

Facu Faculty of Engineering and Informatics

Department of Applied Computer Science and AI

Coursework 1  
Artificial Intelligence for credit card fraud detection  
Group coursework

Nurin Mushahar 23032399

Olamide Oladimeji 23027790

Benaiah Okara 23041060

Monika Kumor 18010628

# Abstract

This paper examines AI's contribution to the fight against credit card fraud. We examine different machine learning methods, concentrating on how they can be applied to large, unbalanced datasets that are commonly used in fraud detection. Important obstacles are noted in the study, including the requirement for real-time processing and the difficulty of reproducing research results because fraud data is confidential. Our review sheds light on the relative merits of various AI algorithms and emphasizes how important model selection and data pre-processing are to fraud detection.

**Table of Content**

[Abstract 1](#_Toc927068235)

[Introduction 3](#_Toc1014664321)

[Problem Description 4](#_Toc798285992)

[Project Motivation 5](#_Toc641518558)

[Objective 5](#_Toc873618240)

[Research Challenges 5](#_Toc761586628)

[Literature Review 6](#_Toc794203741)

[Related Work 6](#_Toc1570604676)

[Algorithms or Methods 7](#_Toc558550342)

[Table 1 9](#_Toc2068520171)

[Table 2 10](#_Toc2012017358)

[Genetic algorithm for feature selection 11](#_Toc543327250)

[Evaluation 13](#_Toc88687844)

[Conclusion 15](#_Toc276838053)

[References 15](#_Toc1374952025)

# Introduction

Fraud is the unethical attainment of goods and services; in recent years this has grown to be a huge problem and is not restricted to any single geographic location. Fraud occurs in several ways and credit cards are one of the most famous targets for fraudulent attacks (Dornadula, et al., 2019). Credit cards are crucial to day-to-day life for a typical cardholder when making purchases, especially with the introduction of virtual cards that are compatible with various smart devices. While this makes life easy for consumers, it also inadvertently enables an attractive environment for fraudsters.

The Federal Trade Commission (FTC) reports that there were about 1579 data breaches totalling 179 million data points, with credit card theft being the most common type of breach (Ileberi, E, et al., 2022). Tokenization and credit card data encryption are two of the many methods available to secure credit card transactions stated by Iwasokun, et al.(2018). Although these techniques work well in most situations, they do not completely guard against fraudulent credit card transactions. To counteract this, more research in the last decade has consisted of using machine learning (ML) techniques to detect fraudulent credit card transactions.

As a branch of artificial intelligence (AI), machine learning (ML) enables computers to learn from experience (data) and enhance their prediction capabilities without having to be specifically programmed to do so. In this work, we review different techniques of credit card fraud detection that employ machine learning algorithms and evaluation metrics. According to Carcillo, et al. (2021) in the last decade, rigorous machine learning research for credit card fraud detection has led to the evolution of supervised, unsupervised, and semi-supervised techniques that computerized the identification of fraudulent patterns from sizeable proportions of datasets.

# Problem Description

According to The UK Annual Fraud Report (2023), there had been a total of £556.3 million fraud losses on UK-issued cards in 2022. This is a 6% rise as compared to the total amount in 2021 at £524.5 million. As also mentioned in the same report, the total spending on both credit and debit cards reached £1 trillion in 2022.

With the substantial transactions made in the year alone, fraud detection is impossible with only the use of human analysts. There will be a considerable number of datasets to analyse and gather the patterns, hence there is a need for firm and rapid methods to detect and prevent fraud, since the number of cases continue to grow annually.

# Project Motivation

Due to the fraudulent practices always evolving, detection and prevention strategies need to be strong and flexible. This project is driven by the need to improve fraud detection mechanisms through the investigation of state-of-the-art technology, cloud infrastructure, and sophisticated artificial intelligence (AI) approaches. Through a thorough analysis of the current literature, our goal is to pinpoint and emphasize the essential methods that have worked well in the field of fraud detection.

## Objective

* Emphasize the key methods, cloud infrastructure and services, and AI approaches used in fraud detection while keeping an eye on the body of current research.
* To create a research report on cloud AI capabilities when applied to the financial fraud dataset, as well as a piece of analysis and an AI demonstration on potential enhancements to financial fraud detection.

## Research Challenges

Credit Card Fraud Detection (CCFD) relies heavily on the continuous development of Artificial Intelligence (AI) and ongoing research into more proficient models. While this work’s main focus is analyzing existing methods, it is crucial to anticipate and resolve potential challenges. The principal issue to address involves discerning differences between various algorithms and how they perform with a given dataset. Given the heavily imbalanced nature of the dataset, it is essential to balance it before model training. Several methods cater to this specific task, and the model’s performance may vary based on the chosen approach.

Another challenge lies in identifying fraudulent transactions, typically flagged when a suspicious purchase occurs. Analyzing customers’ behaviours is crucial to prevent further cases of credit card fraud, however, this raises serious privacy concerns that must be taken into consideration (Awoyemi John O., et al., 2017) As a result, anonymized attributes are present in the datasets used to create machine-learning models. Detecting frauds is also difficult due to the ever-changing classification of fraudulent transactions (Thennakoon A., et al., 2019).

Furthermore, the diversity of credit card fraud data can adversely affect the model’s performance. While the proposed solution may excel with static data, it encounters difficulties in real-time detection. The above points are the main reasons why most published research on Credit Card Fraud Detection (CCFD) is unreproducible, which is a major obstacle when using machine learning techniques to solve the presented problem..

# Literature Review

## Related Work

The dataset provided by (Kaggle, 2017) was used and this includes purchases made by a cardholder over a two-day period, or two days in September 2013. Of the 284,807 transactions in total, 492 transactions, or 0.172% of the transactions, are fraudulent. (Dornadula, Nath, & Geetha, 2019) proposed to create and implement an approach to fraud detection for streaming transaction data with the goal of analysing client transaction history and extracting behavioural patterns. The transactions completed by cards from various groups are aggregated using the sliding window approach (Jiang et al.,2018), allowing the corresponding behavioural patterns of the groupings to be identified.

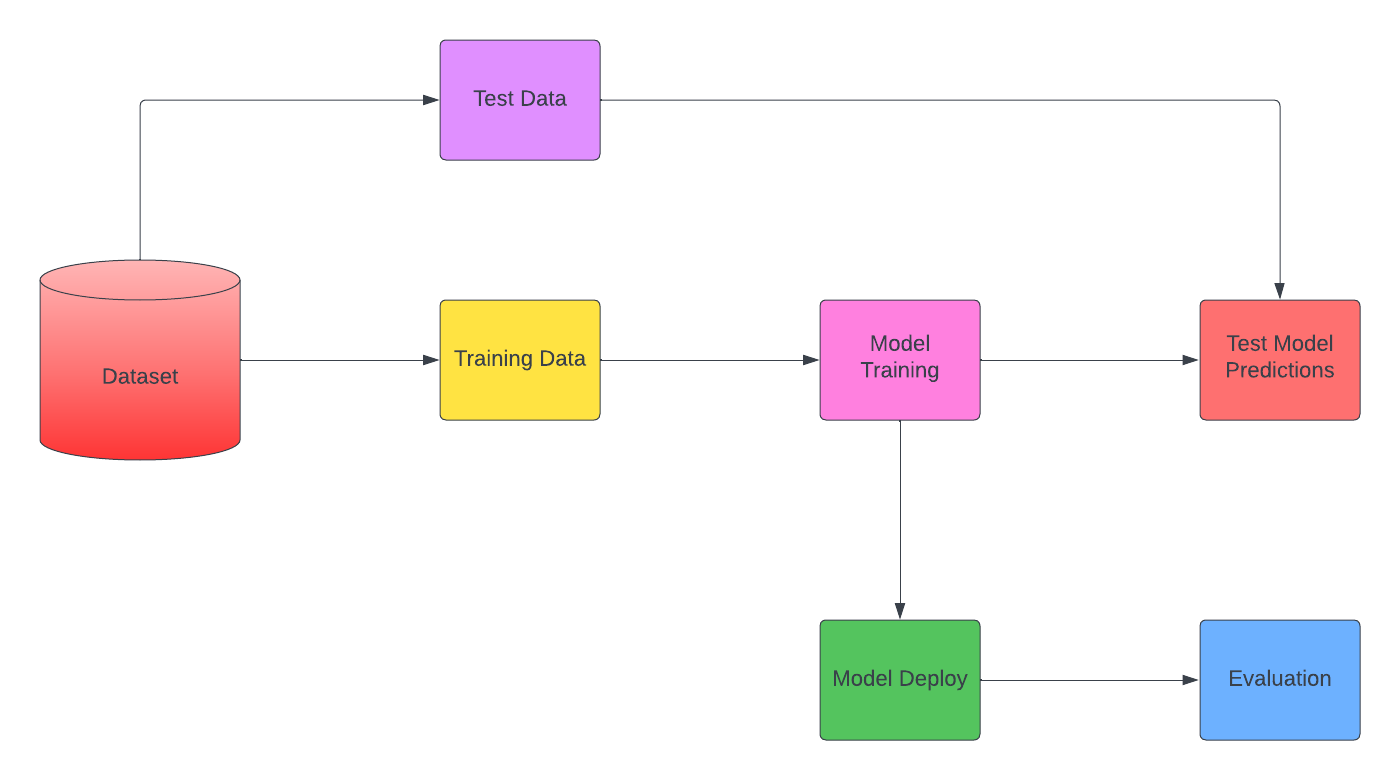
Pre-processing of the dataset is important to effectively train the model. It is essential as there is a confirmed attribute of imbalance of data within the datasets. In this approach, Dornadula, Nath, & Geetha (2019) employed range partitioning and the clustering approach to separate the cardholders into three groups or clusters according to the quantity of their transactions: high, medium, and low. Afterwards using an algorithm (Jiang et al.,2018) the transactions are aggregated into the appropriate categories using the Sliding-Window approach, which involves extracting certain elements from the window to identify the cardholders' behavioural patterns. Features such as the maximum and minimum transaction amounts, the average amount inside the window, and even the amount of time that has passed.

It is a common approach to apply classifiers such as Logistic regression, local Outlier factor, Isolation Forest, Support vector machine (SVM), Decision tree and Random Forest (Chaudhary, Yadav and Mallick, 2012). However, (Warghade, Desai & Patil, 2020) argued that when machine learning algorithms encounter imbalanced datasets, they typically generate classifiers that are not adequate. A common technique to treat the imbalanced dataset is the synthetic minority over-sampling technique (SMOTE) and although overfitting is avoided, the resulting data is synthetic and may not closely resemble the original data. Hence, (Dornadula, Nath, & Geetha, 2019) proposed two approaches to evaluate the accuracy and precision: either employ a one-class classifier or examine the classifier's Matthew Coefficient Correlation (MCC) on the original dataset.

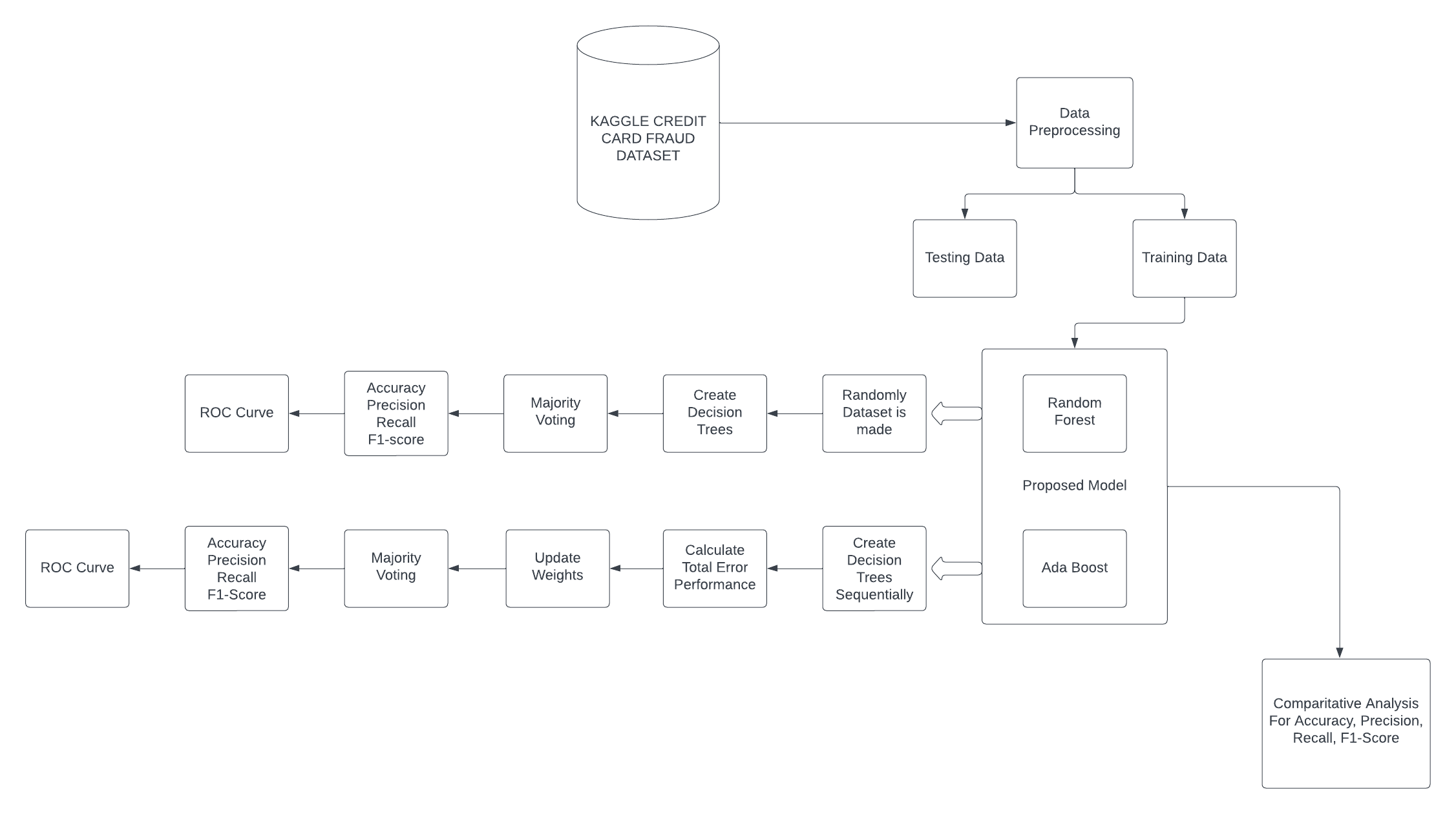
The aim of this approach is to attain the most accurate classifier that can best describe the most recent behaviour pattern of the card holder. (Dornadula, Nath, & Geetha, 2019) Decided to compare the results of the one-class classification and the MCC results against a range of classifiers to determine accuracy and using the SMOTE method to compare the precision of the resulting data. It was found that the optimal parameter for handling dataset imbalance was the Matthews Correlation Coefficient and observed that Logistic regression, decision tree and random forest are the algorithms that gave better results.

# Algorithms or Methods

Jiang, C. et al. (2018) compare AdaBoost and Random Forest. An algorithm with the greatest accuracy, precision, recall, and F1-score will be the most suitable for detecting CCF. In their work, they highlight a detailed architecture diagram (Figure 2), which expands the typical process flow for CCFD (Figure 1). These diagrams were recreated below.

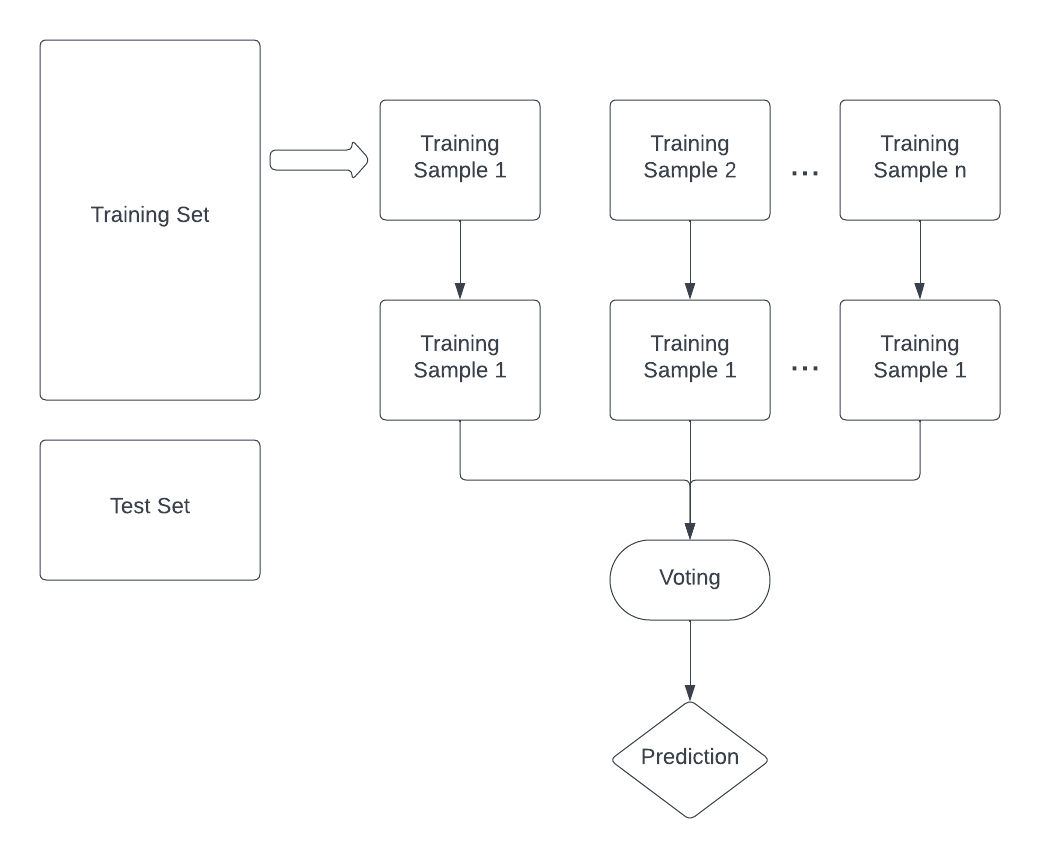


**Figure 1: Process Flow for CCFD**

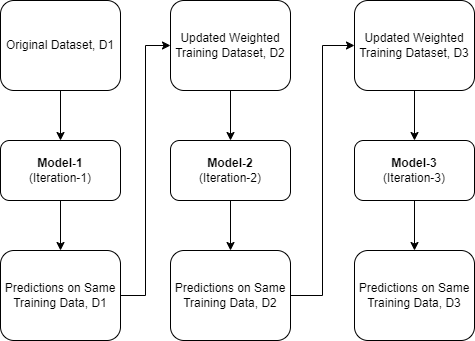


**Figure 2: Architecture Diagram**

Figure 3 and Figure 4 show how Adaboost and Random Forest work. These two algorithms are then compared based on how well they perform with given data. Table 1 and Table 2 contain the summary of their findings. Fraudulent transactions are marked as 1, while legitimate ones are marked as 0.



**Figure 3**



**Figure 4**

|  |  |
| --- | --- |
| **RANDOM FOREST** | **ADABOOST** |
| •It is a widely used supervised learning algorithm  •Can be used for regression and classification purposes  •Mainly used for classification problems  •It creates the decision trees on the sample data and gets a prediction from each  •Better than single decision trees since it reduces over-fitting by averaging the result | •Boosting is one of the ensemble techniques  •Used to build strong classifiers from weak classifiers. This can be done by building a strong model from a weak one.  •One of the most successful boosting algorithms made for binary classification  •Can be built with short decision trees  •Adaboost works well with basic and complex problems  •Adaboost is sensitive to noisy data and outliers |

## **Table 1**

From their findings, it can be determined that despite both models having the same accuracy Random Forest performed better than Adaboost.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **METHODS** | **DATA** | **PRECISION** | **RECALL** | **F1-SCORE** |
| RANDOM FOREST | 0 | 1.00 | 1.00 | 1.00 |
| ACC: 1.0 | 1 | 0.95 | 0.77 | 0.85 |
| ADABOOST | 0 | 0.9994 | 0.9997 | 0.9995 |
| ACC: 1.0 | 1 | 0.78 | 0.64 | 0.71 |

## **Table 2**

Imbalanced datasets are one of the most critical issues that require addressing before model training. An imbalance happens when one class is significantly underrepresented compared to others, posing a potential detriment to prediction accuracy, especially for the minority class. Given that fraudulent transactions happen on a lower frequency compared to legal ones, datasets may exhibit a substantial imbalance. To tackle this challenge numerous techniques have been proposed. In the papers we analysed SMOTE emerges as one of the most utilized methods.

On its own, SMOTE might not produce satisfactory results, however, with the addition of other methods such as Whale Optimization Techniques (WOA) it can help deal with data imbalance (Sailusha, Ruttala, et al., 2020). To check the balance of the binary classifiers, Dornadula, et al. (2019) propose the usage of the Matthew Coefficient Correlation. Below are the outcomes they have observed before (Table 3) and after applying SMOTE (Table 4).

|  |  |  |  |
| --- | --- | --- | --- |
| **METHODS** | **ACCURACY** | **PRECISION** | **MCC** |
| Support Vector Machine | 0.9987 | 0.7681 | 0.5257 |
| Logistic Regression | 0.9990 | 0.875 | 0.6766 |
| Decision Tree | 0.9994 | 0.8854 | 0.8356 |
| Random Forest | 0.9994 | 0.9310 | 0.8268 |

**Table 3**

|  |  |  |  |
| --- | --- | --- | --- |
| **METHODS** | **ACCURACY** | **PRECISION** | **MCC** |
| Logistic Regression | 0.9718 | 0.9831 | 0.9438 |
| Decision Tree | 0.9708 | 0.9814 | 0.9420 |
| Random Forest | 0.9998 | 0.9996 | 0.9996 |

**Table 4**

According to research done by Ileberi E., et al. (2022), they used a credit card transactions dataset that was made by European cardholders (Kaggle,2017). The researcher used classification accuracy to assess the performance of each ML approach. Table 5 shows the recorded outcomes.

|  |  |
| --- | --- |
| **METHODS** | **ACCURACY** |
| Logistic Regression | 97.70% |
| Decision Trees | 95.50% |
| SVM | 97.50% |
| Random Forest | 98.60% |

**Table 5**

To rectify class imbalance, the Synthetic Minority Oversampling Technique (SMOTE) method was used in the data preprocessing phase of the proposed framework (Scikit-Learn).

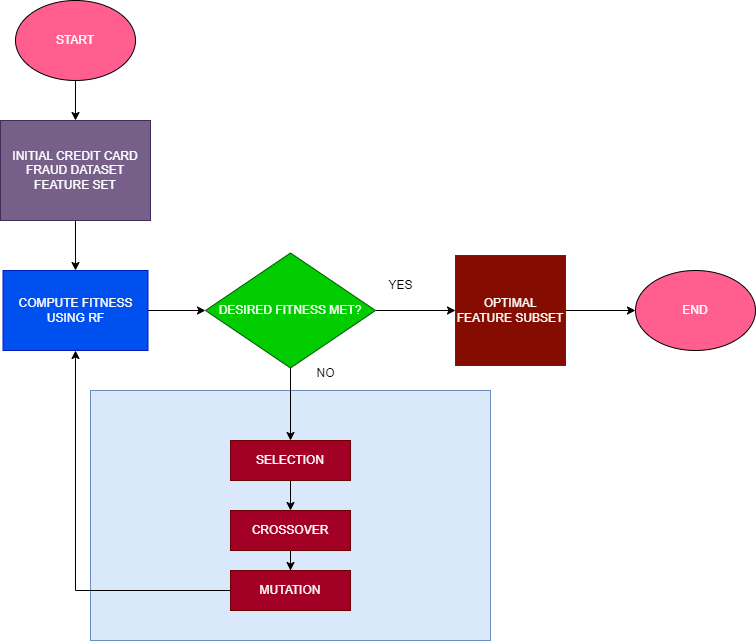
## Genetic algorithm for feature selection

The Genetic Algorithm (GA) is a type of Evolutionary inspired Algorithm (EA) that is often used to solve several optimization tasks with a reduced computational overhead. During the evaluation procedure, in terms of classification accuracy, the most optimal classifier is the RF (implemented with *v*5), This model achieved a noteworthy credit card fraud detection accuracy of 99.98%, And GA-DT (*v*1) achieved an accuracy of 99.92%. The comparison revealed that the GA feature selection approach presented in this paper as well as most of the proposed ML methods that were implemented outperformed the existing techniques. To validate the efficiency of their proposed method, they conducted more experiments using a publicly available synthetic dataset. The dataset contained 24357143 legitimate credit card transactions and 29757 fraudulent ones. The GA-ANN and the GA-DT achieved accuracies of 100%. These results are backed by AUCs of 0.94 and 1, respectively. The other models that performed remarkably well are the GA-RF and the GA-LR with accuracies of 99.95% and 99.96%. However, the GA-LR yielded a low AUC of 0.63.

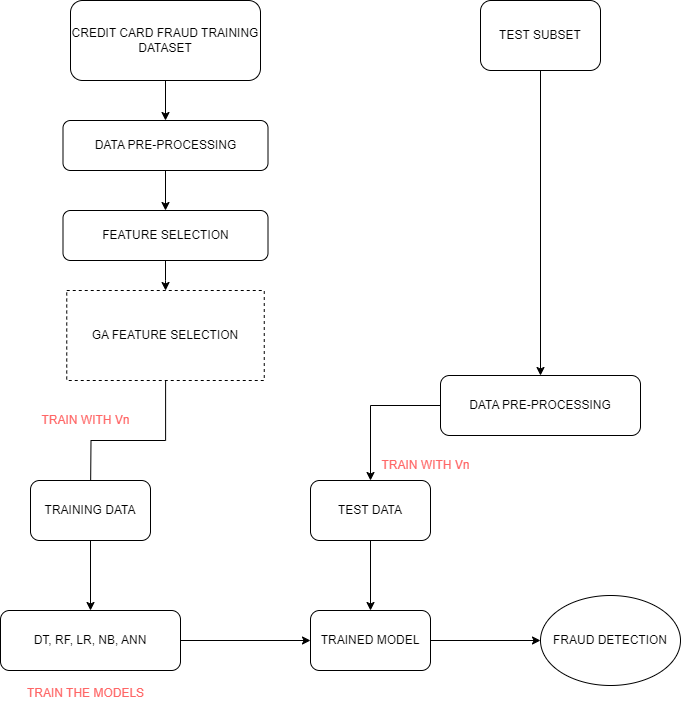
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| V1 | V1 | V1 | V1 | V1 |
| MODEL | ACCURACY | RECALL | PRECISION | F1-SCORE |
| RF | 99.94% | 76.99% | 89.69% | 82.85% |
| DT | 99.92% | 75.22% | 75.22% | 75.22% |
| ANN | 99.94% | 77.87% | 84.61% | 81.10% |
| NB | 98.13% | 84.95 | 6.83% | 12.65% |
| LR | 99.91% | 57.52% | 82.27% | 67.70% |
| V5 | V5 | V5 | V5 | V5 |
| MODEL | ACCURACY | RECALL | PRECISION | F1-SCORE |
| RF | 99.98% | 72.56% | 95.34% | 82.41% |
| DT | 99.89% | 72.56% | 65.07% | 68.61% |
| ANN | 99.08% | 77.87% | 12.27% | 21.20% |
| NB | 99.44% | 57.52% | 15.85% | 24.85% |
| LR | 99.77% | 46.90% | 34.64% | 39.84% |

**Table 6**

In this research (Ileberi, E., et al., 2022), a GA-based feature selection method in conjunction with the RF, DT, ANN, NB, and LR was proposed. The GA was further applied to the dataset and 5 optimal feature vectors were generated. The experimental results that were achieved using the GA-selected attributes demonstrated that the GA-RF (*v*5) achieved an overall optimal accuracy of 99.98%. Furthermore, other classifiers such as the GA-DT(v1) achieved a remarkable accuracy of 99.92%. Figure 5 shows the flowchart proposed in the study and Figure 6 shows the proposed architecture.



**Figure 5**



**Figure 6**

## Evaluation

As explain in this paper, there are various deep learning with machine learning algorithms and techniques to detect fraudulent activity. However, it is vital to understand the strengths and weaknesses each of the techniques own.

|  |  |  |
| --- | --- | --- |
| **Fraud Detection Technique** | **Strength** | **Weakness** |
| Artificial Neural Networks | * Ability to handle large datasets * Best technique to recognise data patterns * Real-time processing for smaller, more focused datasets * By learning intricate patterns, neural networks minimise false positives | * Time consuming with large datasets * More complex data are harder to interpret * Newly gathered data may cause overfitting, inferior performance on the technique * Specifications to use this technique require tuning, which can be time-consuming |
| Decision Trees | * Ability to detect missing values, outliers, and any data quality issues * Delegate between training and testing set * Naturally able to handle both numerical and categorical features | * Data imbalances due to uncommon cases of fraud detection * Biased towards dominant data, less focused on minority data * Unsuitable for monetary value of fraud [[1]](#footnote-2)transactions |
| Genetic Algorithms | * Combines different methods to improve overall performance * Runs data cleaning and data splitting * Post-processing steps include grouping similar transactions, identifying patterns of fraud, flags suspicious transactions | * With deeper learning models, complex data are harder to interpret * Predictions are not well-explained or easy to understand * Inaccuracy could result in deficient performance of the model |
| Case-Based Reasoning (CBR) | * Adaptable to new and evolving fraud patterns * Patterns are detected through real-world cases | * Inability to detect new fraud cases due to the nature of working with historic cases * Relies heavily of the quality of previous cases |
| Support Vector Machines (SVM) | * Robust system * Versatility in usage for both classification and regression tasks. * Wider optimisation (global) | * Difficulty in sustaining large datasets * Takes a longer time to detect * Not suitable for noisy, overlapping data |
| Artificial Immune System (AIS) | * Coherent system integration * Affordable | * Requires a longer period and/or intense training time |

Based on the evaluation table above decision and application of the techniques would need to be based on what the end users are trying to depict and achieve. Strengths in some techniques could potentially become a weakness in another, as it all comes down to which dataset is being used.

# Conclusion

In conclusion, Credit Card Fraud is a continuous and dynamic threat. Combining AI technology with traditional fraud detection methods is the most efficient method for detecting credit card fraud. More specifically, there has been an impressive success when feature selection based on Genetic Algorithm (GA) is combined with machine learning classifiers like Random Forest (RF), Decision Trees (DT), Artificial Neural Networks (ANN), Naive Bayes (NB), and Logistic Regression (LR). The study demonstrated the superiority of the GA-RF (version 5) model, which attained a remarkable 99.98% fraud detection accuracy, and the GA-DT (version 1) model, which achieved a 99.92% accuracy. Further research should try to validate these techniques on a wider range of datasets to confirm their efficiency and adaptability in various credit card fraud detection scenarios.

# References

1. Abd El-Hamid, H., Khalifa, W., Roushdy, M. and Salem, A., 2019. Machine Learning Techniques for Credit Card Fraud Detection. Future Computing and Informatics Journal, 4(2).
2. Asha, R.B. and KR, S.K., 2021. Credit card fraud detection using artificial neural network. Global Transitions Proceedings, 2(1), pp.35-41.
3. Awoyemi, John O., Adebayo O. Adetunmbi, and Samuel A. Oluwadare. "Credit card fraud detection using machine learning techniques: A comparative analysis." 2017 international conference on computing networking and informatics (ICCNI). IEEE, 2017.
4. 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, 557, pp.317-331.
5. Chaudhary, K., Yadav, J. and Mallick, B., 2012. A review of fraud detection techniques: Credit card. International Journal of Computer Applications, 45(1), pp.39-44.
6. Delamaire, L., Abdou, H. and Pointon, J., 2009. Credit card fraud and detection techniques: a review. Banks and Bank systems, 4(2), pp.57-68.
7. Dornadula, Vaishnavi Nath, and Sa Geetha. "Credit card fraud detection using machine learning algorithms." Procedia computer science 165 (2019): 631-641.
8. Ganji, V. R. (2023). Shuffled shepherd political optimization-based deep learning method for credit card fraud detection. *Concurrency and Computation: Practice and Experience*, *35*(10). <https://doi.org/10.1002/cpe.7666>
9. Halvaiee, N. S., & Akbari, M. K. (2014). A novel model for credit card fraud detection using Artificial Immune Systems. In *Applied Soft Computing* (Vol. 24, pp. 40–49). essay, Elsevier Science Publishers.
10. Ileberi, E., Sun, Y. and Wang, Z., 2022. A machine learning based credit card fraud detection using the GA algorithm for feature selection. Journal of Big Data, 9(1), pp.1-17.
11. Iwasokun, G.B., Omomule, T.G. and Akinyede, R.O., 2018. Encryption and tokenization-based system for credit card information security. Int J Cyber Sec Digital Forensics, 7(3), pp.283-93.
12. Jiang, C., Song, J., Liu, G., Zheng, L. and Luan, W., 2018. Credit card fraud detection: A novel approach using aggregation strategy and feedback mechanism. IEEE Internet of Things Journal, 5(5), pp.3637-3647.
13. Meyers, R. A. (2003). Artificial Neural Network. In *Encyclopedia of Physical Science and Technology* (3rd ed., pp. 631–645). essay, Academic Press.
14. Pradipta, Gede Angga, et al. "SMOTE for handling imbalanced data problem: A review." 2021 Sixth International Conference on Informatics and Computing (ICIC). IEEE, 2021.
15. Robles-Velasco, A., Cortés, P., Muñuzuri, J. and Onieva, L., 2020. Prediction of pipe failures in water supply networks using logistic regression and support vector classification. Reliability Engineering & System Safety, 196, p.106754.
16. Sailusha, Ruttala, et al. "Credit card fraud detection using machine learning." 2020 4th international conference on intelligent computing and control systems (ICICCS). IEEE, 2020.
17. Sujatha, M., 2019. A comparative study of credit card fraud detection using machine learning for United Kingdom dataset. International Journal of Computer Science and Information Security (IJCSIS), 17(9), p.2019.
18. Thennakoon, A., Bhagyani, C., Premadasa, S., Mihiranga, S. and Kuruwitaarachchi, N., 2019, January. Real-time credit card fraud detection using machine learning. In 2019 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence) (pp. 488-493). IEEE.
19. Warghade, S., Desai, S. and Patil, V., 2020. Credit card fraud detection from imbalanced dataset using machine learning algorithm. International Journal of Computer Trends and Technology, 68(3), pp.22-28.
20. Yazici, Y., 2020. Approaches to Fraud detection on credit card transactions using artificial intelligence methods. arXiv preprint arXiv:2007.14622.
21. www.kaggle.com. (n.d.). Credit Card Fraud Detection. [online] Available at: https://www.kaggle.com/datasets/mlg-ulb/creditcardfraud/data (Accessed: 15th November 2023).

1. [↑](#footnote-ref-2)