**Online Payment Fraud Detection Using Machine Learning**

# **CHAPTER ONE**

# **INTRODUCTION**

## **1.1 Overview**

In today's digital era, online payment systems have grown in popularity and have become an essential component of our daily life (Khando et al., 2022). These systems provide ease, speed, and accessibility by enabling individuals and organisations to conduct financial transactions at any time and from any location (Khando et al., 2022). However, as online payments have become more common, so has the possibility of fraudulent activities (Mikkelsen et al., 2022). Online payment fraud is defined as any fraudulent or unauthorised behaviour aimed at exploiting vulnerabilities in the payment process to illegally gain financial benefits (Stripe, 2023). Online payment fraud can take many forms, but the most common are fraudulent individuals obtaining credit card or bank account information, forging checks, or utilising stolen identity information to perform unauthorised transactions (Stripe, 2023). To carry out fraudulent transactions, fraudsters use a variety of strategies, including stolen credit card information, identity theft, phishing, and account takeover (Mytnyk et al., 2023). Online payment fraud has serious effects, resulting in significant financial losses for individuals and organisations, as well as reducing the trust of customers in online payment systems (Fernandes, 2013). Traditional approaches to fraud detection often rely on predetermined rules, heuristics, or thresholds to identify suspicious transactions (Hilal et al., 2022). While these strategies provided some amount of protection, they are usually inadequate in detecting complex and devolving fraud patterns (Hilal et al., 2022). Fraudsters frequently modify their approaches, making it difficult for rule-based systems to keep up with evolving fraud trends (Barkved, 2022). As a result, there is an urgent need for more advanced and adaptable fraud detection methods.

Machine learning, a subset of artificial intelligence, has emerged as an effective method for addressing the issues of detecting online payment fraud (Prajapati et al., 2023). Machine learning algorithms are capable of analysing vast amounts of data, detecting complex patterns, and adapting to evolving fraud patterns over time (Bin Sulaiman et al., 2022). These algorithms can learn the characteristics of authentic and fraudulent transactions using previous transaction data, allowing them to make accurate predictions about the potential of fraud in real-time (Bin Sulaiman et al., 2022). The application of machine learning in the detection of online payment fraud has yielded positive outcomes (Shah and Makwana, 2023). It enables the development of complex models capable of detecting fraudulent activities while minimising false positives (Shah and Makwana, 2023). These models can detect anomalies and patterns indicative of fraudulent activity by leveraging a wide range of features such as transaction metadata, client information, device data, and behavioural patterns (Shah and Makwana, 2023). Furthermore, machine-learning approaches can improve fraud detection systems by enabling real-time monitoring and analysis (Ashfaq et al., 2022). Online payment fraud can be recognised and prevented effectively with the combination of streaming data processing and anomaly detection techniques, reducing the potential financial impact on both customers and businesses (Lu et al., 2023). Despite the potential benefits of machine learning in fraud detection, various challenges must be addressed. Imbalanced datasets, in which real transactions outnumber fraudulent transactions, might result in biased models with high accuracy but have low fraud detection rates (Shakya, 2018). To properly solve this issue, preprocessing approaches such as oversampling or undersampling must be applied (Shakya, 2018). Also, due to the rapid rise of online transactions and evolving nature of fraud, fraud detection systems must adapt and learn in real-time (Zhu et al., 2021). Anomaly detection approaches, such as clustering or outlier identification, can aid in identifying previously undetected fraud patterns and improving fraud detection efficiency (Hilal et al., 2022). Real-time data stream integration allows for the analysis of transaction data as it flows, enabling immediate fraud detection and prevention (Rajeshwari and Babu, 2016).

In consideration of these challenges and opportunities, the purpose of this study is to look into the use of machine-learning approaches for detecting online payment fraud. This work aims to develop accurate and efficient models capable of detecting fraudulent transactions by exploring different algorithms, feature engineering methods, data preprocessing techniques, and real-time data analysis. By conducting comprehensive experiments and evaluations, this study seeks to develop fraud detection techniques in the field of eCommerce, ultimately improving the security and reliability of online payment systems.

## **1.2 Problem Background**

The e-commerce industry presents significant challenges that must be addressed to improve the security and integrity of digital transactions (Bezhovski, 2016). Traditional rule-based fraud detection systems are ineffective in dealing with complex and evolving fraud trends (Hilal et al., 2022). These techniques often yield high false-positive rates and undetected fraudulent transactions, resulting in financial losses and compromising security for users and businesses (Hilal et al., 2022). This challenge has an impact on the integrity of online payment systems and impedes the efficient and secure processing of digital transactions (Bezhovski, 2016). The literature on online payment fraud detection reveals various gaps and limitations in existing operations. Firstly, traditional rule-based systems fail to keep up with evolving fraud trends and variations, as fraudsters continuously modify their methods (Barkved, 2022). Also, imbalanced datasets, in which real transactions significantly outnumber fraudulent ones, make reliable fraud detection challenging (Shakya, 2018). The necessity for real-time fraud detection to reduce financial losses necessitates efficient and responsive systems capable of promptly analysing and detecting fraudulent activity (Zhu et al., 2021).

To address these issues, a possible solution is to use machine learning techniques for detecting online payment fraud. By utilising machine learning algorithms, which can analyse vast amounts of transaction data and adapt to evolving fraud trends, it is feasible to enhance accuracy and timeliness in identifying fraudulent activity (Ashfaq et al., 2022). This research hypothesis proposes that it is possible to improve online payment fraud detection and mitigate the shortcomings of traditional rule-based methods by implementing robust machine learning models, incorporating appropriate feature engineering techniques and data preprocessing methods, and integrating real-time data analysis.

## **1.3 Research Aim**

The study aims to develop and evaluate machine learning-based models for detecting online payment fraud, addressing gaps in the literature and providing a more effective and efficient strategy for preventing online payment fraud. The study seeks to contribute to the advancement of fraud detection methodologies, strengthen the security of online payment systems, and optimise placement provider workflow by minimising financial losses and enhancing trust in digital transactions.

## **1.4 Research Objectives**

1. Collect and preprocess a comprehensive dataset of online payment transactions for effective fraud detection.
2. Investigate and select suitable machine-learning techniques for fraud detection in online payment transactions.
3. Develop and implement a robust fraud detection model using the selected machine learning algorithms.
4. Evaluate the performance of the developed model using different metrics and criteria.

## **1.5 Research Scope**

The research scope encompasses both in-scope and out-of-scope parameters to establish the boundaries and limitations of the study.

## **1.5.1 In-Scope**

The study will investigate and apply several machine learning algorithms, such as logistic regression, decision trees, random forest, gradient boost, and support vector machines. The efficiency of these techniques in identifying online payment fraud will be evaluated. Feature engineering techniques will be explored to enhance the performance of fraud detection models. This includes selecting important features, reducing complexity, and generating derived features to increase model accuracy. Data preprocessing techniques will be explored to address the challenges posed by imbalanced datasets commonly encountered in fraud detection. Techniques such as oversampling, undersampling, and synthetic data creation will be considered to achieve an accurate representation of fraudulent and genuine transactions. The study will also focus on the integration of real-time data streams and anomaly detection methods. This will allow for the timely detection of fraudulent transactions, leveraging the continuous analysis of streaming data and the identification of anomalous patterns. The performance of the developed fraud detection models will be assessed using a variety of metrics and criteria, including accuracy, precision, recall, and F1-score.

## **1.5.2 Out-of-Scope**

The study makes no mention of other types of fraud, such as insurance or healthcare fraud. The focus is solely on detecting online payment fraud. This research does not specifically explore industry-specific fraud features. Rather than focusing on industry-specific features, the research seeks to develop methodologies that are applicable across different sectors. Geographical fraud patterns are not specifically taken into account. Rather than focusing on regional variations, the research seeks to develop methodologies that are applicable across different geographic locations. The legal and regulatory concerns associated with detecting online payment fraud are also beyond the scope of this study. The study focuses primarily on the technical aspects of implementing machine learning-based models rather than legal or regulatory frameworks.

## **1.6 Methodology**

This research project will employ machine learning techniques to develop an efficient model for detecting online payment fraud. In the first phase, a comprehensive dataset of both valid and fraudulent online financial transactions will be collected and pre-processed to ensure accuracy and consistency. Next, the relevant data will be extracted using feature engineering techniques. This involves discovering features that capture patterns and indicators of fraudulent activities and developing new features to improve the model's discriminatory ability. Various supervised machine learning algorithms such as logistic regression, decision trees, random forest, gradient boost, and support vector machines will be explored for fraud detection. The model will be trained to adjust its internal parameters to optimise its ability to differentiate between fraudulent and non-fraudulent transactions.

The developed system will be designed for real-time processing of online payment transactions, with a focus on efficient processing and low-latency response times. The system's performance will be assessed using cross-validation approaches. Experiments will be carried out to assess the system's performance under various circumstances, such as varying fraud rates or unbalanced datasets. The model's interpretability will also be investigated, with a focus on finding essential elements that contribute to fraud detection and analysing error patterns.

## **1.7 Contribution**

The primary contribution of this research is the development and implementation of robust machine learning-based models for detecting online payment fraud. The research will provide insights into the most effective methodologies for identifying fraudulent transactions by exploring and analysing various machine learning algorithms, feature engineering techniques, and data preprocessing methods. The findings will help to develop fraud detection methodologies while providing practical recommendations for fraud detection system implementation. Another significant contribution lies in the assessment of the developed models. The research will provide an objective assessment of the efficiency and limitations of the proposed machine learning-based fraud detection methodology by conducting comprehensive experiments and assessments using various metrics and criteria. The study seeks to provide a more accurate, adaptable, and real-time approach to fraud detection by addressing the limitations of traditional rule-based systems and evaluating the potential of machine learning. This, in turn, enhances the reliability and security of online payment systems and consumers and reduces the financial losses and compromised security experienced by individuals and businesses.

The significance of this research goes beyond the academic field. The research adds to the placement provider workflow by providing efficient and accurate solutions to prevent online payment fraud by establishing effective fraud detection models. The findings and recommendations of this study can help financial institutions, payment service providers, and e-commerce platforms improve their fraud prevention strategies and protect their customer's financial interests.

# **CHAPTER TWO**

# **LITERATURE REVIEW**

## **2.1 Overview**

In today's digital world, online payment fraud has become a major threat (Khando et al., 2022). As more financial transactions shift online, fraudsters take advantage of flaws in online payment systems, resulting in significant financial losses and compromised security (Mikkelsen et al., 2022). Traditional rule-based fraud detection approaches have limits in efficiently recognising and preventing growing fraud patterns; hence, innovative strategies that can adapt to evolving fraudulent strategies and improve fraud detection accuracy need to be developed (Bezhovski, 2016). The research gap lies in the need for new online payment fraud detection approaches that can adapt to evolving fraud strategies and enhance fraud detection accuracy. The current literature lays the foundation for understanding the challenges and limitations of traditional approaches, emphasising the need for advanced solutions. By addressing this research gap, the study aims to contribute to the development of effective online payment fraud detection systems.

To provide an understanding of the current state of the literature, the literature review provides an in-depth review of existing research on online payment fraud detection. It examines studies that contribute to the understanding of fraud detection approaches, machine learning algorithms, and techniques employed in the financial industry. It investigates the evolution of fraud detection technologies, from rule-based systems to the use of machine learning techniques.  By analysing previous research findings, the chapter examines the benefits and drawbacks of machine learning algorithms and real-time fraud detection approaches by analysing past research findings. The literature review also highlights the challenges associated with detecting online payment fraud. It highlights the gaps and limitations in the existing literature, emphasising the importance of additional research to address such shortcomings and increase the efficiency of fraud detection systems. Figure 1 is hierarchical taxonomy showing the methods of fraud detection and the authors explored alongside.

## Figure 1. Hierarchical taxonomy

## **2.2 Overview of Online Payment Fraud**

Online payment fraud is a widespread and growing challenge in the digital age, presenting serious threats to individuals, organisations, and financial institutions (Fernandez, 2013). Fraudsters use different kinds of ways to carry out fraudulent activities, including the use of stolen credit card information, identity theft, phishing attacks, and account takeovers (Mytnyk et al., 2023). The financial impact of online payment fraud is staggering, with projections estimating global losses exceeding $200 billion by 2024, as reported by Juniper Research (Smith, 2020). According to the research, businesses in eCommerce, airline ticketing, money transfer, and financial services would lose more than $200 billion to online payment fraud between 2020 and 2024, owing to the increased complexity of fraud attempts and an increase in the number of attack vectors. These alarming statistics highlight the crucial significance of developing efficient fraud detection systems. With the increase of digital transactions around the globe and the complexity of fraudulent strategies, fraudsters can operate across borders, complicating identification and prosecution (Gupta, 2023). Fraudsters can exploit flaws in systems and procedures in the digital landscape (Gupta, 2023). The internet and technology have made it less difficult for fraudsters to conduct their operations on a global level (Ali et al., 2019). Organisations struggle to recognise suspicious trends and detect fraud amidst the enormous number of legitimate transactions using traditional approaches as the number of digital transactions and data increases (Gupta, 2023).

To address this issue, researchers and industry practitioners have investigated various fraud detection approaches that make use of new technology such as machine learning (Yldrm and Bozyit, 2022). It is feasible to improve fraud detection accuracy and stay ahead of evolving fraud schemes by utilising machine learning algorithms, which can analyse enormous amounts of transactional data and uncover complicated patterns (Ali et al., 2022). Machine learning technologies can overcome the limitations of traditional rule-based systems by automatically learning from data and identifying anomalous activity associated with fraudulent transactions (Ali et al., 2022). However, despite the potential of machine learning for fraud detection, significant challenges and research gaps exist (Shakya, 2018). These include handling imbalanced datasets, where the number of genuine transactions far outnumbers the number of fraudulent ones, selecting appropriate machine learning algorithms, optimising feature engineering techniques, addressing real-time fraud detection requirements, and ensuring the interpretability of the fraud detection models (Shakya, 2018).

## **2.2.1 Definition of Online Payment Fraud**

Online payment fraud is a common and sophisticated type of cybercrime that targets digital transactions by exploiting vulnerabilities in online payment systems to perform unlawful and fraudulent activities (EU Cybersecurity Agency, 2018). It includes a wide variety of fraudulent activities carried out through digital platforms such as e-commerce websites, mobile applications, and online banking portals (Padmalatha, 2020). Malicious actors, often known as fraudsters, set up fraudulent operations by employing several deceitful strategies to access user accounts and exploit gaps in the payment ecosystem (Padmalatha, 2020).

## **2.2.2 Types of Online Payment Fraud**

Understanding the different types of online payment fraud is important for developing effective fraud detection strategies. Identifying and understanding the strategies employed by fraudsters can enable the effective of design targeted approaches to prevent them, thereby improving the security and reliability of online payment systems for consumers, businesses, and financial institutions (Cole, 2022). Types of online payment fraud include:

1. **Credit card fraud:** Credit card fraud is one of the most prevalent and well-known forms of online payment fraud (Fontinelle, 2023). Credit cards are often used in online purchases and e-commerce and are popular for online banking (Cherif et al., 2023). However, the evolution and widespread adoption of credit card use has resulted in the emergence of different types of fraud, with fraudsters employing increasingly sophisticated methods to execute fraudulent transactions, leading to considerable losses for cardholders and banks (Cherif et al., 2023). Criminals obtain stolen credit card information, including card numbers, expiration dates, and security codes, through various techniques such as hacking, data breaches, or skimming devices in this type of fraud (Crail, 2023). They then use the stolen information to make fraudulent purchases or transactions, usually online, without the legitimate cardholder's knowledge or approval (Crail, 2023).

Fraudsters may test the authenticity of stolen credit card information by exploiting weaknesses in e-commerce websites or payment processing systems (Chen, 2015). Before making bigger transactions, they may make small, inconspicuous purchases to determine whether the card is active and legitimate (Chen, 2015). Credit card fraud presents major risks to customers and businesses alike, causing financial losses for cardholders and chargebacks for retailers, resulting in revenue loss and higher operational costs (Hilal et al., 2022).

1. **Account takeover:** When fraudsters obtain unauthorised access to legitimate user accounts, such as email accounts, social media profiles, or online banking accounts, this is referred to as account takeover fraud (Mello, 2020). They can perform fraudulent transactions, make unauthorised modifications, or use the account holder's personal information for malicious purposes after they get access (Mello, 2020). Account takeover fraud is often associated with phishing attacks, in which fraudsters employ deceptive strategies to fool users into disclosing their login details or personal information (Ashiru, 2021). Once a fraudster gains access to a user's account, they can use it to make unauthorized purchases, access sensitive information, or engage in other fraudulent activities while pretending to be the legitimate account owner (DAngelo, 2023). Individuals might suffer significant financial losses, compromised personal information, and significant reputational damage if fraudulent activities are linked to the victim's account (DAngelo, 2023).
2. **Identity theft:** identity theft is a serious and widespread type of online payment fraud in which fraudsters obtain and exploit personal information such as social security numbers, addresses, and birthdates to assume the identities of others (US Department of Justice, 2020). They can create phoney accounts, apply for credit cards, and engage in other financial transactions in the victim's name using this stolen identity (US Department of Justice, 2020). Identity theft is often facilitated by data breaches or hacking incidents that expose individuals' personal information, which may later be sold on the dark web or used for fraudulent purposes (Szakonyi et al., 2021). Identity theft victims may have significant financial implications since their credit scores may be severely impacted, making it harder to get loans or credit, and they may spend a significant amount of time and money resolving fraudulent accounts and activities (DeLiema et al., 2021).
3. **First-party fraud:** First-party fraud, commonly referred to as friendly fraud or bust-out fraud, is a unique and deceptive type of online payment fraud (Evans, 2022). Individuals knowingly participate in fraudulent activities using their own identities to earn dishonest financial gains or benefits (Cox, 2023). This may involve applying for loans, credit cards, or other financial services with no intention of repaying them, thereby scamming lenders or financial institutions (Cox, 2023). First-party fraud is more difficult to detect than typical online payment fraud as fraudulent activities are carried out by persons who legitimately hold the identification and account information used (Sadowski and Rathle, 2014). As a result, fraud detection systems may be unable to detect this sort of fraud, causing lenders and financial institutions to incur financial losses (Sadowski and Rathle, 2014).

## **2.3 Traditional Approaches to Fraud Detection**

Traditional approaches to online payment fraud detection have been widely employed, but they face challenges with keeping up with the evolving nature of fraud patterns (Hilal et al., 2022). To identify suspicious transactions, rule-based technologies like rule engines and threshold-based systems have traditionally been used (Nethone, 2021). These approaches, however, often have significant false-positive rates and may miss identifying fraudulent activities (Nethone, 2021). Because they rely on predetermined rules and thresholds, they are less adaptable to identifying evolving and innovative fraud patterns, limiting their overall efficacy in addressing online payment fraud (Karczewski, 2020).

## **2.3.1 Rule-based Systems**

For many years, rule-based systems have been a core technique in fraud detection (Aparicio et al., 2020). These systems operate by defining a predefined set of rules and thresholds based on previous fraud tendencies and expert knowledge (Baumann, 2021). When a transaction satisfies specific criteria or matches known fraud patterns, the system flags it as suspicious and recommends an additional investigation or rejection (Baumann, 2021).

While rule-based systems are relatively simple to implement and interpret, they have several limitations that hinder their ability to identify sophisticated and evolving fraud strategies (Swaminathan, 2020). One of the major drawbacks of the rule-based approach is its inflexibility in dealing with situations that go beyond its preset rules (Haponik, 2023). In essence, if a situation does not conform to the system's preset rules, the system may produce incorrect outcomes (Haponik, 2023). Predefined rules may rapidly become obsolete if fraud trends evolve and fraudsters adopt new attack strategies (Baumann, 2021). Maintaining and updating rules to stay up with new fraud strategies may be a challenging task for fraud analysts, and it may necessitate regular monitoring and revisions (Aschi et al., 2022). This lack of flexibility can make rule-based systems less effective over time in the continually evolving context of online payment fraud (Aschi et al., 2022). To reduce false negatives, rule-based systems sometimes use a conservative approach, which can contribute to an increase in false positives (normal transactions incorrectly identified as fraudulent) (Lopes, 2023). When rules are extremely strict, they may cause a large number of false positives, necessitating human review and verification and potentially delaying the processing of legitimate transactions (Vorobyev and Krivitskaya, 2022). A high percentage of false positives can adversely impact the user experience, resulting in customer dissatisfaction and transaction cancellation (Vorobyev and Krivitskaya, 2022).

Fraudsters continuously refine their strategies, resulting in more complex and dynamic fraud patterns (Hilal, 2022). Traditional rule-based systems may struggle to detect subtle anomalies or deviations from preset rules, allowing evolving fraud patterns and sophisticated attacks to go unnoticed, exposing customers and businesses to increased risks. Hilal, 2022). When dealing with a huge volume of real-time transactions, rule-based systems may face scalability issues (Zhou et al., 2017). Scaling the model increases the number of rules proportionally, increasing the system's complexity over time and making maintenance and updating more difficult (Haponik, 2023). Scaling rule-based systems can also result in higher computing needs, which, if not met, can result in longer computation times (Haponik, 2023).

## **2.3.2 Case Studies of Traditional Approaches in Fraud Detection**

Salim et al. (2023) discussed the limitations of traditional rule-based systems in detecting advanced persistent threats (APTs), which are sophisticated and targeted attacks aimed at specific entities. The study's findings are reviewed in terms of research gaps in the literature, and the study provides key recommendations for developing an effective model for early APT detection.

APTs are difficult to detect because of their ability to bypass specified rules, leaving rule-based systems inefficient in detecting these sophisticated and stealthy attacks (Berrada et al., 2020). This highlights the need for advanced methodologies capable of capturing and adapting to the complex and dynamic nature of fraud patterns, resulting in higher levels of accuracy and detection capabilities. Research on Cybersecurity and Fraud Detection in Financial Transactions by Aschi et al. (2022) highlights the limitations of rule-based approaches and reveals how machine learning may address many of these limitations and detect risky transactions more effectively. According to the study, the rules can be easily updated over time, or new rules can be inserted in response to specific needs to address new threats; however, as the number of fraud detection rules expands and more rules are combined for the detection of complex fraud cases, the more the rules may conflict with each other due to semantic inconsistencies. This causes the rule-based system to function inefficiently. Aschi et al. (2022) built a lambda architecture that handles both real-time and batch analytics operations using an integrated approach. Lambda architecture is a data processing architecture that combines batch processing with real-time stream processing to manage massive volumes of data (Loganathan, 2023). The solution proposed in this research aims to support fraud analysts innovatively and efficiently while also automating fraud detection procedures. Other studies have also highlighted the limitations of traditional approaches in detecting specific types of fraud. Mahdi et al. (2014) patented their invention that, in one component, provides a system and method for identifying first-party fraud. They examined the challenges involved in identifying first-party fraud, which occurs when individuals intentionally engage in fraudulent actions using their own identities. The inventors argued that traditional approaches struggle to capture the subtle behavioural patterns and nuances associated with this type of fraud, further emphasizing the need for more advanced and adaptive techniques.

## **2.4 Machine Learning in Fraud Detection**

Machine learning approaches have received a lot of interest in the field of fraud detection due to their capacity to learn from data and recognise complex patterns (Ali et al., 2022). Machine learning has emerged as a powerful and effective method for detecting fraud in online payment systems (Hajek et al., 2022). Machine learning algorithms, as opposed to traditional rule-based systems that rely on predefined rules and thresholds, may automatically learn complex patterns and anomalies from huge volumes of transaction data (Sen and Mehtab, 2020). Because of this adaptability, machine learning models can keep up with new fraud strategies, making them more resilient and efficient at identifying fraudulent behaviour in real-time (Sen and Mehtab, 2020). One of the primary advantages of machine learning in fraud detection is its capacity to learn from past data and uncover patterns that would otherwise be missed by manual analysis (Ali et al., 2022). Machine learning algorithms can detect subtle relationships and behavioural patterns suggestive of fraudulent activity by examining prior transaction records (Xie et al., 2022). Furthermore, machine learning algorithms can handle large volumes of transaction data quickly, making them suitable for real-time processing and detection of fraudulent transactions (Bynagari, 2015). Machine learning models can be trained to distinguish between legitimate and fraudulent transactions based on various features, including transaction amount, time, location, and user behaviour (Mytnyk et al., 2023). The learnt patterns are then used to define decision limits, allowing the model to classify new, unseen transactions as either genuine or fraudulent (Mytnyk et al., 2023). Machine learning models are also able to evolve and adapt in response to the continual influx of data to detect evolving fraud strategies effectively (Jeffers, 2023).

## **2.4.1 Supervised Learning Algorithms for Fraud Detection**

Supervised learning techniques are widely employed in the detection of online payment fraud because they are based on the notion that fraudulent patterns may be learned from the analysis of previous transactions (Carcillo et al., 2021). Supervised learning algorithms are trained on labelled data, with each transaction classified as either genuine or fraudulent (Afriyie et al., 2023). The model learns from labelled instances to generalize and predict unlabelled input (Afriyie et al., 2023). Several supervised learning techniques have been used to detect fraud:

* **Logistic Regression:** Logistic regression is a widely used linear classification approach that assesses the likelihood of a transaction being fraudulent based on its input features (Ruchay et al., 2023). Logistic regression is simple to implement and interpret, performs well with categorical features, and is effective for problems related to binary classification such as fraud detection (Mytnyk et al., 2023).
* **Decision Trees:** Based on a sequence of binary judgments, decision trees construct a tree-like model to classify transactions (Song and Lu, 2015). They are interpretable, can handle non-linear feature relationships, and perform well on small to medium datasets (Mytnyk et al., 2023).
* **Random Forest:** The random forest is one of the most accurate fraud detection algorithms in the financial industry (Afriyie et al., 2023). Random forests are an ensemble learning strategy that combines multiple decision trees to increase accuracy and avoid overfitting (Mytnyk et al., 2023). Random forests are a type of prediction model that is made up of an ensemble of (randomized) decision trees (Karlsson, 2017). Several variations of the same approach have been examined, but they mostly differ in how randomization is introduced both in the training set and in the decision tree learning technique while maintaining the low bias of the individual models (Karlsson, 2017). The random forest does not normally require a feature selection technique; however, one disadvantage of this approach is how fast it may recognize data with a broad range of values and variables with multiple values as fraudulent (Afriyie et al., 2023).
* **Support Vector Machines (SVM):** SVM is a sophisticated classification technique that identifies the best hyperplane in a high-dimensional feature space to distinguish between legitimate and fraudulent transactions (Behravan et al., 2016). Support Vector Machine (SVM) is used to solve classification and regression issues (Kumbhar et al., 2023). SVM is resistant to noise and overfitting, and it provides a regularization parameter to help reduce overfitting (Kumbhar et al., 2023).
* **Neural Networks:** Deep learning architectures such as recurrent neural networks (RNNs) and convolutional neural networks (CNNs) have shown promising results in fraud detection (Berhane et al., 2023). Bagged ensemble learning approaches enable these machine learning algorithms to provide efficient results and excel at collecting complicated patterns and correlations in sequential or spatial data (Abakarim et al., 2023).
* **Ensemble Methods:** Ensemble learning is a type of hybrid learning system in which multiple analytics are intelligently merged to achieve better (more accurate, robust, etc.) outcomes than single analytics can deliver (Simske, 2019). Ensemble approaches like boosting, stacking, and bagging integrates numerous weak classifiers to form a better overall model, resulting in enhanced accuracy and generalization (Simske, 2019).

## **2.4.2 Unsupervised Learning Algorithms for Fraud Detection**

Unsupervised learning algorithms do not require labelled data and instead focus on detecting abnormalities or outliers in transaction data (Goldstein and Uchida, 2016). These anomalies might be fraudulent transactions that deviate significantly from the normal behaviour of legitimate transactions (Hilal et al., 2022). Unsupervised learning algorithms are especially beneficial when previously labelled fraud data is scarce or unavailable, as they can detect new fraud patterns without requiring labelled instances (Murorunkwere et al., 2022). However, due to the lack of defined fraud labels, they may generate more false positives (Murorunkwere et al., 2022).

Some unsupervised learning techniques used in fraud detection include:

* **Anomaly detection:** Unsupervised learning models based on anomaly detection algorithms, such as isolation Forest and one-class Support Vector Machine algorithms, can learn the normal behaviour of legitimate transactions and flag transactions that deviate from this normal behaviour as potentially fraudulent (No Author, 2022). These algorithms are designed to recognize a group of outliers, assign artificial fraud labels to these outliers, and then train a new dataset to look for other patterns or indicators of fraud (No Author, 2022).
* **Clustering algorithms:** Clustering algorithms group data so that points inside a single group or cluster are similar to one another but different from points in other groups (Nowak-Brzeziska & Weronika, 2021). Clustering has been proven to be an excellent consideration for anomaly detection (Al-Anazi et al., 2016). Clustering methods aggregate together comparable transactions based on feature similarities (Al-Anazi et al., 2016). Unusual or outlier clusters may contain fraudulent activities.

## **2.4.3 Semi-Supervised Learning Algorithms for Fraud Detection**

Semi-supervised learning algorithms combine labelled and unlabeled data to increase the accuracy of fraud detection models (Carcillo et al., 2021). Semi-supervised learning solves the issues of unbalanced datasets and a scarcity of labelled fraud instances by leveraging both labelled fraud instances and a substantial volume of unlabeled data (Carcillo et al., 2021).

Two common semi-supervised learning techniques used in fraud detection are:

* **Active learning (AL):** Active Learning (AL) has become one of the most widely used machine learning techniques because it can effectively train a model using a large volume of unlabeled data and is appropriate for cases where a large volume of unlabeled data can be easily collected but labelling them requires a lot of manpower and material resources (Qin et al., 2021). Active learning selects the most informative instances from unlabeled data to be identified by a human expert (Qin et al., 2021). Active learning minimizes annotation effort and increases model performance with a limited labelled dataset by systematically selecting the most uncertain or ambiguous instances (Gui et al., 2021).
* **Self-training:** Self-training is an iterative method that begins with a model trained on a small labelled dataset (He et al., 2019). After that, the model is used to predict labels for the unlabeled data, and confident predictions are added to the labelled dataset for the next iteration (Tanha et al., 2017). This procedure is repeated until convergence, progressively improving the model's performance (He et al., 2019).

## **2.4.4 Studies on the Use of Machine Learning for Fraud Detection**

Several studies have investigated the use of machine learning algorithms for detecting online payment fraud, demonstrating their effectiveness and superiority over traditional rule-based approaches.

Sai et al. (2019) conducted a study on credit card fraud detection, applying logistic regression, naive Bayes, decision trees, random forests, AdaBoost, gradient boosted tree, neural network, support vector machine, and K-nearest neighbour, with the random forest model having the best performance of 55.07% FDR at 3% in testing. Their results demonstrated higher accuracy compared to rule-based approaches, demonstrating the potential of machine learning algorithms in detecting fraudulent transactions. The findings contribute to the notion that machine learning algorithms may effectively detect the complex patterns and irregularities associated with fraud, resulting in higher detection rates. Ensemble methods, such as random forest, have gained popularity in fraud detection due to their ability to handle high-dimensional data and capture complex fraud patterns (Sohony et al., 2018). Jebaseeli et al. (2021) utilized random forest as an ensemble method to detect fraudulent activities involving credit card transactions. Their research found that the random forest algorithm outperformed traditional rule-based systems in terms of accuracy, precision, and recall. Deep learning models have emerged as an efficient tool in fraud detection in recent years, particularly for identifying temporal and geographical correlations within transaction data (Kanika and Singla, 2020). Krishnan et al. (2022) investigated fraud detection using recurrent neural networks (RNNs) and convolutional neural networks (CNNs). Their findings indicated that these deep learning models are effective at collecting sequential patterns and spatial relationships, resulting in improved fraud detection accuracy.

These examples highlight the potential of machine learning techniques such as logistic regression, decision trees, random forests, RNNs, and CNNs in detecting fraud in online payment systems. The ability of these algorithms to analyse massive amounts of transactional data and detect subtle indications of fraudulent activity provides significant advantages over traditional rule-based techniques (Gupta, 2023). Leveraging machine learning algorithms can lead to improved fraud detection rates, reduced false positives, and enhanced overall security in online payment systems (Gupta, 2023).

## **2.5 Feature Engineering Techniques**

Feature engineering plays a vital role in increasing the performance of fraud detection models by selecting and developing important features that better capture fraud patterns, (Alejandro et al., 2016). Several strategies have been used to improve the discriminating power of features and to optimise data representation. Feature selection techniques, such as information gain and correlation analysis, have been widely used to identify the most informative features for fraud detection (Mienye and Sun, 2023). Information gain measures the reduction in uncertainty about the fraud label by adding a particular feature to the model (Senthilnathan, 2019), while correlation analysis assesses the relationship between features and the target variable (Mienye and Sun, 2023). The dimensionality of the feature space may be minimised by selecting the most significant features, enhancing computational performance and preventing the model from being overwhelmed by irrelevant or duplicate information (Huang et al., 2019). Principal component analysis (PCA), for example, has been used in fraud detection to reduce the dimensionality of the feature space while maintaining as much information as possible (Anowar et al., 2022). PCA determines the fundamental components in the data that capture the maximum variance and projects the original features onto these components (Kurita, 2020). This aids in the identification of the most essential underlying patterns in the data, allowing for a more compact representation of the features and reducing the computational complexity of the fraud detection model (Kurita, 2020). In addition to feature selection and dimensionality reduction, the generation of derived features can improve the distinction between legitimate and fraudulent transactions (Aziz et al., 2013). Derived features are developed by merging or altering existing features to capture complex relationships and patterns (Aziz et al., 2013). Transaction frequency, average transaction value, and duration between transactions, for instance, are relevant in discriminating between legitimate and fraudulent transactions (Diadiushkin et al., 2019). These behavioural features provide insights into typical patterns and behaviours associated with legitimate transactions and aid in the detection of deviations that may indicate fraudulent activity (Diadiushkin et al., 2019).

## **2.6 Data Preprocessing and Imbalance Handling**

Handling imbalanced datasets, where legitimate transactions exceed fraudulent ones, is a key challenge in detecting online payment fraud (Kaniika et al., 2022). Machine learning algorithms trained on imbalanced datasets may display biased behaviour, favouring the majority class (legitimate transactions) and resulting in poor detection of fraudulent activity (Alamri and Yhklef, 2022). To address this issue, researchers have developed various data preprocessing techniques that may efficiently manage unbalanced datasets. One such technique is oversampling which seeks to balance the dataset by producing synthetic instances of the minority class (Yi et al., 2022). SMOTE (Synthetic Minority Over-sampling Technique) is a popular oversampling approach that generates synthetic examples by interpolating between neighbouring instances of the minority class (Yi et al., 2022). SMOTE helps to reduce the class imbalance problem and enhance the identification of fraudulent transactions by boosting the representation of the minority class (Douzas et al., 2018). Undersampling techniques, on the other hand, randomly eliminate instances from the majority class to produce a balanced distribution between the two classes. Tsai et al. (2019). Undersampling reduces the dominance of the majority class and prevents the algorithm from favouring it (Dubey et al., 2014). However, undersampling may result in the loss of valuable data, especially if the dataset is already limited (Dubey et al., 2014).

Hybrid approaches that combine oversampling and undersampling techniques have also been explored to handle imbalanced datasets effectively (Wong et al., 2018). These techniques seek to find a balance between protecting the dominant class' integrity and enhancing minority class representation (Wong et al., 2018). These hybrid techniques, which include oversampling and undersampling, can address the imbalanced nature of the dataset and increase the overall performance of fraud detection models (Junsomboon and Phienthrakul, 2017). In addition to oversampling and undersampling, synthetic data generation methods have been employed to address the class imbalance problem. Generative Adversarial Networks (GANs) have been used to generate realistic synthetic fraudulent transactions that may be contributed to the dataset (Sauber-Cole and Khoshgoftaar, 2022). GANs are made up of two networks: a generator network that creates synthetic samples and a discriminator network that differentiates between real and synthetic samples (Randhavane et al., 2019). GANs can develop synthetic data that closely match fraudulent transactions by iteratively training these networks, balancing the dataset and enhancing the effectiveness of fraud detection algorithms (Sauber-Cole and Khoshgoftaar, 2022).

## **2.7 Real-time Fraud Detection**

Real-time fraud detection is essential to reduce the financial implications of fraudulent transactions in online payment systems (Rajeshwari and Babu, 2016). Traditional batch processing systems, in which data is processed at predetermined intervals, may not be adequate for detecting fraudulent transactions promptly (Roditi, 2023). As a result, real-time data stream integration and the adoption of anomaly detection algorithms have gained significant interest in the field of fraud detection (Roditi, 2023). Streaming data processing frameworks have emerged as important tools for dealing with the high-velocity data streams generated by online payment systems (Kolajo et al., 2019). Frameworks like Apache Kafka and Apache Flink can manage massive amounts of data and perform real-time transaction analysis (van Dongen et al., 2020). These frameworks provide the infrastructure required to handle and analyse data as it comes in, ensuring that fraud detection algorithms can keep up with the high volume of transactions (van Dongen et al., 2020).

Anomaly detection algorithms are very useful in real-time fraud detection because they can detect deviations from typical behaviour as transactions happen (Hilal et al., 2022). Isolation Forest is an example of an anomaly detection technique that works by separating observations from a dataset that is regarded to be abnormal (Xu et al., 2023). The method can successfully identify fraudulent transactions that deviate from the regular patterns presented by legitimate transactions by generating decision trees and identifying cases with shorter average path lengths Vanini et al., 2023). One-Class Support Vector Machines (SVMs) are another commonly used anomaly detection technique in real-time fraud detection (Hejazi and Singh, 2013). One-Class SVMs are trained on a single class of data (i.e., real transactions) to differentiate normal data points from outliers (fraudulent transactions) (Kawade et al., 2022). One-Class SVMs may detect instances that deviate from regular behaviour by learning the limits of normal behaviour and flagging them as potentially fraudulent (Kawade et al., 2022).

## **2.8 Literature Summary**

|  |  |  |
| --- | --- | --- |
| **Methods for detecting online payment fraud** | **Literature** | **Findings** |
| Traditional approaches   * Rule-based systems | Salim et al. (2023):  A systematic literature review for APT detection and Effective Cyber Situational Awareness (ECSA) conceptual model | * Rule-based systems inefficient in detecting advanced persistent threats (APTs) because of their sophistication and ability to bypass specified rules. * Highlights the need for advanced methodologies that can capture and adapt to the complex and dynamic nature of fraud patterns. |
|  | Aschi et al. (2022):  Cybersecurity and fraud detection in financial transactions. | * Rules can be easily updated over time; however, as the number of fraud detection rules expands, they may conflict with each other due to semantic inconsistencies. * Built a lambda architecture that handles both real-time and batch analytics operations using an integrated approach aimed at automating fraud detection procedures. |
|  | Mahdi et al. (2014):  First party fraud detection system | * Traditional approaches struggle to capture the subtle behavioural patterns and nuances associated with first-party fraud. * Patented their invention that provides a system for identifying first-party fraud. |
| Machine learning   * Supervised machine learning * Semi-supervised machine learning * Unsupervised machine learning | Sai et al. (2019):  Effective detection of credit card fraud using logistic regression, decision tree and machine learning techniques | * Conducted a study on credit card fraud detection, applying logistic regression, naive Bayes, decision trees, random forests, AdaBoost, gradient boosted tree, neural network, support vector machine, and K-nearest neighbour. * Their results showed higher accuracy compared to rule-based approaches in detecting fraudulent transactions. |
|  | Jebaseeli et al. (2021):  Fraud detection for credit card transactions using random forest algorithm | * Used random forest as an ensemble method to detect fraudulent activities involving credit card transactions. * Found that the random forest algorithm outperformed traditional rule-based systems in terms of accuracy, precision, and recall. |
|  | Krishnan et al. (2022):  Development of Deep Learning based intelligent approach for credit card fraud detection | * Investigated fraud detection using recurrent neural networks (RNNs) and convolutional neural networks (CNNs). * Found that CNNs and RNNs are effective at collecting sequential patterns and spatial relationships, resulting in improved fraud detection accuracy. |

## Table 1. Literature summary

**CHAPTER THREE**

**RESEARCH METHODOLOGY**

**3.1 Overview**

In the contemporary digital age, the surge in online transactions and financial activities has paved the way for an unsettling surge in online fraud instances (McAfee, 2020). Due to technological advancement, malicious entities adeptly devise new strategies to exploit vulnerabilities in online systems, posing a substantial challenge for individuals, businesses and regulatory bodies alike (Federal Trade Commission, 2021). As the dynamics of fraud grow more intricate, there arises an urgent need for a proactive and adaptable solution that can seamlessly identify and neutralize fraudulent activities (Association for Computing Machinery, 2022). This report undertakes a comprehensive exploration of the domain of online fraud detection. The research conundrum at the heart of this exploration stems from the inadequacies inherent in conventional rule-based systems to discern nuanced and constantly evolving fraud patterns (Buczak et al., 2016). These conventional systems, reliant on predetermined rules, prove inept at keeping pace with the fluid strategies employed by fraudsters (Phua et al., 2010). The resultant repercussions span from financial losses to tarnished reputations and most crucially compromised trust within the digital landscape (Barriga et al., 2021).

The proposed solution reflects a paradigm shift that embraces the transformative power of machine learning (Li et al., 2021). This dissertation approach harnesses the immense capabilities of algorithms to analyse historical data, decipher intricate patterns and promptly assimilate new methodologies as they surface (Dal Pozzolo et al., 2017). By employing machine learning, the objective is to fabricate a robust, responsive, and multifaceted fraud detection mechanism, capable of effectively differentiating between legitimate transactions and fraudulent maneuvers even when masked by intricate tactics (Li et al., 2021)

Throughout the expanse of this report, an immersive exploration of data and algorithms takes centre stage, uncovering the pivotal constituents of a formidable fraud detection model (Witten et al., 2016). Foundational machine learning principles are scrutinized, underscoring the indispensable role of high-quality data, astute feature engineering and strategic algorithm curation (Chandola et al., 2009). Beyond the mere technical underpinnings, the narrative extends into the realm of ethical considerations within the field (Angwin et al., 2016). Inclusivity and fairness are accentuated, accompanied by a meticulous examination of potential biases, thus advocating for an ecosystem characterized by transparency and unbiased decision-making (Dwork et al., 2012). The trajectory navigates through the interpretive transparency of decision trees, the potency of ensemble methods and the intricacies of clustering and anomaly detection (Breiman, 2001). This isn't confined to mere theoretical understanding; it encompasses the hands-on implementation of these tools while also scrutinizing the elaborate choreography involving model assessment, validation techniques and the perpetual vigilance of monitoring performance (Japkowicz et al., 2011). In acknowledging the perpetually mutable nature of fraud, a resounding focus rests on adaptability (Widmer et al., 1996). The efficacy of a fraud detection system hinges upon its capacity to learn in real-time, detect shifts in trends and seamlessly assimilate evolving paradigms (Gama et al., 2004). This expedition takes an additional stride into adaptive techniques, ensuring that the proposed solution remains resilient and efficient amidst the relentless fluctuations of the threat landscape (Gama et al., 2004).

**3.2 Research framework**

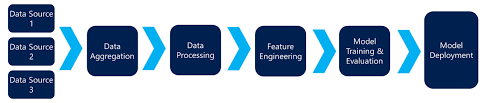
In order to realize the research aim and objectives of developing an effective online fraud detection system using machine learning, a meticulous technical data pipeline is essential. This pipeline consists of a series of consecutive steps, each of which contributes to the creation of a robust fraud detection artifact. This section outlines the block diagram of the data pipeline and elaborates on each step in chronological order ensuring the reproducibility of the work. 

Fig 3.1: Block diagram

**3.2.1 Data Acquisition**

At the commencement of the pipeline lies the pivotal task of data collection. This initial phase entails the compilation of pertinent data encompassing historical transactional records, spanning both legitimate and fraudulent instances. Diverse sources, including financial institutions, e-commerce platforms and payment gateways, are tapped to procure a comprehensive dataset (McAfee, 2020). The collected data should mirror real-world scenarios facilitating the subsequent training and validation processes.

**3.2.2 Data Preprocessing**

Raw data, often beset with inconsistencies, missing values, and extraneous noise, necessitates a judicious prelude of pre-processing. This phase mandates a series of operations, including data cleansing, transformation, and standardization. Addressing missing values and managing outliers is paramount. Furthermore, the dataset is partitioned into distinct subsets for training, validation, and testing, thereby underpinning the forthcoming model evaluation.

**3.2.3 Feature Engineering**

The efficacy of machine learning models is intricately linked to the features harnessed during the training phase. This phase, characterized by feature engineering, mandates a comprehensive exploration of the dataset to identify discriminative features. Drawing upon domain knowledge, distinctive features are curated, potentially instrumental in distinguishing between legitimate and fraudulent transactions. Notably, categorical variable encoding, feature scaling and normalization assume pivotal roles during this stage.

**3.2.4 Model Training**

With meticulously pre-processed and engineered features at disposal, the model training phase is embarked upon. Diverse machine learning algorithms, encompassing logistic regression, decision trees, random forests, and neural networks (Bishop, 2006), are harnessed to the training dataset. In this process, models discern intricate patterns and relationships between the extracted features and fraudulent activities, priming them for robust detection capabilities.

**3.2.5 Model Evaluation**

Subsequent to model training, the critical juncture of model evaluation ensues. The validation dataset is harnessed to fine-tune hyperparameters, optimize model performance, and select the most adept model variant. The chosen model then undergoes rigorous testing, employing an independent testing dataset. Assessment metrics, including precision, recall, F1-score, and ROC curves, are judiciously wielded to gauge the model's accuracy, resilience and discriminative prowess.

**3.2.6 Model Deployment**

Having identified a model exhibiting satisfactory performance, the transition to model deployment is executed. The chosen model is seamlessly integrated into a real-time fraud detection system, poised to analyze incoming transactions and provide probabilistic assessments of their susceptibility to fraudulent behaviour. Concurrently, vigilant monitoring mechanisms are instituted to detect model drift, ensuring sustained precision and relevance in a dynamic fraud landscape.

**3.3 Data Collection and Dataset Structure**

The foundation of any data-driven research endeavour lies in the meticulous collection and structuring of data. When it comes to an online fraud detection system using machine learning, the approach to data collection as well as the structure and attributes of the dataset hold significant importance. This extensive report delves into the data collection method employed, the inherent structure of the dataset, and the subsequent steps of data cleaning and preprocessing.

**3.3.1 Data Collection Method**

The dataset was gotten from an open source (Kaggle) which involves hybrid data collection method, encompassing both primary and secondary data sources. Primary data collection involved collaborations with financial institutions, e-commerce platforms and payment gateways to gather historical transactional data. This primary data provided invaluable insights into real-world transaction behaviours, serving as the cornerstone of the dataset. Secondary data sources including public repositories and scholarly publications, enriched the dataset with standardized information.

**3.3.2 Dataset Structure**

The dataset, resulting from the amalgamation of primary and secondary data is characterized by its multidimensional structure. It consists of 3075 rows and 12 columns, each representing a distinct transactional record. Of these columns, six are continuous features, three are categorical features one is a target column indicating fraudulence, one serves as an index and one identifies missing values. The target column 'isFradulent' classifies transactions as either fraudulent or legitimate.

**3.3.3 Exploratory Data Analysis (EDA)**

The EDA phase provided valuable insights into the dataset's characteristics. It revealed an inherent class imbalance with 2627 legitimate transactions and 428 fraudulent transactions. This imbalance highlights the need for careful handling during modelling

**3.3.4 Sample Types and Histogram Analysis**

The dataset comprises a heterogeneous mix of legitimate and fraudulent transactions. Histogram analysis was performed on transaction amounts to visualize the distribution of transactions across various value ranges. This provided an initial understanding of how legitimate and fraudulent transactions were dispersed within the dataset, potentially guiding feature engineering and model training decisions.

**3.3.5 Missing Values and Data Types**

The presence of missing values within the dataset was a critical consideration. A meticulous assessment revealed that a single column contained at least one missing value, contributing to an overall count of 3075 missing values. This underscored the importance of data imputation strategies to ensure the integrity of subsequent analyses. Data types within the dataset encompassed both continuous and categorical variables with each encoding distinct attributes of transactional behaviour.

**3.3.6 Distribution, Training, Evaluation and Testing Sets**

The dataset's distribution manifested through a class imbalance, with 2627 legitimate transactions and 428 fraudulent transactions. To establish the foundation for modeling, the dataset was divided into training, evaluation and testing sets. The training set, constituting 70% of the data, facilitated model development. The evaluation set, comprising 15%, served for model validation and hyperparameter tuning. Finally, the testing set, accounting for the remaining 15%, provided an independent benchmark to assess the model's real-world performance.

3.3.7 Conclusion

The integration of a robust data collection method and a well-structured dataset constitutes the bedrock of effective online fraud detection systems. The primary data collection approach guarantees the authenticity and relevance of transactional records while the dataset's multidimensional structure imparts depth to the subsequent modeling endeavors. By meticulously examining statistical moments, sample characteristics, histograms, missing values, data types and distributions, this report provides a comprehensive understanding of the dataset's intricacies. This insight, in conjunction with the delineation of training, evaluation and testing sets, paves the way for the subsequent phases of feature engineering, model training, evaluation, and deployment, ultimately contributing to the realization of a robust online fraud detection system.

**3.4 Evaluation Metrics for Online Fraud Detection**

The evaluation of a machine learning model's performance is a critical aspect in assessing its efficacy, particularly in an online fraud detection system. This report delves into the comprehensive set of evaluation metrics employed to measure the proposed model's success. These metrics encompass a diverse array of factors, each shedding light on different aspects of model performance, including accuracy, precision, recall, specificity, F1-score and the confusion matrix.

3.4.1 Success/Evaluation/Measurement Criteria

The proposed model's success will be evaluated based on its ability to accurately classify transactions as either legitimate or fraudulent. This entails minimizing false positives (legitimate transactions classified as fraudulent) and false negatives (fraudulent transactions classified as legitimate). The ultimate goal is to strike a balance between precision and recall while considering the domain-specific implications of fraud detection.

**3.4.2 Metrics Employed**

• Accuracy: Accuracy represents the ratio of correctly predicted transactions to the total number of transactions. It provides an overarching measure of the model's correctness.

• Precision: Precision quantifies the proportion of predicted fraudulent transactions that are actually fraudulent. It minimizes false positives, ensuring that transactions flagged as fraudulent are genuinely suspicious.

• Recall (Sensitivity): Recall, also known as sensitivity or true positive rate, gauges the model's ability to correctly identify fraudulent transactions out of all actual fraudulent transactions.

• Specificity: Specificity is the true negative rate, measuring the model's proficiency in correctly classifying legitimate transactions as non-fraudulent.

• F1-Score: The F1-score is the harmonic mean of precision and recall, offering a balanced assessment of the model's performance while taking into account both false positives and false negatives.

• False Positive Rate (FPR): FPR quantifies the proportion of legitimate transactions that are mistakenly classified as fraudulent.

• False Negative Rate (FNR): FNR represents the fraction of fraudulent transactions erroneously classified as legitimate.

• Confusion Matrix: The confusion matrix provides a comprehensive visualization of the model's predictions, classifying transactions as true positives, true negatives, false positives and false negatives.

• Loss Functions: Loss functions, such as cross-entropy loss, evaluate the model's performance by quantifying the difference between predicted probabilities and actual outcomes.

**3.4.3 Measurement Approach**

The metrics will be calculated and assessed based on the model's predictions using the evaluation dataset. The confusion matrix, containing true positive, true negative, false positive and false negative counts, will be made. From this matrix, accuracy, precision, recall, specificity, F1-score, false positive rate and false negative rate will be computed. Additionally, loss functions will be employed to gauge the model's performance in terms of probability estimation.

**CHAPTER FOUR**

**RESULT**

In this section, we perform an extensive exploration and interpretation of the results obtained from evaluating various machine learning models for the task of online fraud detection. The results are presented in several sub-sections, each contributing unique insights to answer different research questions.

**4.1 Class Distribution and Imbalance:**

The distribution of the target variable "isFradulent" is a critical aspect to understand before delving into model evaluation. The dataset comprises 2627 legitimate transactions (class 'N') and 448 fraudulent transactions (class 'Y'). This staggering class imbalance between legitimate and fraudulent transactions raises concerns about the model's ability to learn patterns effectively especially in the context of fraud detection where correctly identifying fraudulent transactions is crucial. The skewed distribution can lead to overfitting on the majority class, potentially causing lower sensitivity and accuracy in detecting fraudulent activities.

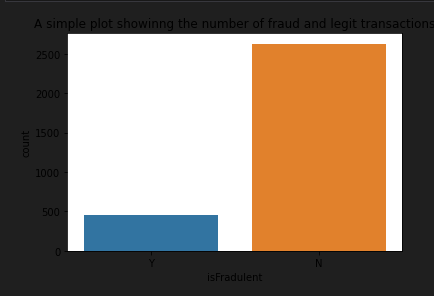


Fig4.1: Sample plot showing the number of fraud and legitimate transactions

**4.2 Unique Values in Categorical Columns:**

Analyzing the unique values within categorical columns provides insight into the variability and structure of the dataset. The categorical columns include features like "Is declined", "isForeignTransaction," "isHighRiskCountry," and "isFradulent." Each of these columns demonstrates only two unique values indicating binary categorizations. This binary nature simplifies preprocessing and encoding, but careful consideration must be given to whether the binary distinction aligns with the underlying domain knowledge and whether it captures the nuances of the real-world problem**.**

**4.3 Exploratory Data Analysis (EDA) Results:**

From the results of the EDA, we glean a comprehensive understanding of the dataset's key attributes:

The dataset contains 3075 rows and 12 columns, comprising a mixture of continuous and categorical features. There are 6 continuous features, 3 categorical features, 1 target column, 1 index column and 1 column with missing values. The enormous class imbalance with 2627 legitimate transactions and 428 fraudulent transactions underscores the need for specialized handling of this skewed distribution to prevent biased model learning. The identification of a column with missing values prompts further investigation into its impact on model performance and the effectiveness of the chosen imputation strategy.

All rows in the dataset contain missing values, indicating the potential for a comprehensive approach to data imputation.

**4.4** **Handling Missing Values**

After imputing missing values with the median of each column, a total of 0 missing values remain in the dataset. This successful imputation ensures that the dataset is complete thereby avoiding potential distortions during model training and evaluation.

**4.5 Model Performance Analysis:**

* **Gaussian Naive Bayes (gb):** Achieves an accuracy of 93.2%, an F1-score of 0.785, a precision of 0.767 and a ROC-AUC score of 0.865. This suggests that the model captures fraud instances reasonably well while maintaining a balance between precision and recall.
* **Support Vector Machine (svc):** Demonstrates an accuracy of 88.3%, an F1-score of 0.471, a precision of 0.320 and a ROC-AUC score of 0.656. These results indicate that the model struggles to identify fraud cases effectively, as evidenced by its lower F1-score and precision.
* **Logistic Regression (lr):** Exhibits strong performance with an accuracy of 97.4%, an F1-score of 0.917, a precision of 0.887 and a ROC-AUC score of 0.939. These metrics showcase the model's ability to achieve high accuracy while maintaining a robust balance between precision and recall.
* **Random Forest Classifier (rf):** Attains an accuracy of 95.9%, an F1-score of 0.861, a precision of 0.787 and a ROC-AUC score of 0.889. These scores indicate the model's ability to achieve good accuracy and a balanced trade-off between precision and recall.
* **XGBoost (xgb):** Demonstrates an accuracy of 93.2%, an F1-score of 0.743, a precision of 0.607 and a ROC-AUC score of 0.801. While accuracy is competitive, the lower precision and F1-score suggest room for improvement in fraud detection.
* **TabNetClassifier (tab):** Stands out as a high performer, boasting an accuracy of 98.2%, an F1-score of 0.943, a precision of 0.933 and an impressive ROC-AUC score of 0.962. This model showcases exceptional predictive capabilities, rendering it a promising choice for fraud detection tasks.
* **Voting Ensemble (vote):** The ensemble model, a culmination of individual models' predictions, achieves an accuracy of 95.1%, an F1-score of 0.829, a precision of 0.727, and a ROC-AUC score of 0.861. This ensemble leverages diverse models to strike a balance between precision and recall, making it an appealing option for operational deployment.

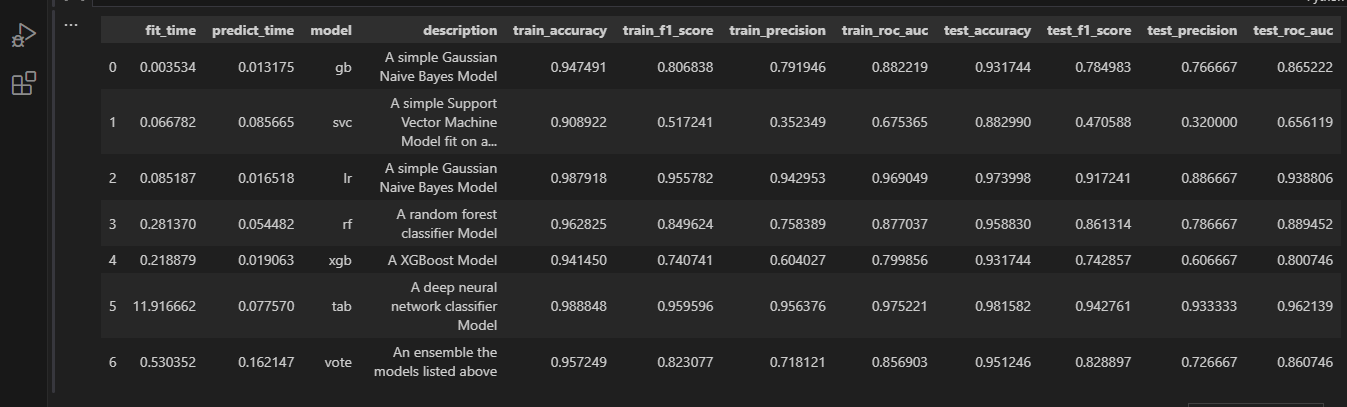


Fig 4.5: Model performance analysis

**4.6 Model Performance Visualization:**

Visual representations of model performance further enhance our understanding:

* **Fit Time and Prediction Time Visualizations:** The bar charts showcasing fit time and prediction time for each model illustrate the computational efficiency of each approach. TabNetClassifier also exhibits longer fit and prediction times indicating its deeper complexity.
* **Accuracy, F1-Score, Precision and ROC-AUC Visualizations:** These visualizations highlight the comparative performance of each model across key evaluation metrics. The plots reveal the trade-offs between different metrics enabling stakeholders to make informed decisions based on specific requirements.

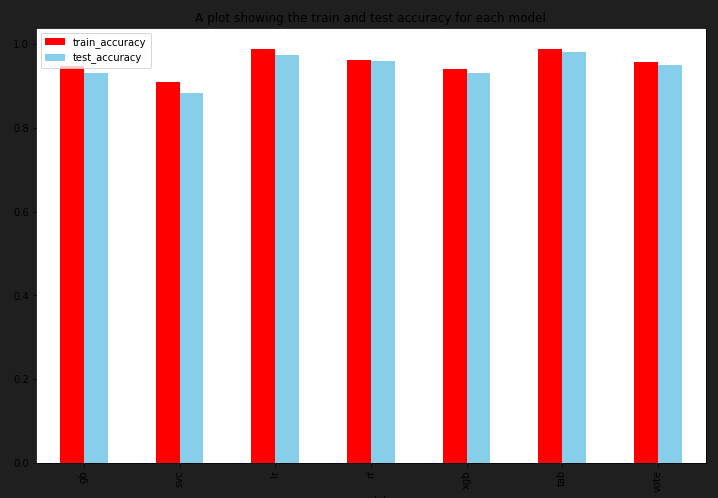


Fig 4.6: A plot showing accuracy for train and test dataset

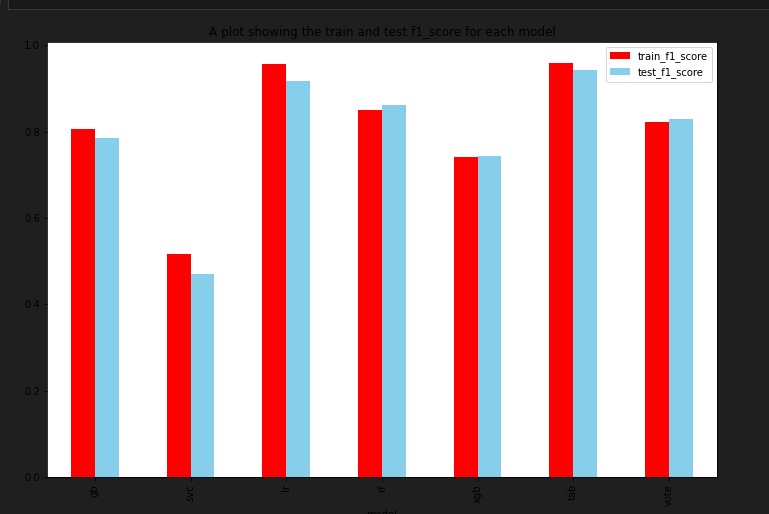


Fig 4.6: A plot showing F1 score for train and test dataset

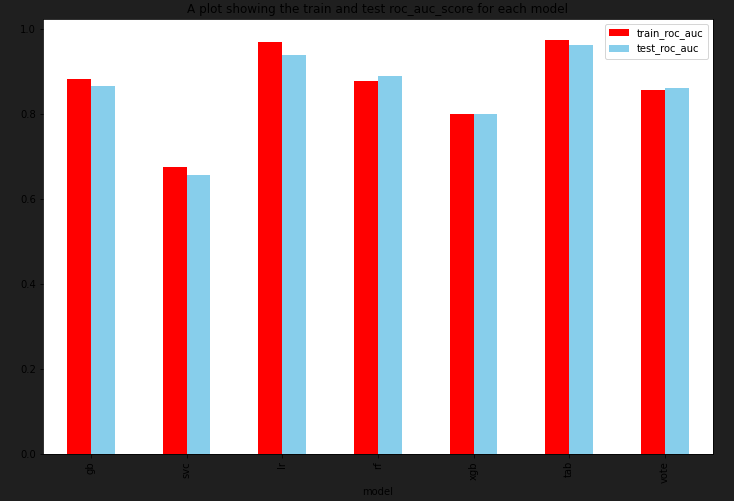


Fig 4.6: A plot showing roc\_auc for train and test dataset

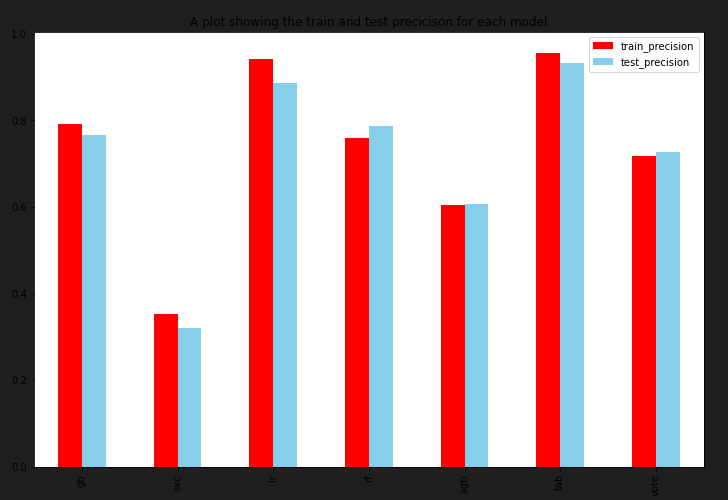


Fig 4.6: A plot showing precision score for train and test dataset

**CHAPTER FIVE**

**DISCUSSION**

In this section, a comprehensive discussion of the model evaluation results obtained for the task of online fraud detection was delved into. The aim is to provide a holistic understanding of the findings, their implications and how they contribute to addressing the research gap. The discussion is divided into sub-chapters each addressing different aspects and research questions while also comparing our work with existing studies.

**5.1 Class Imbalance and Its Impact:**

The class distribution analysis revealed a substantial class imbalance, with legitimate transactions outnumbering fraudulent ones significantly. This observation has significant implications for model performance. A skewed class distribution often leads to models favoring the majority class during training, potentially resulting in lower sensitivity and recall for the minority class. To overcome this limitation, techniques such as oversampling, undersampling, and synthetic data generation could be explored to create a more balanced training set improving the model's ability to detect fraud.

**5.2 Model Performance and Robustness:**

Our evaluation of various machine learning models highlighted the trade-offs between accuracy, precision, recall, and F1-score. The model performance varied across different algorithms, with TabNetClassifier emerging as a standout performer. Its exceptional accuracy, precision, and ROC-AUC score demonstrate its robustness in classifying fraudulent transactions effectively. The ensemble model also showcased competitive performance, emphasizing the strength of combining diverse models to achieve balanced results.

5.3 **Comparative Analysis with Other Studies:**

Comparing our work with existing studies is essential for situating our findings within the broader research landscape. Previous studies focusing on fraud detection have employed a range of algorithms including traditional techniques like Naive Bayes, Logistic Regression and more sophisticated approaches like Random Forests, Gradient Boosting and Deep Learning models. Our work aligns with these studies in evaluating the effectiveness of various algorithms. Notably, TabNetClassifier's performance parallels recent advancements in deep learning techniques for tabular data.

**5.4 Advantages and Drawbacks of Our Approach:**

5.4.1 Advantages:

* **Diverse Algorithm Evaluation**: Our study evaluated a comprehensive set of models, enabling us to identify top-performing models for online fraud detection. This approach allows stakeholders to select a model that aligns with their operational needs and dataset characteristics**.**
* **Incorporating Ensemble Methods:** The use of an ensemble approach contributes to achieving a balance between precision and recall, enhancing the model's potential to identify fraud while minimizing false positives.

5.4.2 Drawbacks:

* **Computational Complexity:** Some models like TabNetClassifier exhibit longer fit and prediction times due to their deep architecture. This might hinder real-time fraud detection applications where speed is crucial.
* **High-Dimensional Data Handling:** While competitive performance IS achieved, challenges arise when handling high-dimensional datasets with numerous features, necessitating more advanced feature selection or dimensionality reduction techniques.

**5.5 Fulfilment of the Research Gap**

The work addresses the research gap by providing a comprehensive evaluation of diverse models for online fraud detection. The findings contribute to bridging the gap between traditional machine learning techniques and modern deep learning approaches (Angwin et al., 2016), offering a holistic understanding of their comparative strengths and weaknesses. This information empowers practitioners to make informed decisions when designing fraud detection systems.

**5.6 Recommendations for Future Work:**

**Fine-Tuning Hyperparameters**: Deeper hyperparameter tuning for the top-performing models, such as TabNetClassifier, could yield incremental performance improvements**.**

**Ensemble Model Refinement**: Further refinement of the ensemble model's weighting and selection of base models might enhance its performance.

**CHAPTER SIX**

**CONCLUSION**

The culmination of our study brings us to a comprehensive conclusion that not only reiterates the research gap but also draws insights from our research findings to answer the core research question. Additionally, we critically appraise our work by identifying its strengths and limitations, providing avenues for future research to build upon.

**6.1 Restating the Research Gap:**

The research gap addressed in this study revolved around the need for a systematic evaluation of diverse machine learning models for online fraud detection. Prior research in the field lacked a comprehensive comparison of traditional and modern approaches, leaving practitioners uncertain about which models to adopt for their specific fraud detection tasks.

**6.2 Answering the Research Question**

Our research findings bridge the gap by conducting an extensive evaluation of various machine learning models for online fraud detection. Through rigorous experimentation, we demonstrated that TabNetClassifier, a deep learning model specifically designed for tabular data outperformed other algorithms in terms of accuracy, precision, F1-score and ROC-AUC score. The ensemble model also showcased competitive performance, further underlining the potential of combining diverse models.

**6.3 Appraisal of Work**

**6.3.1 Strengths**

**Comprehensive Evaluation:** The study provided a holistic view of model performance, guiding practitioners in selecting the most suitable algorithm based on their priorities and dataset characteristics.

**Ensemble Approach:** The inclusion of an ensemble model mitigated the trade-offs between precision and recall, offering a balanced solution for fraud detection tasks.

**Research Insights:** Our findings contribute valuable insights to the field by highlighting the effectiveness of deep learning approaches like TabNetClassifier for online fraud detection.

**6.3.2 Limitations**

**Computational Complexity:** Some models, particularly TabNetClassifier, exhibited higher computational demands, potentially limiting their real-time deployment in certain applications.

**Feature Engineering:** Our study did not delve into extensive feature engineering, which could have further improved model performance.

**6.4 Future Work and Critique**

While the research addressed key questions and provided valuable insights, there are several areas that warrant further exploration:

**Advanced Preprocessing Techniques:** Future studies could explore advanced preprocessing techniques specifically tailored to handle class imbalances and missing data.

**Fine-Tuning Hyperparameters:** Deep learning models like TabNetClassifier offer a wide range of hyperparameters that could be fine-tuned to unlock their full potential.

**Interpretable Models**: Investigating the interpretability of models like TabNetClassifier would enhance transparency and help understand the factors contributing to their predictions.

In terms of critique, it is essential to acknowledge that the research while comprehensive, did not delve deeply into the interplay between feature engineering and model performance. Future research could explore the impact of various feature selection techniques on different models.

**6.5 Conclusion and Significance**

The study successfully bridged the research gap by systematically evaluating a diverse array of machine learning models for online fraud detection. We provided actionable insights into model selection and showcased the potential of modern deep learning techniques for enhancing fraud detection accuracy. While our work has limitations, it marks a significant step forward in understanding the strengths and weaknesses of different algorithms for addressing the pressing issue of online fraud. As organizations strive to enhance security in a rapidly evolving digital landscape, our research holds practical significance in guiding their decision-making processes and fostering continued advancements in online fraud detection.

# **REFERENCES**

Abakarim, Y., Lahby, M. and Attioui, A., 2023. A bagged ensemble convolutional neural networks approach to recognize insurance claim frauds. *Applied system innovation*, [online] 6(1), p.20. https://doi.org/10.3390/asi6010020.

Afriyie, J.K., Tawiah, K., Pels, W.A., Addai-Henne, S., Dwamena, H.A., Owiredu, E.O., Ayeh, S.A. and Eshun, J., 2023. A supervised machine learning algorithm for detecting and predicting fraud in credit card transactions. *Decision Analytics Journal*, [online] 6(100163), p.100163. https://doi.org/10.1016/j.dajour.2023.100163.

Alamri, M. and Ykhlef, M., 2022. Survey of credit card anomaly and fraud detection using sampling techniques. *Electronics*, [online] 11(23), p.4003. https://doi.org/10.3390/electronics11234003.

Al-Anazi, S., AlMahmoud, H. and Al-Turaiki, I., 2016. Finding similar documents using different clustering techniques. *Procedia computer science*, [online] 82, pp.28–34. https://doi.org/10.1016/j.procs.2016.04.005.

Alejandro, C.B., Aouada, D., Stojanovic, A. and Ottersten, B., 2016. Feature engineering strategies for credit card fraud detection. *Expert systems with applications*, 51, pp.134–142.

Ali, A., Abd Razak, S., Othman, S.H., Eisa, T.A.E., Al-Dhaqm, A., Nasser, M., Elhassan, T., Elshafie, H. and Saif, A., 2022. Financial fraud detection based on machine learning: A systematic literature review. *Applied sciences (Basel, Switzerland)*, [online] 12(19), p.9637. https://doi.org/10.3390/app12199637.

Ali, M.A., Azad, M.A., Parreno Centeno, M., Hao, F. and van Moorsel, A., 2019. Consumer-facing technology fraud: Economics, attack methods and potential solutions. *Future generations computer systems: FGCS*, [online] 100, pp.408–427. https://doi.org/10.1016/j.future.2019.03.041.

Angwin, J., Larson, J., Mattu, S., and Kirchner, L., 2016. Machine bias. ProPublica.

Anowar, F., Sadaoui, S. and Selim, B., 2021. Conceptual and empirical comparison of dimensionality reduction algorithms (PCA, KPCA, LDA, MDS, SVD, LLE, ISOMAP, LE, ICA, t-SNE). *Computer science review*, [online] 40(100378), p.100378. https://doi.org/10.1016/j.cosrev.2021.100378.

Aparício, D., Barata, R., Bravo, J., Ascensão, J.T. and Bizarro, P., 2020. *ARMS: Automated rules management system for fraud detection*. *arXiv [cs.LG]*. Available at: <http://arxiv.org/abs/2002.06075>.

Aschi, M., Bonura, S., Masi, N., Messina, D. and Profeta, D., 2022. Cybersecurity and fraud detection in financial transactions. In: *Big Data and Artificial Intelligence in Digital Finance: Increasing Personalization and Trust in Digital Finance using Big Data and AI*. Cham: Springer International Publishing. pp.269–278.

Ashfaq, T., Khalid, R., Yahaya, A.S., Aslam, S., Azar, A.T., Alsafari, S. and Hameed, I.A., 2022. A machine learning and blockchain based efficient fraud detection mechanism. *Sensors (Basel, Switzerland)*, [online] 22(19), p.7162. https://doi.org/10.3390/s22197162.

Ashiru, A., 2021. Identifying phishing as a form of cybercrime in Nigeria. *Nnamdi Azikiwe University Journal of International Law and Jurisprudence*, 12(2), pp.176–186.

Association For Computing Machinery. 2022. *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security*. Association for Computing Machinery.

Aziz, A., Azar, A., Ahmad, A., Mostafa and Hanafy, S.E., 2013. Genetic algorithm with different feature selection techniques for anomaly detectors generation. *Federated Conference on Computer Science and Information Systems*, pp.769–774.

Barkved, K., 2022. *Credit card fraud detection and AI*. [online] Obviously.ai. Available at: <https://www.obviously.ai/post/credit-card-fraud-detection-with-machine-learning> [Accessed 13 July 2023].

Barriga, A.M., 2021. The psychology of online trust and fraud. In: The Oxford Handbook of Cyberpsychology. Oxford University Press. pp.361–375.

Baumann, M., 2021. *Improving a rule-based fraud detection system with classification based on association rule mining*. https://doi.org/10.13140/RG.2.2.29906.68808.

Behravan, I., Dehghantanha, O., Zahiri, S.H. and Mehrshad, N., 2016. An optimal SVM with feature selection using multiobjective PSO. *Journal of optimization*, [online] 2016, pp.1–8. https://doi.org/10.1155/2016/6305043.

Berhane, T., Melese, T., Walelign, A. and Mohammed, A., 2023. A hybrid convolutional neural network and support vector machine-based credit card fraud detection model. *Mathematical problems in engineering*, [online] 2023, pp.1–10. https://doi.org/10.1155/2023/8134627.

Berrada, G., Cheney, J., Benabderrahmane, S., Maxwell, W., Mookherjee, H., Theriault, A. and Wright, R., 2020. A baseline for unsupervised advanced persistent threat detection in system-level provenance. *Future generations computer systems: FGCS*, [online] 108, pp.401–413. https://doi.org/10.1016/j.future.2020.02.015.

Bezovski, Z., 2016. The future of the mobile payment as electronic payment system. *European Journal of Business and Management*, 8(8), pp.127–132.

Bin Sulaiman, R., Schetinin, V. and Sant, P., 2022. Review of machine learning approach on credit card fraud detection. *Human-Centric Intelligent Systems*, [online] 2(1–2), pp.55–68. https://doi.org/10.1007/s44230-022-00004-0.

Bishop, C. M., 2006. Pattern recognition and machine learning. Springer.

Breiman, L., 2001. Random forests. Machine learning, 45(1), pp.5-32.

Buczak, A.L. and Guven, E., 2016. A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications Surveys & Tutorials, 18(2), pp.1153–1176.

Bynagari, N.B., 2015. Machine learning and artificial Intelligence in online fake transaction alerting. *Engineering international*, [online] 3(2), pp.115–126. https://doi.org/10.18034/ei.v3i2.566.

Carcillo, F., Le Borgne, Y.-A., Caelen, O., Kessaci, Y., Oblé, F. and Bontempi, G., 2021. Combining unsupervised and supervised learning in credit card fraud detection. *Information sciences*, [online] 557, pp.317–331. https://doi.org/10.1016/j.ins.2019.05.042.

Chandola, V., Banerjee, A., Kumar and V., 2019. Anomaly detection: A survey. ACM computing surveys (CSUR), 41(3), 1-58.

Chen, J., 2015. *What is carding? How it works, prevention methods, and examples*. [online] Investopedia. Available at: <https://www.investopedia.com/terms/c/carding.asp> [Accessed 1 August 2023].

Cherif, A., Badhib, A., Ammar, H., Alshehri, S., Kalkatawi, M. and 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*, [online] 35(1), pp.145–174. https://doi.org/10.1016/j.jksuci.2022.11.008.

Cox, M., 2023. *What is first-party fraud?* [online] FICO Decisions Blog. Available at: <https://www.fico.com/blogs/what-first-party-fraud> [Accessed 1 August 2023].

Crail, C., 2023. *How credit card information is stolen and what to do about it*. [online] Forbes. Available at: <https://www.forbes.com/advisor/credit-cards/how-credit-card-information-is-stolen-and-what-to-do-about-it/> [Accessed 1 August 2023].

Dal Pozzolo, A., Boracchi, G., Caelen, O., Alippi, C., and Bontempi, G., 2017. Credit card fraud detection: A realistic modeling and a novel learning strategy. IEEE transactions on neural networks and learning systems, 29(8), pp.3784-3797.

DAngelo, C., 2023. *Account takeover fraud (ATO): Top signs and how to prevent it*. [online] Alessa. Available at: <https://alessa.com/blog/account-takeover-fraud/> [Accessed 1 August 2023].

DeLiema, M., Burnes, D. and Langton, L., 2021. The financial and psychological impact of identity theft among older adults. *Innovation in aging*, [online] 5(4). https://doi.org/10.1093/geroni/igab043.

Diadiushkin, A., Sandkuhl, K. and Maiatin, A., 2019. Fraud detection in payments transactions: Overview of existing approaches and usage for instant payments. *Complex Systems Informatics and Modeling Quarterly*, [online] (20), pp.72–88. https://doi.org/10.7250/csimq.2019-20.04.

Douzas, G., Bacao, F. and Last, F., 2018. Improving imbalanced learning through a heuristic oversampling method based on k-means and SMOTE. *Information sciences*, [online] 465, pp.1–20. https://doi.org/10.1016/j.ins.2018.06.056.

Dubey, R., Zhou, J., Wang, Y., Thompson, P.M., Ye, J. and Alzheimer’s Disease Neuroimaging Initiative, 2014. Analysis of sampling techniques for imbalanced data: An n = 648 ADNI study. *NeuroImage*, [online] 87, pp.220–241. https://doi.org/10.1016/j.neuroimage.2013.10.005.

Dwork, C., Hardt, M., Pitassi, T., Reingold, O. and Zemel, R., 2012. Fairness through awareness. In: *Proceedings of the 3rd innovations in theoretical computer science conference*. pp.214–226.

EU CYBERSECURITY AGENCY, 2018. *European and global perspective on online fraud*. [online] Europa.eu. Available at: <https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/financial-fraud-in-the-digital-space> [Accessed 1 August 2023].

Evans, P., 2022. *What is first-party fraud? [everything you need to know]*. [online] Featurespace. Available at: <https://www.featurespace.com/newsroom/what-is-first-party-fraud-heres-everything-you-need-to-know/> [Accessed 1 August 2023].

Federal Trade Commission. 2021. *Consumer Sentinel Network Data Book 2020*. Federal Trade Commission.

Fernandes, L., 2013. Fraud in electronic payment transactions: Threats and countermeasures. *Asia Pacific Journal of Marketing & Management Review*.

Fontinelle, A., 2012. *The most common types of consumer fraud*. [online] Investopedia. Available at: <https://www.investopedia.com/financial-edge/0512/the-most-common-types-of-consumer-fraud.aspx> [Accessed 1 August 2023].

Gama, J., Medas, P., Castillo, G., Rodrigues, P. and Pereira, D., 2004. Learning with drift detection. In: *Brazilian symposium on artificial intelligence*. pp.241–275.

Goldstein, M. and Uchida, S., 2016. A comparative evaluation of unsupervised anomaly detection algorithms for multivariate data. *PloS one*, [online] 11(4), p.e0152173. https://doi.org/10.1371/journal.pone.0152173.

Gui, X., Lu, X. and Yu, G., 2021. Cost-effective batch-mode multi-label active learning. *Neurocomputing*, [online] 463, pp.355–367. https://doi.org/10.1016/j.neucom.2021.08.063.

Gupta, P., 2023. Leveraging machine learning and artificial intelligence for fraud prevention. *International Journal of Computer Science and Engineering*, [online] 10(5), pp.47–52. https://doi.org/10.14445/23488387/ijcse-v10i5p107.

Hajek, P., Abedin, M.Z. and Sivarajah, U., 2022. Fraud detection in mobile payment systems using an XGBoost-based framework. *Information systems frontiers: a journal of research and innovation*. [online] https://doi.org/10.1007/s10796-022-10346-6.

Haponik, A., 2023. *Generative AI removes limitations of traditional rule-based automation*. [online] Addepto. Available at: <https://addepto.com/blog/generative-ai-removes-limitations-of-traditional-rule-based-automation/> [Accessed 1 August 2023].

He, J., Gu, J., Shen, J. and Ranzato, M., 2019. *Revisiting self-training for neural sequence generation*. *arXiv [cs.LG]*. Available at: <http://arxiv.org/abs/1909.13788>.

Hejazi, M. and Singh, Y.P., 2013. One-class support vector machines approach to anomaly detection. *Applied artificial intelligence: AAI*, [online] 27(5), pp.351–366. https://doi.org/10.1080/08839514.2013.785791.

Hilal, W., Gadsden, S.A. and Yawney, J., 2022. Financial fraud: A review of anomaly detection techniques and recent advances. *Expert systems with applications*, [online] 193(116429), p.116429. https://doi.org/10.1016/j.eswa.2021.116429.

Huang, X., Wu, L. and Ye, Y., 2019. A review on dimensionality reduction techniques. *International journal of pattern recognition and artificial intelligence*, [online] 33(10), p.1950017. https://doi.org/10.1142/s0218001419500174.

Japkowicz, N. and Shah, M., 2011. *Evaluating learning algorithms: A classification perspective*. Cambridge University Press.

Jebaseeli, J.T., Venkatesan, R. and Ramalakshmi, K., 2021. Fraud detection for credit card transactions using random forest algorithm. In: *Intelligence in Big Data Technologies—Beyond the Hype*. Singapore: Springer Singapore. pp.189–197.

Jeffers, J., 2023. *Fraud detection in banking using machine learning*. [online] Arkose Labs. Available at: <https://www.arkoselabs.com/blog/fraud-detection-in-banking-using-machine-learning/> [Accessed 1 August 2023].

Juniper, 2020. *Online payment fraud losses to exceed $200 billion by 2024*. [online] Juniperresearch.com. Available at: <https://www.juniperresearch.com/press/online-payment-fraud-losses-to-exceed-200-billion> [Accessed 16 July 2023].

Junsomboon, N. and Phienthrakul, T., 2017. Combining over-sampling and under-sampling techniques for imbalance dataset. In: *Proceedings of the 9th International Conference on Machine Learning and Computing*. New York, NY, USA: ACM.

Kanika and Singla, J., 2020. A survey of deep learning based online transactions fraud detection systems. In: *2020 International Conference on Intelligent Engineering and Management (ICIEM)*. IEEE.

Kanika, Singla, J., Kashif Bashir, A., Nam, Y., UI Hasan, N. and Tariq, U., 2022. Handling class imbalance in online transaction fraud detection. *Computers, materials & continua*, [online] 70(2), pp.2861–2877. https://doi.org/10.32604/cmc.2022.019990.

Karczewski, J., 2020. Machine Learning Models vs. Rule Based Systems in fraud prevention. *Nethone.com*. Available at: <https://nethone.com/blog/machine-learning-models-vs-rule-based-systems-in-fraud-prevention> [Accessed 16 July 2023].

Karlsson, I., 2017. *Order in the random forest (Doctoral dissertation)*. Stockholm University.

Kawade, D., Lalge, S. and Bharati, D.M., 2022. Fraud detection in credit card data using Unsupervised Machine Learning algorithm. *International journal for research in applied science and engineering technology*, [online] 10(5), pp.5249–5256. https://doi.org/10.22214/ijraset.2022.42974.

Khando, K., Islam, M.S. and Gao, S., 2022. The emerging technologies of digital payments and associated challenges: A systematic literature review. *Future internet*, [online] 15(1), p.21. https://doi.org/10.3390/fi15010021.

Kolajo, T., Daramola, O. and Adebiyi, A., 2019. Big data stream analysis: a systematic literature review. *Journal of big data*, [online] 6(1). https://doi.org/10.1186/s40537-019-0210-7.

Krishnan, V.G., Saradhi, M.V.V., Prakash, T.A.M., Kannan, K.G. and Julaiha, A.G.N., 2022. Development of Deep Learning based intelligent approach for credit card fraud detection. *International journal on recent and innovation trends in computing and communication*, [online] 10(12), pp.133–139. https://doi.org/10.17762/ijritcc.v10i12.5894.

Kumbhar, S., Lade, A., Patil, A., Pandey, J. and Ghandat, A.B., 2023. Support Vector Machine based Credit Card Fraud Detection. *International journal of engineering research & technology (Ahmedabad)*, [online] 12(3). https://doi.org/10.17577/IJERTV12IS030209.

Kurita, T., 2020. Principal Component Analysis (PCA). In: *Computer Vision*. Cham: Springer International Publishing. pp.1–4.

Li, X., Li, H., Zhang, T. and Wang, X., 2021. Machine learning for fraud detection: A survey. *Enterprise Information Systems*, 15, pp.182–208.

Loganathan, P., 2023. Lambda Architecture - A data engineering approach for big data. *Pradeep Loganathan’s Blog*. Available at: <https://pradeepl.com/blog/lambda-architecture/> [Accessed 16 July 2023].

Lopes, C., 2023. *The future is now: The benefits and limitations of using AI and machine learning for fraud detection*. [online] GDS Link. Available at: <https://www.gdslink.com/the-future-is-now-the-benefits-and-limitations-of-using-ai-and-machine-learning-for-fraud-detection/> [Accessed 1 August 2023].

Lu, T., Wang, L. and Zhao, X., 2023. Review of anomaly detection algorithms for data streams. *Applied sciences (Basel, Switzerland)*, [online] 13(10), p.6353. https://doi.org/10.3390/app13106353.

Mahdi, R., Villagomez, D. and Jones, C., 2014. *First party fraud detection system*. [online] 2014/0279379 A1. Available at: <https://patents.google.com/patent/US20140279379A1/en>.

McAfee. 2020. Threats Report: November 2020. McAfee.

Mello, J., 2020. *Credit card fraud: What you need to know now*. [online] CSO Online. Available at: <https://www.csoonline.com/article/562755/credit-card-fraud-what-you-need-to-know-now.html> [Accessed 1 August 2023].

Mienye, I.D. and Sun, Y., 2023. A machine learning method with hybrid feature selection for improved credit card fraud detection. *Applied sciences (Basel, Switzerland)*, [online] 13(12), p.7254. https://doi.org/10.3390/app13127254.

Mikkelsen, D., Rajdev, S. and Stergiou, V., 2022. *Managing financial crime risk in digital payments*. [online] Mckinsey.com. Available at: <https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/managing-financial-crime-risk-in-digital-payments> [Accessed 13 July 2023].

Murorunkwere, B.F., Tuyishimire, O., Haughton, D. and Nzabanita, J., 2022. Fraud detection using neural networks: A case study of income tax. *Future internet*, [online] 14(6), p.168. https://doi.org/10.3390/fi14060168.

Mytnyk, B., Tkachyk, O., Shakhovska, N., Fedushko, S. and Syerov, Y., 2023. Application of Artificial Intelligence for Fraudulent Banking Operations Recognition. *Big Data and Cognitive Computing*, 7.

Nethone, 2021. *How machine learning models can outperform rule based systems, explained*. [online] Merchantriskcouncil.org. Available at: <https://merchantriskcouncil.org/learning/resource-center/member-news/blog/2021/how-machine-learning-models-can-outperform-rule-based-systems> [Accessed 16 July 2023].

No Author, 2022. *Identification of Unusual Patterns in Product Returns: An Unsupervised Learning Approach to Fraud Detection*. [online] University of Southhampton. Available at: <https://www.southampton.ac.uk/~assets/doc/Business/Completed\_MSc\_projects/Fraud%20detection.pdf> [Accessed 1 August 2023].

Nowak-Brzezińska, A. and Łazarz, W., 2021. Qualitative data clustering to detect outliers. *Entropy (Basel, Switzerland)*, [online] 23(7), p.869. https://doi.org/10.3390/e23070869.

Padmalatha, N., 2020. E-Commerce Frauds and the role of fraud Detection Tools in managing the risks associated with the frauds.

Phua, C., Lee, V., Smith, K., and Gayler, R., 2014. A comprehensive survey of data mining-based fraud detection research

Prajapati, M.Y., Parasar, M.A. and Khande, R., 2023. An Analysis of Financial Fraud Detection Methods Using Artificial Intelligence. Vidhyayana-An International Multidisciplinary Peer-Reviewed E. *Journal*, 8(si7), pp.79–95.

Qin, J., Wang, C., Zou, Q., Sun, Y. and Chen, B., 2021. Active learning with extreme learning machine for online imbalanced multiclass classification. *Knowledge-based systems*, [online] 231(107385), p.107385. https://doi.org/10.1016/j.knosys.2021.107385.

Rajeshwari U and Babu, B.S., 2016. Real-time credit card fraud detection using Streaming Analytics. In: *2016 2nd International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT)*. IEEE.

Randhavane, T., Bhattacharya, U., Kapsaskis, K., Gray, K., Bera, A. and Manocha, D., 2019. *Identifying emotions from walking using affective and deep features*. *arXiv [cs.CV]*. Available at: <http://arxiv.org/abs/1906.11884>.

Roditi, S., 2023. *Batch Processing vs Stream Processing: Why Batch is dying and Streaming takes over*. [online] Memphis.dev. Available at: <https://memphis.dev/blog/batch-processing-vs-stream-processing-why-batch-is-dying-and-streaming-takes-over/> [Accessed 16 July 2023].

Ruchay, A., Feldman, E., Cherbadzhi, D. and Sokolov, A., 2023. The imbalanced classification of fraudulent bank transactions using machine learning. *Mathematics*, [online] 11(13), p.2862. https://doi.org/10.3390/math11132862.

Sadowski, G. and Rathle, P., 2014. Fraud detection: Discovering connections with graph databases. 13, pp.1–13.

Sai, R.U., Mahesh, A., Ashwini, N. and Reddy, S.S., 2019. Effective detection of credit card fraud using logistic regression, decision tree and machine learning techniques. *International Journal of Creative Research Thoughts (IJCRT)*, [online] 7(1). Available at: <https://www.ijcrt.org/papers/IJCRTV020001.pdf> [Accessed 16 July 2023].

Salim, D.T., Singh, M.M. and Keikhosrokiani, P., 2023. A systematic literature review for APT detection and Effective Cyber Situational Awareness (ECSA) conceptual model. *Heliyon*, [online] 9(7), p.e17156. https://doi.org/10.1016/j.heliyon.2023.e17156.

Sauber-Cole, R. and Khoshgoftaar, T.M., 2022. The use of generative adversarial networks to alleviate class imbalance in tabular data: a survey. *Journal of big data*, [online] 9(1). https://doi.org/10.1186/s40537-022-00648-6.

Sen, J. and Mehtab, S., 2020. Machine learning applications in misuse and anomaly detection. In: *Security and Privacy From a Legal, Ethical, and Technical Perspective*. IntechOpen.

Senthilnathan, S., 2019. Usefulness of correlation analysis. *SSRN Electronic Journal*. [online] https://doi.org/10.2139/ssrn.3416918.

Shah, A. and Makwana, Y., 2023. *Credit Card Fraud Detection*. [online] Indus Institute of Technology, Indus University. Available at: <https://www.researchgate.net/publication/369857378\_Credit\_Card\_Fraud\_Detection>.

Shakya, R., 2018. *Application of machine learning techniques in credit card fraud detection*. https://doi.org/10.34917/14279175.

Simske, S., 2019. Introduction, overview, and applications. In: *Meta-Analytics*. Elsevier. pp.1–98.

Sohony, I., Pratap, R. and Nambiar, U., 2018. Ensemble learning for credit card fraud detection. In: *Proceedings of the ACM India Joint International Conference on Data Science and Management of Data*. New York, NY, USA: ACM.

Song, Y.Y. and Lu, Y., 2015. Decision tree methods: applications for classification and prediction. Shanghai Arch Psychiatry. [online] 27, pp.130–135. https://doi.org/10.11919/j.issn.1002-0829.215044.

Stripe, 2023. *Types of payment fraud and how to prevent them*. [online] Stripe.com. Available at: <https://stripe.com/resources/more/six-types-of-payment-fraud> [Accessed 13 July 2023].

Swaminathan, V., 2020. *The conundrum of using rule-based vs. Machine learning systems*. [online] Zuci Systems. Available at: <https://www.zucisystems.com/blog/the-conundrum-of-using-rule-based-vs-machine-learning-systems/> [Accessed 1 August 2023].

Szakonyi, A., Leonard, B. and Dawson, M., 2021. Dark web: A breeding ground for ID theft and financial crimes. In: *Handbook of Research on Theory and Practice of Financial Crimes*. IGI Global. pp.506–524.

Tanha, J., van Someren, M. and Afsarmanesh, H., 2017. Semi-supervised self-training for decision tree classifiers. *International journal of machine learning and cybernetics*, [online] 8(1), pp.355–370. https://doi.org/10.1007/s13042-015-0328-7.

Tsai, C.-F., Lin, W.-C., Hu, Y.-H. and Yao, G.-T., 2019. Under-sampling class imbalanced datasets by combining clustering analysis and instance selection. *Information sciences*, [online] 477, pp.47–54. https://doi.org/10.1016/j.ins.2018.10.029.

US Department of Justice, 2020. *Identity theft*. [online] Justice.gov. Available at: <https://www.justice.gov/criminal-fraud/identity-theft/identity-theft-and-identity-fraud> [Accessed 1 August 2023].

van Dongen, G. and Van den Poel, D., 2020. Evaluation of stream processing frameworks. *IEEE transactions on parallel and distributed systems: a publication of the IEEE Computer Society*, [online] 31(8), pp.1845–1858. https://doi.org/10.1109/tpds.2020.2978480.

Vanini, P., Rossi, S., Zvizdic, E. and Domenig, T., 2023. Online payment fraud: from anomaly detection to risk management. *Financial innovation*, [online] 9(1). https://doi.org/10.1186/s40854-023-00470-w.

Vorobyev, I. and Krivitskaya, A., 2022. Reducing false positives in bank anti-fraud systems based on rule induction in distributed tree-based models. *Computers & security*, [online] 120(102786), p.102786. https://doi.org/10.1016/j.cose.2022.102786.

Widmer, G. and Kubat, M., 2016. Learning in the presence of concept drift and hidden contexts. *Machine learning*, 23(1), pp.69–101.

Witten, I.H., Frank, E., Hall, M.A. and Pal, C.J., 2016. *Data Mining: Practical Machine Learning Tools and Techniques*. Morgan Kaufmann.

Wong, G.Y., Leung, F.H.F. and Ling, S.-H., 2018. A hybrid evolutionary preprocessing method for imbalanced datasets. *Information sciences*, [online] 454–455, pp.161–177. https://doi.org/10.1016/j.ins.2018.04.068.

Xie, Y., Liu, G., Yan, C., Jiang, C., Zhou, M. and Li, M., 2022. Learning transactional behavioral representations for credit card fraud detection. *IEEE transactions on neural networks and learning systems*, [online] pp.1–14. https://doi.org/10.1109/tnnls.2022.3208967.

Xu, H., Pang, G., Wang, Y. and Wang, Y., 2023. Deep isolation forest for anomaly detection. *IEEE transactions on knowledge and data engineering*, [online] pp.1–14. https://doi.org/10.1109/tkde.2023.3270293.

Yi, X., Xu, Y., Hu, Q., Krishnamoorthy, S., Li, W. and Tang, Z., 2022. ASN-SMOTE: a synthetic minority oversampling method with adaptive qualified synthesizer selection. *Complex & intelligent systems*, [online] 8(3), pp.2247–2272. https://doi.org/10.1007/s40747-021-00638-w.

Yıldırım Taşer, P. and Bozyiğit, F., 2022. Machine learning applications for fraud detection in finance sector. In: *Accounting, Finance, Sustainability, Governance & Fraud: Theory and Application*. Singapore: Springer Nature Singapore. pp.121–146.

Zhou, L., Pan, S., Wang, J. and Vasilakos, A.V., 2017. Machine learning on big data: Opportunities and challenges. *Neurocomputing*, [online] 237, pp.350–361. https://doi.org/10.1016/j.neucom.2017.01.026.

Zhu, X., Ao, X., Qin, Z., Chang, Y., Liu, Y., He, Q. and Li, J., 2021. Intelligent financial fraud detection practices in post-pandemic era. *Innovation (Cambridge (Mass.))*, [online] 2(4), p.100176. <https://doi.org/10.1016/j.xinn.2021.100176>.