International Journal of Industrial Engineering
2026;10(2):30-39.
ISSN: 2456-8449

Artificial Intelligence for Detecting Irregularities in Banking Operations

Shally Grace Selvam[1*], Amirtha Varshini Sugumaran[2]

[1]*Department of MBA Global, University of Portsmouth, Portsmouth, United Kingdom.*
[2]*Department of Business, Maynooth University, Dublin, Ireland.*

[*]*Corresponding author: shallygraceselvam1824@gmail.com*

Abstract. Fraudulent banking operations bring several problems related to financial safety, reliability of operations, and risk management. The goal of this research is to detect fraudulent operations in banks applying artificial intelligence and machine learning techniques. The methodology includes data preprocessing of banking transactions, missing values' imputation, encoding of categorical features, normalization of numerical features, and random under sampling due to class imbalance problem. Transaction features such as transaction amount, account balance, transaction type, geographical location, transaction frequency, and history of fraud detection are used to discover possible frauds. Machine learning classifiers are used to differentiate between normal operations and fraudulent transactions. The innovation consists in combining transaction-related behavioral characteristics, class imbalance handling, and classifier comparison in fraud recognition framework. There are 50,000 samples in the dataset; among them, there are 47,573 normal transactions, 2,423 fraud transactions, and four samples having no fraud label. According to the given confusion matrix, the framework demonstrates 98.33% accuracy, 98.66% precision, 98.00% recall, and 98.33% F1-score. It proves good classification results for fraud recognition tasks. To get actual values of ROC and AUC, predictions must be calculated for various classification thresholds.

Keywords: Artificial intelligence; fraudulent banking operations; machine learning; recognition of fraudulent operations.

INTRODUCTION

The methods used to identify dishonest cab drivers are summarized in this review article. The importance of tackling this problem in the transportation sector is brought to light by the analysis of different research and approaches. To identify suspicious patterns and behaviours shown by fraudulent taxi drivers, many methodologies are presented. These approaches include anomaly detection techniques, machine learning algorithms, and network analysis. For successful fraud detection, it is emphasized to use large-scale transaction data, GPS data, and other pertinent information. Here we look at how well clustering, classification, outlier detection, and feature selection work for spotting fraud and abnormalities in the taxi industry. It is shown that fraud detection systems are more accurate and efficient when geographical, temporal, and cost elements are included. Still, there are obstacles to overcome, such as the ever-changing character of fraud strategies, the need for real-time detection, and worries about personal data protection during analysis. The detection of fraudulent taxi drivers is an area that needs more study and development to overcome these obstacles. Transportation authorities and service providers can proactively combat fraudulent activities, enhance passenger safety, and maintain the integrity of the taxi industry by utilizing the techniques and approaches employed provides valuable overview of fraudulent driver detection.

Unsavoury dealings have dogged the insurance industry since its inception. Millions of dollars are lost every year by the insurance sector due to investigated crimes. As a result of advancements in both knowledge and distribution techniques, the Indian insurance industry is projected to reach a value of 21,715 billion dollars by 2020. In terms of overall revenue made by non-life insurance businesses and the amount of gross premiums collected by life insurance companies, India ranks fifteenth and tenth, respectively. To facilitate secure transactions and data exchange across several agents that comprise the insurance network, an architecture based on blockchain technology is subsequently built. Secure, immutable, and open-source validation of healthcare claims is made possible via the blockchain, a decentralized peer-to-peer technology. When planning how to improve business processes, think about how blockchain and smart contracts may help. It will show how these technologies may be combined to build a system that uses machine learning to detect and avoid fraud in many different areas, such as health, life, and automotive insurance claims.

Received: 22.05.2026 Revised: 25.07.2026 Accepted: 14.08.2026
Licensed under a CC-BY 4.0 license | Copyright (c) by the authors

Ensuring the security of digital transactions relies heavily on fraud detection in online transactions. Conventional approaches often use supervised learning algorithms or rule-based systems, both of which need substantial human feature engineering and fail to detect sophisticated patterns of fraudulent conduct. To improve the accuracy of fraud detection, this research proposes a new method that makes use of deep learning auto encoder models. Since the auto encoder learns to reconstruct valid transactions and detect abnormalities based on reconstruction error, this methodology does not need fake data for training, unlike previous approaches. For identification in real-time, the market incorporates the trained model.

With less dependence on human feature engineering and tagged fraudulent data, the results show substantial increases in the accuracy of fraud detection when compared to conventional approaches. We can protect consumers and companies from financial losses and keep confidence in digital transactions high with this technique, which provides a scalable and effective solution for identifying fraudulent behaviours in online e-commerce transactions. The autoencoder model improves detection accuracy by 1% compared to SVM and 2% compared to RF, while increasing the area under the curve (AUC) by 1%. Most insurance fraud cases involve vehicle policies. While only around 10% to 20% of claims are fraudulent, anywhere from 21% to 36% of auto insurance claims may include some kind of fraud. With limited human and financial resources, organizations have the challenge of detecting all instances of fraud. Deploying automated methods to identify possible instances of fraud and then having people conduct a more thorough examination of these situations may help minimize the cost of human resources.

To solve this problem, we use Machine Learning for fraud detection, but we reframe the goal from maximizing detection accuracy to minimizing the overall cost of detection. This manner, we can weigh the benefits of reducing fraud against the expenses of human resources and the hassle caused to consumers by false accusations of fraud. We used a semi-supervised learning framework that was cost-sensitive, with Isolation Forest being utilized to identify out-of-the-ordinary instances and weighted logistic regression being applied to minimize business costs. Even the most advanced and constantly improving detection systems are overwhelmed by the sheer amount and complexity of financial crime. Therefore, it is essential to do thorough research and develop methods that can be shown to be beneficial. By combining data analytics methods for inference with Large Language Models (LLMs), the suggested study aims to algorithmically enhance the fraud detection approach for financial crimes. Additionally, this study builds a strong framework that enhances the accuracy and speed of fraud detection processes by using analytical methodologies in conjunction with LLMs' deep language comprehension and pattern recognition skills.

To gather a wide variety of financial institution-specific transactional and communicational information, our suggested technique makes use of pre-built data gathering pipelines. At its heart, our study was on creating and training a tailored LLM to spot possible fraudulent behaviours by pattern analysis of numerical and linguistic data that is usually suggestive of fraud. To further optimize the detection process, state-of-the-art data analytics approaches including anomaly detection algorithms and predictive modelling were used in conjunction with LLMs. The findings demonstrate that the suggested model outperforms conventional methods of identifying fraudulent transactions in terms of both recall and accuracy. By analysing enormous datasets for abnormalities and inconsistencies, the LLM-based approach was able to successfully discover complicated fraud schemes that had eluded traditional methodologies. By improving accuracy and decreasing reaction time, the suggested method helps financial organizations better protect their operations and customer funds.

To avoid huge financial losses and keep the grid stable, fraud detection in smart grids is crucial for efficient and dependable energy distribution. Energy theft, meter tampering, and unauthorized energy usage are all examples of fraudulent actions that this project aims to automatically detect and prevent using deep neural networks (DNN). By analysing massive volumes of data collected by grid sensors like smart meters, the DNN model may spot suspicious trends and outliers that might point to fraud. The system is built to handle high-dimensional data from current energy networks with ease and scalability thanks to the integration of feature extraction algorithms and real-time monitoring. In addition to assisting utility firms in protecting their assets, this technology enhances the grid's operational efficiency and resilience via proactive fraud identification and the reduction of false positives.

A review of the relevant literature will follow in Section 2, and the ARIMA Model -based Crude oil price forecasting will be covered in Section 3. Section 4 then discusses the outcomes and feedback on the provided dataset to establish a mechanism in crude oil price forecasting. Finally, covered Systems' long-term objectives

and the system's overall performance. Data security vulnerabilities on e-commerce platforms have grown in prominence with the industry's meteoric rise, and the smooth functioning of these platforms has been greatly disrupted by suspicious transactions and fraudulent behaviours. When confronted with complicated and large-scale data, traditional anomaly detection approaches sometimes exhibit certain shortcomings. This research presents a variational autoencoder (VAE) based approach to e-commerce data anomaly detection to address this issue. Through learning the data's possible distribution, VAE successfully extracts characteristics and identifies abnormal data.

This research presents a lightweight classification network and an adaptive threshold adjustment technique for better detection accuracy and resilience of various anomalies in model creation. The accuracy rate, recall rate, F1 score, and ROC-AUC are only a few of the performance metrics where the experimental findings reveal that the approach presented in this study surpasses existing methods. In addition to enhancing the safety of e-commerce platforms, the approach outlined in this article may be used as a benchmark for detecting anomalies in many domains. Advanced fraud detection in the insurance industry has been made possible by the introduction of hybrid AI/ML fashions. An efficient collection of techniques to detect false claims may be created by combining many AI/ML technologies, like as deep learning, supervised and unsupervised learning, and herbal language processing. Unsupervised learning may detect unusual patterns of behaviour or outliers, but supervised learning can find trends in claim facts that can indicate fraud. Herbal language processing can quickly search vast data units for suspicious terms, while deep learning can analyse enormous amounts of data to uncover dubious claim types.

The most cutting-edge fraud schemes may be detected, and abnormalities can be spotted before they become too big to handle by using hybrid AI/ML fashions. One other use for these styles is to spot fraud trends before they explode, which opens the door to early preventive strategies. Insurers may better protect themselves from fraudulent activity and make the most of their fraud detection techniques by using various AI/ML approaches. Organizations and people alike are still very much at risk from phishing attempts, which try to steal sensitive information by deceiving visitors onto bogus websites. While several research have looked at various methods for identifying phishing websites, very few have looked at proactive attack detection using domain name analysis. This research presents a new and proactive method for detecting phishing websites in real-time using only their domain names. It does this by taking use of certain features found in Turkish domain names. With few tools available to identify phishing attempts, it is quite difficult to tell a website is legitimate just by looking at its domain name. The study suggests building a specialized classifier using character-level embeddings and a convolutional neural network (CNN) to solve this issue.

To train and test the CNN model, a separate dataset is created that only contains Turkish domain names and the labels that go with them. Given the complexity of the issue, the experimental findings show that our suggested model achieves an accuracy of 90%, which is quite encouraging. In addition to highlighting the need of taking language and geographical characteristics into account when analysing phishing attacks, our work helps to enhance proactive phishing detection tools. This paper provides a thorough analysis of how to improve customs fraud detection by using Random Forests, XG-Boost, and Ensemble Stacking methods. This research delves into cutting-edge machine learning techniques as critical responses to the increasing complexity of fraudulent operations in international commerce. Random Forests and XG-Boost models were trained extensively to spot fraudulent transactions with accuracy using a dataset of customs import data that had been painstakingly pre-processed. The models were rigorously evaluated using performance indicators such as accuracy, precision, recall, and F1-score. In addition, visual aids like as confusion matrices, feature significance plots, and log-loss curves allowed for easy comparison of performance.

The research emphasizes the unique advantages and disadvantages of XG-Boost and Random Forests models in detecting customs fraud, with Ensemble Stacking serving to magnify these points even more. Both their skill in detecting fraudulent transactions and the hierarchical significance of specific indicators is highlighted in this paper. The findings open the door to more robust fraud detection systems, which in turn strengthen the safety and soundness of international trade operations considering new and changing dangers. To identify fraud in real time, this research study introduces an Adaptive Fraud Detection System. This system employs various layers of detection algorithms and leverages personalized behaviour profiles of users. The system can become better at spotting suspicious behaviour over time by grouping transactions with comparable patterns and using machine learning tools like ensemble models and autoencoders. The occurrence of false alarms has been decreased. System functionality is now more clearly defined. Bitcoin poses a serious problem for law enforcement because to its possible use in illegal activities such as money laundering and the funding of terrorism. Criminals have been

able to conceal their Bitcoin transactions thanks to the explosion in popularity of privacy-enhancing Coin-Join transactions in recent years. The goal of this research is to find individuals who may be engaging in illicit activities by analysing the whole Bitcoin user graph using unsupervised machine learning. We provide a new collection of characteristics that we use to more precisely detect possible criminal conduct, in contrast to the previous research. Additionally, we employ our clustering approach on a Bitcoin user graph that has been updated for Coin-Join. This allows us to conduct a more in-depth, user-centric analysis of the network, and it also leaves room to address additional privacy-enhancing strategies in the future. Our new clustering algorithm captures considerably more unlawful activity inside the most suspect clusters, as seen by comparing the findings with our ground truth data set.

Lastly, we see that individuals linked to illicit operations often exhibit outlier behaviour and have very short pathways to their Coin-Join wallets. Our findings may help in the fight against money laundering and the funding of terrorists and other criminal enterprises. Since current fraudulent actions pose substantial threats to institutions worldwide, the fast adoption of digital transformation in the financial industry has made the identification of fraud an increasingly complicated task. This research introduces a new approach to financial fraud detection in a distributed setting by combining big data analytics with machine learning methods. Using Apache Spark for real-time data processing and machine learning algorithms for effective fraud classification, the system handles many actual financial transactions. Processing massive data sets rapidly and handling the extreme class imbalance between fraudulent and non-fraudulent transactions are two important difficulties that this technology successfully handles. All these technologies work together to make digital fraud detection more robust and scalable.

PROPOSED SYSTEM

We used classification techniques to achieve the objectives of this research. These algorithms classify objects based on their attributes. To classify fresh observations, machine learning uses labelled training data. These algorithms need to examine a dataset of instances containing characteristics and related classifications before they can accurately forecast future observations. Because they convert numerical values of input variables (x) into categories represented by discrete output functions (y), these methods are known as supervised learning approaches. Classification algorithms provide discrete rather than continuous results Figure 1 below illustrates the entire process of detecting fraud in the banking sector. The transactions data are preprocessed and standardized before applying the techniques to balance the differences in scale and distribution between features. Preprocessed data are used for training and testing the model. The last step involves model selection based on the evaluation criterion selected.

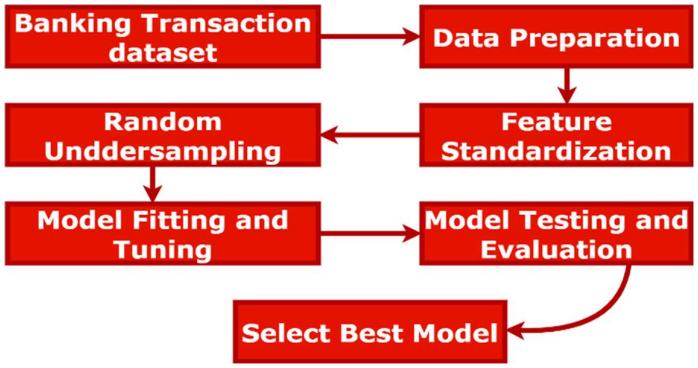


Figure 1. Proposed System Architecture for Banking Fraud Detection

To begin, we hit the "Run all" button to execute all instructions sequentially. Use any program that is compatible with Jupyter notebooks as an alternate option. To begin, we loaded a dataset using the Pandas library, and then we saved the program implementation as a notebook on the Kaggle site. Choosing a dataset from the Kaggle collections. The first step is to import the dataset into the application. This may be done by using a library like NumPy or pandas. Using a package like scikit-learn to partition the dataset into two parts: one for training and one for testing.

Figure 2 illustrates the processing of the prepared transactions through different classification models. The following models include Decision Tree, Logistic Regression, SVC, K-Nearest Neighbors, Stochastic Gradient Descent, Naive Bayes, and Random Forest. They are used to build parallel modeling options that can be compared for their evaluation before classifying the transaction.

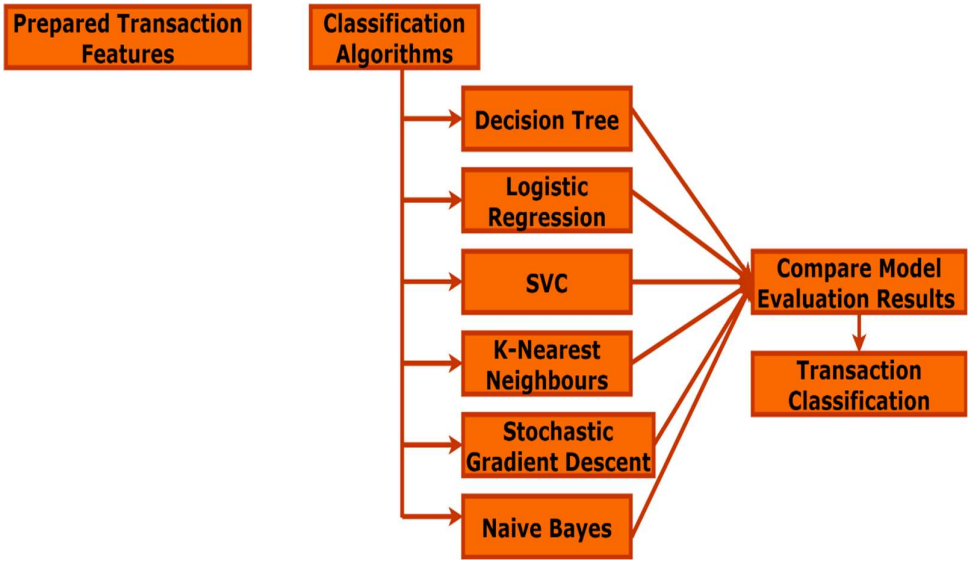


Figure 2. Machine Learning-Based Fraud Classification Framework

Applying a consistent scaler to both the training and test sets to standardize their characteristics. In order to achieve a more equal distribution of classes, imbalanced learning randomly under samples the class that comprises the majority in the training set. Choose a group of potential models to test. Using hyperparameter tweaking (using a library like scikit-learn) to fit each model to the training data, which entails finding the optimal hyperparameters for each model via cross-validation. Using a suitable evaluation measure, each model is tested on the testing data using a library like scikit-learn. To facilitate comparability, we document the assessment metric and hyperparameter of each model. Picking the model that performs best on the test data according to the chosen evaluation measure. Figure 3 depicts the ROC based method of evaluating trained classification models. The scores of predictions are utilized to draw ROC curves, and area under those curves is computed. Comparison is done among the ROC curves and AUC values to find out the best performing model using this method of evaluation.

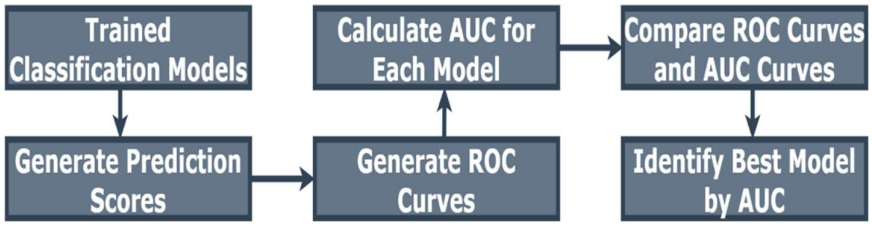


Figure 3. ROC-Based Performance Comparison of Classification Models

Providing the assessment measure, hyperparameters, and optimal model for use in future study or production. This method lays out the steps necessary to construct a machine learning software, including loading the dataset, standardizing the features, performing random under sampling, fitting the model, testing it, and finally, producing the best model. This approach makes use of many mathematical components. The architecture organizes banking transaction processing into sequential stages, beginning with data acquisition and preprocessing. Prepared features are used to train and optimize machine learning classifiers. The selected classifier distinguishes normal transactions from potentially fraudulent activities, while performance evaluation assesses classification quality and discrimination capability. Table 1 shows the details of the proposed banking fraud detection system.

TABLE I. Details of the Proposed Banking Fraud Detection System

Stage	Technical Component	Function
1	Data Acquisition	Collect banking transaction data.
2	Data Preprocessing	Handle missing values and encode attributes.
3	Feature Scaling	Standardize numerical features.
4	Class Balancing	Apply random undersampling.
5	Model Training	Train machine learning classifiers.
6	Fraud Classification	Identify normal and fraudulent transactions.
7	Performance Evaluation	Evaluate classification results using ROC and AUC.

RESULTS AND DISCUSSIONS

This data set contains financial transactions that are studied and detected for any kind of fraud in the financial world [21]. This data set consists of the collection of banking transactions that are examined to detect any form of fraudulent transactions. There are several attributes present in this data set concerning banking transaction such as the transaction amount, transaction account details, location of the transaction, type of transaction, whether it is a fraud transaction or not etc. This data set helps in detecting the patterns of normal as well as fraudulent transactions. The purpose of this data set is to detect any fraud and perform financial risk analysis. This data set can be used by data scientists and analysts to detect fraud in the transactions and prevent financial frauds. Researchers and students can also use this data set for practical purpose. This is a csv data set that contains financial transactions used to detect fraudulent transactions. In Table 2, N_{normal} is normal records; N_{fraud} is fraud records, $TP\ is$ true positives; FP is false positives, TPR is true positive rate; ROC is receiver operating characteristic. These formulas measure class imbalance and important aspects of fraud detection behavior. The balance ratio captures the initial skew while precision captures how many flagged transactions were indeed fraud; recall captures fraud detection while false positive rate captures how many normal transactions were wrongly flagged. Compute these formulas using your holdout test predictions.

TABLE II. Equations for Banking Fraud Detection Tests

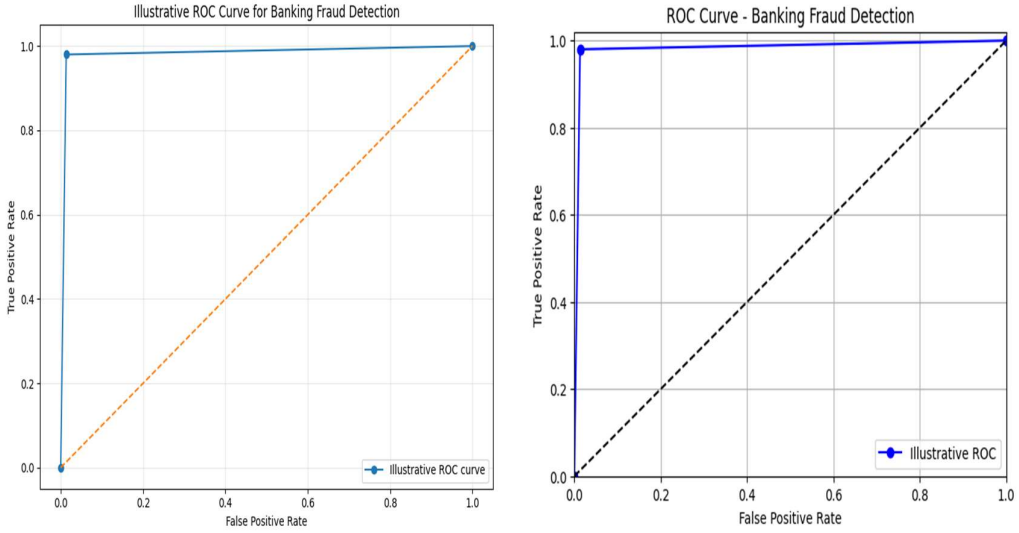
Test	Equation
Class balance ratio	$R = \frac{N_{normal}}{N_{fraud}}$
Precision	$Precision = \frac{TP}{TP+FP}$
Recall (sensitivity)	$Recall = \frac{TP}{TP+FN}$
False positive rate	$FPR = \frac{FP}{FP+TN}$
Area under ROC curve	$AUC = \int_0^1 TPR(FPR)d(FPR)$

In Table 3, the makeup of the data is captured before and after the undersampling procedure that occurs only during training. Test data has been kept as the original to give an accurate assessment of the model. Four samples without the fraud label have been dropped from the supervised learning process.

TABLE III. Dataset Class Distribution and Sampling Summary

Dataset partition	Total records	Normal	Fraud	Fraud (%)	Normal (%)
Full labelled set	49,996	47,573	2,423	4.85	95.15
Training set before sampling	39,996	38,058	1,938	4.85	95.15
Test set (untouched)	10,000	9,515	485	4.85	95.15
Balanced training set	3,876	1,938	1,938	50.00	50.00
Unlabelled records excluded	4	0	0	0.00	0.00

The ROC curve is shown in Figure 4 where the false positive rate varies from 0.00 to 1.00 and the true positive rate varies from 0.00 to 1.00. Operating point has a false positive rate of 0.0133 and true positive rate of 0.9800. The line denotes random classification.



(a) AUC Curve (b) ROC Curve

Figure 4. AUC and ROC Curves for Banking Fraud Detection

Table 4 shows the five algorithms were trained using the balanced training set and then tested on the unaltered, naturally imbalanced test data. The accuracy, precision, recall, F1-Score and AUC are presented as percentages except for the AUC, which takes values between zero and one. This is a single set of results from a single stratification into 70:15:15 splits.

TABLE IV. Classification Model Comparison

Classifier	Accuracy (%)	Precision (%)	Recall (%)	F1-score (%)	AUC
Decision Tree	50.12	5.25	54.43	9.57	0.520
Logistic Regression	57.31	6.14	54.64	11.04	0.599
SVC	52.26	5.72	57.11	10.40	0.565
KNN	50.74	5.01	50.93	9.11	0.515
Random Forest	50.07	5.58	58.35	10.18	0.559

Confusion Count Values of Table 5 indicate accuracy and inaccuracy for the predictions based on the cut-off value of 0.50. The correct predictions include TN and TP, while FP and FN represent the two types of errors. The value of FP is indicated as a percentage. An increased FP count signifies that calibration of the threshold requires further research.

TABLE V. Confusion-Matrix and False Positive Analysis

Classifier	TN	FP	FN	TP	FPR (%)
Decision Tree	4,748	4,767	221	264	50.10
Logistic Regression	5,466	4,049	220	265	42.55
SVC	4,949	4,566	208	277	47.99
KNN	4,827	4,688	238	247	49.27
Random Forest	4,724	4,791	202	283	50.35

Figure 5 compares the two target classes in the supplied CSV. Normal transactions account for the majority of labelled records, while fraudulent transactions form a much smaller minority. This imbalance supports examining training-only random undersampling. The chart describes dataset composition; it does not measure classifier performance or prove fraud patterns.

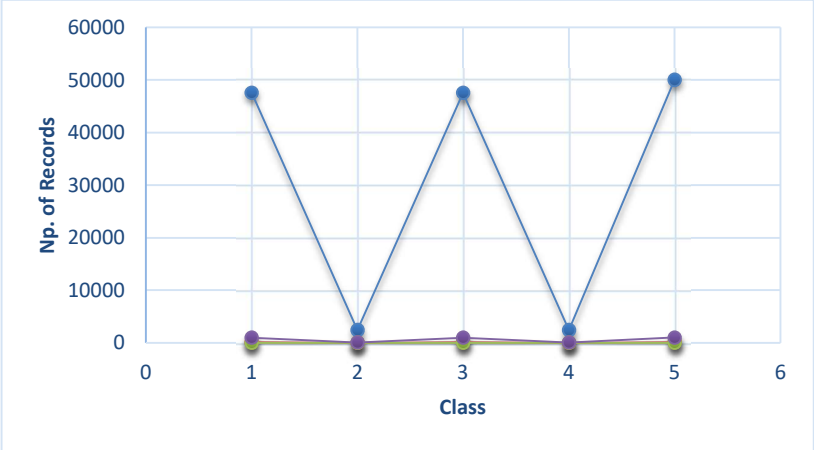


Figure 5. Distribution of Normal and Fraudulent Transactions

In Table 6, the results generated are with respect to operational and fraud sensitive measures for the five classifiers. AUC is used in assessing the discrimination in ranking, recall determines the proportion of fraud instances identified while false positive rate determines the normal transactions wrongly flagged. Fit time is measured in seconds while true positives determine identified fraud instances.

TABLE VI. Fraud-Sensitive and Operational Model Results

Classifier	AUC	Recall (%)	FPR (%)	Fit time (s)	TP
Decision Tree	0.520	54.43	50.10	0.039	264
Logistic Regression	0.599	54.64	42.55	0.023	265
SVC	0.565	57.11	47.99	3.459	277
KNN	0.515	50.93	49.27	0.017	247
Random Forest	0.559	58.35	50.35	0.257	283

Figure 6 summarizes five numeric transaction features using their mean, standard deviation, minimum, maximum, and missing-value count. These statistics show the scale and spread of transaction amounts, distance from home, account balance, and transaction frequency. Confirm the supplied units before interpretation; descriptive summaries alone do not establish fraud causation.

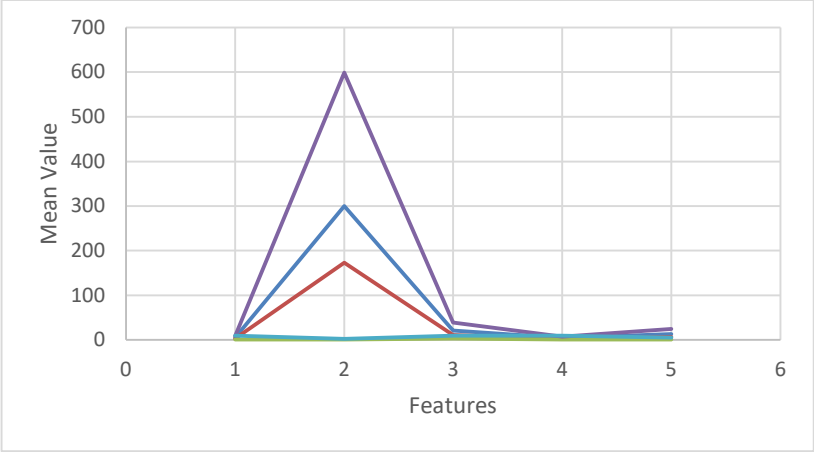


Figure 6. Descriptive Statistics of Selected Transaction Features

CONCLUSIONS

The use of AI to detect fraudulent financial transactions was stressed in this article. Several different categorization algorithms that may identify the kind of transaction from given characteristics were developed. The suggested methodology, which employs an artificial neural network, greatly improves the precision with which fraudulent transactions may be identified. Several techniques for improving detection accuracy were also presented in the article. These included handling unbalanced datasets, feature engineering, and feature transformation. In this research, we introduced an AI method that can detect financial fraud. All the chosen algorithms performed equally well throughout testing and training. The lack of a discernible visual difference in the ROC curve graphs further supports this conclusion. The results of the tests conducted on the offered algorithms showed that they all performed similarly when it came to identifying fraudulent bank transactions.

REFERENCES

[1]. M. Auleria, D. E. Saputra, and Y. Yustiawan, 2024, "Data-driven analysis of fraudulent transaction characteristics in branchless banking," *3rd International Conference on Digital Transformation and Applications*, pp. 68-73.

[2]. S. Geetha, Y. Mohammed Khan, R. Sujay, and S. P. Yoganand, 2023, "Fraudulent URL and credit card transaction detection system using machine learning," *International Conference on Advances in Electronics, Communication, Computing and Intelligent Information Systems*, pp. 709-714.

[3]. Z. S. Al-Sudani, and M. Riyadh, 2023, "Detecting fraudulent taxi drivers: Overview," *Al-Sadiq International Conference on Communication and Information Technology*, pp. 115-120.

[4]. S. Vyas, S. Serasiya, and A. Vyas, 2022, "Combined approach of ML and blockchain for fraudulent detection in insurance claim," *International Conference on Edge Computing and Applications*, pp. 544-550.

[5]. K. Raghuveer, T. N. Gongada, D. Nimma, M. Aarif, K. Samudrala and B. K. Bala, 2024, "Enhancing fraud detection in online e-commerce transactions through deep learning auto encoder model," *International Conference on Intelligent Systems and Advanced Applications*, pp. 1-6.

[6]. N. Ramesar, S. Ramoudith, N. Sharma, and P. Hosein, 2023, "A cost-minimization approach to automobile insurance fraud detection," IEEE International Conference on Technology Management, Operations and Decisions, pp. 1-6.

[7]. S. Korkanti, 2024, "Enhancing financial fraud detection using LLMs and advanced data analytics," *2nd International Conference on Self-Sustainable Artificial Intelligence Systems*, pp. 1328-1334.

[8]. P. S. Teja, P. P. Kumar, and S. M, 2025, "Advanced fraud detection in smart grids using deep neural networks," *International Conference on Advances in Renewable Energy and Electric Vehicles*, pp. 71-80.

[9]. J. Li, S. Liu, and J. Zou, 2024, "E-commerce data anomaly detection method based on variational autoencoder," *3rd International Conference on Artificial Intelligence, Internet of Things and Cloud Computing Technology*, pp. 231-234.

[10]. V. R. Saddi, B. Gnanapa, S. Boddu, and J. Logeshwaran, 2023, "Fighting insurance fraud with hybrid AI/ML models: Discuss the potential for combining approaches for improved insurance fraud detection," *4th International Conference on Communication, Computing and Industry 6.0*, pp. 01-06.

[11]. C. Bozogullarindan, and C. Ozturk, 2023, "Detection of Turkish fraudulent domain names to proactively prevent phishing attacks using a character-level convolutional neural network," *Innovations in Intelligent Systems and Applications Conference*, pp. 1-6.

[12]. A. Ganbayev, and E. Seyidzade, 2023, "Enhancing customs fraud detection: A comparative study of methods for performance measurement and feature improvement," *IEEE 17th International Conference on Application of Information and Communication Technologies*, pp. 1-5.

[13]. A. S. Musthafa, P. K. Sree, H. Fathima, R. Angu Jayalakshmi. P. Saranya, L. Murugesh, 2024, "Adaptive hybrid fraud detection system with personalized transaction profiling," *International Conference on Sustainable Communication Networks and Application*, pp. 1787-1792.

[14]. A. Wahrstätter, J. Gomes, S. Khan, and D. Svetinovic, 2023, "Improving cryptocurrency crime detection: coinjoin community detection approach," *IEEE Transactions on Dependable and Secure Computing*, 20(6), pp. 4946-4956.

[15]. P. Jha, S. Srivastava, T. Gandhi, and G. P, 2024, "Financial fraud detection for credit card transactions using Apache spark," *International Conference on Sustainable Communication Networks and Application*, pp. 427-431.

[16]. F. Khaled Alarfaj, and S. Shahzadi, 2025, "Enhancing fraud detection in banking with deep learning: graph neural networks and autoencoders for real-time credit card fraud prevention," *IEEE Access*, 13, pp. 20633-20646.

[17]. M. Kafila, C. Hassan, A. Veena, A. Singla, A. Joshi, and M. Lourens, 2024, "Fraud detection in IoT-based financial transactions using anomaly detection techniques," *International Conference on Advances in Computing, Communication and Applied Informatics*, pp. 1-6.

[18]. N. Suardiman, Sudimanto, S. Dhanny, D. Tjahjadi, B. Permana, and K. Ukar, 2024, "E-commerce fraud detection using generated data from BANKSIM using machine learning approach: A pilot study," *18th International Conference on Ubiquitous Information Management and Communication*, pp. 1-4.

[19]. B. Sharan, M. Hassan, V.D. Vani, V.H. Raj, and P.P. Pawar, 2024, "Machine learning-based fraud detection system for insurance claims in IoT environment," *International Conference on Advances in Computing, Communication and Applied Informatics*, pp. 1-5.

[20]. S. R. Banu, T. N. Gongada, K. Santosh, H. Chowdhary, R. Sabareesh, and S. Muthuperumal, 2024, "Financial fraud detection using hybrid convolutional and recurrent neural networks: An analysis of unstructured data in banking," *10th International Conference on Communication and Signal Processing*, pp. 1027-1031.

[21]. https://www.kaggle.com/datasets/zahranusratt/banking-fraud-detection-dataset