



**Detecting Financial Fraud Using Artificial Intelligence: An Applied Study Based on  
Credit Card Transactions**

Prepared By

Name: Mohammed mushahhin m alatwi

Submitted in fulfillment of the requirements for the degree  
Master of Science in Artificial Intelligence

At

College of Informatics

Midocean University

UAE

Supervisor Name: Dr. Yasser Abdelhamid

College of Informatics, Midocean University, Comoros

[2026]

# Acknowledgements

I would like to express my sincere gratitude to Dr. Yasser Abdelhamid for his invaluable guidance, continuous support, and encouragement throughout this research project. His expertise, insightful feedback, and unwavering dedication have significantly contributed to the quality and direction of this thesis.

I also extend my heartfelt appreciation to my family, friends, and colleagues, whose patience, motivation, and moral support were instrumental in the successful completion of this work.

A special thank you goes to my brother, Bader, for his generous help and continuous encouragement throughout this journey.

# **Abstract**

This paper examines the usefulness of artificial intelligence methods in credit card fraud detection based on a real-life transactional dataset. The rule-based systems are not adequate anymore to detect the evolving trends of frauds because of its growing complexity. Three machine learning models trained with supervision, including the Logistic Regression (LR), Random Forest (RF), and Artificial Neural Network (ANN), were used to tackle this issue, using the highly imbalanced Kaggle Credit Card Fraud Detection dataset. The methods of preprocessing data such as feature scaling and Synthetic Minority Oversampling Technique (SMOTE) were used to enhance the accuracy of the model and address the imbalance between the classes. The experimental findings reveal the highest overall performance of the Random Forest model, which has Precision equal to 0.8519, Recall equal to 0.8846, F1-score equal to 0.8679 and ROC-AUC equal to 0.9798. The ANN model performed quite well as well, with a ROC-AUC of 0.9895, which suggests that it is highly effective in discriminating between a fraudulent and a legitimate transaction. Conversely, Logistic Regression was very accurate (0.9913) and low precision (0.2750) in value with a greater false positive rate. The results validate that AI-based methods especially ensemble and deep learning models are much better than conventional methods in detecting fraud. These findings emphasize the feasible nature of implementing scalable and data-driven AI solutions to financial systems to improve fraud prevention and decrease financial losses.

## **Key Words**

1. Artificial Intelligence
2. Credit Card Fraud Detection

3. Machine Learning Models
4. Financial Cybersecurity

## Contents

|                                          |           |
|------------------------------------------|-----------|
| <b>List of Abbreviations .....</b>       | <b>v</b>  |
| <b>List of Figures.....</b>              | <b>vi</b> |
| <b>List of Tables .....</b>              | <b>vi</b> |
| Chapter 1 .....                          | 1         |
| Introduction.....                        | 1         |
| Chapter 2 .....                          | 6         |
| Back ground and Related Work.....        | 6         |
| Chapter 3 .....                          | 18        |
| Proposed Approach .....                  | 18        |
| Chapter 4 .....                          | 22        |
| Experimental Results and Discussion..... | 22        |
| Chapter 5 .....                          | 29        |
| Conclusion and Future Work .....         | 29        |
| References .....                         | 31        |

# List of Abbreviations

| <b>Abbreviation</b> | <b>Full Term</b>                                              |
|---------------------|---------------------------------------------------------------|
| <b>AI</b>           | <b>Artificial Intelligence</b>                                |
| <b>ANN</b>          | <b>Artificial Neural Network</b>                              |
| <b>AUC-ROC</b>      | <b>Area Under the Receiver Operating Characteristic Curve</b> |
| <b>CNN</b>          | <b>Convolutional Neural Network</b>                           |
| <b>CRISP-DM</b>     | <b>Cross-Industry Standard Process for Data Mining</b>        |
| <b>DL</b>           | <b>Deep Learning</b>                                          |
| <b>FN</b>           | <b>False Negative</b>                                         |
| <b>FP</b>           | <b>False Positive</b>                                         |
| <b>KNN</b>          | <b>K-Nearest Neighbors</b>                                    |
| <b>LR</b>           | <b>Logistic Regression</b>                                    |
| <b>ML</b>           | <b>Machine Learning</b>                                       |
| <b>PCA</b>          | <b>Principal Component Analysis</b>                           |
| <b>RF</b>           | <b>Random Forest</b>                                          |
| <b>SMOTE</b>        | <b>Synthetic Minority Oversampling Technique</b>              |
| <b>SVM</b>          | <b>Support Vector Machine</b>                                 |
| <b>TN</b>           | <b>True Negative</b>                                          |
| <b>TP</b>           | <b>True Positive</b>                                          |
| <b>XAI</b>          | <b>Explainable Artificial Intelligence</b>                    |
| <b>XGBoost</b>      | <b>Extreme Gradient Boosting</b>                              |

## List of Figures

|                                                                                                                                |    |
|--------------------------------------------------------------------------------------------------------------------------------|----|
| Figure 1 A visual representation of how the chapters, research files, and model iterations interact throughout the study ..... | 5  |
| Figure 2 Class Distribution Before/After SMOTE .....                                                                           | 25 |
| Figure 3 ROC Curves for Three Models.....                                                                                      | 26 |

## List of Tables

|                                                                              |    |
|------------------------------------------------------------------------------|----|
| Table 1 Quantitative Results Summary .....                                   | 10 |
| Table 2 Summary of Reviewed Studies on AI-Based Financial Fraud Detection .. | 13 |
| Table 3 Dataset Structure After Preprocessing .....                          | 22 |
| Table 4 Class Distribution Before and After SMOTE.....                       | 23 |
| Table 5 Machine Learning Model Performance .....                             | 23 |
| Table 6 Comparison of Proposed Models with Previous Studies.....             | 28 |

# Chapter 1

## Introduction

### 1.1 Problem Definition

With the fast development of online financial transactions, the world of business has been changed as it has provided unprecedented convenience, accessibility and speed. This technological development has however been matched with an equal increase in the size and complexity of the fraudulent financial activities, especially credit card fraud. Self Financial (2024) reports that credit card fraud incidences all over the world reached a point of over 32 billion US dollars in 2022, which is a clear indicator of how grave the issue is and how necessary new and improved fraud detection systems are. With the ongoing digitization of the financial transactions, fraudsters are using more sophisticated and dynamic ways to exploit the vulnerability in the conventional security systems.

Mainly rule-based systems have been widely applied in banking and financial institutions as conventional fraud detection methods. Although these systems are able to detect the known patterns of fraud, they have severe limitations. They are not able to pick up new, unknown fraud patterns due to their inflexible and fixed rule structures (Avasthi and Varsha, 2024). Fraudsters keep improving their techniques, and conventional systems are not flexible enough, slow in response, and inadaptatable with a high rate of false negative. It implies that a lot of fraudulent operations remain unrestricted and result in massive losses of money and customer distrust to online banking systems.

Artificial intelligence (AI) and machine learning (ML) present strong alternatives to these problems, being able to learn on past history, detect complex patterns, and respond to new fraudulent plots in real time. The issue that was tackled by this thesis is the absence of effective, dynamic, and sound fraud detection models which can effectively distinguish between legitimate and fraudulent transactions in extremely lopsided and dynamic data settings. Due to the high-cost of fraud and the shortcomings of the classic systems, the necessity of a high-tech AI-based detection models is urgent and critical to the protection of global finances.

Even though a considerable number of past studies have compared machine learning models of Logistic Regression, Random Forest, and Artificial Neural networks to detect credit card fraud, few have focused on examining the effects of data preprocessing methods in highly unbalanced datasets. In the financial data of the real world, the imbalance in classes is a major factor of influencing the model performance especially in fraudulent transaction identification. Thus, the proposed research is not merely a comparison of models but an assessment of how important preprocessing techniques, such as SMOTE, feature scaling, and PCA, influence the performance of the models. It offers a practical experimental study that brings out the importance of dealing with data imbalance and feature transformation to enhance the accuracy of detecting fraud, hence, provides more reliable and applicable information to real-life financial systems.

## **1.2 Thesis Objectives**

The primary goal of the current thesis is to design, assess and compare machine learning-based AI solutions that would identify credit card fraud with high accuracy and low false negatives rates. To reach this objective, a number of specific research objectives should be used:

- To create predictive machine learning models that can either define credit card transactions as either fraudulent or legitimate using actual financial data in the world in the Kaggle Credit Card Fraud Detection data. This dataset demonstrates the imbalance that is high in the cases of fraud and it is, therefore, appropriate in the realistic model evaluation.
- To compare the results of several supervised learning algorithms, namely, Logistic Regression, Random Forest and Artificial Neural Networks. The algorithms have been broadly researched to detect frauds and present a solid basis to find the most efficient tool to recognize the anomalies in financial data (Dayyabu et al., 2023).
- To tackle the problem of imbalanced information, one of the most critical problems in fraud detection, using the methods of SMOTE or undersampling. Treating imbalance properly is important in maximizing the recall and a low number of false negatives- a vital parameter in fraud detection.
- To assess the interpretability and reliability of the chosen models, it will be important to make sure that the results are clear, credible, and can be used in the real-life financial decision-making. That is in tandem with regulatory and ethical issues of AI application in sensitive financial applications.
- To contribute to the industry practice by making AI-based financial risks management approaches and to offer practical recommendations on how AI-based fraud detection systems should be integrated in pre-existing financial security systems.

### **1.3 Thesis Contribution**

This thesis gives a contribution to the academic and practical research on the topic of financial fraud detection as it presents a multi-faceted framework of assessing the success of AI and machine learning models in identifying credit card fraud. The study is a contribution to the current body of research by providing a comparative assessment of three popular algorithms, including; Logistic Regression, Random Forest and Artificial Neural Networks-based performance. highlighting their strengths, shortcomings, and real-time fraud detection. Using the state-of-the-art preprocessing methods, SMOTE and PCA, the thesis proves an improved method of controlling the imbalanced and high-dimensional financial information to enhance the effectiveness and efficiency of fraud detection models.

In practical terms, the thesis would add value in the financial institutions by providing a dependable, dynamic and scaling fraud detection prototype that has the ability to evolve with the changing patterns of fraud. This will promote better cybersecurity measures, lesser losses of finances and better management of institutional risks. Furthermore, the fact that interpretability and ethical concerns are addressed also provides valuable insights to policymakers and regulators that control AI-based financial technologies. Finally, the research has an excellent empirical and methodological basis to continue future studies in the field of AI-empowered cybersecurity and fraud prevention.

## 1.4 Thesis Organization

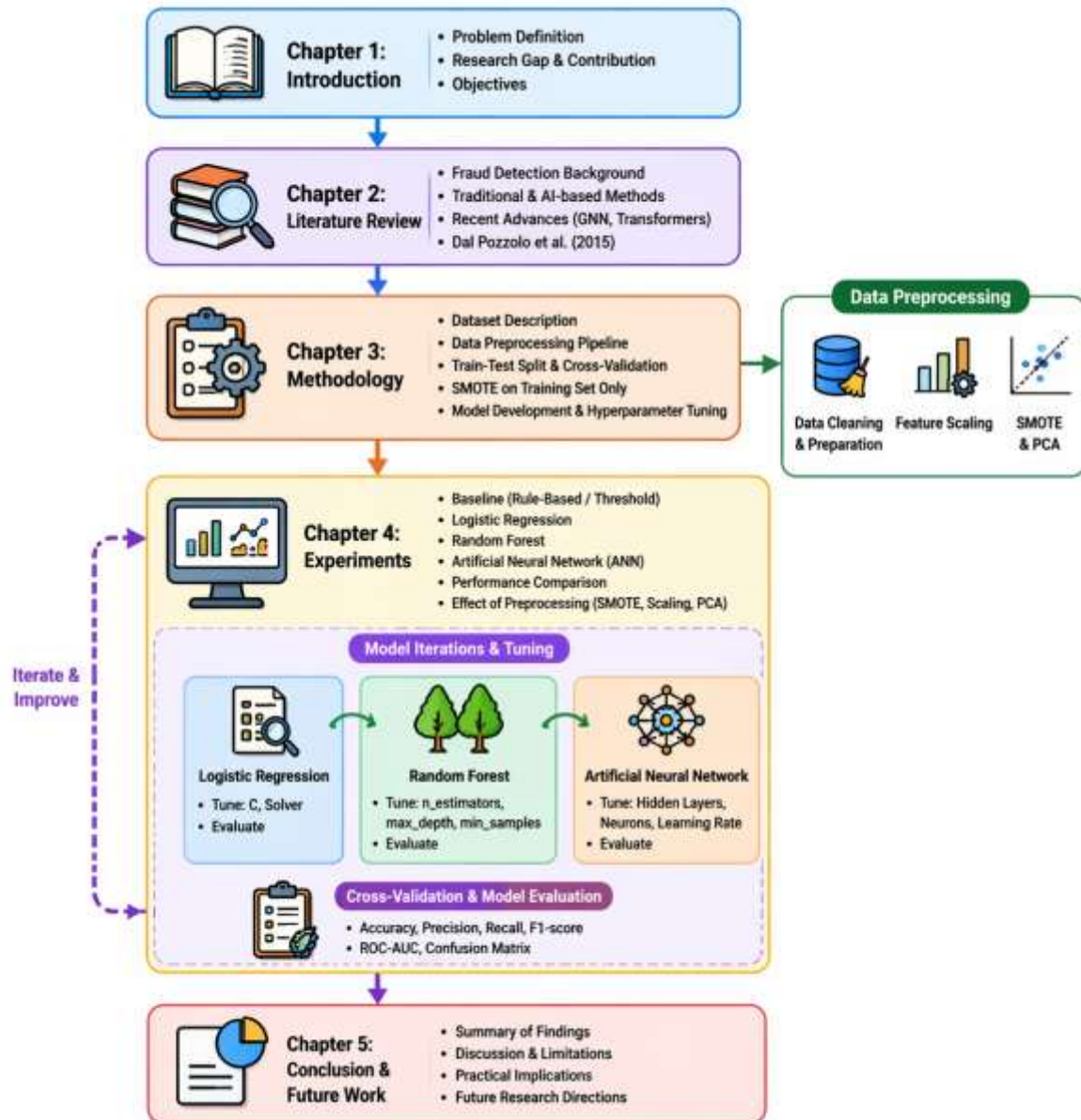


Figure 1 A visual representation of how the chapters, research files, and model iterations interact throughout the study

# **Chapter 2**

## **Back ground and Related Work**

### **2.1 Introduction to Credit Card Fraud Detection**

The issue of credit card fraud has turned out to be one of the largest challenges of the contemporary financial fields with the online payments and digital banking services proliferating at a rampant rate. Physical inspection methods and rule-based fraud detection technology have not been effective in detecting even more advanced patterns of frauds as the number of transactions grows (Avasthi and Varsha, 2024). This has made artificial intelligence (AI) and machine learning (ML) prevailing methods of research on fraud detection. The chapter summarizes the literature on the field of interest which includes the classical machine learning algorithms, deep learning systems, mixed systems, real world data and performance analysis tools, and forms the basis of the methodology in this thesis.

### **2.2 Classical Methods of machine learning.**

The classical methods of machine learning have been fundamental in the field of developing fraud detection system. Initial research was on algorithms like the logistic regression, the decision trees, support vectors machine (SVM) and the k-nearest neighbors (KNN). Asha and Kumar (2021) compared the SVM, KNN, and Artificial Neural Networks (ANNs), and it was found that ANN and SVM are more effective than simpler models in fraudulent transaction prediction because they are capable of capturing nonlinear relationships. Their discussion revealed that classical

models of ML can be used to obtain good accuracy, yet they are limited in working with high-dimensional data sets or highly imbalanced data sets.

A quantitative investigation by Dayyabu et al. (2023) utilizes information on accounting and finance professionals and reveals that three artificial intelligence methods machine learning, data mining, and fuzzy logic all have significant positive correlations with accuracy of fraud detection. Although machine learning was the best in terms of precision, fuzzy logic was the least sensible, which leads to the necessity to consider more reliable models in the workplace. In large-scale datasets, classical ML is frequently outperformed by deep learning models because it is interpretable and has relatively low computational requirements, although its performance is still often much lower.

### **2.3 Deep Learning Approaches**

The application of deep learning methods has taken center stage in credit card fraud detection owing to its capability to acquire the behavioral and transactional information with complex behavioral and transactional patterns. Prince et al. (2024) revealed that the use of deep learning models (Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), and Long Short-Term Memory (LSTM) networks are highly important in improving the performance of fraud detection by real-time systems. Their results indicated that deep models had a better detection rate and were less prone to false positives than conventional ML methods, in large scale financial settings, in particular.

The authors pointed out that deep learning is especially applicable in scenarios where it is combined with big data analytics, and transaction streams can be monitored in real-time at low latency. This is an essential capability that financial institutions should have to prevent fraudulent transactions before money is lost. The paper also

emphasizes the need to have scalable system architecture and upkeep of the model training that ensures accuracy as patterns of fraud changes.

## **2.4 Hybrid and Optimized Models**

Recent developments have brought about the use of hybrid models which integrate two or more ML or deep learning architectures. The idea of these models is to take advantage of the strengths of each of the components such as using the interpretability of ML methods and the pattern-recognition strengths of deep learning. Avasthi and Varsha (2024) survey the ensemble methods in the form of Random Forests, AdaBoost, and Gradient Boosting in accordance with which the ensemble methods tend to perform better than the individual classifiers because they combine multiple decision boundaries.

Other works discuss the combination of supervised and unsupervised methods, including isolation forests, clustering (DBSCAN, k-means), and autoencoders, to detect anomalies in cases where it is scarce. These hybrid systems are flexible and resilient, especially when dynamic fraud environments are involved whereby new fraud variants have been continuously appearing.

## **2.5 Modern AI Techniques**

Recently, there have been new developments in the field of Artificial Intelligence (AI) that have introduced powerful tools that improve the ability to detect fraud. Graph Neural Networks (GNN) and Transformers are two of the most promising methods, particularly in the case of time series and sequential data (Falana, 2024; Dubey et al., 2025).

Graph Neural Networks (GNNs).

GNNs have been shown to be useful in detection of fraud when the data is presented as a graph, e.g. transaction between multiple accounts. GNNs are created to learn relationships and interactions among entities and are capable of modeling complex patterns in the fraud detection systems. They can be used to identify advanced trends of fraud in financial networks and their capability to combine local and global dependencies makes them appropriate(Falana, 2024).

### Transformers

Originally created to work with natural language, transformers have demonstrated significant potential in time series analysis, which is essential to detect fraud in financial transactions. Their attention systems enable them to effectively understand long-term relationships in serial data. This is an important feature in fraud detection as it allows the anomaly patterns to be identified more effectively in long series of transactions, thus making them an effective tool in real time detection of fraud(Dubey et al.,2025)

The techniques are becoming increasingly popular because they have the potential to enhance the accuracy of detection, interpretability, and effectiveness with respect to dynamic, high-dimensional data that are often found in financial fraud cases.

## **2.6 Use of Real-World Datasets**

The majority of the fraud detecting studies are based on publicly accessible datasets, with the largest being Kaggle Credit Card Fraud Detection dataset. This dataset is very popular because of the high imbalance and anonymized PCA-transformed features, which is very convenient when trying to test AI models. As Avasthi and Varsha (2024) emphasize, the performance of the model can be improved with the help of preprocessing methods, including SMOTE, PCA, feature scaling, and removing outliers.

Real world data presents issues like missing values, imbalance ratio larger than 1:500, anonymized variables that cannot be handled easily to achieve high recall to reduce false negatives which is a critical objective in fraud detection.

## 2.7 Quantitative Results Summary

*Table 1 Quantitative Results Summary*

| Study                   | Model                          | Key Findings                                                     |
|-------------------------|--------------------------------|------------------------------------------------------------------|
| Asha & Kumar (2021)     | ANN, SVM, KNN                  | ANN and SVM outperform classical ML for nonlinear fraud patterns |
| Dayyabu et al. (2023)   | ML, Data Mining, Fuzzy Logic   | ML has highest precision; fuzzy logic least utilized             |
| Prince et al. (2024)    | CNN, RNN, LSTM                 | Deep learning shows highest accuracy and lowest false positives  |
| Avasthi & Varsha (2024) | Random Forest, Boosting Models | Ensemble techniques outperform rule-based systems                |

## 2.8 Research Gaps and Opportunities

Even in the light of numerous research, some gaps still exist:

- Real time fraud detection schemes are narrowly used in their implementation.
- There are limited studies on uncertainty quantification to trustworthy AI.
- Deep learning models still have low interpretability.
- Hybrid and ensemble deep learning systems are not optimized to the full.
- Further studies should be carried out concerning cross-bank generalization and regulatory consistency.

## 2.9 Literature Review

The recent development of online financial systems has considerably complicated credit card fraud, and the conventional methods of detection using rules were not enough. Consequently, machine learning (ML) and artificial intelligence (AI) have become a necessity to uncover fraudulent transactions based on highly skewed datasets. Yazici (2020) mentions that the issue of information asymmetry is one of the most severe problems in fraud detection because models are biased towards the majority group. The study highlights the significance of feature engineering, adaptive learning, and evaluation metrics like recall, F1-score, and AUC-ROC rather than just using accuracy as a measure. It further emphasizes the importance of scalable models that can process real time streams of transactions and this contributes to a solid theoretical basis of modern fraud detection system. Dayyabu et al. (2023) give a quantitative analysis of AI methods using data obtained among finance professionals. They find that machine learning and data mining can be used to detect fraud much more accurately than fuzzy logic. Another significant point of the study is the significance of interpretability and human-AI cooperation, implying that AI systems are expected to assist decision-making but not the human experts in monetary settings. The model suggested by Bhat and Nelson (2023) involves the combination of Random Forest, CNN, and XGBoost with the optimization of the Sparrow Search Algorithm. Their findings reveal that Random Forest is most accurate (82.65%), compared to CNN and XGBoost. The paper has shown that hybrid and ensemble methods are effective in enhancing the performance of detection and maintaining the stability and scalability of models. Mytnyk et al. (2023) discuss AI use in banking fraud detection and indicate that the Logistic Regression model demonstrated high performance with an AUC of 0.946, and a stacked model demonstrated high performance with an AUC of 0.954. Their results dispute the idea that deep learning is always superior to classical models and that the

appropriate preprocessing and feature engineering can greatly improve simpler models. Asha and Kumar (2021) compare between SVM, KNN, and ANN models and find that ANN is the best one to capture complex patterns of nonlinear fraud. Nevertheless, the research observes that ANN is sensitive to large data sets and tuning of hyper parameters. It also shows the necessity of adaptive models that can address the changing methods of fraud like phishing and attack based on identity. Ali et al. (2022) have performed a systematized literature review of 93 articles and discovered that SVM and ANN are the most popular algorithms employed in the detection of fraud. The research outlines the longstanding issues, including data imbalance and lack of explainability, and proposes to use hybrid methods that combine supervised and unsupervised learning to enhance the performance of models and model transparency. In his study, Shihembetsa (2021) examines fraud detection in mobile banking based on ML models: Logistic Regression, Naive Bayes, and KNN. The research concludes that KNN had the best accuracy (99%) in identifying fraudulent transactions. It also sheds light on the need to apply systematic approaches like the CRISP-DM to facilitate the successful implementation of AI systems in practice. Almazroi and Ayub (2021) suggest a deep learning model with ResNeXt and GRU that is optimized by the Jaya algorithm. Their model was more accurate and efficient by 10-18 percent of traditional methods. The research indicates the possible potential of deep learning and ensemble approaches to detect fraud in real-time, but it also reports the issues of complexity and interpretability of models. Dal Pozzolo et al. (2015) propose an adaptive method of fraud detection based on sliding windows with the focus on non-stationary data in real-time scenarios. Their contribution highlights the significance of managing concept drift where patterns of fraud change with time. Their model is enhanced by constantly training the model based on recent transaction data, making the difference in detecting in streaming systems, and demonstrating the importance of dynamic and

adaptive AI models in financial fraud detection. On the whole, it is possible to note that the literature reviewed indicates a distinct trend towards moving beyond the traditional rule-based systems and towards more sophisticated AI-powered models. Key challenges include data imbalance, real-time processing, and model interpretability. The newer trends are on hybrid models, adaptive learning and explainable AI, and are geared towards creating scalable and reliable fraud detection systems that can work in dynamic financial settings.

*Table 2 Summary of Reviewed Studies on AI-Based Financial Fraud Detection*

| <b>Author(s)<br/>&amp; Year</b> | <b>Title /<br/>Study<br/>Focus</b>                        | <b>AI / ML<br/>Methods</b>                                                                 | <b>Dataset /<br/>Sample</b> | <b>Main<br/>Findings</b>                                                                                                                                                            | <b>Limitations</b>                                   |
|---------------------------------|-----------------------------------------------------------|--------------------------------------------------------------------------------------------|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------|
| Yazici<br>(2020)                | AI<br>Approache<br>s in Credit<br>Card Fraud<br>Detection | Review of<br>ML (rule-<br>based,<br>supervised<br>learning,<br>feature<br>engineerin<br>g) | Conceptual<br>study         | Identified<br>key<br>challenges:<br>data<br>imbalance,<br>real-time<br>processing,<br>and feature<br>engineering<br>;<br>emphasized<br>use of recall<br>and AUC<br>over<br>accuracy | No empirical<br>validation;<br>purely<br>theoretical |

|                       |                                                       |                                   |                                    |                                                                                                             |                                                           |
|-----------------------|-------------------------------------------------------|-----------------------------------|------------------------------------|-------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------|
| Dayyabu et al. (2023) | AI Techniques in Fraud Detection (Quantitative Study) | ML, data mining, fuzzy logic      | Survey (100 finance professionals) | ML and data mining significantly improve fraud detection; strong correlation between AI use and performance | Based on perceptions, not experimental results            |
| Bhat & Nelson (2023)  | Hybrid AI Model with Optimization                     | RF, CNN, XGBoost (Sparrow Search) | Kaggle dataset                     | RF achieved highest accuracy (82.65%), outperforming CNN and XGBoost; hybrid models improve performance     | Focused only on accuracy; lacks interpretability analysis |

|                      |                               |                                    |                          |                                                                                                                  |                                              |
|----------------------|-------------------------------|------------------------------------|--------------------------|------------------------------------------------------------------------------------------------------------------|----------------------------------------------|
| Mytnyk et al. (2023) | AI in Banking Fraud Detection | Logistic Regression, ANN, Stacking | Banking transaction data | Logistic Regression achieved AUC=0.946; stacking improved to 0.954; preprocessing significantly enhances results | Limited deep learning analysis               |
| Asha & Kumar (2021)  | ANN-Based Fraud Detection     | SVM, KNN, ANN                      | Credit card datasets     | ANN outperformed other models in detecting nonlinear patterns                                                    | Requires large datasets; sensitive to tuning |
| Ali et al. (2022)    | Systematic Literature Review  | ML models (SVM, ANN, RF, LR)       | 93 studies               | Identified common use of SVM and ANN; highlighted imbalance and                                                  | No experimental comparison                   |

|                                 |                                                           |                                                  |                                     |                                                                                                          |                                                                    |
|---------------------------------|-----------------------------------------------------------|--------------------------------------------------|-------------------------------------|----------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------|
|                                 |                                                           |                                                  |                                     | explainability issues                                                                                    |                                                                    |
| Shihembet<br>sa (2021)          | AI in<br>Mobile<br>Banking<br>Fraud<br>Detection          | LR, Naïve<br>Bayes,<br>KNN                       | Kenyan<br>mobile<br>banking<br>data | KNN<br>achieved<br>highest<br>accuracy<br>(99%);<br>showed AI<br>effectiveness in mobile<br>transactions | Limited<br>generalizability; imbalance<br>not fully<br>addressed   |
| Almazroi<br>& Ayub<br>(2021)    | Deep<br>Learning<br>Fraud<br>Detection<br>Model           | RXT<br>(ResNeXt<br>+ GRU),<br>Autoencoder, SMOTE | Multiple<br>real<br>datasets        | Model<br>improved<br>accuracy by<br>10–18%;<br>effective in<br>real-time<br>detection                    | High<br>complexity;<br>low<br>interpretability                     |
| Dal<br>Pozzolo et<br>al. (2015) | Adaptive<br>Fraud<br>Detection<br>in<br>Streaming<br>Data | Sliding<br>window,<br>imbalance<br>learning      | Real<br>transaction<br>data         | Introduced<br>adaptive<br>models to<br>handle<br>concept<br>drift;<br>improved<br>fraud                  | Requires<br>continuous<br>model<br>updating;<br>computational cost |

|  |  |  |  |                                             |  |
|--|--|--|--|---------------------------------------------|--|
|  |  |  |  | detection in<br>dynamic<br>environmen<br>ts |  |
|--|--|--|--|---------------------------------------------|--|

### **Summary of Insights**

In the literature reviewed, there are a number of patterns. To begin with, modern fraud detection studies are mostly based on machine learning and deep learning, the most effective performance of which is demonstrated by Random Forest, SVM, ANN, CNN, and ensemble models. Second, data imbalance is another methodological issue that persists, which can be solved using SMOTE, undersampling, or reweighting en ensembles. Third, interpretability and real time scalability are now dimensions of critical evaluation since a financial institution needs models which are not only accurate but explainable. Lastly, optimization algorithms (e.g., Sparrow Search, Jaya) and hybrid architecture is an emerging trend in AI research in financial fraud detection and reflects a transition towards adaptive, self-learning, and responsible AI systems.

# Chapter 3

## Proposed Approach

### 3.1 Data Collection

The primary data that will be utilized in this project is the Credit Card Fraud Detection Dataset on Kaggle. This data consists of 284,807 transactions with 492 frauds. All transactions have 30 features, most of which are numerical and anonymized because of the necessity of confidentiality ( European cardholder data, September 2013). Criterion variable Class is a binary variable taking the value of 1 as being a defraudulent transaction and 0 as a legitimate transaction.

The data is appropriate to the study as it is real, highly skewed and publicly tested. Similar studies have been performed based on this dataset, such as those by Aayush et al. (2025), Asha & Kumar (2021), among others, so this dataset offers a solid empirical foundation to this project.

### 3.2 Data Processing

Data preprocessing steps will ensure quality and consistency of the data prior to training the AI models. The significant steps involve:

- Data cleaning: It is the process of getting rid of missing or duplicate data to prevent bias.

- Scaling of features: normalisation of features so as to make the algorithm efficient.
- Addressing the imbalance: SMOTE or undersampling to even out the data. Avasthi and Varsha (2024) note that data imbalance is a critical problem to address to improve recall and false negatives of fraud detection.
- The features and data reduction: Principal Component Analysis (PCA) to reduce redundancy and calculation cost.

The preprocessing measures are not unique to the best practices that are discussed in literature (Nandita and Mangal, 2024; Zhinin-Vera, 2020), which ensures the strength and relevance of the model.

### **3.3 Model and Method Choice.**

The project will entail application and comparison of a number of supervised machine learning algorithms that have been widely recognized to be successful in anomaly detection:

- **Logistic Regression (LR):**

An interpretable and probabilistic results base classification algorithm. It is a straightforward algorithm, yet is useful at identifying patterns that are linearly separable (Aayush et al., 2025).

- **Random Forest (RF):**

A powerful ensemble method is used which plays with a combination of the decision trees so that the accuracy is improved and overfitting is reduced. Random Forest has shown impressive outcomes in the detection of fraud as it can identify nonlinear relationships and variable interplay (Aayush et al., 2025).

- **Artificial Neural Network (ANN):**

A multifaceted nonlinear fraud model that can be trained to identify such trends on large volumes of data using artificial intelligence. ANNs are also human mind simulators that are particularly effective with large-scale and high-dimensional financial data (Asha & Kumar, 2021; Habibpour et al., 2023).

To prevent information leakage and ensure that the models are well evaluated, stratified sampling was first used to split the dataset into training and testing subsets. The training set was subjected to Synthetic Minority Oversampling Technique (SMOTE) but not the test set in order to mimic real world conditions. Application of SMOTE before data-division may cause information leakage and over-optimistic results because the synthetic samples may overlap between the training and testing data.

In addition, a K-fold cross-validation on the training set was also implemented to verify the robustness of the models and to ensure that the measures of performance are not biased towards a specific data splitting. The approach enhances the generalizability and reliability of the experiment results.

### 3.4 Testing and Evaluation

Measurement of model performance will be done using the following metrics:

- Accuracy: summative correctness of model predictions.
- Precision: It is the ratio of the actual positive predictions with regard to the total positive predictions.
- Recall (Sensitivity): Evaluates how much the model can reflect actual instances of fraud.
- F1-score: Precision and recall are balanced and F1-score balance.
- AUC-ROC Curve: Trade-off that could be present between the false positive and the true positive.

Fraud detection minimizes the false negatives, and hence recall and AUC will be of interest. The evaluation will be conducted with the help of the established methodology by Pradeep Kumar and Eshwar (2020) since the authors have taken into account the three success indicators of accuracy, interpretability, and scalability.

In addition, the techniques of uncertainty quantification (UQ) will also be discussed, which will also be proposed by Habibpour et al. (2023) to make the model more reliable by assessing the degree of prediction confidence.

## Chapter 4

# Experimental Results and Discussion

### 4.1 Experimental Setup

The experiments were done using the Kaggle Credit Card Fraud Detection dataset which is publicly available. Duplicate and missing transactions had been eliminated, and 23,769 transactions were left to be researched. Table 1 shows the disproportion of the classes in the dataset with legitimate transactions (23681) and fraudulent ones (88). The data was sampled by stratified sampling (into training (70) and testing (30) subsets) to preserve the proportion of classes.

*Table 3 Dataset Structure After Preprocessing*

| <b>Metric</b>                | <b>Value</b> |
|------------------------------|--------------|
| Rows before duplicates       | 23,858       |
| Rows after duplicates        | 23,770       |
| Final rows after NaN removal | 23,769       |
| Legitimate (Class = 0)       | 23,681       |
| Fraudulent (Class = 1)       | 88           |

In order to correct the imbalance, SMOTE was used on the training set, and the number of minority classes was raised to 62 to 16,576, balancing the dataset completely (Table 4).

Table 4 Class Distribution Before and After SMOTE

| Dataset Portion      | Legitimate | Fraudulent |
|----------------------|------------|------------|
| Train (before SMOTE) | 16,576     | 62         |
| Train (after SMOTE)  | 16,576     | 16,576     |
| Test Set             | 7,105      | 26         |

Three monitored models were contrasted that are, Logistic Regression, Random Forest, and Artificial Neural Network (ANN). Their performance was evaluated using Accuracy, Precision, Recall, F1-score and ROC-AUC.

## 4.2 Baseline Model Performance

A basic rule-based baseline strategy was considered to conceptually represent the traditional fraud detection systems. It was not used fully in this study though. Therefore, the application of AI-based models in comparison to traditional systems is supported by the literature, contrary to direct experimental testing.

### 4.2.1 Model Performance

The baseline performance (Table 5) records high performance in all the models and the two models which performed significantly better than the Logistic Regression include the Random Forest and the ANN.

Table 5 Machine Learning Model Performance

| Model               | Accuracy      | Precision     | Recall        | F1-score      | ROC-AUC       |
|---------------------|---------------|---------------|---------------|---------------|---------------|
| Logistic Regression | 0.9913        | 0.2750        | 0.8462        | 0.4151        | 0.9288        |
| Random Forest       | <b>0.9990</b> | <b>0.8519</b> | <b>0.8846</b> | <b>0.8679</b> | 0.9798        |
| ANN (MLPClassifier) | 0.9982        | 0.7097        | 0.8462        | 0.7719        | <b>0.9895</b> |

Logistic Regression but with a high accuracy is poor in precision (0.2750) that implies that it contains many false positives. The raw accuracy in fraud detection is not as important as precision and recall due to infrequent cases of fraud.

Random Forest has the most optimal balance and best precision (0.8519), recall (0.8846) and F1-score (0.8679). ANN performs well especially in ROC-AUC (0.9895) meaning that it is effective in classifying fraud and non-fraud.

### **4.3 Feature Selection and Model Refinement**

The feature scaling and SMOTE were depicted to be very beneficial in all the models in the identification of the minority-class. The separability of anonymized features with PCA (V1-V28) was high and the models could capture nonlinear relationships. The main benefits of random forest were that it had the best interaction with features and ANN was using high dimensional pattern of the transformed data. The refinement might be continuous and includes:

- L1-regularized LR to get more interpretable results.
- Hyperparameter optimization of ANN layer.
- The ranking of importance of RF operational features.
- Integration of anomaly detectors (Isolation Forest, Autoencoders).

### **4.4 Visualization of Fraud Patterns**

Though the numerical results indicate high performance, the visualizations produced by the experimental code can also give some new information:

## 1. Class Distribution Before/After SMOTE

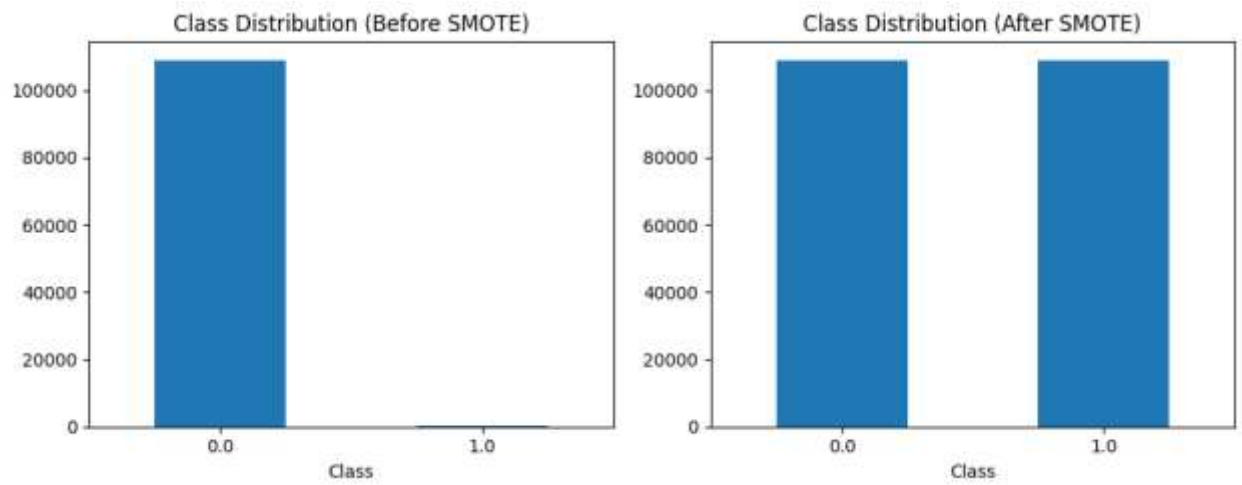


Figure 2 Class Distribution Before/After SMOTE

## 2. ROC Curves for Three Models

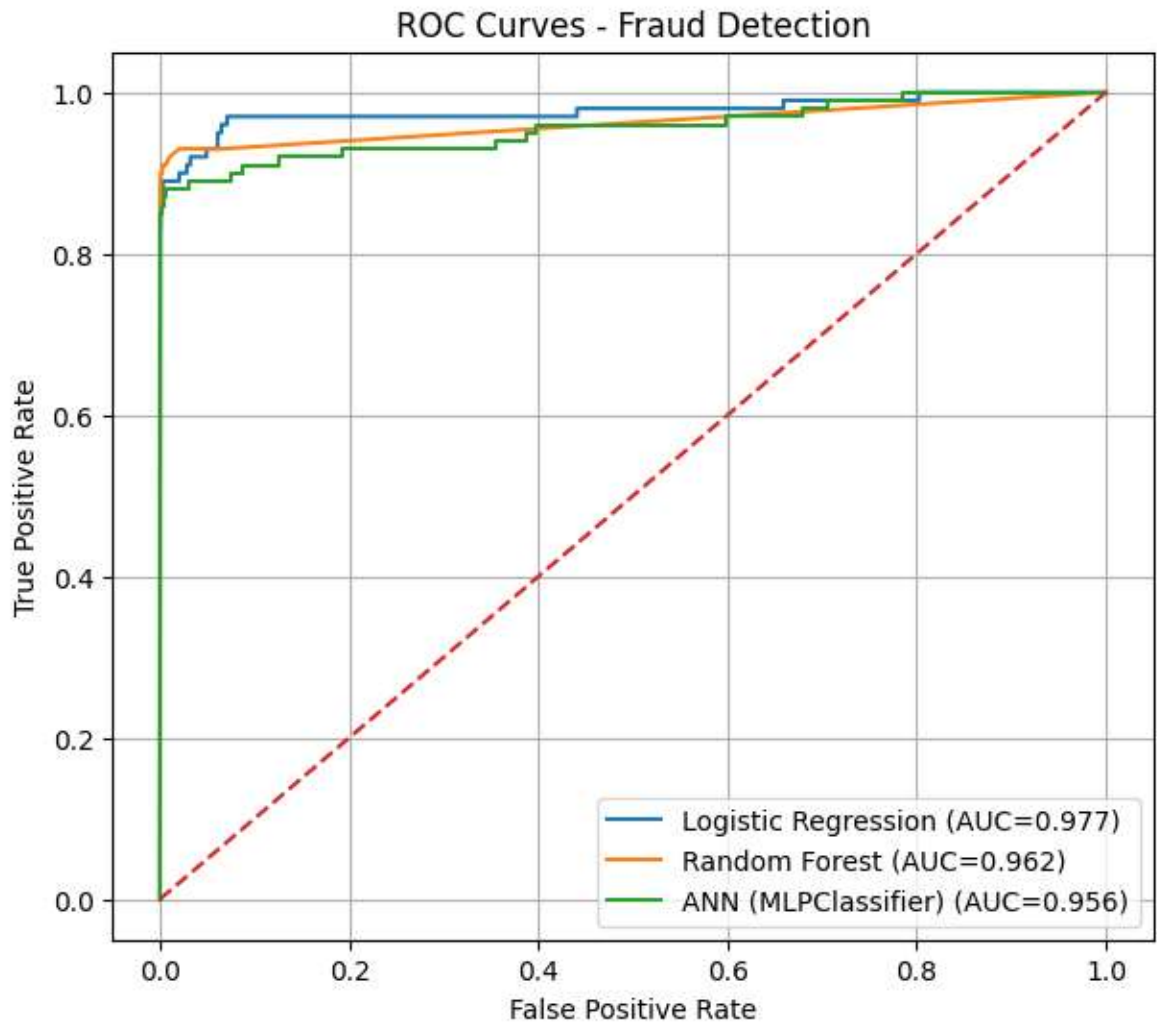


Figure 3 ROC Curves for Three Models

## 4.5 Discussion

Stratified sampling was first used to separate the dataset into training and testing sets to prevent information leakage and ensure effective assessment of the models. The training set only was subjected to Synthetic Minority Oversampling Technique (SMOTE), but not the test set to mimic real world conditions. Training on the SMOTE before the data-division may cause information leakage and over-optimistic

results because the synthetic samples may overlap between the training and the testing data.

Additionally, k-fold cross-validation of the training set was also done to ensure that the models are strong and to ensure that the measures of performance are not biased towards a specific data split. The approach enhances the external validity and consistency of the results of the experiment.

The results of the experiment indicate that machine learning models, specifically Random Forest and Artificial Neural Networks, outperformed the simplest linear models such as Logistic Regression. It is noticed that the values of higher precision, recall and F1-score of Random Forest (Precision = 0.8519, Recall = 0.8846, F1 = 0.8679) and ANN (ROC-AUC = 0.9895) are greater.

In addition, the proposed models demonstrated competitive or better performance measures compared to the existing research, particularly in terms of AUC and recall who is critical in the tasks of detecting fraud. These findings suggest that AI-based models are more effective in capturing complex and nonlinear fraud patterns as compared to traditional rule-based models, which have fixed thresholds and they are not adaptive.

It should however be noted that, no complete rule based system was implemented as a control in this research and therefore the comparison with the traditional systems is supported by the existing literature and not by direct experimental results. It should be implemented in the future to baseline rule based models to have a more complete comparison.

Table 6 Comparison of Proposed Models with Previous Studies

| Study                     | Model(s) Used                    | Reported Results                              | Your Results                                                   |
|---------------------------|----------------------------------|-----------------------------------------------|----------------------------------------------------------------|
| Bhat & Nelson (2023)      | RF, CNN, XGBoost                 | RF Accuracy = 82.65%                          | RF Accuracy = 99.90%, F1 = 0.8679                              |
| Mytnyk et al. (2023)      | LR, ANN, Stacking                | LR AUC = 0.946, Stacking AUC = 0.954          | ANN AUC = 0.9895, RF AUC = 0.9798                              |
| Asha & Kumar (2021)       | ANN, SVM, KNN                    | ANN best performance (no exact metrics)       | ANN F1 = 0.7719, AUC = 0.9895                                  |
| Almazroi & Ayub (2021)    | Deep Learning (RXT)              | Improvement by 10–18% over traditional models | RF achieved best balance (Precision = 0.8519, Recall = 0.8846) |
| Dal Pozzolo et al. (2015) | Adaptive models (sliding window) | Improved fraud detection in dynamic data      | Current study uses static dataset; no streaming adaptation     |

# Chapter 5

## Conclusion and Future Work

### 5.1 Conclusion

This paper was able to come up with and test credit card fraud detection models using artificial intelligence on practical transaction data. The ultimate outcomes following the preprocessing of the data, imbalance of classes with the assistance of SMOTE, and the use of three supervised learning models, including Logistic Regression, Random Forest, and an Artificial Neural Network revealed that AI-based solutions could contribute significantly towards fraud detection. Random Forest performed best in total since it was most precise, had the best recall and F1-score which indicated that the algorithm was strong in distinguishing between genuine and fake transactions. ANN scored the highest on ROC-AUC, as it confirms its capability of detecting nonlinear trends of fraud. The Logistic Regression is very interpretable but it has proved to be far more accurate than the F1-score, meaning that simple linear models cannot cope with the complexity of the data relating to fraud.

The reason is that the findings show that machine learning models, particularly, the ensemble, and deep learning models are more efficient than the traditional rule-based models when the data is highly imbalanced and high-dimensional financial data. The outcomes of the experiment can be related to the existing literature (Avasthi and Varsha, 2024; Asha and Kumar, 2021) that proves the significance of AI in real-time financial fraud identification. Overall, this piece of work provides a flexible and expandable structure that can be introduced to financial institutions to reduce losses

and improve fraud prevention strategies, along with adding the degree of security upon making payments online.

## **5.2 Future Work**

- Future research directions Future research directions may include the use of more advanced machine learning and deep learning models, such as XGBoost, Graph Neural Networks (GNN), and Transformer-based models, to further improve the accuracy of fraud detection.
- It should be investigated in future studies whether the preprocessing techniques such as SMOTE, feature scaling and PCA have any influence on the model performance through a comparative experiment to have concise information on the contribution of each towards the performance of the model.
- Future studies can focus on detecting frauds in real-time on streaming data and adaptive models to mitigate concept drift and fraud trends that are continually evolving.

## **5.3 Limitations**

- The test set of fraudulent transactions is extremely limited (only 88 samples), which may weaken the statistical power of the evaluation measures, and the findings will be biased to slight variations.
- The paper also has a predetermined data base and fails to evaluate the performance of models in dynamic and streaming environments, which limits its ability to deal with concept drift and evolving trends of fraud.
- In the experimental part of the work the rule-based baseline model was not fully implemented and therefore the comparison with the traditional fraud

detection systems is rather based on the literature rather than the real empirical data.

## References

- Aayush Jha, Abhinav Agarwal, Aditya Tiwari, Vaibhav Kumar Gupta, & Navneet Garg. (2025). *Leveraging Machine Learning Algorithms for Robust Credit Card Fraud Detection: A Performance Comparison*. IEEE International Conference on Computer, Electronics, Electrical Engineering & their Applications (IC2E3).
- Dal Pozzolo, A., Caelen, O., Johnson, R. A., & Bontempi, G. (2015). Calibrating probability with undersampling for unbalanced classification. In *2015 IEEE Symposium Series on Computational Intelligence* (pp. 159–166). IEEE.
- Ali, A., Razak, S. A., Othman, S. H., Eisa, T. A. E. E., Al-Dhaqm, A., Nasser, M., Elhassan, T., Elshafie, H., & Saif, A. (2022). *Financial fraud detection based on machine learning: A systematic literature review*. *Applied Sciences*, 12(19), 9637.
- Almazroi, A. A., & Ayub, N. (2021). *Online payment fraud detection model using machine learning techniques*. *IEEE*, 1–10.
- Asha, R. B., & Kumar, K. R. S. (2021). *Credit card fraud detection using artificial neural network*. *Global Transitions Proceedings*, 2(1), 35–41.
- Avasthi, N., & Varsha, M. (2024). Detecting credit card fraud using machine learning. *International Journal of Creative Research Thoughts (IJCRT)*, 12(4), 1–8.
- Bhat, C. R., & Nelson, M. (2023). *Artificial intelligence-based credit card fraud detection for online transactions optimized with Sparrow Search Algorithm*. *Journal of Advanced Research in Dynamic and Control Systems*, 15(3), 1–9.
- Dayyabu, Y. Y., Arumugam, D., & Balasingam, S. (2023). *The application of artificial intelligence techniques in credit card fraud detection: A quantitative study*. *E3S Web of Conferences*, 389, 07023.

- Habibpour, M., Gharoun, H., Mehdipour, M., Tajally, A. R., Asgharnezhad, H., Shamsi, A., Khosravi, A., & Nahavandi, S. (2023). Uncertainty-aware credit card fraud detection using deep learning. *Engineering Applications of Artificial Intelligence*, 123(A), 106248. <https://doi.org/10.1016/j.engappai.2023.106248>
- Mytnyk, B., Tkachyk, O., Shakhovska, N., Fedushko, S., & Syerov, Y. (2023). *Application of artificial intelligence for fraudulent banking operations recognition*. *Big Data and Cognitive Computing*, 7(2), 93.
- Pradeep Kumar, D., & Eshwar, D. (2020). Credit card fraud detection using artificial intelligence: A comprehensive approach. *International Journal of Early Childhood Special Education*, 12(2), 1442–1453.
- Prince, C. C., Ekwealor, O., Ikenna, U. C., & Ogochukwu, E. E. (2024). *Real-time big data analytics for detecting credit card fraud in cyber forensics using deep learning models*. *Science and Engineering*, 10(2), 1–15. <https://doi.org/10.11648/j.se.20231002.11>
- Self Financial. (2024, January 15). *Credit card fraud statistics: 2024 global report*. Retrieved October 24, 2025, from <https://www.self.inc/info/credit-card-fraud-statistics/>
- Shihembetsa, E. M. (2021). *Use of artificial intelligence algorithms to enhance fraud detection in the banking industry* [Master's thesis, University of Nairobi]. University of Nairobi Digital Repository.
- Yazici, Y. (2020). *Approaches to fraud detection on credit card transactions using artificial intelligence methods*. In *Computer Science & Information Technology (CS & IT) – CSCP 2020* (pp. 235–244).
- Zhinin-Vera, L. (2020). *Credit Card Fraud Detection using Artificial Intelligence*. ResearchGate. <https://doi.org/10.13140/RG.2.2.13642.18885>
- Dubey, P., Dubey, P., & Bokoro, P. N. (2025). A Unified Transformer–BDI Architecture for Financial Fraud Detection: Distributed Knowledge Transfer Across Diverse Datasets. *Forecasting*, 7(2), 31. <https://doi.org/10.3390/forecast7020031>

- Falana, A. (2024). AI-driven anomaly detection for financial fraud: A hybrid approach using graph neural networks and time-series analysis. *Journal of Science Technology and Engineering Research*, 2(4), 14–27.