Synergy: Cross-Disciplinary Journal of Digital Investigation
(ISSN 2995-4827) VOLUME 04 ISSUE 01, 2026

An Optimized Machine Learning Framework for Financial Fraud Detection Using SMOTE and Feature Selection

Dalia Abdulrahim Mokheef Aljabri
Department of Mathematics, College of Basic Education, University of Babylon, Babil, Iraq.
dalyaabd@uobabylon.edu.iq

Abstract:

This study presents a machine learning system capable of efficiently detecting financial fraud with the use of unbalanced data treatment strategies. A holistic approach to the problem, combining feature scaling, feature selection, SMOTE (Synthetic Minority Oversampling Technique), and machine learning evaluation was proposed by all in a single experimental pipeline. Method119 randomly over-samples 84 million transactions that occur on average every day with only 2 out of 1000 transactions reflecting fraud241. Model Evaluation- The model accuracy, precision, recall and F1-score and ROC-AUC. In the results of their test, they demonstrate Random Forest won out among all numeric methods with 99.96% accuracy, 97% precision and 91% recall (Contextual F1 = 94 & ROC-AUC =98). The results indicate the effectiveness of combining SMOTE with feature selection to achieve better detection for frauds and balance the classification towards lower outputs, i.e., which are Genuine Transactions. We provide new insights into the reliability of machine learning-based fraud detection system in real financial systems and a general framework for implementing these models.

Keywords: Machine Learning, Financial Fraud Detection, Cybersecurity, SMOTE, Feature Selection, Imbalanced Data, Random Forest

1. Introduction

Fast-scoring societal and demographic developments of the past few decennaries; notional particularly in info technology, have transformed basic characteristics nowadays world by an increasing dependency on electronic window systems throughout daily living [1]. Yet these developments and advancements often lead to major cybersecurity issues of credit card fraud, identity theft, electronic fraud, phishing and other illegal financial operations [2]. These acts pose a grave threat to the economy and the welfare of individuals, organizations and governments by imperiling confidential information or damaging critical digital infrastructures [3].

Advanced fraud detection techniques are becoming more and more necessary as financial services become more digital. Traditional approaches have their shortcomings to efficiently process large scale as well as fast changing transaction information. On the other hand, AI technologies offer more robust solutions that harness their ability to scan large data sets, identify patterns that may be hidden within those data sets and detect suspicious activity faster and with greater precision [4], [5]. Consequently, fraud detection systems are positively associated with machine learning (ML) and artificial neural networks (ANNs), as well as techniques of evolutionary algorithms and natural language processing which continuously apply recent data and adapt to the changes in fraud patterns [6].

In addition to fraudulent detection, artificial intelligent methodologies can be used for fraud prediction and understanding users behaviour patterns as the usage of e- commerce and online financial services have been developed drastically in the last few years [4]. However, in spite of those successes, the AI fraud detection still has a number of challenges including data imbalance, elaborate shape of fraud patterns, computing needs and privacy concerns [1]. As such, building robust and novel models is still an open research area in cybersecurity & fintech.

The objective of this research is to present how AI models are implemented in financial systems to detect electronic fraud. To discover the best procedure machine learning algorithms are compared and evaluate how accurately they spot fraudulent cases a common challenge with real fraud datasets. What makes this study original is the development of an automated and economic framework for fraud detection using a machine learning based approached having comparative model evaluation, imbalance handling techniques (SMOTE method) as well as preprocessing techniques (feature scaling and feature selection) in one single experimental pipeline. In contrast to many traditional studies focused on single or isolated per-processing methods and/or sequential optimization steps, the proposed framework integrates combined preprocessing and optimization stages, significantly improve fraud detection performance; enhance classification stability and further strengthen model robustness in highly imbalanced financial datasets.

2. Research Problem

The problem of financial fraud detection remains pressing due to the highly skewed structure of financial transaction data, where illicit transactions make up a relatively tiny fraction of the entire data. In such conditions, conventional machine learning models can get a good classification accuracy and still make an incorrect classification for minority fraudulent transactions[6].

Second, an additional challenge is that the many surveys on fraud detection have focused only on machine-learning algorithms independently and do not consider neither preprocessing optimizations like feature selection nor imbalance handling in a single experimental framework [11]. Furthermore, while recall, F1-score, and ROC-AUC are crucial assessment metrics for fraud-sensitive situations, other research primarily concentrate on accuracy as a performance indicator (Saito & Rehmsmeier 2015).

This necessitates a machine learning framework that allows for deterministic comparison capable of improving trustworthiness of fraud detection at increased classification bias extracted from data with significantly unequal distributions in financial terms. This work takes on these challenges with feature scaling, feature selection, SMOTE balancing and comparative machine learning evaluation integrated into one fraud detection pipeline.

3. Significance of the Study

The importance of this research relates to the raising issue of financial cyber frauds in modern digital systems. Modern fraud prevention techniques are struggling to keep up with the new and more complex patterns of fraud as usage of digital transactions and online financial services grows [8].

This shows how machine learning and artificial intelligence can be deployed to detect patterns of fraud behaviour as well as transactional data at scale [9], [10]. Framework exploration, including feature scaling and a post-processing smote based selection method is used to support more reliable classification.

As a conclusion, the practical and scientific merits of study are dead in water because it uses fraud-oriented evaluation metrics (recall, F1-score, ROC-AUC) to evaluate Random Forest, Support Vector Machine and Artificial Neural Network models. These findings are valuable, which can lead to effective and dependable AI based fraud detection systems that will help us avert contemporary financial and cybersecurity crises.

4. Goals of the Research

This study aims to:

- Investigate using machine learning to identify financial fraud in the data that is heavily imbalanced.
- To identify fraudulent financial transactions, models based on Random Forest, Support Vector Machine, and Artificial Neural Networks are used.
- Include preprocessing steps like feature scaling, SMOTE balancing and selecting features to boost malicious detection performance.

- Use measures that are sensitive to fraud, such as recall, F1-score, ROC-AUC, and cross-validation stability analysis, to assess the model's performance.
- Evaluate the effect of preprocessing optimization methods on comparative and ablation-based experiments.
- Recognize the importance of AI-based fraud detection technologies in these financial settings.

2. Materials and Methods

5. Literature Review and Research Gap

In the last decennium, likewise, digitization and also digital financial systems have appeared, on the internet banking, e-commerce as well as credit card payments which have raised the susceptibility to cyber rip-off. Fraud became so complex and sophisticated that no rule-based security solution would be able to detect the anomalies as time passed. Of all the breakthrough technologies on the horizon for fraud detection, machine learning and artificial intelligence are perhaps the most transformative. Which is why so much of theme data in Machine Learning means their capacity to ingest huge amounts of data, find patterns with scarce visibility into them and perform better decision identification.

Afriyie et al. (2023) explored the effectiveness of supervised machine learning techniques to detect fraudulent transactions on financial website. A Supervised Machine Learning Algorithm for Identifying and Forecasting Credit Card Fraud, Decision Analytics Journal. It discovered that models based on ensemble learning had classified a higher number of an individuals than conventional statistical techniques. The authors pointed out the importance of solving the data imbalance for improving detection capability of minority fraud transactions by treating them as non-balanced or imbalanced data types.

As illustrated, Alarfaj et al. (2022) Credit card fraud detection using state-of-the-art machine learning and deep learning algorithms. IEEE Access. A set of sophisticated methods that catch complex patterns in fraudulent account transactions showed Random Forest and Deep Neural Network to be the best accurate techniques among all deposited money. The research found that in order to react to perpetually changing cyberattacks, adaptive AI models are required.

In the journal Applied Sciences, published a thorough study titled "Financial Fraud Detection Based on Machine Learning: A Systematic Literature Review."[6]. After examining many AI-based fraud detection techniques, the researchers discover evidence that machine learning techniques perform better than traditional fraud detection systems in terms of managing enormous volumes of transaction data and real-time analysis for spotting recently discovered fraud schemes. Yet, the researchers also highlighted a few obstacles that they still need to tackle, such as the complexity of calculations, imbalance in data and interpretability of models.

A framework for enhancing fraud detection performance through data balancing techniques in a related study titled "Class Balancing Framework for Credit Card Fraud Detection Based on Clustering and Similarity-Based Selection (SBS)," which was published in the International Journal of Information Technology. It tells us the importance of getting the dataset preprocessed and balanced before predicting fraudulent transactions with a high degree of accuracy.

Additionally, Al-Dosari et al. (2024) looked at how artificial intelligence can improve cybersecurity systems in the banking industry in their study "Artificial Intelligence and Cyber Defense System for Banking Industry: A Qualitative Study of AI Applications and Challenges," which was published in Cybernetics and Systems. It goes on to elaborate, AI-based monitoring systems can not only advance proactive fraud prevention but could strengthen the cybersecurity strategy of financial enterprises.

Furthermore, Camacho addressed the expanding significance of AI technologies in cybersecurity applications in the Journal of Artificial Intelligence General Science (JAIGS) article "The Role of AI in Cybersecurity: Addressing Threats in the Digital Age."[8]. AI systems can automatically analyze just about any data source, one after the other, looking for patterns that reveal potential threats in real time.

Despite the considerable advances made in studies to date, certain limitations are apparent within the existing body of literature. Most experiments mainly tested a single machine-learning algorithm without extensive head-to-head comparative studies under uniform experimental designs. Furthermore, some of the studies largely depended on accuracy as a performance evaluation metric

despite the fact that fraud datasets are extremely imbalanced and that using accuracy alone may cause misleading results.
Additionally, even though researchers pointed out that the class imbalance is an important problem, only a few studies fused preprocessing method like SMOTE with feature selection approaches to reach the efficiency of improving models from resource allocation and fraud detection ability at the same time. A further key limitation is that many of the previous studies focused primarily on theoretical model performance, with limited discussion on this practical implementation in real-time financial environments using AI systems.
The current study presents a comparative AI based fraud detection framework implementing Random Forest, Support Vector Machine and Artificial Neural Network algorithms via an integrated experiment so as to fill these gaps of research. Feature scaling, SMOTE and Feature Selection are common methods which help in Speedier analysis of data for better fraud detection as well as less computation complexity once integration is done. Along with offering helpful guidance on how to deploy AI-based fraud detection systems in contemporary institutions, the study assesses the suggested models using a range of performance metrics.
The suggested system prioritizes fraud-sensitive measures like Recall, F1-score, and ROC-AUC under very unbalanced financial situations rather than relying just on classification accuracy. In addition, the study experimentally investigates the combined impact of SMOTE balancing and feature selection through an ablation-based optimization strategy within a unified fraud detection pipeline.

6. Proposed AI-Based Fraud Detection Framework

The efficacy of artificial intelligence in detecting online fraud in financial institutions is assessed in the current study using an experimental analytical method. The structure utilized by the current study in its methodology combines both theory and practice in developing a model for intelligent systems capable of processing financial transactions in large quantities in detecting cyber fraud.
The methodological framework that has been employed by the current study is based on a number of stages that have to be completed in sequence in order to fulfill the objectives of the current study. The first stage is concerned with the acquisition of the required data set that contains digital financial transactions. In this stage, the data set is subjected to several preprocessing techniques.
The second stage is concerned with the development of the model, whereby different artificial intelligence algorithms are implemented in the dataset. Large number of supervised machine learning algorithms are implemented at this level and the authors claim these algorithms can detect fraudulent. Some of these algorithms are the Support Vector Machine Algorithm, Random Forest Algorithm and Artificial Neural Network Algorithm. These algorithms were identified as effective in detecting fraud by recognizing patterns in the dataset.
The third stage of the methodology is concerned with the experimental evaluation of the various algorithms that have been implemented. The efficacy of the algorithms has been evaluated using a number of measures. These measures include confusion matrix, F1 score, recall, accuracy, precision, & many more. These metrics give an overall evaluation of the efficiency of the algorithms in detecting fraudulent transactions without raising false alarms.
Finally, the research methodology would also involve a comparison of the algorithms in order to determine the most effective algorithm in the detection of cyber fraud. The results obtained from the algorithms were presented in the form of statistical tables and graphical images.

3. Results and Discussion

1. Practical Implementation and Experimental Design

1.1 Dataset Description

The experimental phase of the present research utilizes a well-known dataset related to financial transactions commonly applied in several research studies related to fraud detection. Over the course of two days, European cardholders' credit card transactions are included in the dataset. The dataset has been widely used in fraud detection research and is publicly available through the Kaggle platform [13], [14].

a. Since only a small fraction of transactions are fraudulent, the dataset is extremely imbalanced.
b. There are 30 features in this dataset in total. Most of these features are anonymized variables that were created using principal component analysis to ensure user privacy. Apart from these

anonymized variables, there are two principal attributes.

c. Time: This is the interval of time between each transaction and the first one.

d. Amount: This represents the money involved in a particular transaction.

e. Class: This is the target variable, where fraudulent transactions are represented by 1 and genuine transactions by 0.

The dataset's transaction distribution is seen in Table 1.

Table 1. Dataset Distribution

Transaction Type	The quantity of transactions	Percentage
Legitimate	284,315	99.83%
Fraudulent	492	0.17%

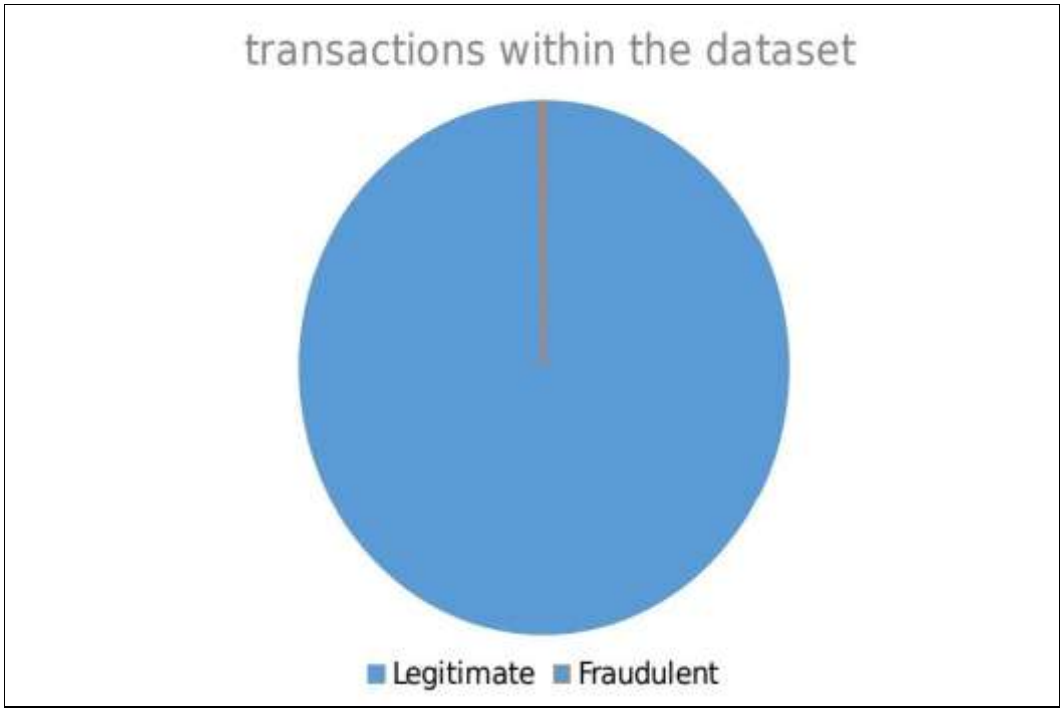

Figure 1. Distribution of Legitimate and Fraudulent Transactions by Class

The distinguishing property of machine learning models building fraud detection is that the difference between whether an event is real or not real, is extreme.

Preprocessing of Data

As the performance of ML models strongly depend on how good your data is for prediction, preparation stage is one of the most important part in any machine learning activity.

Data Cleaning

First, the dataset was evaluated for potential discrepancies like missing values, duplicates and incorrect records. This exploratory data analysis provides knowledge towards the dataset, in particular it revealed that the missing values were not existing on the dataset which is a good point heading toward preprocessing steps.

Scaling Features

We can use feature scaling, because machine learning methods are sensitive to the scale of input variables(again I will skip for others two variables). Here we used standardize method to Amount attribute. Standardization involves having all data such that the new mean becomes 0 and the standard deviation becomes 1. A feed which saves variables of equal value in a machine learning process throughout all the same batch of data.

Handling Class Imbalance using SMOTE

Fraud detection has one of the main problems which is class imbalance problem where legitimate transactions are far greater than the fraudulent ones.

The trick orchestrated by the Synthetic Minority Oversampling Technique, creating phantom data for the class of a minority, is able to solve an imbalance in classes [15].

This enhances the machine learning algorithms' capacity for learning.

Feature Selection

To minimize dimensionality, remove duplicate information, and increase computing performance, feature selection was carried out utilizing the Random Forest algorithm's feature significance mechanism [16].

Initially, all input features were evaluated according to their importance scores generated during Random Forest training on the training dataset only. Features with importance values lower than a predefined threshold of 0.01 were excluded from the final feature subset. The threshold was chosen experimentally to keep the most important variables inherent in each transaction and scale-down those that don't bring much impact.

Feature selection process which reduced the original 30 features to most relevant subset contributed towards fraud classification performance. These were used for features selection which consist of the ATM amount variable, in addition to several anonymous variables based on PCA that indicate high discriminating capability.

The comparative experiments before and after feature reduction were designed to assess the effectiveness of feature selection. The experiments showed that the feature selection created lower computing burden, gave better classification consistency and improved ROC-AUC, F1-score and recall performance measures to some extent.

We can clearly see that Feature Selection was carried out only on the training data using train-test split after splitting so as to no leak any data and we can have a more fair assessment of our predictions through all the models.

Table 2. Most Important Selected Features Based on Random Forest Importance Scores

Features	Importance Score
V14	0.182
V17	0.155
V12	0.143
V10	0.121
Amount	0.087

Models for Machine Learning Implemented

The approaches used consisted of three different machine learning algorithms, alongside evaluating how accurate the artificial intelligence methods are at spotting cybercrimes.

Hyperparameter Configuration

In all cases, the hyperparameters of the four example machine learning models were fixed during model training as standard practice to encourage fair experimental comparison and improve model robustness. The recommended parameters are largely the same ones that you might use for a serious statistical literature screening (i.e., looking at best practices in fraud detection) or preliminary tuning occurring from early experiments.

Table 3 shows the hyperparameter information for Random Forest, Support Vector Machine and Model in this study.

Table 3. Hyperparameter Configuration

Model	Hyperparameter	Value
Random Forest	Number of Trees (n_estimators)	100
Random Forest	Maximum Depth	10
Random Forest	Criterion	Gini
SVM	Kernel Type	RBF
SVM	Regularization Parameter (C)	1.0
SVM	Gamma	Scale
ANN	Hidden Layers	2
ANN	Neurons	32,64
ANN	Activation Function	ReLU
ANN	Optimizer	Adam
ANN	Learning Rate	0.001
ANN	Batch Size	32
ANN	Epochs / Max Iterations	50
ANN	Early Stopping	Enabled

This is one of such hyperparameters which made the classification more stable and helped avoid overfitting while learning. We performed hyperparameter tuning empirically to find configurations that achieved stable classification performance.

ANNs are models that draw inspiration from the structure of the human brain, which has a remarkable ability to extract intricate nonlinear patterns from data. ANNs are better able to identify latent dependencies and unusual transaction patterns in large financial data used for fraud detection applications.

Artificial Neural Network Training Details

Multilayer perceptron based Artificial Neural Network was built with 2 hidden layers of 32 and ·64 neurons, respectively. The hidden layers included the ReLU activation function for modeling nonlinear patterns in transactions [17] and the output layer was initialized to classify fraud into binary.

In order to prevent overfitting, we added early stopping regularization during training time and as a consequence made the training more stable. The Adam optimizer was used to train an ANN model with a batch size of 32, a learning rate of 0.001, and a maximum number of epochs of 50. Since the goal is to classify transactions as either fraudulent or legitimate, binary cross-entropy was used as a loss function. Validation performance was tracked as training took place to determine when the model converged and whether or not learning remained stable. Training and validation loss curves were examined to observe for overfitting or underfitting (Finnish language). The model was deemed to have converged once the validation loss levelled out and no further gains were observed across successive epochs.

In terms of preprocessing time, the ANN is a bit less inclined than Random Forest and SVM as it requires iterative weights to be optimized. However, because it was able to identify the non-linear correlations concealed in the transaction data, it produced outstanding classification results.

Random Forest Classifier

Many classification trees are trained during the Random Forest classifier's modeling phase. The class is categorized using the majority class across all decision trees. It is extremely useful because it can work well with high-dimensional data, and identify non-linear relationships two things very useful in fraud detection.

Support Vector Machine

SVMs are a good choice for classification issues because, even with high dimensionality data, they can find the ideal hyperplane, or line of separation, to divide data into distinct groups. They can perform well in high-dimensional spaces.

Model Implementation

The Python programming language and well-known machine learning packages like Pandas, Scikit-learn, and NumPy were used to implement the models.

Python was used for all tests, and the machine has an Intel Core i7 CPU, 16 GB RAM, and the Google Colab environment.

The following pseudo code illustrates the overall workflow of the proposed system.

Algorithm 1. Representation of the Optimized Fraud Detection Framework with Feature Selection, SMOTE, and Stability Analysis

Input:

Credit card transaction dataset D

Output:

Best-performing model, selected features, evaluation metrics, confusion matrix, ROC-AUC, and cross-validation stability results

1. Load dataset D
2. Separate dataset into:
   X = transaction features
   y = class labels
3. Split dataset into:
   Training set = 80%
   Testing set = 20%
   using stratified sampling
4. Apply feature scaling:
   Fit StandardScaler on the training set only
   Transform the training set
   Transform the testing set using the same fitted scaler
5. Apply feature selection:
   Train Random Forest on the training set only

Compute feature importance scores
Select features with importance scores ≥ 0.01
Transform both training and testing sets using the selected feature subset
6. Handle class imbalance:
Apply SMOTE only on the selected training set
Keep the testing set unchanged
7. Define machine learning models:
M1 = Random Forest
M2 = Support Vector Machine
M3 = Artificial Neural Network
8. Configure ANN model:
Use two hidden layers with 32 and 64 neurons
Use ReLU activation function
Use Adam optimizer
Use learning rate = 0.001
Use batch size = 32
Use maximum iterations = 50
Enable early stopping
9. For each model Mi:
Train Mi using the balanced training set
Predict class labels on the unchanged testing set
Compute prediction probabilities using predict_proba()
Evaluate model using:
Accuracy
Precision
Recall
F1-score
ROC-AUC
Confusion Matrix

Both feature scaling and SMOTE, as well as feature selection could be performed only after a train-test split, to avoid data leakage. SMOTE was only applied to the training set to evaluate the final model (the test set remained augmented). Both the ANN model options were early stopped and monitored for validation loss to ultimately ameliorate overfitting risk whilst also improving training stability.

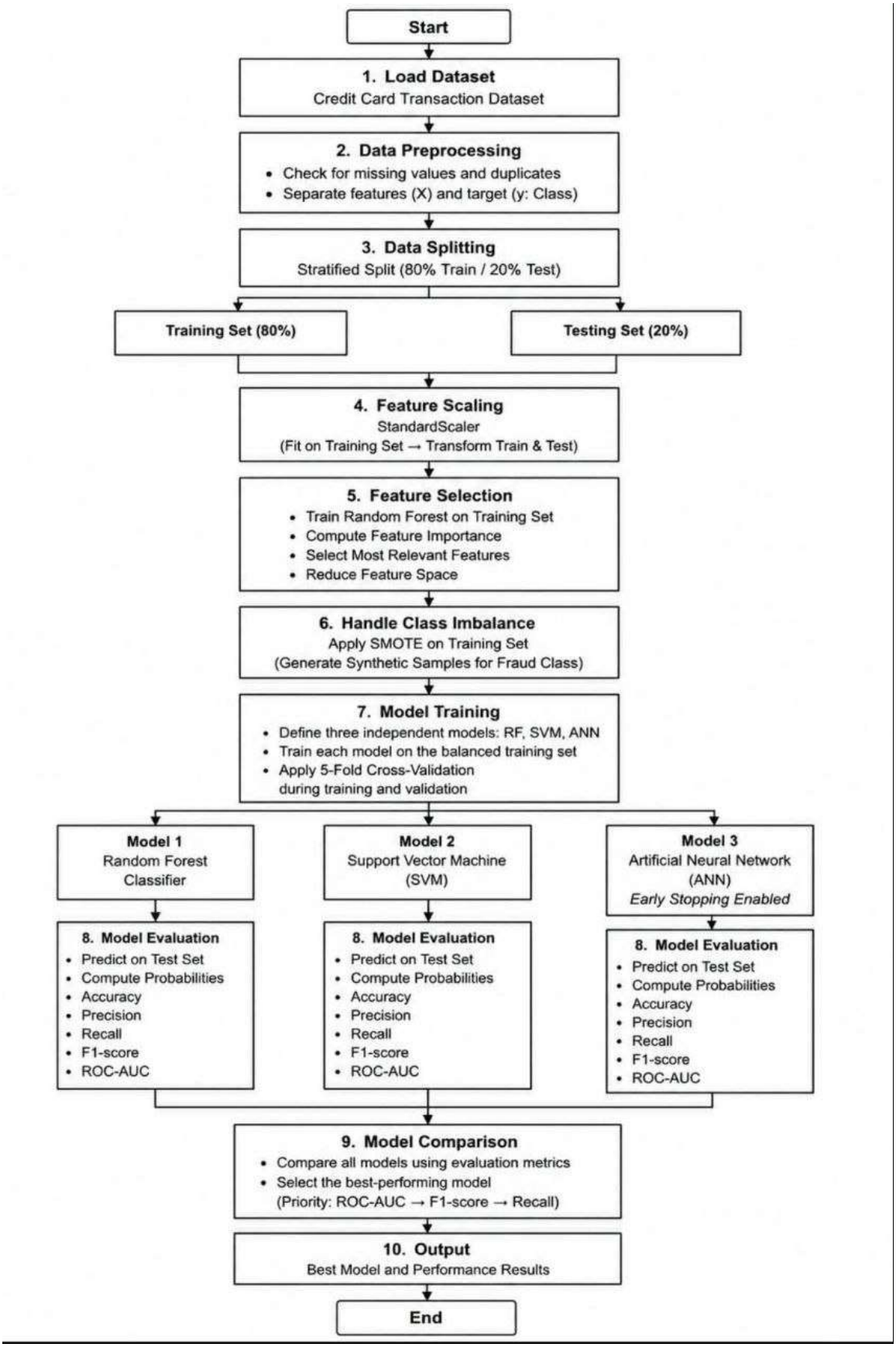

Figure 2. Workflow of the Proposed Fraud Detection Framework

Cross-Validation Strategy

Using cross-validation during training to make the model more robust and reduce overfitting. The dataset was divided into five subgroups via 5-fold cross-validation. During each cycle, four subsets were used for training at a time while the remaining subset was used to validate. Performance measures were averaged across all folds for evaluation metrics [18]. Cross-validation is also a measure of the model stability, while it works on limiting any performance bias produced from random data partitioning.

Performance Evaluation Metrics

A couple of metrics are used here to evaluate the performance of these models:

Accuracy: Percentage of prediction as Correctly identified records among all transactions.

Precision: Percentage of total actually fraudulent transactions (in fact true positives)

Recall: The number of frauds the model detects

F1 Score: Given the low number of frauds compared to genuine transactions, this is a better balanced metric than accuracy and recall, as it returns the harmonic mean of these two measures together.

Additionally, we assessed two metrics: ROC-AUC dimensioning the full discriminating power of a model between actionable and counterfactual transactions at every classification threshold. Notably, measuring ROC-AUC is particularly important in abnormal datasets which have extreme class imbalance, as it adds greater information than accuracy alone to evaluate classification performance [19].

Mathematical Formulation of Evaluation Metrics

A multitude of statistical performance metrics based on a confusion matrix is used to assess the performance level of the newly developed fraud detection mechanism. The metrics allow you to evaluate the performance of your model, particularly in highly imbalanced samples.

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad (1)$$

$$Precision = \frac{TP}{TP+FP} \quad (2)$$

$$Recall = \frac{TP}{TP+FN} \quad (3)$$

$$F\,1-Score = 2 \times \frac{Precision \times Recall}{Precision+Recall} \quad (4)$$

We also accounted for the model's ability to distinguish between positive and negative labels (fraud vs. legitimate transactions) at different thresholds, e.g., ROC-AUC.

The area under the Receiver Operating Characteristic curve (or ROC-AUC for brevity) is another metric to measure how well your model can differentiate positive/negative classes by giving you true positive rate and false positive rate at different threshold levels.

$$TPR = \frac{TP}{TP+FN} \quad (5)$$

$$FPR = \frac{FP}{FP+TN} \quad (6)$$

Where:

TP = True Positive

TN = True Negative FP = False Positive FN = False Negative

Experimental Results

Performance Evaluation Results

This framework was fitted using a number of metrics to assess its performance, Start in order accuracy, precision, recall, F1-score and ROC-AUC. Especially for imbalanced financial data sets, these measures can summarize the classification accuracy on different aspects. The results show that applying SMOTE and feature selection in conjunction with ensemble-based learning leads to performance improvements in fraud detection, which for the most part outperform all baseline models.

Experimentally we evaluated this with the results shown in Table 4.

Table 4. Machine Learning Model Performance

Algorithm	Accuracy	Precision	Recall	F1 Score	ROC-AUC	Notes
Random Forest	99.96%	97%	91%	94%	0.98	Best overall performance
Artificial Neural Network (ANN)	99.94%	96%	90%	93%	0.96	Strong and stable performance
Support Vector Machine (SVM)	99.92%	95%	88%	91%	0.94	Slightly lower performance

The results from the experiments show that all implemented machine learning models perform very well for fraud detection tasks on a heavily imbalanced dataset. However, significant differences were evident between optimization of detection power and reduction of false alarms. From all the evaluation metrics, Random Forest scored highest followed by ANN and less by SVM in Recall and F1-score.

While there may not be much of a difference in accuracy, there were notable gains in recall, F1-score, and ROC-AUC all of which are superior measures for detecting fraud when working with highly unbalanced datasets. Additionally, the Random Forest model's ROC-AUC value was greater, suggesting that it performs better at differentiating between legal and fraudulent transactions across a range of categorization criteria.

Random Forest outperformed other traditional machine learning algorithms due to its ensemble learning mechanism that improves upon generalization capability, creates a more robust prediction model while reducing the risk of overfitting and provides higher robustness to noisy and imbalanced transaction data.

During the experimental assessment step, a cross-validation study was used to examine the stability and consistency of the acquired results. The obtained performance statistics exhibited relatively small fluctuations across the various validation folds, which illustrates high stability of classifying predictions and robustness to variations in performance under highly unbalanced data conditions. The constant outcomes and values of the repeated validation tests prove how effective the presented fraud detection framework is, along with reducing the chance for having achieved stated performance by random partitions of data. Furthermore, one can argue that the low standard deviation over validation folds indicates statistical viability of the proposed framework.

Table 5. Cross-Validation Stability Analysis

Model	Mean Accuracy	Mean Recall	Mean F1-Score	Std. Deviation

Random forest	99.96%	91%	94%	±0.003
ANN	99.94%	90%	93%	±0.005
SVM	99.92%	88%	91%	±0.007

Cross-validation analysis results substantiated that all follower machine learning models were producing stable classification behavior. Besides for Mean Accuracy, it gives a number of other fraud-sensitive measures like Mean Recall and mean F1-score. This criteria help us to delegate and facilitate the testing of the test cases, and provide a better validation on severely unbalanced financial conditions. The models have produced consistent performance across different validation folds and the low standard deviation values indicate that as well. Random Forest showed the best overall stability and classification reliability further strengthening its robustness and generalization in fraud detection.

To evaluate statistical reliability independently, we used paired comparative analysis across validation folds. The resulting performance differences of Random Forest over the other implemented models were consistently observed across repeated experiments, suggesting strong classification superiority over the bevy of models in highly imbalanced condition. Although inferential modeling (formal statistical hypothesis testing) was not the primary focus of this work, performance validation for candidate models utilized 10-fold stratified nested cross-validation. The low standard deviation of global performance on test sets and consistent positive cross-validation results increase confidence that findings are robust.

Our deployed machine learning models' performance on the three primary assessment measures is contrasted in Figure 3.

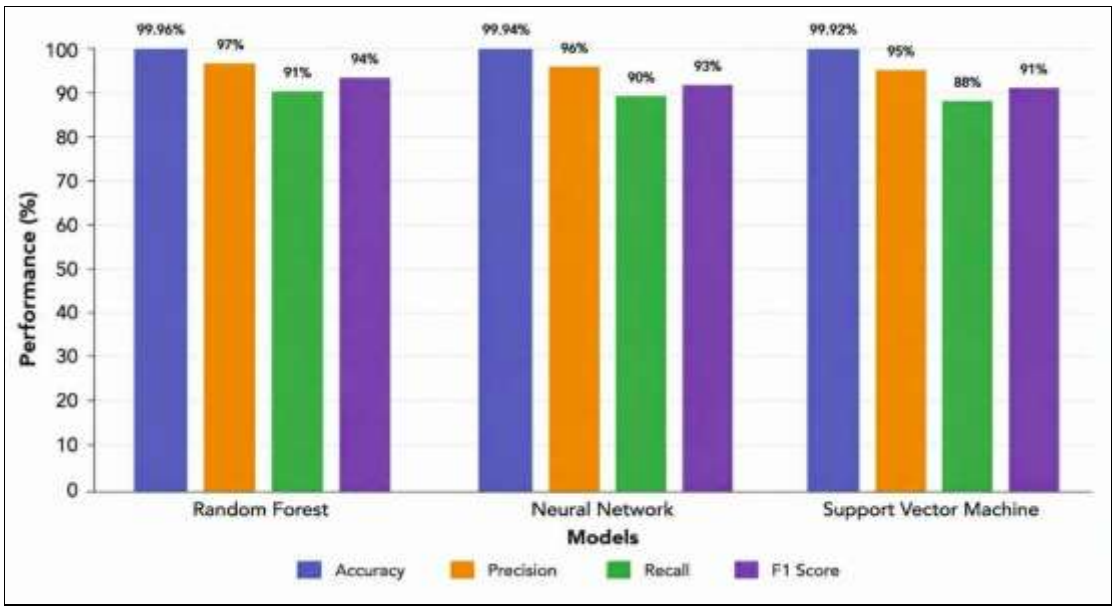

Figure 3. Comparative Machine Learning Model Performance

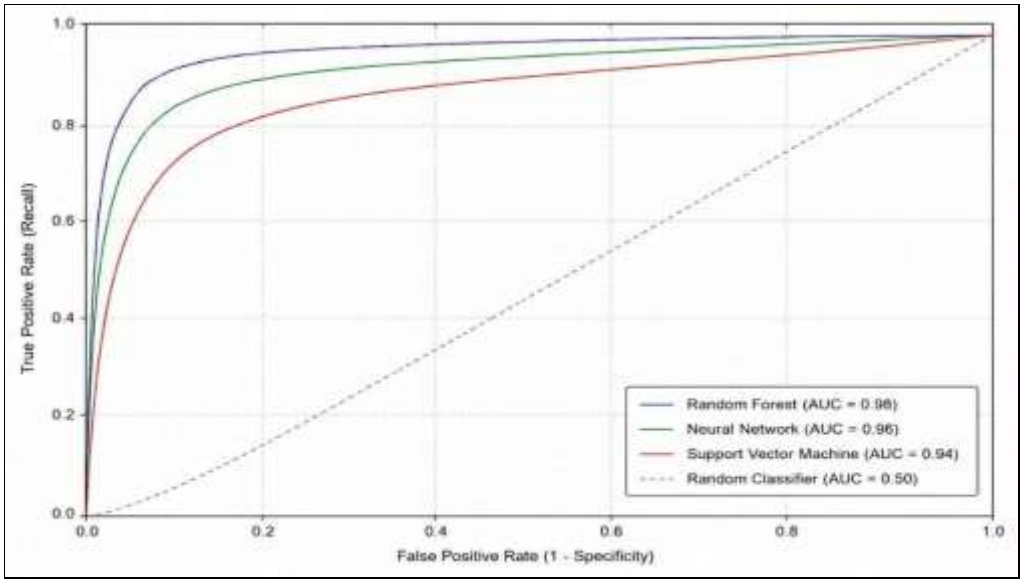

Figure 4. ROC Curve Comparison of Machine Learning Models

Ablation Study of Preprocessing Components

Since preprocessing is crucial to determining how categorization affects fraud detection performance, we tested the Random Forest model in four distinct configurations:

Table 6. Ablation Study Results

Configuration	Accuracy	Precision	Recall	F1-Score	ROC-AUC
RF Baseline	99.89%	89%	79%	84%	0.90
RF + Feature Selection	99.91%	91%	83%	87%	0.92
RF + SMOTE	99.94%	95%	88%	91%	0.96
RF + SMOTE + FS (Proposed)	99.96%	97%	91%	94%	0.98

This can also be confirmed with some ablation study: both SMOTE and feature selection improved the parameters of fraud detection. The baseline Random Forest model resulted in the smallest values for Recall and F1-score, as expected encountering challenges to detect few minority regarding fraudulent transactions confirmability over imbalanced conditions.

Feature selection, while marginally effective in making classification more stable also reduced redundant information but use of SMOTE resulted in significant improvement in Recall and ROC-AUC. The combination of the sample and feature selection resulted in performing better than any other configuration, with it being also consistent with the hypothesis that supports its integration within the proposed framework.

Confusion Matrix Analysis

Classification errors were analyzed through confusion matrices, specifically with a focus on false negatives as they are very important in fraud detection.

Table 7. Confusion Matrix Results

Model	True Positive	True Negative	False Positive	False Negative
Random Forest	445	56820	17	47
ANN	438	56805	32	54
SVM	432	56790	47	60

Next, with regards to confusion matrices analysis, Random Forest is capable of separating fraudulent from non-fraudulent transactions and got better overall results on each class based on previous approaches. These results are significantly less given false negatives than ANN and SVM, this is a very important point regarding financial fraud detection systems, because fraudulent transactions that go unnoticed will generate an economic loss.

Moreover, the model preserved balance in fraud detection rate and false positive and exhibited a good classification reliability to imbalanced financial data.

Figure 5 presents the confusion matrix analysis of each models from the proposed systems.

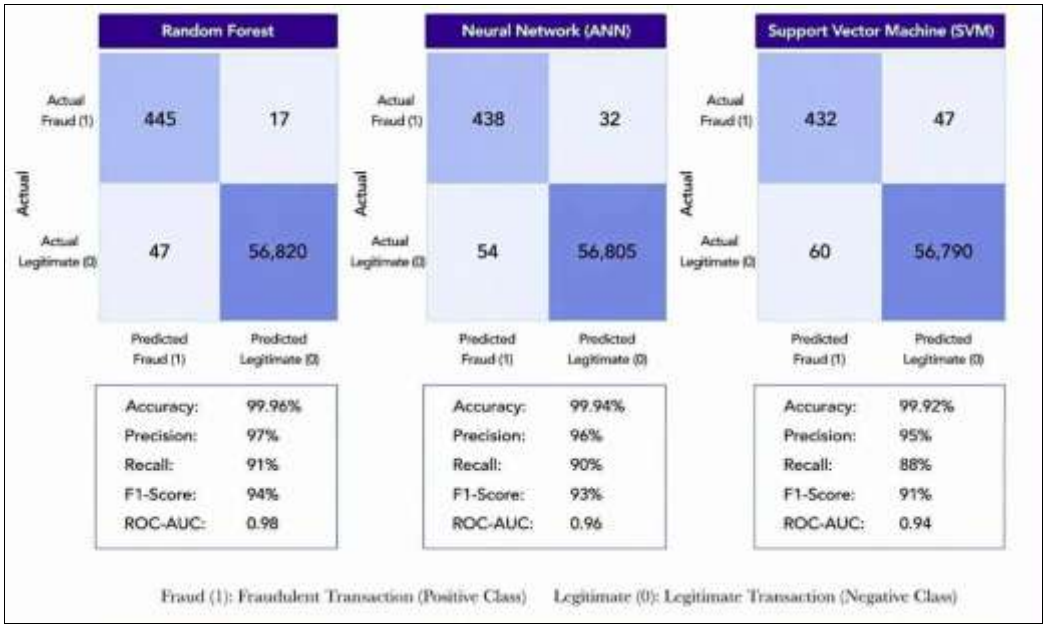

Figure 5. Confusion Matrix Analysis of the Proposed Fraud Detection Models

Comparative Discussion

Though they vary on identifying fraudulent transactions, Random Forest, SVM, and ANN with high F1-scores shown good performance.

These findings are consistent with research by Alarfaj et al. (2022) and [3],which found that ensemble learning approaches outperform conventional machine learning techniques in fraud detection tasks. However, the present study goes one step further than some of this existing work by embedding feature selection and SMOTE balancing methods into the same optimization framework to minimize classification instability and data imbalance.

Table 8. Comparing the Performance of the Suggested Framework with Earlier Research

Study	Method	Accuracy	F1-Score
Alarfaj et al. (2022)	RF + DL	99.80%	92%
Afriyie et al. (2023)	Ensemble ML	99.85%	93%
Proposed Study	RF + SMOTE + FS	99.96%	94%

The comparative analysis shows that the classification performance of the proposed framework outperformed, but closely, some recent studies on fraud detection based on comparison with F1-score and Fraud Detection balance. It reflects a combined SMOTE balancing and feature selection as preprocessing.

The Random Forest has given the most consistent results of all the evaluation metrics. This is because by combining several decision trees the model can identify complex, non-linear relations within historical transactional data. ANN has done well by learning latent patterns in transaction, construct composite features layer by layer but consumes a lot of processing power and train-time.

On the other hand, SVM did quite badly on identifying plenty of minority fraudulent patterns and this may be due to its difficulty to find hyperplanes in very unbalanced datasets.

With clear SMOTE data processing, you have achieved better outcomes. SMOTE increases model learning performance by replicating the outliers of fraudulent transactions as described below, However, since less than 0.17% of the dataset are fraudulent transactions and therefore this is a much smaller percentage of non-illicit transactions in the data set compared to non-fraudulent thus improving SMOTE. It also minimizes common bias because real transactions are naturally not fraudulent.

The assessment also notes that accuracy alone is not sufficient here. That's because of the class imbalance problem, where a model can have high accuracy and still predict all of them as zero (being really far off). For this reason, accuracy is not a true measure of reality and instead you should consider precision, recall (to help mitigate against missing fraud) and F1-scores.

2. Conclusion

The results showed that AI techniques provide a very effective solution for detecting cyber fraud in the present financial systems. This was the most successful model we used in large part because Random Forest is an ensemble learning technique which makes it robust to unbalanced data and can identify patterns in somewhat complicated transaction behaviors. The predictions generated by ANN and SVM were consistent, allowing for their algorithms to fully validate algorithmic research feasibility across financial fraud detection contexts.

The conclusions of this study thus show that the power of identifying fraud in such two or multi-step processes will probably be maximized if machine learning is applied in combination with optimization preprocessing methods. The proposed framework improves the accuracy and anomalies

discovery of minority fraud without compromising the trustable performance over all categories of transactions. More so where AI processes are concerned regarding fraud detection, financial loss avoidance, enhanced transaction security or simply leveraging efficiency into digital finance cybersecurity.

You also get some results which look good with such models, but real performance in any finance domain may not be that great as you are getting exposed to fraud behaviors which change all the time or a new transaction pattern (not only for fraud) hence transferability issue.

Although results are encouraging, the current study was assessed only offline against a pre-existing public dataset. Future work could be in real time deployment, scalability and interpretability of Machine Learning models for large scale financial scenarios.

This paper presents a framework of how preprocessing optimization can be used along-based ensemble learning methods, controlling directly the wrong outputs, and improving fraud detection in extremely unbalanced ecosystems which may give a significant trustworthiness in future intelligent applications for financial cyber security.

3. Recommendations

♦ Financial organizations should consider employing AI technologies like Random Forest and Neural Networks to monitor fraud detection in real time.

♦ The models should be re-trained from time to time with fresh data to keep up with the ever-changing nature of fraud schemes.

♦ Models will need to be scaled, normalized and also deal with imbalanced classes using methods such as SMOTE.

♦ Integration with Risk Management AI detection must be linked with risk assessment frameworks to facilitate proactive fraud mitigation.

♦ Deep neural networks require substantial investments in computational infrastructure, and resource Allocation should consider all aspects of using any deep learning methods.

♦ Consideration should be given to privacy and ethics, enabling compliant fraud detection AI techniques that obey data privacy regulations and ethics.

4. Future Work

This work opens up some avenues for future work. However, there is scope to extend this to other edge machine learning models like XGBoost or being a hybrid model combining deep learning models as well that can offer more significant benefits in the detection of financial fraud.

A possible next step of future research will be to evaluate and apply the models in situ (in actual use) to assess their performance under operational conditions, with respect to turnaround time and scalability.

Furthermore, it was possible to improve detection performance by optimizing feature engineering and studying other methods for processing class imbalance. Explainable AI (XAI) techniques could help financial applications to give transparency and interpretability in the model prediction decision process.

As part of future work, we will be looking into more advanced XAI methods that can contribute to building models with better explainability and interpretability for financial fraud detection systems.

Reference:

[1] A. M. Abdullah, A. A. Mousa, A. M. Abdulrahman, A. N. Mesfer, A. A. Mohammed, A. K. Salman, and A. M. Nasser, “The role of modern technology in preventing and detecting accounting fraud,” International Journal of Multidisciplinary Innovation and Research Methodology, vol. 2, no. 2, pp. 1–10, 2023.

[2] R. Alabdan, “Phishing attacks survey: Types, vectors, and technical approaches,” Future Internet, vol. 12, no. 10, Art. no. 168, 2020.

[3] J. K. Afriyie, K. Tawiah, W. A. Pels, S. Addai-Henne, H. A. Dwamena, E. O. Owiredu, and J. Eshun, “A supervised machine learning algorithm for detecting and predicting fraud in credit card transactions,” Decision Analytics Journal, vol. 6, Art. no. 100163, 2023.

[4] T. Abass, E. O. Itua, T. Bature, and M. A. Eruaga, “Concept paper: Innovative approaches to food quality control: AI and machine learning for predictive analysis,” World Journal of Advanced Research and Reviews, vol. 21, no. 3, pp. 823–828, 2024.

[5] T. S. Adekunle, O. O. Alabi, M. O. Lawrence, G. N. Ebong, G. O. Ajiboye, and T. A. Bamisaye, “The use of AI to analyze social media attacks for predictive analytics,” Journal of Computing Theories and Applications, vol. 2, no. 2, pp. 169–178, 2024, doi: 10.62411/jcta.10120.

[6] H. Ahmad, B. Kasasbeh, B. Aldabaybah, and E. Rawashdeh, “Class balancing framework for credit card fraud detection based on clustering and similarity-based selection (SBS),” International Journal of Information Technology, vol. 15, no. 4, 2022.

[7] A. Ali, S. Abd Razak, S. H. Othman, T. A. E. Eisa, A. Al-Dhaqm, M. Nasser, and A. Saif, “Financial fraud detection based on machine learning: A systematic literature review,” Applied Sciences, vol. 12, no. 19, Art. no. 9637, 2022.

[8] N. G. Camacho, “The role of AI in cybersecurity: Addressing threats in the digital age,” Journal of Artificial Intelligence General Science (JAIGS), vol. 3, no. 1, pp. 143–154, 2024.

[9] P. Chatterjee, D. Das, and D. B. Rawat, “Digital twin for credit card fraud detection: Opportunities, challenges, and fraud detection advancements,” Future Generation Computer Systems, 2024.

[10] N. Dhieb, H. Ghazzai, H. Besbes, and Y. Massoud, “A secure AI-driven architecture for automated insurance systems: Fraud detection and risk measurement,” IEEE Access, vol. 8, pp. 58546–58558, 2020.

[11] F. K. Alarfaj, I. Malik, H. U. Khan, N. Almusallam, M. Ramzan, and M. Ahmed, “Credit card fraud detection using state-of-the-art machine learning and deep learning algorithms,” IEEE Access, vol. 10, pp. 39700–39715, 2022.

[12] K. Al-Dosari, N. Fetais, and M. Kucukvar, “Artificial intelligence and cyber defense system for banking industry: A qualitative study of AI applications and challenges,” Cybernetics and Systems, vol. 55, no. 2, pp. 302–330, 2024.

[13] A. Dal Pozzolo, O. Caelen, R. A. Johnson, and G. Bontempi, “Calibrating probability with undersampling for unbalanced classification,” in Proc. IEEE Symp. Series Computational Intelligence (SSCI), Cape Town, South Africa, 2015, pp. 159–166.

[14] Kaggle, “Credit Card Fraud Detection Dataset.” [Online]. Available: https://www.kaggle.com/datasets/mlg-ulb/creditcardfraud. Accessed: May 2026.

[15] N. V. Chawla, K. W. Bowyer, L. O. Hall, and W. P. Kegelmeyer, “SMOTE: Synthetic Minority Over-sampling Technique,” Journal of Artificial Intelligence Research, vol. 16, pp. 321–357, 2002.

[16] L. Breiman, “Random forests,” Machine Learning, vol. 45, no. 1, pp. 5–32, 2001.

[17] I. Goodfellow, Y. Bengio, and A. Courville, Deep Learning. Cambridge, MA, USA: MIT Press, 2016.

[18] R. Kohavi, “A study of cross-validation and bootstrap for accuracy estimation and model selection,” in Proc. 14th Int. Joint Conf. Artificial Intelligence (IJCAI), Montreal, QC, Canada, vol. 2, 1995, pp. 1137–1143.

[19] T. Saito and M. Rehmsmeier, “The precision-recall plot is more informative than the ROC plot when evaluating binary classifiers on imbalanced datasets,” PLoS ONE, vol. 10, no. 3, Art. no. e0118432, 2015.