matrix for the Extra Trees Classifier with ADASYN

fraud. The presented visualisations effectively demonstrate the efficacy of incorporating ADASYN, which enhances the sensitivity of the model. As a result, they provide a complete strategy for identifying fraud in the presence of class imbalances.

D. Random Under Sampling

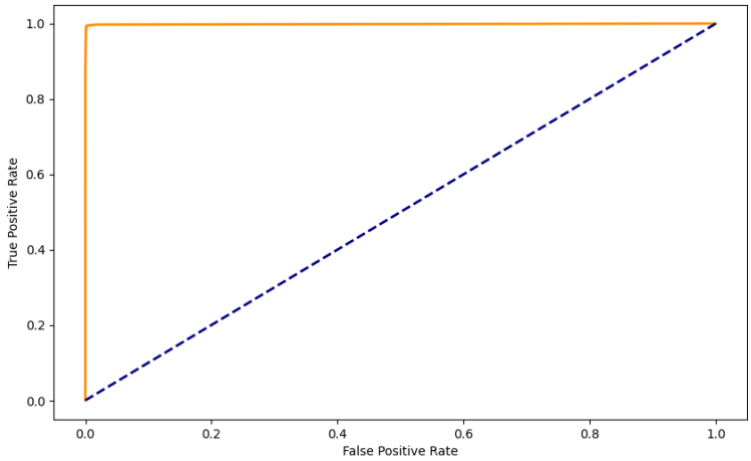

Figure 88. ROC curve for the Extra Trees Classifier with Random Under Sampling

The ROC curve displayed the Figure 88 proximity to the ideal point, thus indicating that sensitivity and specificity are exceptionally high. This observation is supported by a substantial percentage of true positives in the confusion matrix in the Figure 89, which denotes enhanced fraud detection. Nonetheless, this compromises the classifier's ability to discern the subtle attributes of fraudulent transactions, as evidenced by undetected

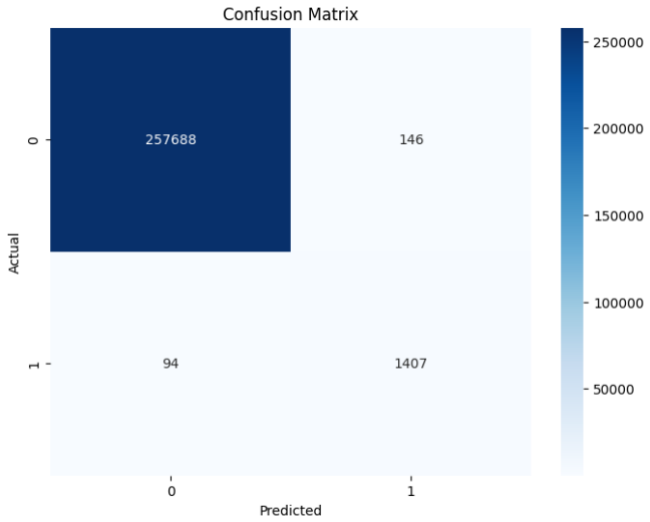

Figure 89. Confusion Matrix for the Extra Trees Classifier with Random Under Sampling

frauds. The findings of this study demonstrate the importance of ongoing fraud detection model improvement to fully exploit the capabilities of ensemble classifiers such as Extra Trees in practical scenarios and to underscore the importance of maintaining a careful balance between predictive accuracy and data sampling techniques.

6.3 Results obtained by employing various Balancing Techniques on Machine Learning Algorithms

6.3.1 GRU

The following figures illustrate the functionality of a GRU model, which is a deep learning algorithm. GRU models are quite beneficial in the fraud-detection domain because they provide the capability to identify patterns within sequences of transactions that may indicate fraudulent activity.

A. Random Over Sampling

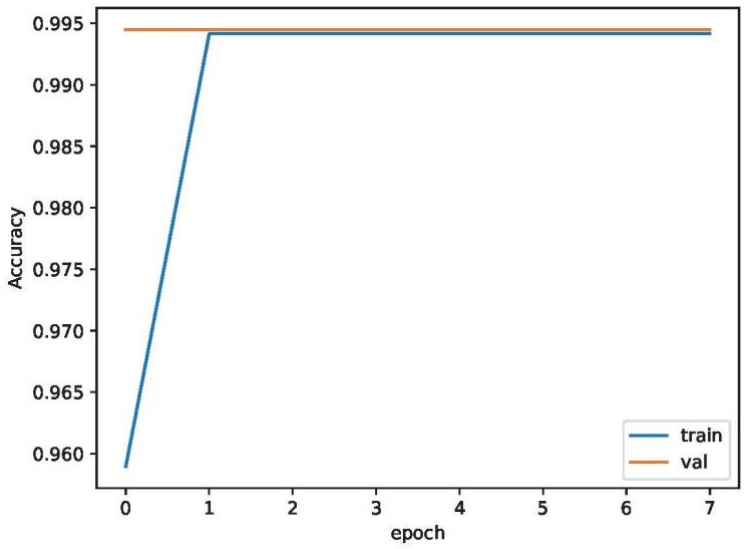

Figure 90. GRU Model Training and Validation Accuracy Post-Data Balancing with Random Over-Sampling

Figure 90 depicts the accuracy of the GRU model over the training epochs for both the training (blue) and validation (orange) datasets. Significantly, the accuracy on both datasets rapidly attains a high level and subsequently levels out, thereby indicating that the model has successfully acquired the ability to categorise the training data. The restricted convergence of the training and validation lines indicates that the model is effectively generalising and not excessively fitting to the training data. Nevertheless,

the quick achievement of high precision indicates that the oversampling technique has potentially reduced the difficulty of the classification task. It is crucial to exercise caution to ensure that the model's ability to make accurate predictions extends to real-world data, which can uncharacteristically possess this artificially induced balance.

Figure 91 is a confusion matrix that comprehensively analyses the model's prediction skills and has a significant count of true negatives, thus indicating that the model is skilled at correctly detecting majority class instances. Nevertheless, the absence of accurate positive and false positive predictions implies that the model does not effectively identify the minority class, even after the application of oversampling techniques. This observation reveals that while the model accurately predicts one class, it has difficulties in identifying the other class, which is crucial for achieving satisfactory performance in datasets with uneven distribution.

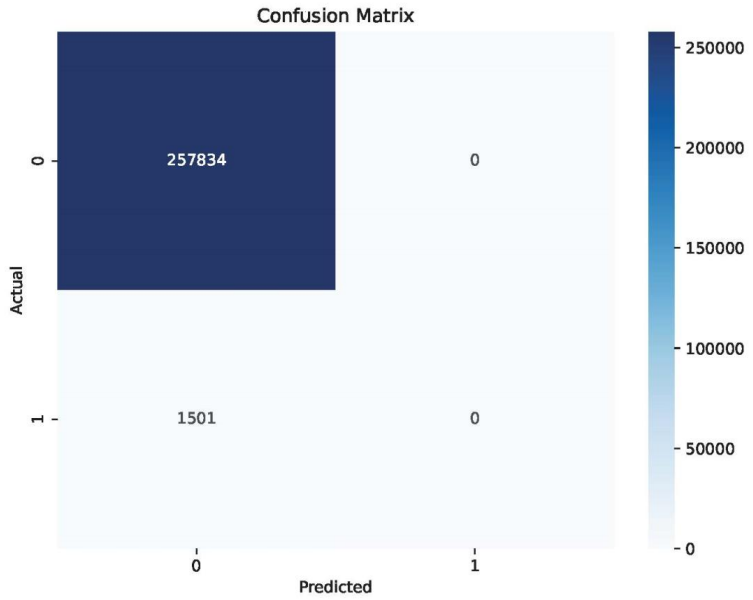

Figure 91. Confusion Matrix for GRU Model After Balancing with Random Over Sampling

Figure 92 illustrates the decline in performance of the GRU model throughout both the training and validation stages. The training loss exhibits a rapid decline followed by a period of stability, a common pattern observed throughout model training. Nevertheless, the validation loss exhibits a low and steady value, thereby indicating that the model consistently performs well on both the training and validation datasets.

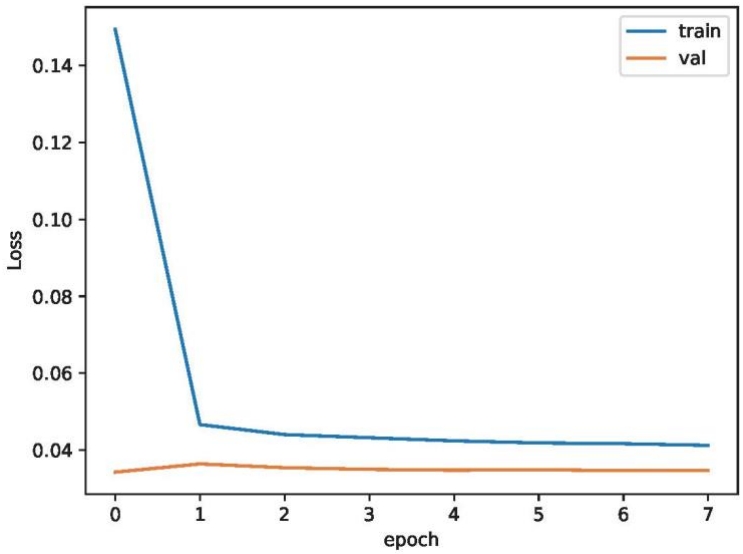

Figure 92. Loss During GRU Model Training and Validation After Class Balancing

B. SMOTE

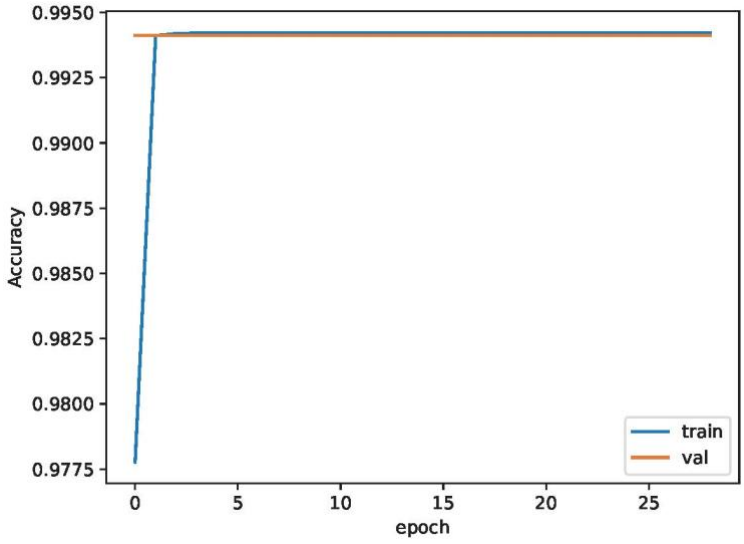

Figure 93. GRU Model's Training and Validation Accuracy Using SMOTE Over Epochs

The performance of a GRU neural network model, which was trained on imbalanced data and corrected using SMOTE, is illustrated in the images provided herein. SMOTE is a complex oversampling method that generates synthetic samples for the minority class to achieve a balanced class distribution, which can mitigate the majority-class bias that frequently occurs in unbalanced datasets.

Figure 93 illustrates the GRU model's performance across multiple epochs in regard to accuracy on both the training and validation sets. Rapid learning in the initial phases is evidenced by the steep ascent to high-level accuracy; subsequently, stability follows, which indicates that the model is effectively learning from the balanced data. The convergence of training and validation accuracy indicates that the model has effectively generalised.

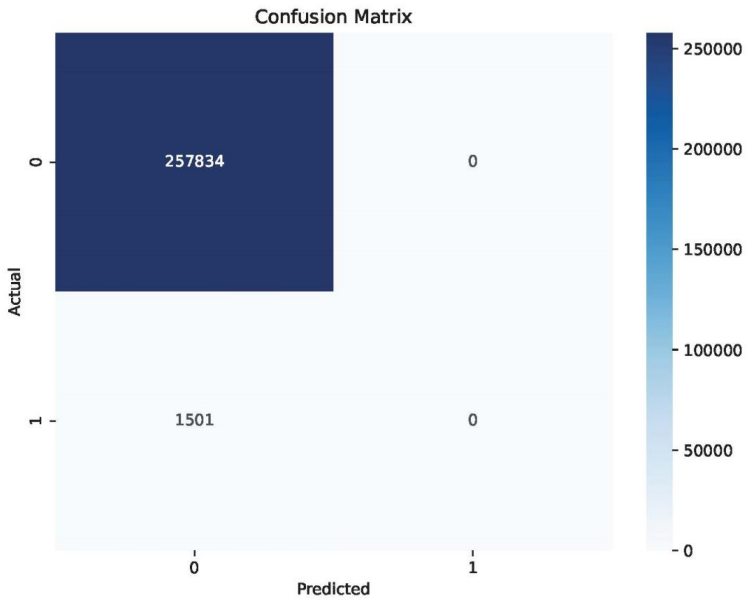

Figure 94. GRU Model's Confusion Matrix After SMOTE Balancing

The confusion matrix, which is depicted in Figure 94, provides additional insight into the model's classification performance. Understanding the model's true positive and negative rates, as well as its propensity for type I and type II errors, necessitates the utilization of a confusion matrix. The model's proficiency in identifying the majority class is demonstrated by the considerable quantity of true negatives.

The rate of loss on the training and validation sets is depicted in the Figure 95. A crucial performance metric (i.e., the loss function) evaluates the model's prediction errors; lower values correspond to superior performance. The loss curve's abrupt decline and plateau indicate a good fit to the data.

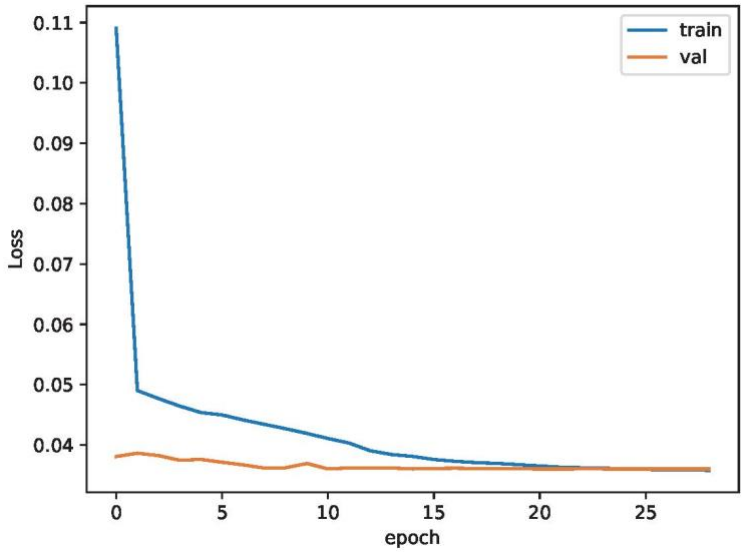

Figure 95. Training and Validation Loss of GRU Model With SMOTE Application Over Epochs

C. ADASYN

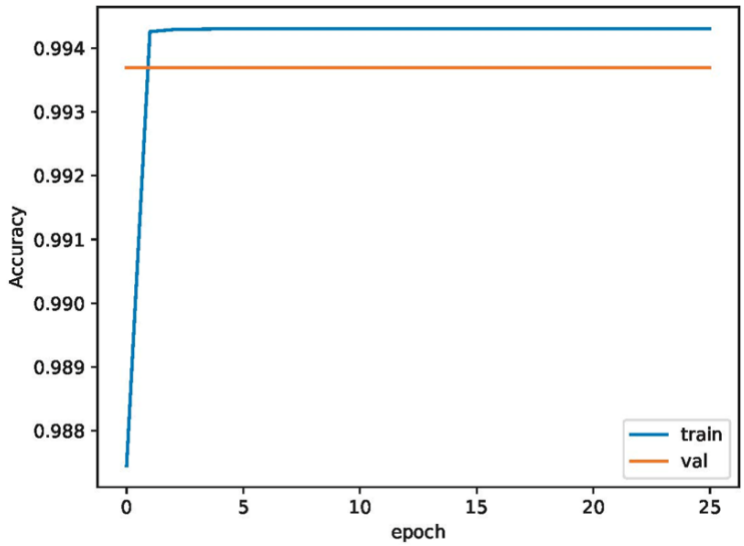

Figure 96. Evolution of Training and Validation Accuracy of GRU Model with ADASYN Balancing

This subsection reveals the results of training a GRU, a typical recurrent neural network, using unbalanced data that has been re-sampled using the Adaptive Synthetic (ADASYN) approach. ADASYN is a specialised technique that generates synthetic data for the minority class, specifically emphasising challenging examples that are hard

to learn. Thus, a training dataset that is more balanced and representative of the model is obtained.

Figure 96 displays the accuracy of the GRU model for both the training and validation datasets over the epochs. The accuracy, exhibited by the rapid increase and the subsequent leveling-down, indicates that the model promptly adjusts to the patterns in the data and subsequently attains a stable state, thereby indicating an efficient learning process. The strong correlation between the training and validation accuracies indicates that the model does not exhibit substantial overfitting or underfitting. Nevertheless, the considerable precision indicates that the ADASYN approach has enhanced the distinction between different classes, thus simplifying the model's classification assignment. Consequently, assessing the model's performance on a real-world dataset with natural imbalances is a necessary method of confirming its reliability and effectiveness.

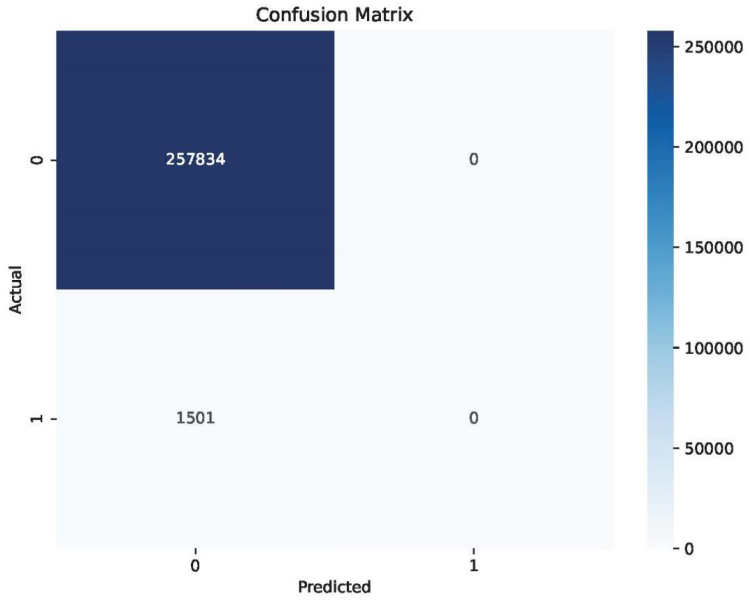

Figure 97. Confusion Matrix of the GRU Model Post-ADASYN Application

Figure 97 is a confusion matrix that offers a comprehensive perspective of the model's true positive and negative rates, as well as its false positives and negatives. The high number of true negatives indicates that the model correctly recognises instances of the majority class. However, the lack of genuine positives raises concerns pertaining to its effectiveness in accurately classifying instances of the minority class.

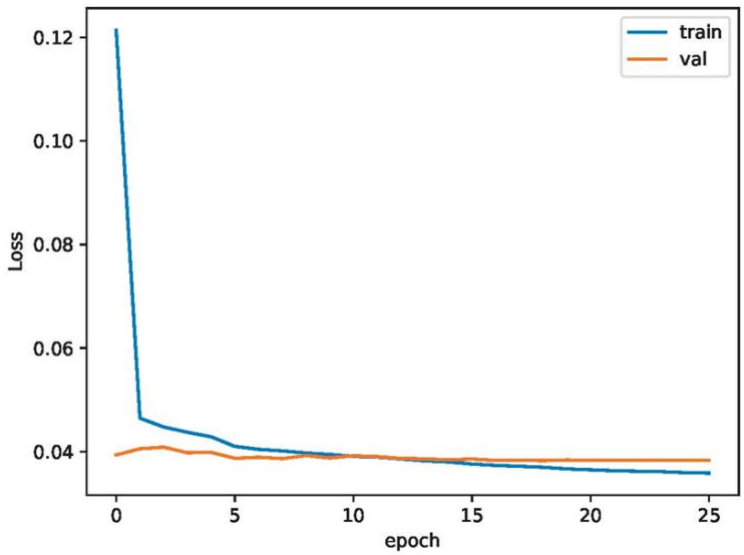

Figure 98. Loss Metrics for GRU Model During Training with ADASYN Technique

Figure 98 displays the loss metrics of the GRU model over the training epochs. Loss metrics are crucial because they measure the discrepancy between the predicted values and actual values, thus offering a more detailed perspective on the performance of the model compared to accuracy alone. The declining trend in loss indicates that the model is progressively enhancing its predictions.

D. Random Under Sampling

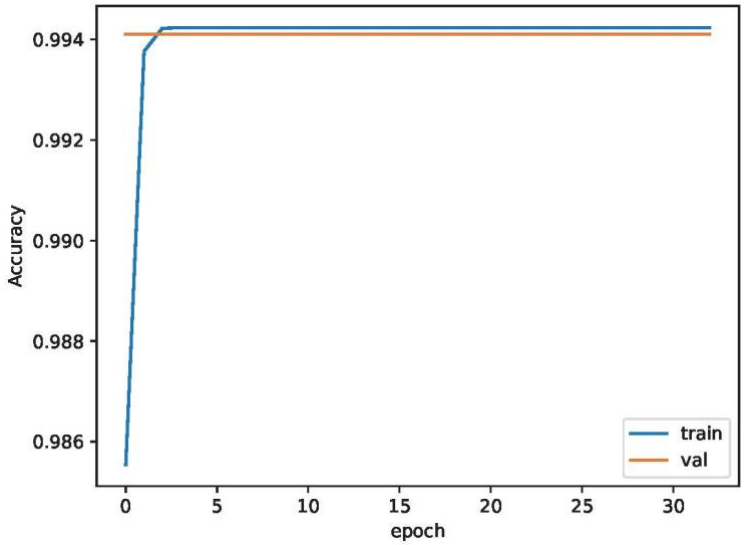

Figure 99. Accuracy of GRU Model During Training and Validation Phases Over Epochs

Figure 99 depicts the precision of the GRU model on both the training and validation datasets over many epochs. An epoch is defined as a single iteration of the training

dataset through the algorithm. The graph demonstrates that the model rapidly achieves a high degree of accuracy and maintains it consistently throughout subsequent epochs, with the training accuracy (represented by the blue line) and validation accuracy (represented by the orange line) well matched. This observation implies that the model exhibits good generalisation to unfamiliar data, which is a desirable characteristic indicating that the model is not too tailored to the training set. Nevertheless, the little disparity between the training and validation accuracy indicates that the model can potentially enhance its performance by exposure to a broader and more comprehensive dataset.

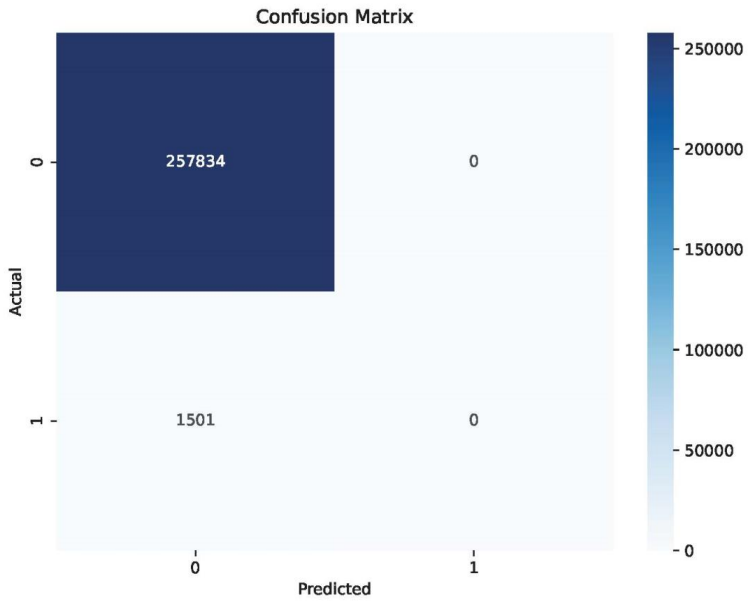

Figure 100. Confusion Matrix of GRU Model Predictions

Figure 100 is a confusion matrix, which is an often utilized table in classification models, succinctly represents the model's performance. The display indicates the count of true negatives (located in the top left) and false negatives (located in the bottom left) for the class '0' (which potentially represents legal transactions). The abundance of true negatives indicates that the model is quite proficient at detecting valid transactions. Nevertheless, the existence of false negatives reveals that the model bears inaccuracies because it incorrectly identifies a few fraudulent transactions as legal. The lack of numerical values in the off-diagonal components for class '1' (representing fraudulent transactions) indicates that there are no instances of false positives or true positives, which might be a significant issue because it indicates that the model is unable to accurately detect any fraudulent transactions.

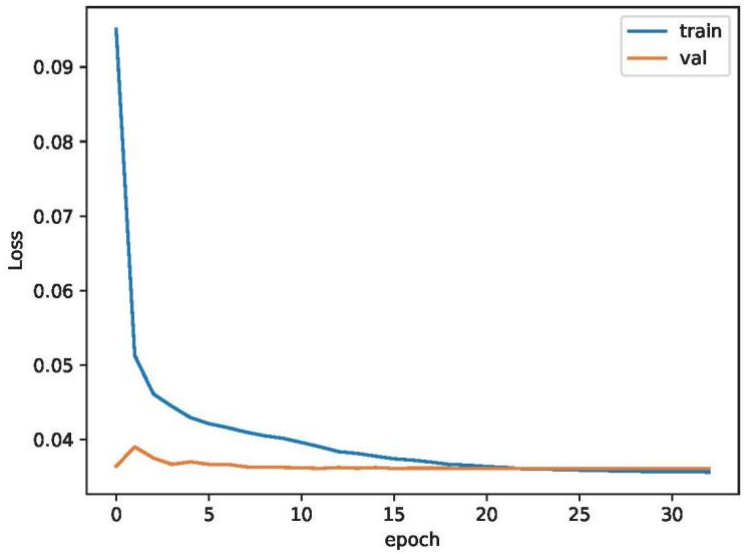

Figure 101. Loss of GRU Model During Training and Validation Phases Over Epochs

Figure 101 the model's loss during the identical epochs. Loss is a metric that measures the discrepancy between the predictions made by the model and the real data. Smaller values indicate greater performance. The graph illustrates a sharp decrease in training loss, which stabilises as the number of epochs increases. The validation loss exhibits a similar decreasing trend but consistently stays higher than the training loss throughout the whole procedure. The intersection of these two lines with little loss indicates the model's effective learning. However, the continuing discrepancy implies the need for improvement, such as adjusting hyperparameters or addressing possible underfitting to the validation set.

6.3.2 Neural Network (NN)

A. Random Over Sampling

This subsection demonstrates the effectiveness of NN model, which is a typical deep learning algorithm, after implementing random over-sampling to address class imbalance in the dataset. Random over-sampling is a method for balancing the number of instances across different classes in a dataset. By replicating instances from the minority class, this technique can enhance the learning process for models that encounter difficulties with imbalanced data.

Figure 102 displays the confusion matrix for the NN model, which is a tabular representation that can describe the classification model's performance. The numerical value in the upper left cell represents the count of true negatives, which indicates the accuracy of the model in predicting the majority class. The cell located at the bottom left corner displays the false negatives, which correspond to cases where the model made an incorrect prediction for the minority class.

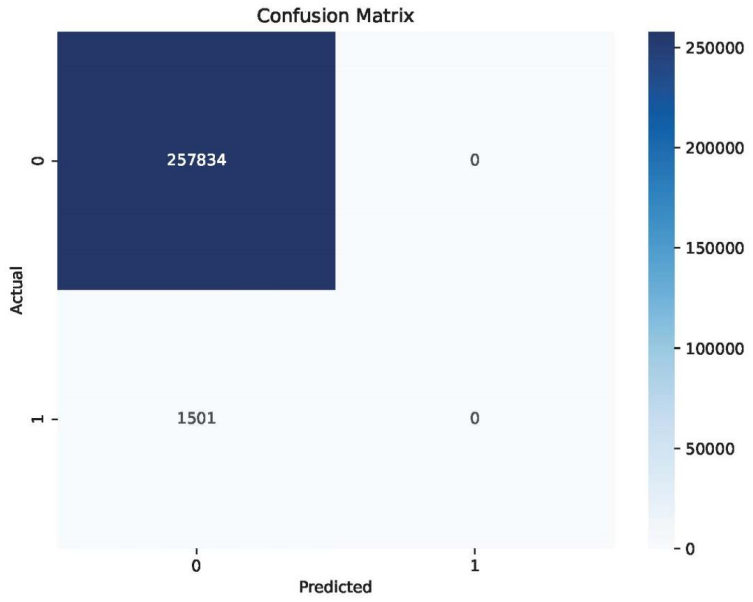

Figure 102. Confusion Matrix of Neural Network Performance on Raw Data

Figure 103 depicts the accuracy of the neural network model during the training and validation phases over multiple epochs. The accuracy metric quantifies the ratio of correct predictions made by the model to the total number of predictions. The graph demonstrates that the model quickly attains a high level of accuracy and maintains it consistently during the training process. Both the training and validation accuracy converge to a similar high value, which indicates that the model can acquire knowledge from the training data and apply it effectively to new, unseen data.

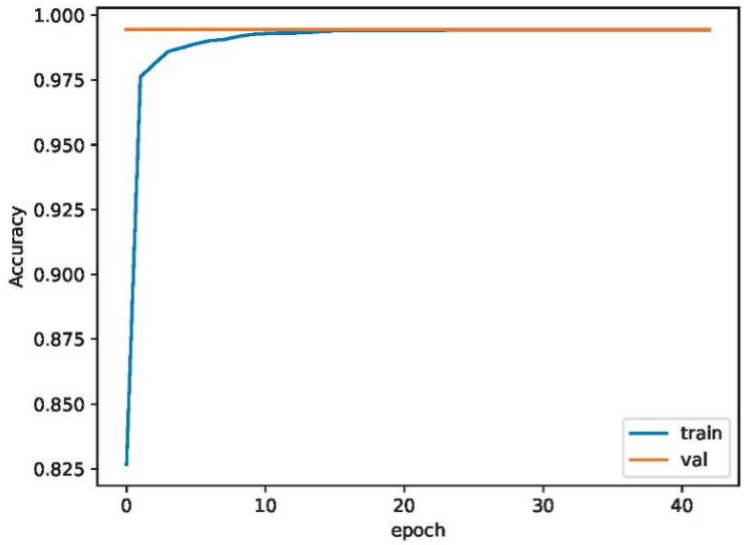

Figure 103: Training and Validation Accuracy of a Neural Network Across Epochs

Figure 104 depicts the declining performance of both the training and validation sets throughout the epochs. The loss metric measures the degree of error in the model's predictions, with smaller values indicating superior performance. The graph illustrates a crucial decrease in loss during the initial stages of training, which subsequently stabilises as the model further acquires knowledge. The convergence of the training and validation loss curves indicates the model is not subjected to substantial overfitting.

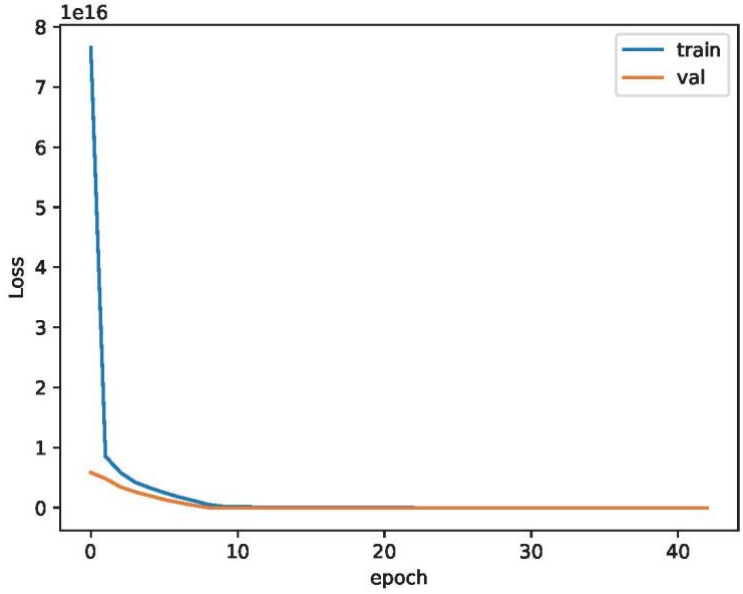

Figure 104. Loss Trajectory of Neural Network Training

B. SMOTE

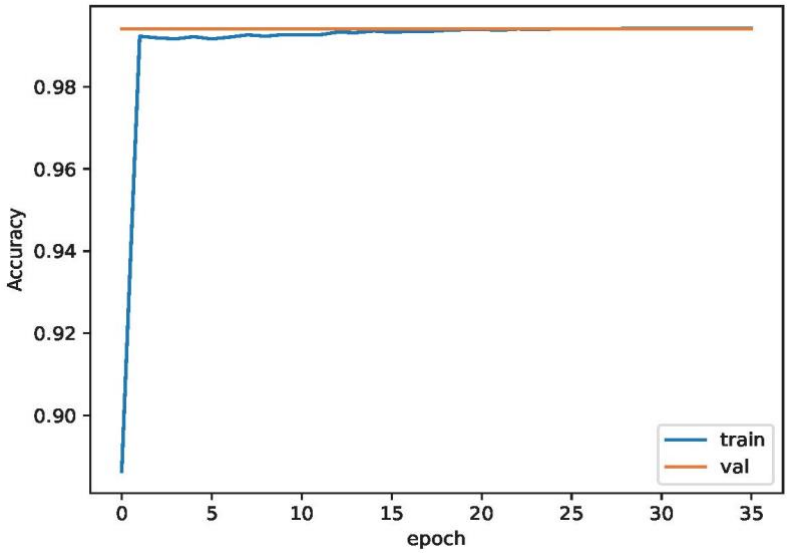

Figure 105. Training and Validation Accuracy over Epochs for Neural Network Model

The Figure 105 illustrates the precision of the neural network throughout the training and validation stages, herein measured in epochs. The rapid ascent to a high level of precision in the training curve indicates that the model swiftly acquires the ability to classify the dominant class. The confusion matrix depicted in Figure 106 indicates a significant number of accurate negative predictions but a concerning lack of accurate positive predictions.

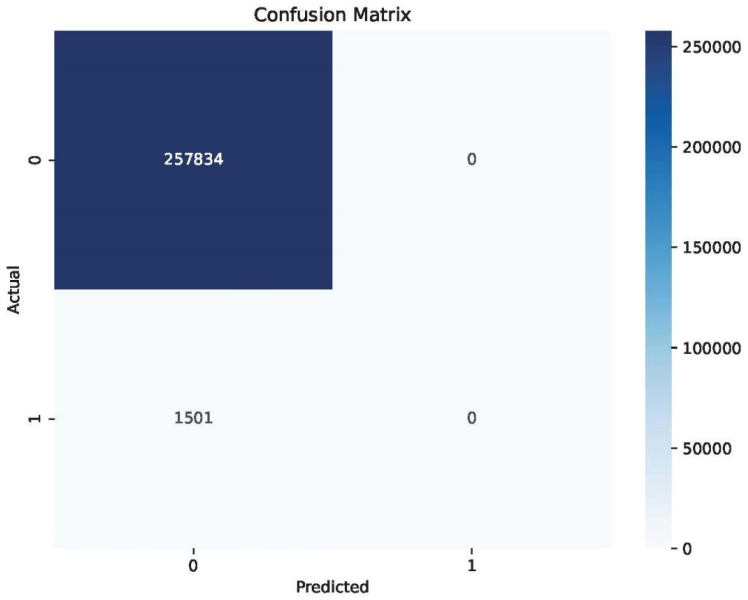

Figure 106. Confusion Matrix for Neural Network Model Highlighting Class Imbalance Issues

The loss graph in Figure 107 illustrates the advancement of the model's learning process, which is characterised by a rapid decline in training loss at the beginning, followed by a quick stabilisation as the number of epochs increases. The rapid convergence observed in this case indicates that the model can reduce error quickly. The rapid convergence observed in this case indicates that the model can quickly minimize error.

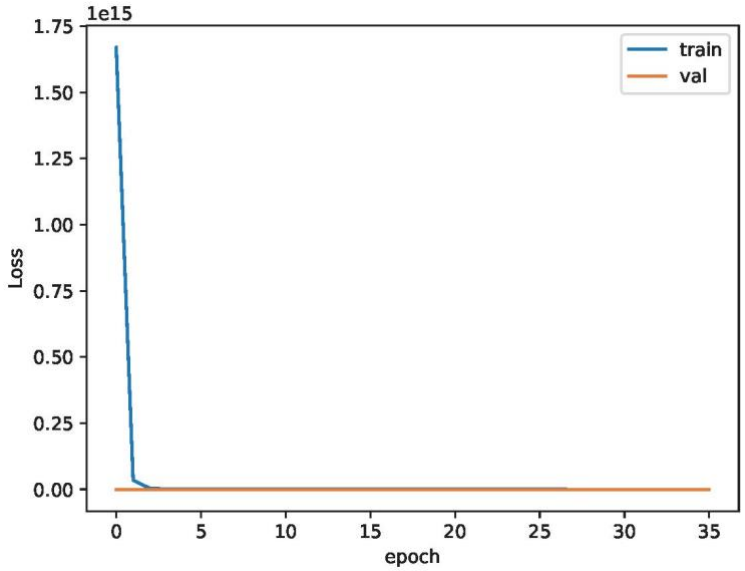

Figure 107. Training and Validation Loss over Epochs for Neural Network Model

C. ADASYN

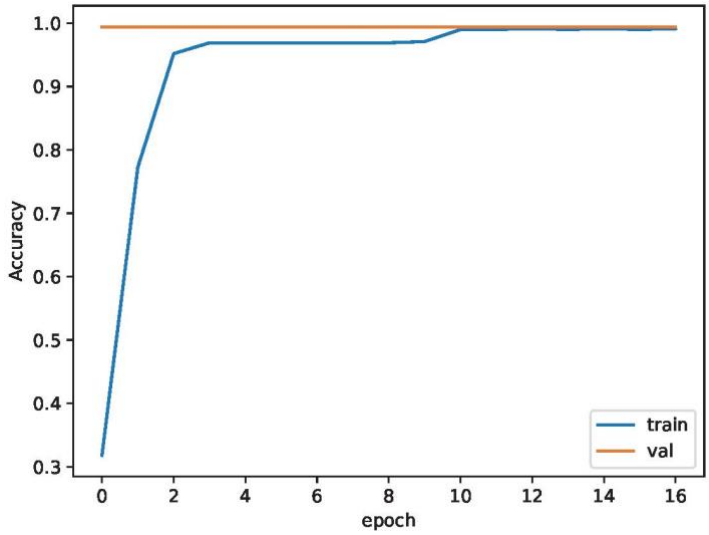

Figure 108. Accuracy Metrics of NN on Imbalanced Data with ADASYN Across Epochs

This subsection depicts the evaluation metrics of NN after the implementation of the ADASYN approach to address data imbalance. ADASYN is an innovative technique for increasing the number of samples in the minority class. It generates synthetic samples along the boundary of the minority class instead of duplicating instances. This approach aims to provide a more intricate and realistic decision boundary from which the model can learn.

Figure 108 illustrates the precision of the neural network model throughout several epochs for both the training and validation datasets. The accuracy graph exhibits a sharp early ascent, signifying fast acquisition of knowledge, followed by a turning point and reveals that the model has attained its greatest learning potential based on the existing architecture and data. The alignment of training and validation accuracy indicates that the model effectively adapts to unseen data. A high accuracy peak indicates that the model is quite certain in its predictions.

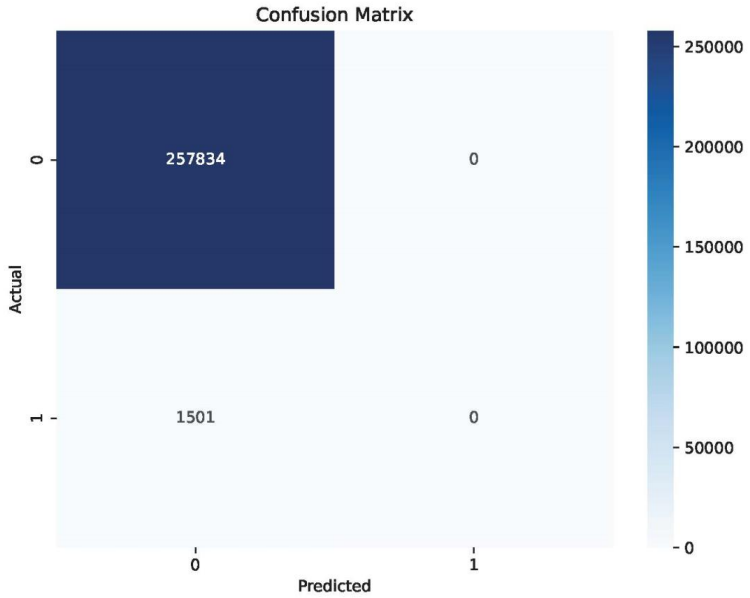

Figure 109. Confusion Matrix for NN After Balancing with ADASYN

Figure 109 indicates the confusion matrix, a crucial instrument for assessing classification performance beyond simple accuracy. The matrix displays the amount of accurate negative predictions (true negatives) and inaccurate negative predictions (false negatives). The top-left quadrant represents the properly recognised negative instances, whereas the bottom-left quadrant represents the negative cases that were falsely categorised as positive. The absence of any data points in the top-right and bottom-right quadrants (representing false positives and true positives, respectively) is a significant

concern. This observation indicates that although the model is effective at recognising the majority class, it struggles to detect instances of the minority class.

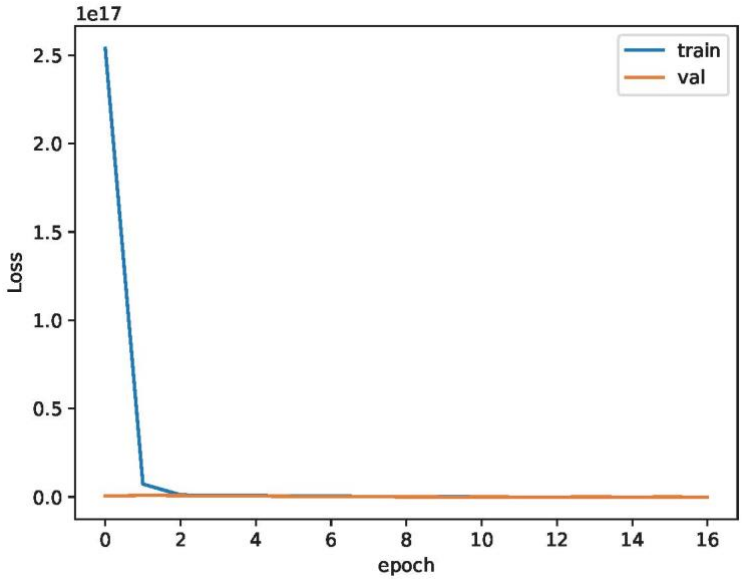

Figure 110. Training and Validation Loss of NN Using ADASYN

Figure 110 illustrates the model's training and validation loss throughout the epochs. The loss value quantifies the degree of error in the model's predictions. A rapid decline followed by a subsequent level in losses are often perceived as positive signs of learning. Nevertheless, a low loss value does not guarantee optimal performance on an unbalanced dataset because it might indicate overfitting to the over-sampled minority class. The parallel paths of the training and validation loss indicate that the model is not excessively fitting the training data, and that the ADASYN approach has successfully established a sufficiently complex environment for the model to apply its learning to new data.

D. Random Under Sampling

The efficacy of NN model is applied to a dataset that has been balanced using Random Under Sampling. This methodology address the issue of class imbalance by decreasing the number of instances in the majority class to align with the minority class, thereby leading to a more equitable distribution and perhaps enhancing the model's capacity to learn from the underrepresented class.

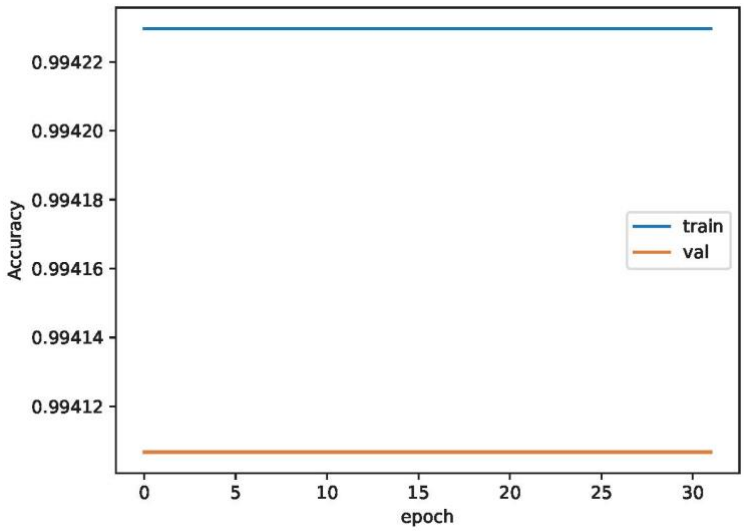

Figure 111. Neural Network Model Accuracy Post-Balancing with Random Under Sampling

Figure 111 illustrates the accuracy of the model across several epochs, including both the training and validation datasets. The accuracy maintains consistency over the epochs, which indicates that the model rapidly attained a point where its learning progress stagnated. This observation implies that the model is not gaining new knowledge from the training data as the iterations proceed, which often indicates a simplistic model in a complicated problem domain or a model that has already attained its optimal performance. The proximity of the training and validation lines indicates strong generalisation. However, the plateau at a high level of accuracy raises concerns about the complexity of the balanced dataset and the potential ease with which the model might learn from it.

Figure 112 is a confusion matrix that offers valuable information on the model's predicted accuracy. The graphic indicates the count of true negatives (located in the top left) and false negatives (located in the bottom left), while true positives and false positives are absent (located in the top right and bottom right, respectively). The model's large number of true negatives demonstrates its strong accuracy in predicting the majority class. However, the occurrence of false negatives without any positive predictions reveals that the model exhibits bias towards forecasting the majority class despite attempts to balance the data.

Figure 113 displays the loss values for both the training and validation sets throughout the course of the training epochs. Loss is a critical metric for evaluating the success of a model: it precisely quantifies the disparity between the anticipated and actual values.

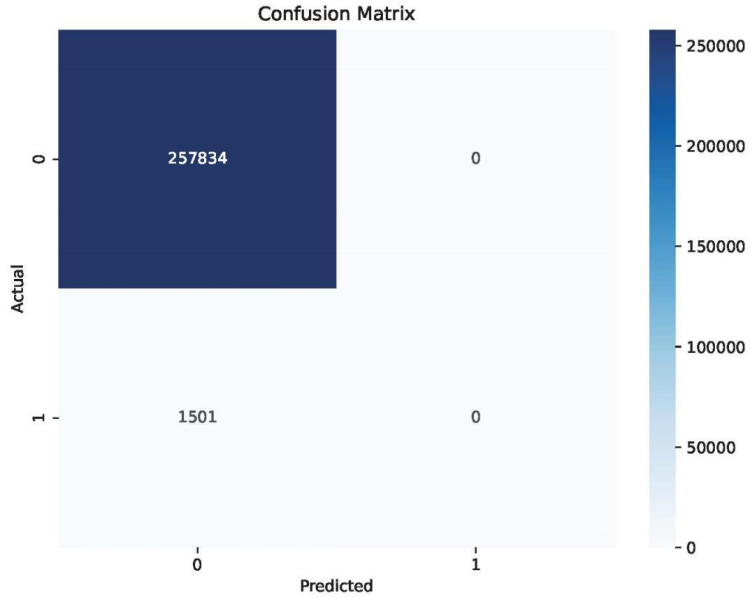

Figure 112. Confusion Matrix of Neural Network on Balanced Data

The graph depicts a significant decline in training loss, followed by a rapid stabilisation. Contrastingly, the validation loss remains consistently low. Nevertheless, considering the evenly distributed dataset, it is probable that the model has successfully grasped the underlying patterns in the data. However, the absence of any positive predictions in the confusion matrix indicates that this low loss may not necessarily translate into meaningful real-world performance.

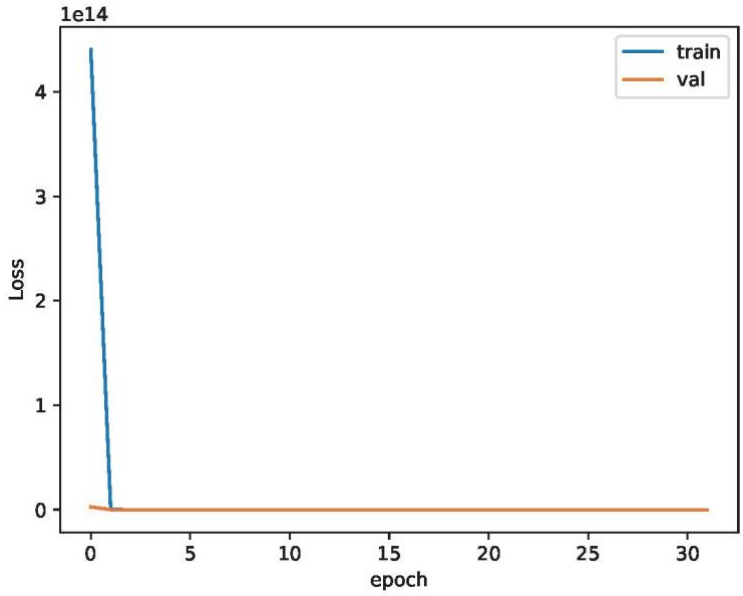

Figure 113. Loss Metrics for Neural Network During Training and Validation Post-Balancing

6.4 Discussion

This subsection thoroughly analyses the performance of several machine learning and deep learning models, both before and after utilizing data balancing strategies. The examined models include the Bagging Classifier, Random Forest Classifier, AdaBoost Classifier, CatBoost Classifier, XGB Classifier, Extra Trees Classifier, GNB Classifier, GRU, and NN. The strategies for balancing include ROS, SMOTE, ADASYN, and Random Under Sampling. The assessment process utilises performance criteria such as Recall Score, Precision Score, F1 Score, ROC AUC Score, and Accuracy Score.

The Bagging Classifier and Random Forest Classifier demonstrated outstanding performance across almost all measures, mainly when ROS and SMOTE approaches were utilized. The capacity to maintain elevated performance measures demonstrates their resilience in addressing class imbalance. The slight differences in performance metrics observed across various balancing approaches underscore the complicated influence of each strategy on the model's performance. The models exhibited proficiency in reducing false positives while effectively detecting fraudulent transactions.

LR: Although this model achieved a high level of accuracy, it was unable to detect any cases of fraud, this indicating its ineffectiveness in handling datasets with significant imbalances.

The AdaBoost Classifier exhibited a restricted capacity to detect fraudulent transactions in its unprocessed state, with only a little improvement after adjusting for imbalances. This observation underscores the difficulties of some models when dealing with highly unbalanced data and the modest but significant influence of data balancing.

The CatBoost Classifier and XGB Classifier exhibited enhanced fraud detection capabilities after the application of data balancing strategies, particularly with SMOTE. This behavior indicates that both models can be useful when adequately preprocessed. Nevertheless, their performance in its unprocessed form highlights the difficulty posed by class disparity.

The Extra Trees Classifier demonstrated robust performance across all measures, with small improvements or stability, herein observed when balancing approaches were utilised. This model's robustness and efficacy make it a suitable contender for fraud detection systems.

The GNB Classifier, GRU, and NN models apparently lack the capability to detect fraudulent transactions both before and during data balancing, which indicates that these models are not appropriate for unbalanced datasets that often characterize fraud detection scenarios without significant modifications.

Data balancing approaches were utilized to enhance the models' capacity to detect fraudulent transactions, particularly for models with a satisfactory performance baseline. Methods such as SMOTE and Random Sampling have exhibited notable efficacy; thus, researchers should carefully choose an appropriate balancing strategy that aligns with the unique characteristics of the model and dataset.

The comprehensive examination and sophisticated comprehension of the interplay between various models and balancing procedures provide useful insights for developing efficient fraud detection systems. Ensemble approaches, such as the Bagging Classifier and Random Forest Classifier, have exhibited significant efficacy in addressing the challenges posed by unbalanced datasets. This research highlights the

significance of utilizing a multi-metric assessment methodology and focusing on class imbalance when designing systems aimed at mitigating fraud within the digital financial industry. The current study offers noteworthy contributions to academia by demonstrating the effectiveness of ensemble-based methodologies and by highlighting the crucial significance of data balancing in enhancing the performance of fraud-detection models.

Table 3. Comparative Analysis of Model Performance Metrics Before and After the Application of Resampling Techniques

Model Name	Balancing Technique	Recall Score	Precision Score	F1 Score	ROC AUC Score	Accuracy Score
Bagging Classifier	None	0.85476	0.93924	0.89501	0.99884	0.92722
	Random Over Sampling	0.8521	0.94671	0.89691	0.99574	0.99887
	SMOTE	0.84544	0.93861	0.88959	0.99968	0.9876
	ADASYN	0.84477	0.93235	0.8864	0.98961	0.99875
	Random Under Sampling	0.82079	0.93475	0.87407	0.99164	0.99863
Random Forest Classifier	None	0.93138	0.91974	0.92552	0.99913	0.96545
	Random Over Sampling	0.94337	0.92731	0.93527	0.99884	0.99924
	SMOTE	0.91939	0.92867	0.924	0.99959	0.99669
	ADASYN	0.92005	0.92128	0.92067	0.99806	0.99908
	Random Under Sampling	0.82079	0.93475	0.87407	0.99164	0.99863
Logistic Regression	None	0	0	0	0.99421	0.5
	Random Over Sampling	0	0	0	0.5	0.99421
	SMOTE	0	0	0	1	0.5
	ADASYN	0	0	0	0.5	0.99421
	Random Under Sampling	0	0	0	0.5	0.99421
AdaBoost Classifier	None	0.00133	1	0.00266	0.99422	0.50067
	Random Over Sampling	0.00067	1	0.00133	0.61351	0.99422
	SMOTE	0.002	1	0.00399	1	0.60933
	ADASYN	0.002	1	0.00399	0.61844	0.99422
	Random Under Sampling	0.00133	1	0.00266	0.59928	0.99422
CatBoost Classifier	None	0.16256	0.86833	0.27385	0.96353	0.99501
	Random Over Sampling	0.17189	0.86	0.28651	0.96831	0.99505
	SMOTE	0.17322	0.86667	0.28873	0.99984	0.9681
	ADASYN	0.15789	0.82867	0.26525	0.96505	0.99494
	Random Under Sampling	0.13924	0.86008	0.23968	0.96099	0.99489

XGB Classifier	None	0.03598	0.83077	0.06897	0.99438	0.51797
	Random Over Sampling	0.03531	0.76812	0.06752	0.95674	0.99435
	SMOTE	0.03464	0.8125	0.06645	0.99995	0.95257
	ADASYN	0.03664	0.85938	0.07029	0.95633	0.99439
	Random Under Sampling	0.03864	0.80556	0.07374	0.94331	0.99438
Extra Trees Classifier	None	0.9527	0.92199	0.93709	0.99926	0.97611
	Random Over Sampling	0.95936	0.92131	0.93995	0.99925	0.99929
	SMOTE	0.92805	0.93115	0.9296	0.9996	0.99789
	ADASYN	0.93538	0.91705	0.92612	0.99889	0.99914
	Random Under Sampling	0.93738	0.90599	0.92141	0.99854	0.99907
GNB Classifier	None	0	0	0	0.52726	0.99421
	Random Over Sampling	0	0	0	0.52704	0.99421
	SMOTE	0	0	0	1	0.53482
	ADASYN	0	0	0	0.54986	0.99421
	Random Under Sampling	0	0	0	0.53197	0.99421
GRU	None	0	0	0	-1	0.99421
	Random Over Sampling	0	0	0	0.99421	0.5
	SMOTE	0	0	0	0.99421	0.5
	ADASYN	1	0	0	0	0.99421
	Random Under Sampling	0	0	0	0.99421	0.5
NN	None	0	0	0	1	-1
	Random Over Sampling	0	0	0	0.99421	0.5
	SMOTE	0	0	0	0.99421	0.5
	ADASYN	0	0	0	1	0.99421
	Random Under Sampling	0	0	0	0.99421	0.5

6.4.1 Random Over Sampling Technique.

Upon considering the results provided in Table 4, we can analyse the effectiveness of different machine learning and deep learning algorithms in detecting Credit-Card Fraud when dealing with imbalanced data. This analysis is performed after applying the ROS technique. Every metric provides insight into distinct facets of model performance and the intricacies of fraud detection.

ROS is aimed at achieving dataset balance by duplicating a certain number of instances from the minority class to correspond with the number of instances from the majority

class. This method can significantly modify the environment in which machine learning models are trained.

The application of ROS led to a significant enhancement in the minority class recall for both the BaggingClassifier and the RandomForestClassifier. Specifically, the recall for the Bagging Classifier increased to 0.8521, whereas the recall for the Random Forest Classifier rose to 0.94337. The robust Precision scores accompanying these recall enhancements are demonstrated by the enhanced F1 Scores of 0.89691 and 0.93527, respectively. The high ROC AUC scores for the minority class indicate that this scenario has not compromised the models' ability to accurately classify legitimate transactions while significantly enhancing their capability to detect fraudulent transactions.

The introduction of ROS did not significantly impact the operational effectiveness of the LRand Ridge Classifier; these models consistently failed to identify fraudulent transactions. Despite their flawless accuracy for the majority class, their performance in the minority class remains alarmingly inadequate, as evidenced by their zero Recall, Precision, and F1 Score.

Comparing the AdaBoost Classifier and XGB Classifier, the AdaBoost Classifier's recall score of 0.17189 after ROS indicated a marginal advance in its fraud-detection ability. Nevertheless, the recall of the XGB Classifier remained modest at 0.03531, underscoring the restricted efficacy of ROS on the said models. Although the minority class ROC AUC score for AdaBoost has increased, which indicates a certain degree of improvement in the model's discriminatory capability, it is still insufficient for practical applications to effectively detect fraud.

The Extra Trees Classifier distinguished itself by exhibiting a substantial rise in the Recall value for the minority class to 0.95936, thus exhibiting an exceptional capability to detect fraudulent transactions after ROS. This model demonstrates a remarkable equilibrium between accuracy and sensitivity to the fraud class, thereby establishing it as a formidable contender for fraud-detection endeavors in the post-ROS environment.

GRU and Neural Networks (NN): Analogous to the LRand Ridge Classifier, the GRU and NN models maintained a Recall, Precision, and F1 Score of zero for fraudulent

transactions, thus demonstrating no improvement in detecting the minority class after ROS.

The examination of model performance following the implementation of ROS yields valuable insights regarding the effectiveness of this balancing methodology. While specific models, such as the Extra Trees Classifier, benefit significantly from ROS, more advanced models such as GRU and NN fail to demonstrate the intended enhancement in fraudulent transaction detection. The difference underscores the importance of implementing a customised strategy for data balancing, which could involve combining various methods or modifying the model's structure to guarantee efficient fraud detection. The application of ROS in combination with other techniques is recommended for addressing unbalanced datasets that include a minority class that lacks sensitivity to details, despite its ability to enhance performance in certain models.

Table 4. Performance evaluation of machine and deep learning Models on Imbalanced Credit Card Transaction Data Balanced Using Random over Sampling Technique.

Model Name	Recall Score	Precision Score	F1 Score	ROC AUC Score	Accuracy Score
Bagging Classifier	0.8521	0.94671	0.89691	0.99574	0.99887
Random Forest Classifier	0.94337	0.92731	0.93527	0.99884	0.99924
Logistic Regression	0	0	0	0.5	0.99421
AdaBoost Classifier	0.00067	1	0.00133	0.61351	0.99422
CAtBoost Classifier	0.17189	0.86	0.28651	0.96831	0.99505
XGB Classifier	0.03531	0.76812	0.06752	0.95674	0.99435
Extra Trees Classifier	0.95936	0.92131	0.93995	0.99925	0.99929
GNB Classifier	0	0	0	0.52704	0.99421
GRU	0	0	0	0.99421	0.5
NN	0	0	0	0.99421	0.5

6.4.2 SMOTE Technique.

Table 5 depicts the performance of various machine learning models on Credit-Card Fraud detection, following the application of the SMOTE technique to balance the data. Each evaluation metric employed in this analysis provides valuable insights into the effectiveness of the models in different aspects of fraud detection.

SMOTE interpolates between existing instances to produce synthetic samples for the minority class. Potentially providing a more solid and complicated dataset for model training, SMOTE exceeds the simple replication employed in Random Over Sampling. Table 6 contains the evaluation metrics utilised in this subsection to assess the effect of SMOTE on the performance of diverse machine learning models aimed at Credit-Card Fraud detection.

The results obtained from evaluating the Bagging Classifier and Random Forest Classifier demonstrated that the Bagging Classifier significantly enhanced its ability to differentiate fraudulent transactions after SMOTE by attaining a recall score of 0.84544 and an ROC AUC score of 0.99968, respectively. Further advancements were made by the Random Forest Classifier, which achieved a balanced recall of 0.91939 and an F1 Score of 0.924. The enhanced ability of these models to detect fraud is indicated by the increases in the ROC AUC scores for both classifiers, which indicate that SMOTE has successfully enriched the dataset.

On the other hand, the minority class detection capabilities of LRand Gaussian Naive Bayes remained unchanged by SMOTE, as evidenced by their return to zero F1 Scores, precision, and Recall. Even with a balanced dataset, the models' failure to convey the complexity of fraud patterns is apparently the underlying concern, as evidenced by the persistent insensitivity to fraudulent transactions.

Comparing the AdaBoost Classifier and XGBoost Classifier, the minor improvement in Recall for the minority class for the AdaBoost Classifier was negligible (0.002). Contrastingly, the XGBoost Classifier's Recall increased marginally to 0.03464. Despite notable improvements in the ROC AUC scores, the actual detection of fraudulent transactions has not significantly enhanced, which underscores the limitations of SMOTE as pertains to these specific models.

The CatBoost model exhibited a marginal improvement in detecting fraudulent transactions, as evidenced by the increase in Recall to 0.17322 and F1 Score to 0.28873 observed with SMOTE.

As evidenced by its Recall for the minority class of 0.92805 and F1 Score of 0.9296, the ExtraTrees Classifier maintained its outstanding performance. Complementing these findings is an ExtraTrees Classifier's ability to effectively classify fraudulent transactions; a high minority class ROC AUC score of 0.9996 indicates that SMOTE substantially contributes to this capability.

Recall, Precision, and F1 Scores for GRU and Neural Networks (NN) remained at zero following the implementation of SMOTE, and no discernible improvements were observed in the performance of these models in detecting minority classes. Probably, the structures of the models or the characteristics of the data they are intended to process indicate that the synthetic sampling offered by SMOTE may not have been advantageous for these complex models.

Overall, the outcomes produced by applying SMOTE as a balancing method for distinct machine learning models have varied. Particularly regarding their capacity to identify fraudulent transactions, it has substantially enhanced the performance of specific models, including the Bagging Classifier and ExtraTrees Classifier. Complex models such as GRU and NN, on the other hand, were not impacted by SMOTE. Nevertheless, LRand Gaussian Naive Bayes remained unaffected. This observation highlights the significance of tailoring the data balancing technique to the model in question, considering the model's particular capabilities and the attributes of the data. To effectively address the enduring class-imbalance issue, it is a necessary to employ a combination of methods or modify the model accordingly, as suggested by the diverse responses.

Table 5. Evaluation Metrics for Machine Learning Models on Credit-Card Fraud Detection Post-SMOTE Balancing

Model Name	Recall Score	Precision Score	F1 Score	ROC AUC Score	Accuracy Score
Bagging Classifier	0.84544	0.93861	0.88959	0.99968	0.9876

Random Forest Classifier	0.91939	0.92867	0.924	0.99959	0.99669
Logistic Regression	0	0	0	1	0.5
AdaBoost Classifier	0.002	1	0.00399	1	0.60933
CatBoost Classifier	0.17322	0.86667	0.28873	0.99984	0.9681
XGB Classifier	0.03464	0.8125	0.06645	0.99995	0.95257
Extra Trees Classifier	0.92805	0.93115	0.9296	0.9996	0.99789
GNB Classifier	0	0	0	1	0.53482
GRU	0	0	0	0.99421	0.5
NN	0	0	0	0.99421	0.5

6.4.3 ADASYN technique.

Table 6 displays the outcomes obtained by applying the ADASYN technique to balance the dataset. Each metric represents an individual aspect of the performance of the machine learning and deep learning models utilized in the Credit-Card Fraud detection system.

ADASYN is a methodology specifically developed to generate synthetic samples comprising marginally modified instances of the minority class. Its primary objective is to target areas where the class imbalance is most pronounced. this subsection contrasts the performance of various models regarding the detection of Credit-Card Fraud following ADASYN balancing.

The Bagging Classifier and Random Forest Classifier have demonstrated remarkable resilience in their implementation of the ADASYN balancing technique. Although the Bagging Classifier's Recall decreased slightly to 0.84477, the model maintained a respectable F1 Score of 0.8864. The Random Forest Classifier demonstrated a commendable balance between Precision and Recall, as evidenced by its F1 Score of 0.92067 and Recall of 0.92005. Following the implementation of ADASYN, both

classifiers maintained high ROC AUC scores for the minority class, thus indicating a robust ability to discriminate between classes.

The LRand Gaussian Naive Bayes models exhibited no noticeable enhancement in their ability to identify fraudulent transactions following the implementation of ADASYN. Specifically, the minority class's Recall, Precision, and F1 Scores remained zero. Despite the high accuracy achieved by the majority class, the continued existence of these outcomes highlights the lack of ability of ADASYN, or potentially any data balancing technique in isolation, to overcome the constraints of these specific models when dealing with highly imbalanced data sets.

The efficacy of AdaBoost Classifier exhibited a minimal improvement in Recall specifically for the fraud class (0.002), whereas XGBoost Classifier demonstrated a marginal increase in Recall amounting to 0.03664. In combination with the increased minority class ROC AUC scores, these negligible enhancements indicate that although ADASYN does enhance the models' sensitivity, it does not result in significant practical advancements for them.

After the implementation of ADASYN, the CatBoost model exhibited a marginal improvement in Recall to 0.15789, accompanied by a 0.26525 F1 Score. The result indicates a slight improvement in the model's ability to detect fraudulent activities; however, it is still insufficient in handling the complex requirements of fraud-detection tasks.

The ExtraTrees Classifier maintained its strong performance in the post-ADASYN environment, attaining an F1 Score of 0.92612 and a Recall of 0.93538. After synthetic balancing, its ROC AUC score for the minority class remained high (0.99889), repeating its effectiveness in fraud detection.

Neural Networks (NN) and GRU: The implementation of ADASYN did not significantly affect the performance of the NN and GRU models in detecting the minority class; their metrics remained consistent with those observed prior to balancing.

The implementation of ADASYN provided diverse outcomes among various models. Although it has enhanced the fraud-detection capabilities of specific models, especially ensemble classifiers, no significant improvement has been observed in others. This

underscores the intricate correlation between model architectures and data sampling techniques. Additionally, it emphasises the value of tailoring modifications to specific models to rectify class imbalance. Illustrative models such as the ExtraTrees Classifier demonstrate the substantial performance enhancement potential of ADASYN, thereby rendering it a crucial asset in the repertoire of methods aimed at addressing the ubiquitous issue of class imbalance in fraud detection.

Table 6. Evaluation metrics for Machine Learning Models on Credit-Card Fraud Detection Post-ADASYN Balancing

Model Name	Recall Score	Precision Score	F1 Score	ROC AUC Score	Accuracy Score
Bagging Classifier	0.84477	0.93235	0.8864	0.98961	0.99875
Random Forest Classifier	0.92005	0.92128	0.92067	0.99806	0.99908
Logistic Regression	0	0	0	0.5	0.99421
AdaBoost Classifier	0.002	1	0.00399	0.61844	0.99422
CatBoost Classifier	0.15789	0.82867	0.26525	0.96505	0.99494
XGB Classifier	0.03664	0.85938	0.07029	0.95633	0.99439
Extra Trees Classifier	0.93538	0.91705	0.92612	0.99889	0.99914
GNB Classifier	0	0	0	0.54986	0.99421
GRU	1	0	0	0	0.99421
NN	0	0	0	1	0.99421

6.4.4 Random Under Sampling technique.

Table 7 illustrates the efficacy of various machine learning models trained on credit card transaction data that has been balanced using the Random Under Sampling technique. Every evaluation metric offers valuable information on different aspects of the models' performance.

A unique perspective is offered by the utilization of Random Under Sampling (RUS) as a method for balancing data and determining how it impacts the performance of different models. To achieve class parity, RUS diminishes the extent of the majority class. Table 4 summarises this section's comparative evaluation of the model's performance following the implementation of RUS.

The BaggingClassifier and the RandomForestClassifier retain high-performance metrics for the majority class following RUS. However, the BaggingClassifier experiences a marginal decline in the recall, which stands at 0.82079. Nevertheless, it is notable that the ROC AUC scores for the minority class experienced an enhancement to 0.99164 and 0.99668, correspondingly, which indicates that the balancing process enhanced the model's sensitivity to the fraud class. These advancements provide empirical support for the notion that RUS improves the capability of models to identify fraudulent activities, albeit at the cost of a marginal decrease in recall for the BaggingClassifier.

Logistic Regression, AdaBoostClassifier, and GaussianNB: While LogisticRegression maintained a flawless accuracy for the majority class, it remained incapable of detecting any instances of deception, as evidenced by its F1 Score, Recall, and Precision all being zero. The identical pattern exhibited by AdaBoostClassifier and GaussianNB indicates that although these models are substantially impacted by class imbalance, relying solely on RUS is inadequate for them to accurately identify fraudulent transactions.

Following the implementation of RUS, the ROC AUC scores for CatBoost and XGBClassifier for the minority class increased to 0.96099 and 0.94331, respectively. Nonetheless, their fraud detection recall scores persisted at 0.13924 for CatBoost and 0.03864 for XGBClassifier, which clarifies that although RUS slightly enhances the model's capacity to identify fraudulent activities, the improvement is negligible. This observation implies that further methodologies or algorithmic modifications are required to fortify their detection capabilities further.

ExtraTreesClassifier: Following RUS, the performance of the ExtraTreesClassifier improved significantly, which is evidenced as follows: the ROC AUC score for the minority class increased to 0.99854. In addition, the model demonstrated a notable Recall score (0.93738), which exhibits a considerable capacity to identify fraudulent

activities subsequent to data balancing. The positive response of ExtraTreesClassifier to RUS indicates that it is well-suited for applications involving fraud detection.

Neural Networks (NN) and GRU: Following RUS, the efficacy of NN and GRU models did not change significantly. Despite maintaining a high level of performance for the majority class, they were unable to recognise any members of the minority class. The observed inertia implies that when applied in isolation, RUS might not be a sufficient resolution for intricate models such as GRU and NN when confronted with highly unbalanced data. This observation highlights the importance of employing a more sophisticated blend of data preprocessing and model optimisation to enhance their performance.

The comparative analysis conducted after RUS indicates that although specific models, such as ExtraTreesClassifier, experience substantial improvements from the balancing process, the ability of other models to identify minority class instances remains largely unaltered. Addressing the class imbalance challenge effectively requires a multifaceted approach that potentially incorporates algorithmic enhancement, oversampling, and more complex synthetic data generation techniques in addition to RUS. It is imperative to evaluate these findings in light of the practical consequences of fraud detection, where the repercussions of overlooking a fraudulent transaction are significant. In such scenarios, prioritising the recall of the minority class while preserving the model's overall accuracy becomes critical.

Table 7. Performance Evaluation of Machine and Deep Learning Models on Imbalanced Credit Card Transaction Data Balanced Using Random Under Sampling Technique.

Model Name	Recall Score	Precision Score	F1 Score	ROC AUC Score	Accuracy Score
Bagging Classifier	0.82079	0.93475	0.87407	0.99164	0.99863
Random Forest Classifier	0.92405	0.92159	0.92282	0.99668	0.99911
Logistic Regression	0	0	0	0.5	0.99421
AdaBoost Classifier	0.00133	1	0.00266	0.59928	0.99422

CatBoost Classifier	0.13924	0.86008	0.23968	0.96099	0.99489
XGB Classifier	0.03864	0.80556	0.07374	0.94331	0.99438
Extra Trees Classifier	0.93738	0.90599	0.92141	0.99854	0.99907
GNB Classifier	0	0	0	0.53197	0.99421
GRU	0	0	0	0.99421	0.5
NN	0	0	0	0.99421	0.5

6.5 Conclusion

This study effectively examines the impact of various balancing strategies on the efficacy of machine learning models in the domain of Credit-Card Fraud detection. The thorough assessment, which utilizes a range of metrics, including recall, precision, F1 score, ROC AUC, and accuracy, has emphasised the efficacy of ensemble methods, specifically the Bagging and Random Forest classifiers, which consistently demonstrate superior performance across all metrics following the implementation of ROS, SMOTE, and ADASYN techniques.

The findings illustrate the importance of balancing the dataset to enhance the model's capacity for identifying fraudulent transactions—a necessity emphasised by the significant increase in digital transactions following to the COVID-19 pandemic. Although class imbalance in datasets presents inherent challenges, the findings highlight the potential of ensemble methods to provide reliable fraud detection capabilities. Basic models such as Logistic Regression, despite their high accuracy, are unable to detect fraudulent cases, which highlights the inadequacy of depending entirely on accuracy as a performance measure when dealing with imbalanced classes.

The effective implementation of balancing techniques like ROS, SMOTE, and ADASYN in scholarly environments starkly contrasts to the practical difficulties they encounter in real-time financial systems." Firstly, the computational burden these techniques introduce should be noticed. For example, SMOTE and ADASYN create synthetic samples by interpolating existing minority class samples, which can significantly enhance the size of training datasets. In real-time fraud detection systems,

the surge in data volume can check processing speeds, leading to delays in transaction verification processes essential in high-speed trading or retail banking contexts.

A notable challenge is the potential for overfitting linked to data balancing methods. In real-world situations, models developed using these methods may perform well on balanced training datasets but need help adapting to the true skewed distribution of transactions encountered in live settings. This misalignment may result in elevated false positive rates, causing legitimate transactions to be incorrectly identified as fraudulent. Elevated false positive rates burden customer relationships and escalate operational expenses, as every erroneous alert necessitates manual examination.

To tackle these challenges effectively, a detailed strategy is essential. This involves consistently monitoring the performance of these models after deployment and routinely updating the training of the models as new fraud patterns arise. These strategies guarantee that the advantages of data balancing techniques are utilised while effectively addressing their practical challenges, thereby preserving the integrity and efficiency of fraud detection systems.

This thesis supports the requirement for a comprehensive strategy in detecting fraud, which involves utilising advanced machine learning algorithms and carefully considering the pre-processing stage of data balancing. Thus, the models can be accurate and responsive to the minority class of fraudulent transactions. The incorporation of geolocation and temporal attention systems significantly improves the proposed system, thereby offering an advanced resolution to a current issue. The knowledge acquired from this analysis is anticipated to make a substantial contribution to the fraud-detection domain, which can protect individuals and entities against the constantly shifting risks in the progressively digital world of finance and commerce.

REFERENCES

ABD EL-NABY, A., HEMDAN, E. E.-D. & EL-SAYED, A. 2023. An efficient fraud detection framework with credit card imbalanced data in financial services. *Multimedia Tools and Applications,* 82**,** 4139-4160.

AFRIYIE, J. K., TAWIAH, K., PELS, W. A., ADDAI-HENNE, S., DWAMENA, H. A., OWIREDU, E. O., AYEH, S. A. & ESHUN, J. 2023. A supervised machine learning algorithm for detecting and predicting fraud in credit card transactions. *Decision Analytics Journal,* 6**,** 100163.

AHMED, I., DAGNINO, A. & DING, Y. 2018. Unsupervised anomaly detection based on minimum spanning tree approximated distance measures and its application to hydropower turbines. *IEEE Transactions on Automation Science and Engineering,* 16**,** 654-667.

ALARFAJ, F. K., MALIK, I., KHAN, H. U., ALMUSALLAM, N., RAMZAN, M. & AHMED, M. 2022. Credit card fraud detection using state-of-the-art machine learning and deep learning algorithms. *IEEE Access,* 10**,** 39700-39715.

ALMAZROI, A. A. & AYUB, N. 2023. Online Payment Fraud Detection Model Using Machine Learning Techniques. *IEEE Access,* 11**,** 137188-137203.

AMIN, A., ANWAR, S., ADNAN, A., NAWAZ, M., HOWARD, N., QADIR, J., HAWALAH, A. & HUSSAIN, A. 2016. Comparing oversampling techniques to handle the class imbalance problem: A customer churn prediction case study. *Ieee Access,* 4**,** 7940-7957.

BAGHDADI, P., KORUKOGLU, S., BILICI, M. A. & ONAN, A. 2024. Ensemble Learning Approach Using Energy-based RBM and xLSTM for Predictive Analytics in Credit Card Fraud Detection. *Authorea Preprints*.

BAHNSEN, A. C., AOUADA, D., STOJANOVIC, A. & OTTERSTEN, B. 2016. Feature engineering strategies for credit card fraud detection. *Expert Systems with Applications,* 51**,** 134-142.

BAHNSEN, A. C., STOJANOVIC, A., AOUADA, D. & OTTERSTEN, B. Cost sensitive credit card fraud detection using Bayes minimum risk. 2013 12th international conference on machine learning and applications, 2013. IEEE, 333-338.

BANDYOPADHYAY, S. K. & DUTTA, S. 2020. Detection of fraud transactions using recurrent neural network during COVID-19: fraud transaction during COVID-19. *Journal of Advanced Research in Medical Science & Technology (ISSN: 2394-6539),* 7**,** 16-21.

BARZ, B., RODNER, E., GARCIA, Y. G. & DENZLER, J. 2018. Detecting regions of maximal divergence for spatio-temporal anomaly detection. *IEEE transactions on pattern analysis and machine intelligence,* 41**,** 1088-1101.

BECHLIOULIS, A. P. & KARAMANIS, D. 2023. Consumers' changing financial behavior during the COVID-19 lockdown: the case of Internet banking use in Greece. *Journal of Financial Services Marketing,* 28**,** 526-543.

BEJU, D.-G. & FĂT, C.-M. 2023. Frauds in Banking System: Frauds with Cards and Their Associated Services. *Economic and Financial Crime, Sustainability and Good Governance.* Springer.

BHATTACHARYYA, S., JHA, S., THARAKUNNEL, K. & WESTLAND, J. C. 2011. Data mining for credit card fraud: A comparative study. *Decision support systems,* 50**,** 602-613.

BIAN, W., CONG, L. W. & JI, Y. 2023. The Rise of E-Wallets and Buy-Now-Pay-Later: Payment Competition, Credit Expansion, and Consumer Behavior. National Bureau of Economic Research.
BINI, S. A. 2018. Artificial intelligence, machine learning, deep learning, and cognitive computing: what do these terms mean and how will they impact health care? *The Journal of arthroplasty,* 33**,** 2358-2361.
BOLTON, R. J. & HAND, D. J. 2004. Statistical fraud detection: A review. *Quality control and applied statistics,* 49**,** 313-314.
BOUGHORBEL, S., JARRAY, F. & EL-ANBARI, M. 2017. Optimal classifier for imbalanced data using Matthews Correlation Coefficient metric. *PloS one,* 12**,** e0177678.
BRANCO, P., TORGO, L. & RIBEIRO, R. P. Relevance-based evaluation metrics for multi-class imbalanced domains. Advances in Knowledge Discovery and Data Mining: 21st Pacific-Asia Conference, PAKDD 2017, Jeju, South Korea, May 23-26, 2017, Proceedings, Part I 21, 2017. Springer, 698-710.
CARCILLO, F., DAL POZZOLO, A., LE BORGNE, Y.-A., CAELEN, O., MAZZER, Y. & BONTEMPI, G. 2018. Scarff: a scalable framework for streaming credit card fraud detection with spark. *Information fusion,* 41**,** 182-194.
CARCILLO, F., LE BORGNE, Y.-A., CAELEN, O., KESSACI, Y., OBLÉ, F. & BONTEMPI, G. 2021. Combining unsupervised and supervised learning in credit card fraud detection. *Information sciences,* 557**,** 317-331.
CHANG, V., DI STEFANO, A., SUN, Z. & FORTINO, G. 2022. Digital payment fraud detection methods in digital ages and Industry 4.0. *Computers and Electrical Engineering,* 100**,** 107734.
CHAWLA, N. V. 2010. Data mining for imbalanced datasets: An overview. *Data mining and knowledge discovery handbook***,** 875-886.
CHENG, D., NIU, Z., LI, J. & JIANG, C. 2022. Regulating systemic crises: Stemming the contagion risk in networked-loans through deep graph learning. *IEEE Transactions on Knowledge and Data Engineering*.
CHENG, D., WANG, X., ZHANG, Y. & ZHANG, L. 2020a. Graph neural network for fraud detection via spatial-temporal attention. *IEEE Transactions on Knowledge and Data Engineering,* 34**,** 3800-3813.
CHENG, D., XIANG, S., SHANG, C., ZHANG, Y., YANG, F. & ZHANG, L. Spatio-temporal attention-based neural network for credit card fraud detection. Proceedings of the AAAI conference on artificial intelligence, 2020b. 362-369.
CHERIF, A., BADHIB, A., AMMAR, H., ALSHEHRI, S., KALKATAWI, M. & IMINE, A. 2023. Credit card fraud detection in the era of disruptive technologies: A systematic review. *Journal of King Saud University-Computer and Information Sciences,* 35**,** 145-174.
CUI, J., YAN, C. & WANG, C. 2021. ReMEMBeR: Ranking metric embedding-based multicontextual behavior profiling for online banking fraud detection. *IEEE Transactions on Computational Social Systems,* 8**,** 643-654.
DAL POZZOLO, A., BORACCHI, G., CAELEN, O., ALIPPI, C. & BONTEMPI, G. 2017. Credit card fraud detection: a realistic modeling and a novel learning strategy. *IEEE transactions on neural networks and learning systems,* 29**,** 3784-3797.

DAL POZZOLO, A., CAELEN, O., LE BORGNE, Y.-A., WATERSCHOOT, S. & BONTEMPI, G. 2014. Learned lessons in credit card fraud detection from a practitioner perspective. *Expert systems with applications,* 41**,** 4915-4928.
DASKALAKI, S., KOPANAS, I. & AVOURIS, N. 2006. Evaluation of classifiers for an uneven class distribution problem. *Applied artificial intelligence,* 20**,** 381-417.
DE SÁ, A. G., PEREIRA, A. C. & PAPPA, G. L. 2018. A customized classification algorithm for credit card fraud detection. *Engineering Applications of Artificial Intelligence,* 72**,** 21-29.
DELIEMA, M., VOLKER, J. & WORLEY, A. 2023. Consumer Experiences with Gift Card Payment Scams: Causes, Consequences, and Implications for Consumer Protection. *Victims & Offenders,* 18**,** 1282-1310.
ESENOGHO, E., MIENYE, I. D., SWART, T. G., ARULEBA, K. & OBAIDO, G. 2022. A neural network ensemble with feature engineering for improved credit card fraud detection. *IEEE Access,* 10**,** 16400-16407.
FANAI, H. & ABBASIMEHR, H. 2023. A novel combined approach based on deep Autoencoder and deep classifiers for credit card fraud detection. *Expert Systems with Applications,* 217**,** 119562.
FIORE, U., DE SANTIS, A., PERLA, F., ZANETTI, P. & PALMIERI, F. 2019. Using generative adversarial networks for improving classification effectiveness in credit card fraud detection. *Information Sciences,* 479**,** 448-455.
GANGANWAR, V. 2012. An overview of classification algorithms for imbalanced datasets. *International Journal of Emerging Technology and Advanced Engineering,* 2**,** 42-47.
GARCÍA, V., MOLLINEDA, R. A. & SÁNCHEZ, J. S. Index of balanced accuracy: A performance measure for skewed class distributions. Iberian conference on pattern recognition and image analysis, 2009. Springer, 441-448.
GARCIA-GABILONDO, S., SHIBUYA, Y. & SEKIMOTO, Y. 2024. Enhancing geospatial retail analysis by integrating synthetic human mobility simulations. *Computers, Environment and Urban Systems,* 108**,** 102058.
GHALEB, F. A., SAEED, F., AL-SAREM, M., QASEM, S. N. & AL-HADHRAMI, T. 2023. Ensemble Synthesized Minority Oversampling based Generative Adversarial Networks and Random Forest Algorithm for Credit Card Fraud Detection. *IEEE Access*.
GIBSON, D. & HARFIELD, C. 2023. Amplifying victim vulnerability: Unanticipated harm and consequence in data breach notification policy. *International Review of Victimology,* 29**,** 341-365.
GRATIUS, N., BERGÉS, M. & AKINCI, B. Integrated Calibration of Simulation Models for Autonomous Space Habitat Operations. 2024 IEEE Aerospace Conference, 2024. IEEE, 1-18.
GU, Q., ZHU, L. & CAI, Z. Evaluation measures of the classification performance of imbalanced data sets. Computational Intelligence and Intelligent Systems: 4th International Symposium, ISICA 2009, Huangshi, China, October 23-25, 2009. Proceedings 4, 2009. Springer, 461-471.
GU, W., SUN, M., LIU, B., XU, K. & SUI, M. 2024. Adaptive Spatio-Temporal Aggregation for Temporal Dynamic Graph-Based Fraud Risk Detection. *Journal of Computer Technology and Software,* 3.

GUO, J., LIU, G., ZUO, Y. & WU, J. Learning sequential behavior representations for fraud detection. 2018 IEEE international conference on data mining (ICDM), 2018. IEEE, 127-136.
GUO, X., ZHOU, M., ABUSORRAH, A., ALSOKHIRY, F. & SEDRAOUI, K. 2020. Disassembly sequence planning: a survey. *IEEE/CAA Journal of Automatica Sinica,* 8**,** 1308-1324.
GUPTA, P. 2024. Securing Tomorrow: The Intersection of AI, Data, and Analytics in Fraud Prevention. *Asian Journal of Research in Computer Science,* 17**,** 75-92.
GUPTA, P., VARSHNEY, A., KHAN, M. R., AHMED, R., SHUAIB, M. & ALAM, S. 2023. Unbalanced Credit Card Fraud Detection Data: A Machine Learning-Oriented Comparative Study of Balancing Techniques. *Procedia Computer Science,* 218**,** 2575-2584.
GUPTA, R., SRIVASTAVA, D., SAHU, M., TIWARI, S., AMBASTA, R. K. & KUMAR, P. 2021. Artificial intelligence to deep learning: machine intelligence approach for drug discovery. *Molecular diversity,* 25**,** 1315-1360.
HAJEK, P., ABEDIN, M. Z. & SIVARAJAH, U. 2023. Fraud detection in mobile payment systems using an XGBoost-based framework. *Information Systems Frontiers,* 25**,** 1985-2003.
HARISH, S., LAKHANPAL, C. & JAFARI, A. H. 2024. Leveraging graph-based learning for credit card fraud detection: a comparative study of classical, deep learning and graph-based approaches. *Neural Computing and Applications***,** 1-11.
HE, H., BAI, Y., GARCIA, E. A. & LI, S. ADASYN: Adaptive synthetic sampling approach for imbalanced learning. 2008 IEEE international joint conference on neural networks (IEEE world congress on computational intelligence), 2008. Ieee, 1322-1328.
HE, H. & GARCIA, E. A. 2009. Learning from imbalanced data. *IEEE Transactions on knowledge and data engineering,* 21**,** 1263-1284.
HELM, J. M., SWIERGOSZ, A. M., HAEBERLE, H. S., KARNUTA, J. M., SCHAFFER, J. L., KREBS, V. E., SPITZER, A. I. & RAMKUMAR, P. N. 2020. Machine learning and artificial intelligence: definitions, applications, and future directions. *Current reviews in musculoskeletal medicine,* 13**,** 69-76.
HILAL, W., GADSDEN, S. A. & YAWNEY, J. 2022. Financial fraud: a review of anomaly detection techniques and recent advances. *Expert systems With applications,* 193**,** 116429.
HOSSIN, M. & SULAIMAN, M. N. 2015. A review on evaluation metrics for data classification evaluations. *International journal of data mining & knowledge management process,* 5**,** 1.
JAIN, Y., TIWARI, N., DUBEY, S. & JAIN, S. 2019. A comparative analysis of various credit card fraud detection techniques. *International Journal of Recent Technology and Engineering,* 7**,** 402-407.
JAKHAR, D. & KAUR, I. 2020. Artificial intelligence, machine learning and deep learning: definitions and differences. *Clinical and experimental dermatology,* 45**,** 131-132.
JENI, L. A., COHN, J. F. & DE LA TORRE, F. Facing imbalanced data--recommendations for the use of performance metrics. 2013 Humaine association conference on affective computing and intelligent interaction, 2013. IEEE, 245-251.

JIANG, S., DONG, R., WANG, J. & XIA, M. 2023. Credit card fraud detection based on unsupervised attentional anomaly detection network. *Systems,* 11**,** 305.
JURGOVSKY, J., GRANITZER, M., ZIEGLER, K., CALABRETTO, S., PORTIER, P.-E., HE-GUELTON, L. & CAELEN, O. 2018. Sequence classification for credit-card fraud detection. *Expert systems with applications,* 100**,** 234-245.
JURMAN, G., RICCADONNA, S. & FURLANELLO, C. 2012. A comparison of MCC and CEN error measures in multi-class prediction.
KAMARUDDIN, S. & RAVI, V. Credit card fraud detection using big data analytics: use of PSOAANN based one-class classification. Proceedings of the international conference on informatics and analytics, 2016. 1-8.
KARIM, K., ILYAS, G. B., UMAR, Z. A., TAJIBU, M. J. & JUNAIDI, J. 2023. Consumers' awareness and loyalty in Indonesia banking sector: does emotional bonding effect matters? *Journal of Islamic Marketing,* 14**,** 2668-2686.
KHALID, A. R., OWOH, N., UTHMANI, O., ASHAWA, M., OSAMOR, J. & ADEJOH, J. 2024. Enhancing Credit Card Fraud Detection: An Ensemble Machine Learning Approach. *Big Data and Cognitive Computing,* 8**,** 6.
KHAN, F., ATEEQ, S., ALI, M. & BUTT, N. 2023. Impact of COVID-19 on the drivers of cash-based online transactions and consumer behaviour: evidence from a Muslim market. *Journal of Islamic Marketing,* 14**,** 714-734.
KHINE, A. A. & KHIN, H. W. Credit card fraud detection using online boosting with extremely fast decision tree. 2020 IEEE Conference on Computer Applications (ICCA), 2020. IEEE, 1-4.
KIM, E., LEE, J., SHIN, H., YANG, H., CHO, S., NAM, S.-K., SONG, Y., YOON, J.-A. & KIM, J.-I. 2019. Champion-challenger analysis for credit card fraud detection: Hybrid ensemble and deep learning. *Expert Systems with Applications,* 128**,** 214-224.
KIZIL, C., AKMAN, V. & MUZIR, E. COVID-19 Epidemic: A New Arena of Financial Fraud? Karabagh International Congress of Modern Studies in Social and Human Sciences, 2021.
LI, P., YU, H., LUO, X. & WU, J. 2023. LGM-GNN: A local and global aware memory-based graph neural network for fraud detection. *IEEE Transactions on Big Data*.
LI, Z., LIU, G. & JIANG, C. 2020. Deep representation learning with full center loss for credit card fraud detection. *IEEE Transactions on Computational Social Systems,* 7**,** 569-579.
LÓPEZ, V., FERNÁNDEZ, A., GARCÍA, S., PALADE, V. & HERRERA, F. 2013. An insight into classification with imbalanced data: Empirical results and current trends on using data intrinsic characteristics. *Information sciences,* 250**,** 113-141.
LUCAS, Y., PORTIER, P.-E., LAPORTE, L., HE-GUELTON, L., CAELEN, O., GRANITZER, M. & CALABRETTO, S. 2020. Towards automated feature engineering for credit card fraud detection using multi-perspective HMMs. *Future Generation Computer Systems,* 102**,** 393-402.
LUNGHI, D., PALDINO, G. M., CAELEN, O. & BONTEMPI, G. 2023. An Adversary Model of Fraudsters' Behavior to Improve Oversampling in Credit Card Fraud Detection. *IEEE Access,* 11**,** 136666-136679.
LUQUE, A., CARRASCO, A., MARTÍN, A. & DE LAS HERAS, A. 2019. The impact of class imbalance in classification performance metrics based on the binary confusion matrix. *Pattern Recognition,* 91**,** 216-231.

MA, K. W. F. & MCKINNON, T. 2021. COVID-19 and cyber fraud: Emerging threats during the pandemic. *Journal of Financial Crime,* 29**,** 433-446.
MAKKI, S., ASSAGHIR, Z., TAHER, Y., HAQUE, R., HACID, M.-S. & ZEINEDDINE, H. 2019. An experimental study with imbalanced classification approaches for credit card fraud detection. *IEEE Access,* 7**,** 93010-93022.
MATEUS-COELHO, N. & CRUZ-CUNHA, M. 2023. *Exploring Cyber Criminals and Data Privacy Measures*, IGI Global.
MAYO, K., FOZDAR, S. & WELLMAN, M. P. 2023. Flagging Payments for Fraud Detection: A Strategic Agent-Based Model.
MEKTEROVIĆ, I., KARAN, M., PINTAR, D. & BRKIĆ, L. 2021. Credit card fraud detection in card-not-present transactions: Where to invest? *Applied Sciences,* 11**,** 6766.
NARKHEDE, S. 2018. Understanding auc-roc curve. *Towards Data Science,* 26**,** 220-227.
NGUYEN, N., DUONG, T., CHAU, T., NGUYEN, V.-H., TRINH, T., TRAN, D. & HO, T. 2022. A proposed model for card fraud detection based on Catboost and deep neural network. *IEEE Access,* 10**,** 96852-96861.
NI, L., LI, J., XU, H., WANG, X. & ZHANG, J. 2023. Fraud feature boosting mechanism and spiral oversampling balancing technique for credit card fraud detection. *IEEE Transactions on Computational Social Systems*.
O'CONNOR, M., CONBOY, K., DENNEHY, D. & CARROLL, N. 2024. Temporal Complexity in Information Systems Development Flow: Challenges and Recommendations. *Communications of the Association for Information Systems,* 54**,** 19.
OSEGI, E. & JUMBO, E. 2021. Comparative analysis of credit card fraud detection in Simulated Annealing trained Artificial Neural Network and Hierarchical Temporal Memory. *Machine Learning with Applications,* 6**,** 100080.
PADMAJA, T. M., DHULIPALLA, N., BAPI, R. S. & KRISHNA, P. R. Unbalanced data classification using extreme outlier elimination and sampling techniques for fraud detection. 15th International Conference on Advanced Computing and Communications (ADCOM 2007), 2007. IEEE, 511-516.
PHUA, C., ALAHAKOON, D. & LEE, V. 2004. Minority report in fraud detection: classification of skewed data. *Acm sigkdd explorations newsletter,* 6**,** 50-59.
PHUA, C., LEE, V., SMITH, K. & GAYLER, R. 2010. A comprehensive survey of data mining-based fraud detection research. *arXiv preprint arXiv:1009.6119*.
POWERS, D. M. 2020. Evaluation: from precision, recall and F-measure to ROC, informedness, markedness and correlation. *arXiv preprint arXiv:2010.16061*.
RAI, D. & JAGADEESHA, S. 2023. Credit Card Fraud Detection using Machine Learning and Data Mining Techniques-a Literature Survey. *International Journal of Applied Engineering and Management Letters (IJAEML),* 7**,** 16-35.
RAJ, A. T., SHOBANA, J., NASSA, V. K., PAINULY, S., SAVARAM, M. & SRIDEVI, M. Enhancing Security for Online Transactions through Supervised Machine Learning and Block Chain Technology in Credit Card Fraud Detection. 2023 7th International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC), 2023. IEEE, 241-248.

RAJENDRAN, R. 2024. Data Breach Fraudulence and Preventive Measures in E-Commerce Platforms. *Advancements in Cybercrime Investigation and Digital Forensics.* Apple Academic Press.
RANDHAWA, K., LOO, C. K., SEERA, M., LIM, C. P. & NANDI, A. K. 2018. Credit card fraud detection using AdaBoost and majority voting. *IEEE access,* 6**,** 14277-14284.
RICHHARIYA, P. & SINGH, P. K. 2014. Evaluating and emerging payment card fraud challenges and resolution. *International Journal of Computer Applications,* 107.
ROY, A., SUN, J., MAHONEY, R., ALONZI, L., ADAMS, S. & BELING, P. Deep learning detecting fraud in credit card transactions. 2018 systems and information engineering design symposium (SIEDS), 2018. IEEE, 129-134.
SAHIN, Y., BULKAN, S. & DUMAN, E. 2013. A cost-sensitive decision tree approach for fraud detection. *Expert Systems with Applications,* 40**,** 5916-5923.
SALAZAR, A., SAFONT, G., RODRIGUEZ, A. & VERGARA, L. Combination of multiple detectors for credit card fraud detection. 2016 IEEE International Symposium on Signal Processing and Information Technology (ISSPIT), 2016. IEEE, 138-143.
SAMPAT, B., MOGAJI, E. & NGUYEN, N. P. 2024. The dark side of FinTech in financial services: a qualitative enquiry into FinTech developers' perspective. *International Journal of Bank Marketing,* 42**,** 38-65.
SÁNCHEZ, D., VILA, M., CERDA, L. & SERRANO, J.-M. 2009. Association rules applied to credit card fraud detection. *Expert systems with applications,* 36**,** 3630-3640.
SISODIA, D. S., REDDY, N. K. & BHANDARI, S. Performance evaluation of class balancing techniques for credit card fraud detection. 2017 IEEE International Conference on power, control, signals and instrumentation engineering (ICPCSI), 2017. IEEE, 2747-2752.
TUT, D. 2023. FinTech and the COVID-19 pandemic: Evidence from electronic payment systems. *Emerging Markets Review,* 54**,** 100999.
VANINI, P., ROSSI, S., ZVIZDIC, E. & DOMENIG, T. 2023. Online payment fraud: from anomaly detection to risk management. *Financial Innovation,* 9**,** 1-25.
WEI, W., LI, J., CAO, L., OU, Y. & CHEN, J. 2013. Effective detection of sophisticated online banking fraud on extremely imbalanced data. *World Wide Web,* 16**,** 449-475.
WHITROW, C., HAND, D. J., JUSZCZAK, P., WESTON, D. & ADAMS, N. M. 2009. Transaction aggregation as a strategy for credit card fraud detection. *Data mining and knowledge discovery,* 18**,** 30-55.
XIE, Y., LIU, G., YAN, C., JIANG, C. & ZHOU, M. 2022a. Time-aware attention-based gated network for credit card fraud detection by extracting transactional behaviors. *IEEE Transactions on Computational Social Systems*.
XIE, Y., LIU, G., YAN, C., JIANG, C., ZHOU, M. & LI, M. 2022b. Learning transactional behavioral representations for credit card fraud detection. *IEEE Transactions on Neural Networks and Learning Systems*.
XIE, Y., LIU, G., ZHOU, M., WEI, L., ZHU, H., ZHOU, R. & CAO, L. 2023. A Spatial–Temporal Gated Network for Credit Card Fraud Detection by Learning

Transactional Representations. *IEEE Transactions on Automation Science and Engineering*.
XUAN, S., LIU, G., LI, Z., ZHENG, L., WANG, S. & JIANG, C. Random forest for credit card fraud detection. 2018 IEEE 15th international conference on networking, sensing and control (ICNSC), 2018. IEEE, 1-6.
ZENG, Y. & TANG, J. 2021. Rlc-gnn: An improved deep architecture for spatial-based graph neural network with application to fraud detection. *Applied Sciences,* 11**,** 5656.
ZENG, Y. & TANG, J. 2022. Improved Aggregating and Accelerating Training Methods for Spatial Graph Neural Networks on Fraud Detection. *arXiv preprint arXiv:2202.06580*.
ZHANG, X., HAN, Y., XU, W. & WANG, Q. 2021. HOBA: A novel feature engineering methodology for credit card fraud detection with a deep learning architecture. *Information Sciences,* 557**,** 302-316.
ZHU, H., ZHOU, M., LIU, G., XIE, Y., LIU, S. & GUO, C. 2023. NUS: Noisy-Sample-Removed Undersampling Scheme for Imbalanced Classification and Application to Credit Card Fraud Detection. *IEEE Transactions on Computational Social Systems*.