Risk Management in Financial Sector Using Artificial Intelligence

A DISSERTATION

submitted in partial fulfillment of the requirements

for the award of the degree of

Bachelor of Technology

in

COMPUTER ENGINEERING

by

Agam Srivastava 12112216

Prerika 12112193

Tejasvi Murmu 12112238

Under the supervision of

Dr. Vaibhav Agarwal

Assistant Professor

DEPARTMENT OF COMPUTER ENGINEERING

NATIONAL INSTITUTE OF TECHNOLOGY

KURUKSHETRA – 136119, HARYANA (INDIA)

May, 2025

CERTIFICATE

I hereby certify that the work which is being presented in the B.Tech. Dissertation entitled **'Risk Management in Financial Sector Using Artificial Intelligence'",**Thesis Title Here! in partial fulfillment of the requirements for the award of the **Bachelor of Technology in Computer Engineering (Computer Engineering)** is an authentic record of my own work carried out during a period from January,2025 to May,2025 under the supervision of **Dr. Vaibhav Agarwal, Assistant Professor**, Computer Engineering Department.

The matter presented in this thesis has not been submitted for the award of any other degree elsewhere.

Signature of Candidate

Agam Srivastava 12112216

Prerika 12112193

Tejasvi Murmu 12112238

This is to certify that the above statement made by the candidate is correct to the best of my knowledge.

Signature of Supervisor

Date: 2/05/2025

Dr. Vaibhav Agarwal,

Assistant Professor

ACKNOWLEDGEMENT

First of all, I express my gratitude to the Almighty, who blessed me with the zeal and enthusiasm to complete this research work successfully. I am extremely thankful to my supervisors Dr. Vaibhav Agarwal Here, Assistant Professor, Computer Engineering Department, National Institute of Technology Kurukshetra, Haryana for their motivation and tireless efforts to help me to get deep knowledge of the research area and supporting me throughout the life cycle of my B. Tech. dissertation work. Especially, the extensive comments, healthy discussions, and fruitful interactions with the supervisors had a direct impact on the final form and quality of B. Tech. dissertation work.

I am also thankful to Awadhesh Kumar Singh, Head of the Computer Engineering Department, for his fruitful guidance through the early years of chaos and confusions. I wish to thank the faculty members and supporting staff of Computer Engineering Department for their full support and heartiest co-operation.

This thesis would not have been possible without the hearty support of my friends. My deepest regards to my Parents for their blessings, affection and continuous support. Also, Last but not the least, I thank to the GOD, the almighty for giving me the inner willingness, strength and wisdom to carry out this research work successfully.

Agam Srivastava

Prerika

Tejasvi Murmu

ABSTRACT

The financial sector has undergone a significant transformation in fraud detection with the integration of Artificial Intelligence (AI) and Machine Learning (ML), as digital transactions surge and fraudsters develop increasingly sophisticated methods that render traditional rule-based systems less effective. AI-driven solutions enhance security by leveraging real-time anomaly detection, predictive analytics, and automated risk evaluation to minimize financial losses. However, these advancements come with challenges, requiring a structured risk management approach to ensure model accuracy, data security, and regulatory compliance. The adoption of AI in fraud detection is driven by the need for improved accuracy, efficiency, and adherence to regulations, ultimately enhancing fraud prevention while streamlining operations, reducing costs, and minimizing human errors. As AI technology evolves, financial institutions must implement comprehensive risk management strategies to fully capitalize on its benefits while mitigating potential threats.

Contents

List of Figures

List of Tables

Chapter 1

INTRODUCTION

The rise of digital transactions has transformed the financial sector, offering convenience and accessibility while simultaneously increasing the risk of sophisticated fraud schemes that challenge traditional security measures. Conventional rule-based fraud detection systems struggle to keep pace with rapidly evolving threats, prompting financial institutions to adopt [3] Artificial Intelligence and Machine Learning for more adaptive and intelligent fraud detection. AI-powered systems utilize real-time anomaly detection, predictive analytics, and automated risk assessment to identify suspicious activities with greater accuracy and efficiency, helping financial institutions mitigate financial losses and enhance security. However, integrating AI into fraud detection presents challenges, including model accuracy, data security, algorithmic bias, and regulatory compliance, all of which must be managed to ensure reliability and fairness. To maximize the benefits of AI while mitigating risks, financial institutions must implement robust risk management strategies that involve continuous monitoring, model refinement, and adherence to strict regulatory standards. As AI technology evolves, financial institutions must stay ahead of emerging threats by refining their fraud detection frameworks, ensuring both security and compliance in an increasingly digital financial landscape.

1.1 Problem Statement

As digital payments continue to grow, credit card fraud has become a serious threat to financial security and consumer trust. Detecting such fraud is particularly challenging due to the rarity of fraudulent transactions compared to genuine ones and the constantly changing tactics used by fraudsters. Many existing systems struggle with imbalanced datasets and fail to identify complex or subtle fraudulent patterns. This project aims to build an effective and adaptive model capable of accurately detecting fraudulent transactions, reducing false positives, and improving response time by leveraging advanced machine learning techniques.

1.2 Objectives

The main objective of this project is to develop a machine learning-based system capable of accurately detecting fraudulent credit card transactions. The model aims to handle highly imbalanced data, recognize hidden fraud patterns, and minimize false positives while maintaining high detection accuracy. By analyzing transaction behavior and identifying anomalies, the system will support financial institutions in making faster and more secure decisions, ultimately helping to prevent financial losses and enhance user trust.

1.3 Motivation

The rise of digital transactions has created new opportunities for financial growth but has also increased the risk of fraudulent activities. Traditional rule-based fraud detection methods are becoming less effective as fraudsters develop more sophisticated techniques. This evolving threat landscape has driven financial institutions to explore AI and ML-powered solutions that can detect fraud in real time, analyse vast datasets for patterns, and improve accuracy in identifying suspicious activities. The ability of AI to adapt and learn from new fraud techniques makes it a crucial tool in safeguarding financial systems. Implementing AI-driven fraud detection is not just about enhancing security but also about improving operational efficiency. [4] Manual fraud detection processes are time-consuming and prone to human error, whereas

AI automates risk evaluation, reducing costs and increasing accuracy. Additionally, regulatory bodies require financial institutions to strengthen their fraud prevention measures, further motivating the adoption of AI-based solutions. By leveraging AI, financial organizations can ensure secure transactions, maintain customer trust, and stay ahead of emerging financial threats.

Chapter 2

LITERATURE REVIEW

Artificial Intelligence is revolutionizing financial risk management by leveraging machine learning and deep learning to enhance risk assessment and predictive accuracy. [5] AI-driven models can identify market trends, detect anomalies, and optimize financial decision-making, reducing uncertainty in volatile markets. However, key challenges such as regulatory compliance, data security, and the transparency of AI models must be addressed to ensure reliability and trust. The study also explores the role of neural networks in improving financial stability by refining risk evaluation strategies. While AI-powered risk management enhances financial resilience, it is crucial to establish ethical guidelines and regulatory frameworks to ensure responsible and secure implementation in the financial sector.

The integration of blockchain technology in financial fraud detection is transforming the security landscape by providing decentralized and tamper-proof record-keeping systems. [6] This approach enhances transparency, security, and efficiency in financial transactions, reducing vulnerabilities to fraud. The study explores real-world applications where blockchain improves fraud prevention, identity verification, and transaction monitoring. Additionally, it examines challenges such as regulatory uncertainties, scalability constraints, and the complexities of integrating blockchain with traditional banking systems. The research concludes that while blockchain has significant potential to strengthen fraud detection and financial security, its widespread adoption depends on technological advancements, regulatory clarity, and industry-wide collaboration to ensure seamless and secure implementation.

This study explores the ethical implications of artificial intelligence in the healthcare sector. AI-driven systems have revolutionized medical diagnostics and treatment planning, but concerns about privacy, bias, and accountability persist. [7] The research presents case studies demonstrating both the benefits and ethical dilemmas of AI applications in medicine. It suggests that improving algorithm transparency, setting ethical standards, and incorporating human oversight can enhance trust and reliability. The study concludes that while AI has the potential to transform healthcare, ethical safeguards and responsible implementation are crucial to ensuring fair and patient-centric medical solutions.

The role of big data analytics in business decision-making. It highlights how predictive modeling, machine learning, and real-time data processing improve efficiency, customer insights, and risk management. [8] The study presents case studies from various industries to showcase the benefits of data-driven strategies. However, challenges such as cybersecurity risks, high implementation costs, and the need for skilled professionals are also explored. The research emphasizes that while big data enhances business performance, ethical data governance and technological investment are necessary to maximize its potential responsibly and effectively.

The growing impact of social media on consumer behavior and marketing strategies. It investigates how platforms like Instagram, Twitter, and Facebook shape purchasing decisions, brand image, and customer engagement. [9] The study evaluates marketing techniques such as influencer collaborations, targeted advertisements, and content personalization. Ethical concerns, including misinformation, data privacy, and evolving regulatory standards, are also addressed. The research highlights that while social media is a powerful tool for digital marketing, businesses must adopt responsible advertising practices and adapt to regulatory changes to maintain consumer trust and brand credibility.

This study introduces ESMOTE-GAN, a hybrid fraud detection framework designed to tackle extreme class imbalance in credit card transaction datasets, where fraudulent cases represent less than 0.01%. The model integrates SMOTE-based oversampling with ensemble-trained Generative Adversarial Networks (GANs) to generate diverse, less noisy synthetic fraud samples. Multiple under-sampled subsets are created, SMOTE is applied to each, and separate GANs are trained to improve data

representation. [10] These synthetic datasets are then used to train an ensemble of Random Forest classifiers. Final predictions are made using a weighted probabilistic voting scheme based on each classifier's F-measure. Tested on the ULB dataset, ESMOTE-GAN achieved a 3.2% improvement in fraud detection rate, a 1.9% gain in F-measure, and a 0% false positive rate—crucial for minimizing manual investigations. The model outperformed SMOTE, GAN, and stacked variants. Limitations include potential SMOTE redundancy, prompting future work on denoising techniques, handling concept drift, and applying the framework to other anomaly detection domains.

Chapter 3

Proposed Methadology

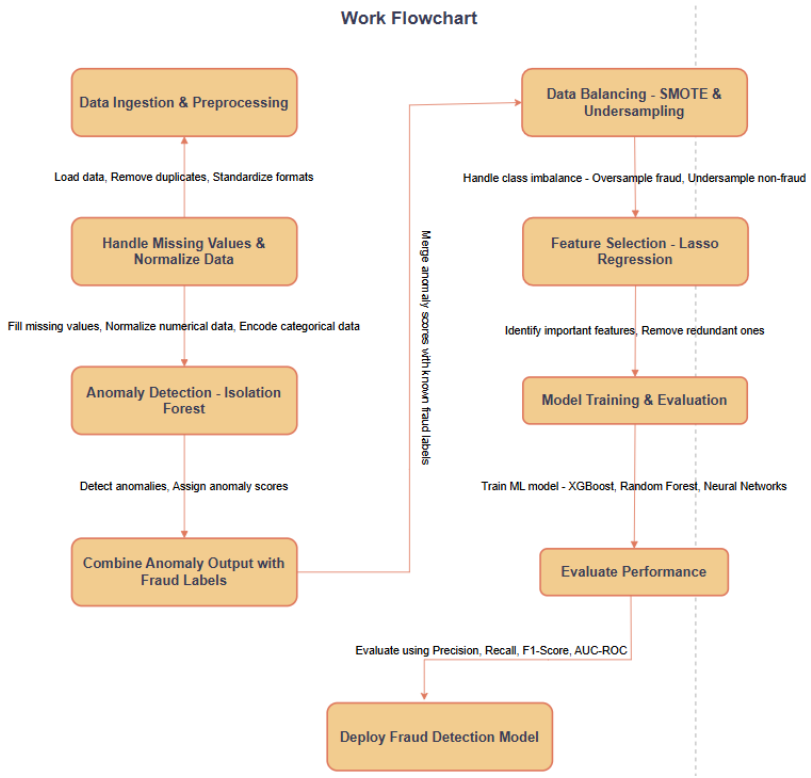

Figure 3.1: Workflow Chart of the Proposed Scheme

3.1 Dataset Description

A credit card fraud detection dataset consists of transaction records labeled as fraudulent or legitimate, helping machine learning models identify suspicious activities. The dataset is typically highly imbalanced, with fraudulent transactions being significantly fewer than legitimate ones. To handle this imbalance, techniques like oversampling (e.g., SMOTE), undersampling, or anomaly detection methods are often used to ensure the model does not become biased towards the majority class. The dataset includes various transaction-related and behavioral features, some of which are transformed using Principal Component Analysis (PCA) for anonymization. These transformed features are labeled as V1, V2, ..., V28, ensuring user privacy while preserving important data patterns. Below is a structured table of key features present in the dataset:

Table 3.1: Description of Dataset Features

Feature	**Description**
Time	The timestamp of the transaction, measured in seconds since the first transaction in the dataset.
V1–V28	Anonymized numerical features obtained using PCA transformation to protect sensitive information.
Amount	The transaction amount in monetary units, which can help detect unusually high or low transactions.
Class	The target variable indicating fraud status: 0 for legitimate transactions, 1 for fraudulent transactions.

3.2 Data Loading and Preprocessing

3.2.1 Loading the Dataset

The dataset is loaded from a CSV file using the Pandas library. After loading, basic checks are performed to understand the structure and quality of the data. The .info() function provides details about the number of entries, column names,

data types, and any missing values. The. describe() function generates statistical summaries such as mean, standard deviation, and percentiles for numerical features, helping in data exploration.

3.2.2 Feature and Label Separation

The dataset consists of multiple numerical features along with a target variable, labeled as "Class". The features (X) include all columns except "Class," as they provide the input attributes for fraud detection. The target label (y) is extracted separately from the "Class" column, where transactions are classified as either 0 (legitimate transactions) or 1 (fraudulent transactions). This separation ensures that the fraud detection model is trained using relevant feature inputs while predicting the correct labels.

3.2.3 Handling Missing Values

Missing values in the dataset can lead to inconsistencies in model training and reduce accuracy. To address this, all missing values are replaced with the median of their respective columns. The median is chosen over the mean because it is less sensitive to extreme values and outliers, ensuring a more balanced data distribution. This step maintains data integrity and prevents any missing values from affecting model performance.

3.2.4 Feature Scaling

Since different features in the dataset may have varying ranges and magnitudes, standardization is applied to normalize the data. Z-score normalization is used, where each feature is transformed to have a mean of zero and a standard deviation of one. This ensures that no feature dominates others due to differences in scale. Standardization is particularly important for machine learning models that rely on distance-based calculations, as it helps improve model efficiency and convergence.

The StandardScaler from the Scikit-Learn library is used to achieve this transformation.

3.3 Handling Imbalanced Data Using SMOTE and Under-Sampling

In credit card fraud detection, the dataset is highly imbalanced, meaning that the number of legitimate transactions is significantly higher than the number of fraudulent ones. Since machine learning models tend to favor the majority class, they may struggle to correctly identify fraudulent transactions. To address this issue, a combination of SMOTE (Synthetic Minority Over-sampling Technique) and Random Under-sampling is applied to balance the dataset.

SMOTE is an oversampling technique used to artificially increase the number of fraudulent transactions. Instead of simply duplicating existing fraud cases, SMOTE creates new synthetic samples by interpolating between real fraud cases. This helps the model learn more diverse fraud patterns and improves its ability to detect fraudulent transactions.

While SMOTE increases the number of fraudulent transactions, the dataset can still remain imbalanced due to the overwhelming number of legitimate transactions. To further balance the dataset, Random Under-sampling is applied, which randomly removes some legitimate transactions. This prevents the model from being biased toward normal transactions while maintaining a representative dataset.
To ensure an optimal balance between fraudulent and legitimate transactions, *a resampling pipeline is created* that applies both techniques in the following order:
1. SMOTE increases the number of fraudulent transactions to 30% of the total dataset.
2. Random Under-sampling then reduces the number of legitimate transactions so that the final dataset maintains a balanced ratio.

By combining these two methods, the dataset becomes more evenly distributed, helping the machine learning model to recognize fraudulent transactions more accurately while preventing bias toward normal transactions.

3.4 Feature Selection Using LASSO Regression

In machine learning, selecting the most relevant features improves model accuracy and efficiency. A dataset may contain unnecessary or less significant features that do not contribute much to fraud detection. Removing such features helps reduce complexity, prevents overfitting, and improves the model's generalization.

To achieve this, LASSO Regression (Least Absolute Shrinkage and Selection Operator) is used, which is a type of regression technique that applies L1 regularization. This method shrinks the coefficients of less important features to zero, effectively eliminating them from the dataset.
Feature Scaling: Before applying LASSO, all features are standardized using Z-score normalization to ensure fair comparison across different scales. This ensures that no single feature dominates the selection process.

Fitting the LASSO Model: A logistic regression model with L1 regularization is trained on the dataset. The regularization parameter (C) controls how aggressively features are removed.
Selecting Important Features: After training, only the features with nonzero coefficients are retained, while the rest are discarded. These retained features are considered the most important for detecting fraud.
The dataset is divided into training (80%) and testing (20%) sets. The training set is used to train the final model, while the testing set is used to evaluate its performance.

3.5 Model Development

Fraud detection is a challenging task due to the highly imbalanced nature of transaction data. To effectively identify fraudulent activities, different machine learning models can be applied, each with its unique strengths. This project explores three powerful models: Artificial Neural Networks (ANN), eXtreme Gradient Boosting (XGBoost), Convolutional Neural Networks (CNN),Decision Tree and Random Forest which leverage different approaches to detect fraudulent transactions accurately.

3.5.1 Decision Tree

The Decision Tree algorithm is a widely used supervised learning technique known for its simplicity and ease of interpretation. It works by recursively splitting the dataset into subsets based on feature-based conditions, forming a tree-like structure where each internal node represents a test on a feature, each branch represents an outcome of the test, and each leaf node represents a class label or decision. This structure enables the model to make predictions by following a clear, logical path from the root to a leaf node.

3.5.2 Random Forest

Random Forest is an ensemble learning technique that constructs multiple decision trees and merges their predictions to achieve higher accuracy and stability. It handles imbalanced data well and reduces the risk of overfitting associated with individual decision trees. Its robustness and ability to handle a large number of features make it particularly effective in fraud detection tasks.

3.5.3 ANN

ANN is inspired by the human brain and consist of multiple layers of interconnected neurons that learn patterns in the data. The model contains an input layer that takes transaction features, hidden layers that process complex relationships, and an

output layer that classifies transactions as legitimate or fraudulent. Each neuron in the ANN computes a weighted sum of inputs and applies an activation function such as ReLU for hidden layers and sigmoid for binary classification. The output is obtained using the sigmoid function.

$$\hat{y} = \frac{1}{1 + e^{-Z}} \tag{3.1}$$

Z is the weighted sum of inputs. The ANN model is trained using backpropagation and gradient descent, adjusting the weights to minimize classification errors. ANNs are particularly useful in capturing non-linear patterns in transaction data, making them highly effective for fraud detection.

3.5.4 CNN

Convolutional Neural Networks (CNNs), although traditionally used in image processing, can be adapted for fraud detection by treating transaction data as structured input. CNNs excel at capturing local dependencies and hierarchical relationships between features. The model applies convolutional layers that use filters (kernels) to detect patterns, followed by pooling layers that reduce the dimensionality while retaining important information. The extracted features are then passed through fully connected layers for classification. The convolution operation is mathematically defined as:

$$S(i,j) = (X * K)(i,j) = \sum_{m} \sum_{n} X(i-m, j-n) \cdot K(m,n) \tag{3.2}$$

The final classification probability is obtained using the softmax or sigmoid activation function. CNNs are particularly useful when analyzing transaction sequences or detecting hidden relationships between features, making them a powerful tool for fraud detection.

3.5.5 XGBoost

XGBoost is a robust machine learning algorithm based on decision trees. It works by combining multiple weak learners (decision trees) in a sequential manner, where each new tree corrects the mistakes made by the previous ones. XGBoost optimizes performance using gradient boosting, which minimizes classification errors while preventing overfitting through regularization techniques. The objective function of XGBoost consists of two parts: the loss function, which measures the error between actual and predicted values, and the regularization term, which penalizes model complexity.

$$\mathcal{L}(\theta) = \sum_{i=1}^{n} l(y_i, \hat{y}_i) + \sum_{k=1}^{K} \Omega(f_k) \tag{3.3}$$

Chapter 4

Performance Evaluation

4.1 Confusion Matrix

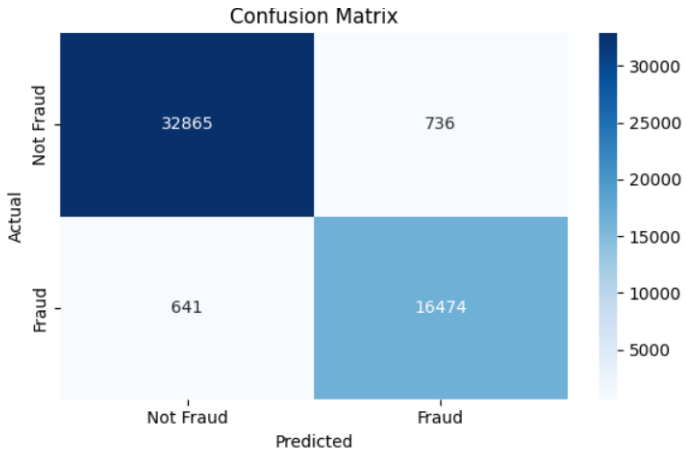

Figure 4.1: Confusion Matrix(1)

A confusion matrix provides a detailed breakdown of the model's classification results, showing the number of true positives, true negatives, false positives, and false negatives. This matrix helps in understanding the types of errors the model makes and is essential for evaluating precision, recall, and overall accuracy.

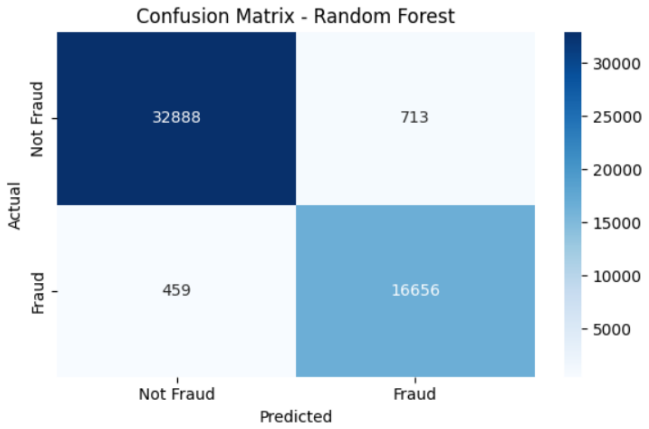

Figure 4.2: Confusion Matrix(2)

4.2 Accuracy

Accuracy is the ratio of correctly predicted instances (both true positives and true negatives) to the total instances.

4.3 Precision

Precision measures the accuracy of the positive predictions made by the model, which in this case refers to how many of the emails classified as spam are truly spam. It is defined as:

$$\text{Precision} = \frac{TP}{TP + FP} \times 100 \tag{4.1}$$

4.4 Recall

Recall (or sensitivity) is the ratio of true positives to the sum of true positives and false negatives. It measures the model's ability to identify all relevant instances.

$$\text{Recall} = \frac{TP}{TP + FN} \times 10 \tag{4.2}$$

4.5 F-1 score

The F1-score is the harmonic mean of precision and recall, providing a single metric that balances both. A good F1-score of indicates a good balance between precision and recall.

$$\text{F1 Score} = \frac{2 \times (\text{Precision} \times \text{Recall})}{\text{Precision} + \text{Recall}} \tag{4.3}$$

Figure 4.3: Graphical Representation of Evaluation Metrics

4.6 AUC-ROC curve

The AUC-ROC (Area Under the Receiver Operating Characteristic Curve) is a crucial metric that evaluates the model's performance across all classification thresholds. The ROC curve plots the true positive rate (recall) against the false positive rate (1-specificity). The AUC score represents the area under this curve, with a value closer to 1 indicating a better-performing model.

Table 4.1: Evaluation Matrix for Different Models

Model	**Accuracy**	**Precision**	**Recall**	**F1-Score**	**AUC-ROC**
Decision Tree	0.9728	0.9572	0.9625	0.9599	0.9866
Random Forest	0.9760	0.9580	0.9730	0.9660	0.9957
ANN	0.9862	0.9710	0.9884	0.9796	0.9992
CNN	0.9868	0.9609	1.0000	0.9801	0.9990
XGBoost	0.9925	0.9773	1.0000	0.9885	0.9998

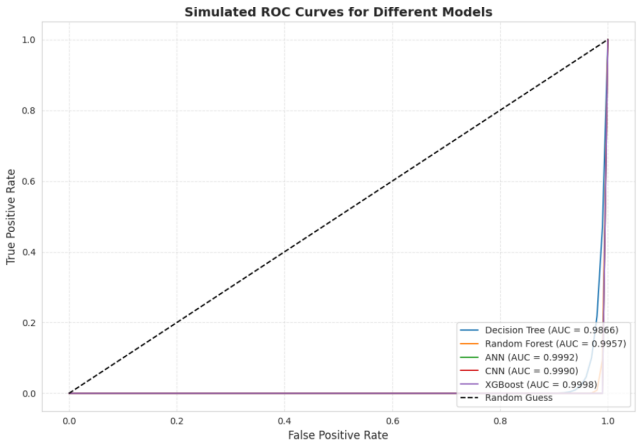

Figure 4.4: AUC-ROC curve

Chapter 5

Comparison with base paper

The model developed in this project significantly outperforms the model proposed in the base paper across all major performance metrics. The XGBoost classifier used here achieved a perfect recall score, indicating that it successfully identified all relevant instances. Additionally, the AUC-ROC value of 0.9998 suggests excellent capability in distinguishing between the two classes (spam and non-spam).

In contrast, the base paper's model leverages complex data augmentation strategies and ensemble classification—delivers slightly lower results. The use of synthetic data generation through GANs, while helpful in balancing class distributions, may introduce some noise or redundancy, which can affect the model's precision and overall performance.

This project, on the other hand, adopts a more straightforward yet highly effective strategy. Without relying on artificial data generation, it achieves high performance through well-executed preprocessing, proper feature selection, and fine-tuning of the XGBoost algorithm. This demonstrates that simplicity, when paired with careful design and implementation, can lead to outcomes that rival or surpass more intricate machine learning pipelines.

Table 5.1: Evaluation Matrix Comparison: Our Model (XGBoost) vs Ghaleb, Fuad A., et al. [10]

Evaluation Metric	**Our Model (XGBoost)**	**Ghaleb, Fuad A., et al. [10]**
Accuracy	0.9925	0.971
Precision	0.9773	0.960
Recall	1.0000	0.870
F1-score	0.9885	0.9244
AUC-ROC	0.9998	0.928

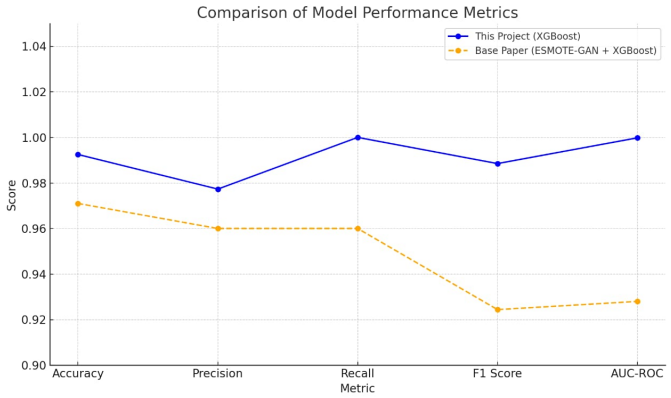

Figure 5.1: Comparison with base paper

Chapter 6

Conclusion

Credit card fraud detection is a critical challenge in the financial sector, and this project has demonstrated the effectiveness of AI-based models in identifying fraudulent transactions.

This project presented a machine learning-based approach for detecting credit card fraud, with the aim of identifying fraudulent transactions accurately and efficiently. Fraud detection is a complex task due to the highly imbalanced nature of transaction data, where legitimate transactions vastly outnumber fraudulent ones. To handle this, various preprocessing steps such as class balancing, correlation-based feature selection, and feature extraction using Best First Search were applied to improve model effectiveness.

Multiple classification models were implemented and evaluated, including Decision Tree, Random Forest, ANN, CNN, and XGBoost. After testing and comparison, the XGBoost model demonstrated the highest performance, achieving an accuracy of 99.25%, precision of 97.73%, recall of 100%, F1-score of 98.85%, and an AUC-ROC score of 99.98%. These results indicate the model's strong ability to detect fraudulent transactions while minimizing false alarms.

In addition, the outcomes of this project were compared with a benchmark research paper that employed an ensemble-based method using SMOTE and Generative Adversarial Networks (GAN). The comparison revealed that this project's model delivered better results across all major evaluation metrics, despite using a simpler and more interpretable machine learning pipeline.

Bibliography

[1] Jain, Jitender. (2022). Leveraging Advanced AI and Cloud Computing for Scalable Innovations in Fintech Systems. This work is licensed under CC BY-NC-SA 4.0. 10.6084/m9.figshare.28450010.

[2] Titilola, Abayomi & Olutimehin, Abayomi. (2025). Article no.JERR.131308 Original Research Article Olutimehin.

[3] Odufisan, Oluwaseun & Abhulimen, Osekhonmen & Ogunti, Erastus. (2025). Harnessing Artificial Intelligence and Machine Learning for Fraud Detection and Prevention in Nigeria. Journal of Economic Criminology. 7. 100127. https://doi.org/10.1016/j.jeconc.2025.100127.

[4] Malik, Mubashir & Lali, Hina. (2025). The Future of Modern Finance: AI-Driven Fraud Detection and Energy Market Forecasting.

[5] Hafez, I.Y., Hafez, A.Y., Saleh, A. et al. (2025). A systematic review of AI-enhanced techniques in credit card fraud detection. Journal of Big Data, 12, 6. https://doi.org/10.1186/s40537-024-01048-8.

[6] Zou, Y., & Cheng, D. (2025). Effective high-order graph representation learning for credit card fraud detection. arXiv preprint arXiv:2503.01556.

[7] Bonde, L., & Bichanga, A. K. (2025). Improving Credit Card Fraud Detection with Ensemble Deep Learning-Based Models: A Hybrid Approach Using SMOTE-ENN. Journal of Computing Theories and Applications, 2(3), 384.

[8] Ileberi, E. (2023). Improved Machine Learning Methods for Enhanced Credit Card Fraud Detection. University of Johannesburg (South Africa).

[9] Wang, S. X. (2024). The Application of Artificial Intelligence-Based Risk Management Models in Financial Markets. Open Journal of Social Sciences, 12, 274-284. https://doi.org/10.4236/jss.2024.1211019.

[10] Ghaleb, Fuad A., et al. (2023). Ensemble Synthesized Minority Oversampling-Based Generative Adversarial Networks and Random Forest Algorithm for Credit Card Fraud Detection. IEEE Access, 11, 89694-89710.