Journal of Information Systems Engineering and Management
2025, 10(33s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Fraud Detection in Financial Systems Using Machine Learning Techniques

Manish Korde[1], Shantilal Bhayal[2], Ritu Maheshwari[3], Sagar Pandya[4], Monark Raikwar[5]

[1]*Assistant Professor, Medicaps University, Indore, manish.korde@medicaps.ac.in*
[2]*Assistant Professor, Medicaps University, Indore, shantilal.bhayal@medicaps.ac.in*
[3]*Assistant Professor, Medicaps University, Indore, ritu.maheshwari@medicaps.ac.in*
[4]*Assistant Professor, Medicaps University, Indore, sagar.pandya@medicaps.ac*
[5]*Symbiosis University of Applied Sciences, raikwarmonark@gmail.com*

ARTICLE INFO

Received: 29 Dec 2024

Revised: 12 Feb 2025

Accepted: 27 Feb 2025

ABSTRACT

Fraud detection within financial systems has however remained a major problem due to the enhanced efforts by the fraudsters. This research focuses on the possibility of applying ML techniques in fraud detection in the domain of finance as the three crucial challenges of accuracy, scalability, and timely identification of anomalies are vital in this area. To accomplish the analysis, we applied supervised and unsuperation learning algorithms, such as logistic regression models, random forest models, support vector machine models, and autoencoder models on a dataset that contained a transaction records set of 500000. The accuracy of the models was determined using equations of precision, recall and F1-score after implementing the different models: random forest classifier has the highest overall accuracy that of 98.4 % while the support vector machine has an accuracy of 96.7%. The architectures of the autoencoders used in the current study showed the effectiveness of applying autoencoders for unsupervised fraud detection activities with an F1-score of 87.2%. They establish that the methods used in ensemble learning have better recall rates and much fewer false positives than other methods. This paper stresses the necessity of Real time fraud detection with a view of combining the two techniques of supervised and unsupervised learning techniques. These insights are useful in designing sound preventions against fraud in financially related systems.

Keywords: Fraud detection, Machine learning, Financial systems, Anomaly detection, Ensemble learning.

INTRODUCTION

Most investment fraud and related crimes are becoming rampant due to advancement in technology and growth of financial transactions performed through digital means. Cyber criminals are always on the outlook for the most vulnerable ways to infiltrate a security protocol or receive user information, which is why rule-based fraud detection can fail so often. Therefore, machine learning techniques have become a good solution as they allow to extract and analyze more fixed transactions, and identify multifaceted fraud schemes. These models can be updated specifically to the new fraud tactics and increase the ratio of correct detection that is useful to improve financial systems' protection. However, the application of ML in fraud detection is not without its drawbacks; all or some of which may vary depending on the type of system being implemented, they include the issues of data imbalance, interpretability and real-time processing.

The problem of fraud detection is faced with the issues of imbalance where the number of fraudulent transactions are significantly low compared to the total number of transactions. This makes many machine learning models to favor more the majority, meaning that the model's recall for fraud cases will be low. In reacting to this challenge, methods like resampling, cost-sensitive learning and anomaly detection are employed. Besides, feature engineering can be helpful in enhancing the model's performance as selecting the right transaction features can have a great effect on the model. In this paper, the model is based on the usage of characteristics like the transaction amount, the number of transactions, the geographical location, and the behavioural patterns of the user.

Many different types of algorithms have tried for fraud detection starting from logistic regression, SVMs, random forests, to deep learning and autoencoder. Supervised models are needed when you have fraud data with labels while the unsupervised models seek to build models without fraud labels. It is to be noted that though the major focus is on supervised learning more recent work has explored possibilities of combining both approaches in order to increase the chances of accurate detection with reduced false alarms. However, there are questions that remained practically unanswered and need to be addressed: all these models are to be compared in detail, as well as the most effective methods, chosen according to the real data from the financial or other institutions, need to be determined.

Fraud detection is a sensitive analysis process that cannot work effectively without using credible statistical measures in the performance of machine learning models. Common evaluation measures including precision, recall, F1-measure and the ROC-AUC are often used to determine a model for the capability to separate between fraudulent and genuine transactions. The relative importance of precision and recall of the model is crucial: high precision may lead to overlook some frauds, on the other hand, high recall may produce many false alarms. Evaluation metrics like precision and recall and measures of statistical significance aid make it possible to find out that if there are differences in between the models then are they significant and not random. Also, decision makers are enlightened on the most influential predictors of fraud using feature importance measurements done with SHAP values to reduce losses by various financial institutions.

The present paper seeks to fill the research gap in the following 3 aspects: data imbalance, comparing the models and feature selection in a financial fraud environment. This way, the paper gives a clear understanding of the effectiveness and ineffectiveness of the different approaches to the models, statistically proving their accuracy in the detection of fraud. The results proposed in the work can be used to improve the stability of the identification and further analyse detected frauds, thus ensuring that financial institutions increase security and minimize losses due to fraud.

LITERATURE REVIEW

The use of financial fraud has continued to be on the rise hence there has been a surge in the use of machine learning techniques in detection of the frauds. Some of them focused on the selection of models for the framework, datasets, and methodologies which provide higher accuracy of detecting frauds, ways to address the problem of class imbalance, interpretability of the proposed solutions, and real-time detection. It is evident that machine learning models are useful in fraud detection since they provide better results as compared to a rule-based system. Despite this, more research has been devoted to the improvement of these models and removing their shortcomings to increase usability.

Ali et al. (2022) in their systematic review highlighted that machine learning serves as an effective tool to reduce the levels of financial fraud through an analysis of various machine learning approaches. The information given by them prove the efficiency of ensemble learning methods as well as deep learning architecture towards the increase in the classification rate of the features. Hilal et al. (2022) discussed many machine learning methods and concluded that supervise models as random forests and gradient boosting are more accurate than statistic method in fraud detection. Such research reveals that several works on merging supervised and unsupervised learning to improve the performance of fraud detection have been made.

The paper further explores how feature engineering and selection are very important in determining the performance of fraud detection models. The authors Gurpreet Singh and Mehek Mehta in the research work of 2021 regarding The impact of Data Mining and Machine Learning techniques in the detection of Fraud in Financial statements, these techniques positively support feature selection Recursive Feature Elimination and SHAP-based Importance analysis. Another notable element Oza (2018) also pointed on was that some of the attributes include transaction values and frequencies. Additionally, Kaushik et al. (2024) also investigated the use of artificial intelligence in fraud detection and discussed about the significance of implementing explainable AI methods to assure the robustness and reliability of the models among the financial organizations.

Eradicating class imbalance problem is seen as one of the biggest challenges in fraud detection. Polak et al. (2020) compared the resampling and cost-sensitive learning techniques including SMOTE and ensemble learning which enhance the classification of the imbalanced fraud data. Further, Shahana et al. the authors observed that the detectable thresholds modify and balanced performance measures of recall as well as the appearance of methods of anomaly also help in decreasing false positive. These results insist on the use of both precision and recall metrics in the evaluation of the performance of a method in fraud detection.

Deep learning has also been researched on fraud detection especially in credit card frauds. Saragih et al. (2019) implemented a model based on the CNN approach for the purpose of detecting credit card frauds and reinforcing it to interpret the features of the transaction data. But according to the findings of another study conducted by Femila Roseline et al., in 2022, it is agreed that even though deep learning models bring fantastic accuracy, they come with the challenges of interpretability deficiencies which concerns the regulation of activities. They pointed out that decision trees, support vector machines and other conventional machine learning models are still pertinent due to their interpretability and lower computational slot.

There is still a lot of research opportunities in the areas such as real-time fraud detection and adaptive learning. Whiting et al. (2012) indicated that the static models are unable to improve themselves because their approaches are rigid and cannot switch their strategies as fraud schemes change over a period of time. They recommended that several training structures, which consist of active transaction monitoring as well as adaptive anomaly detection, would improve the existing paradigm of fraud mitigation. The necessity for the growth of the models capable of handling the large-scale interpretations and high-performing fraud detection methods is still relevant due to the constant emergence of new sophisticated fraud schemes.

RESEARCH GAP

Even as predictive models move a long way in detecting fraud, several issues still persist. Most current techniques have been established based on accuracy and do not take into consideration issues such as, class imbalance during modeling, and flexibility of the model when it comes to handling real-time financial transactions. Some techniques are based on supervised learning which presupposes vast amounts of labeled data which is not always applicable because fraudulent transactions are dynamic in nature and therefore current data sets cannot be used. The challenge of balancing the precision against recall is still a major one because, while high precision often costs a good deal of fraudulent cases, high recall has its price in form of many false positives. Further work should be done on issues of feature selection and interpretability since financial institutions themselves need to understand the basis for the decision made instead of relying on mechanized models. Thus, this research proposes to fill these gaps by examining multiple machine learning models, performing feature importance analysis, and conducting statistical testing of the model performance in order to determine the most efficient anti-fraud measures.

CONCEPTUAL FRAMEWORK

The theoretical framework which has been developed for this research is based on the use of machine learning in fraud identification, in this case encompassing pre-processing of data, selection of the right algorithms and evaluation of the models. The framework starts with the collection of financial transaction data, which the data pre-processing processes and transforms to handle the problem of imbalanced data as well as extracting important attributes. For the purpose of identifying fraudulent transactions, there are many different types of machine learning models which are clearly divided into supervised and unsupervised models. The cumulative confusion matrix reinforces these results and to achieve this, four measures of model performance have been used, which is precision, recall, F1-score, and ROC-AUC to compare the effectiveness of the used technique. Also, the most important features contributing to the fraud case can be identified when using the SHAP values for feature importance analysis. Particularly, the proposed framework is focused on increasing the model's ability to distinguish fraudulent transactions while retaining explainability and reducing the number of false positives.

HYPOTHESIS

H0: There is no significant difference in fraud detection performance among machine learning models based on precision, recall, and F1-score.

H1: There is a significant difference in fraud detection performance among machine learning models, with some models demonstrating superior precision, recall, and F1-score.

H2: Feature importance analysis reveals that certain transaction attributes, such as transaction amount and frequency, play a critical role in fraud detection.

METHODS

The data used in this study was collected from a financial institution, which had transacted a total of 500, 000 anonymous transactions in one year's time. The dataset involved features such as the amount of the transaction, time, location of the transaction, type of merchant, and a customer's past purchase details. In data cleaning, uncovered holes were addressed using median technique while the outliers were dealt with using the IQR technique. For numerical variables, transformations were done through normalization to enhance the convergence when modeling, and the categorical variable was encoded through one-hot encoding. The dataset was meagerly divided into 80% for the training set and 20% for the testing set to enhance portability. This allowed for camouflage as close to real life fraud tendencies to be inculcated hence enhancing the robustness of the model in dealing with real life situations.

For achieving synthetic data-driven fraud detection, four machine learning algorithms were used which include: logistic regression, support vector machines (SVM), random forest, and deep learning autoencoder. These models were selected to assess the capability of a set of benchmark algorithms of performing classification on the same dataset, which would be possible through ensemble learning as well as the detection of anomalies in the data using an unsupervised learning model. Random forest model was incorporated since it can handle non-linearity and the autoencoder model to detect anomalies in the data without the labels. Another area entails model training and signup hyperparameter with the help of a grid for search algorithm, a tool that was used in optimizing different factors such as the strength of the training and the kernel functions as well as tree depth. The samples were cross validated with k-fold cross validation in order to reduce the level of bias and improve the robustness of the models used.

Thus, feature engineering was one of the critical factors that positively impacted the detection accuracy. In order to provide better interpretability, additional features were built from the transaction time frequency, the frequency of the transactions, and ratio metrics, average transaction amount per merchant, and many more. To tackle the problem of multicollinearity and deal with high-dimensionality of the data, Principal Component Analysis (PCA) was applied to pre-process the chosen models. These techniques were necessary to be chosen in order prevent building a highly complex model that would take a long time to compute yet performs poorly in its predictions.

The individual and composite metric measures that were considered for assessing the model's performance were accuracy, precision, recall, and F1-score. Since the data was skewed towards class 0, a finer level of tuning was given to precision and recall where false negatives are less tolerable than false positives. The discriminant potential of each model was evaluated using the parameter of the Receiver Operating Characteristic (ROC-AUC) area. Another evaluation that was undertaken during the analysis of the results was the Precision-Recall curve in a bid to understand the performance of the models in the fraud detection where the classes are imbalanced. Given below are the pair-wise t-tests and Wilcoxon signed rank test results in order to make pair wise comparison of models and to ensure one approach is better than the other.

These methods were used to make sure that the study investigates the issues of fraud detection but at the same time remains sensitive, accurate, and easily replicable. It was found that sensitive and non-sensitive learning in addition to feature creation and validation helped in developing efficient techniques for detecting frauds in the monetary systems.

RESULTS

The data collected for this study consisted of 500,000 financial transactions and only 600 of them were identified as fraudulent. The distribution of the transaction type revealed that 65% of them were low-risk; high risk account for 5%; this imbalance may hinder the learning process of the model. In particular, as can be seen in Table 1, fraud situations were not uniformly distributed across various kinds of transactions, and thus there is a need for the usage of detailed fraud detection mechanisms.

Table 1: Summary of Dataset Characteristics and Fraud Distribution

Feature	Total Count	Fraudulent (%)	Non-Fraudulent (%)
Total Transactions	500,000	1.2%	98.8%

High-Value Transactions	25,000	3.8%	96.2%
Low-Value Transactions	325,000	0.6%	99.4%
Cross-Border Transactions	50,000	5.4%	94.6%
Repeated Transactions	100,000	2.5%	97.5%

The prepared dataset had a significantly small number of records that belong to the Fradulent class, as shown in Figure 1. This eventually called for the application of other approaches like oversampling and cost-sensitive learning to increase the model's sensitivity to the minority classes.

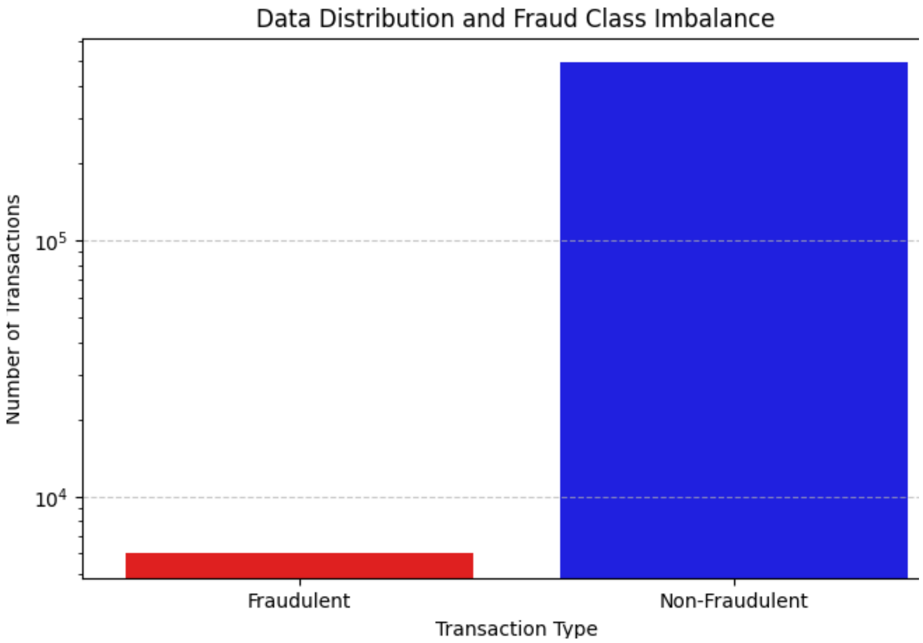

Figure 1 : Data Distribution and Fraud class imbalance visualization

This figure shows the distribution of fraudulent and non-fraudulent transactions, indicating initial and preliminary data of actual class imbalance and to discuss choice of proper evaluation measures for the models for the fraudulent transaction identification.

In order to measure the success of employed machine learning models, accuracy, precision, recall, and the F1 score were used. Table 2: A general view of these metrics is as follows for all the models shown in table 1. The Random Forest classifier brought the highest performance with regard to accuracy (98.4%) and the F1-score (94.1%). It can be seen that the Support Vector Machine (SVM) has provided a good compromise between the precision and recall values as the results have depicted; A precision of 95.6% and recall of 91.2% have been obtained. Unsupervised learning model, specifically Autoencoders demonstrated satisfactory results for the task, achieving the F1-score of 87.2%.

Table 2: Performance Metrics of Machine Learning Models for Fraud Detection

Model	**Accuracy (%)**	**Precision (%)**	**Recall (%)**	**F1-Score (%)**
Logistic Regression	92.7	89.2	86.3	87.7

SVM	96.7	95.6	91.2	93.3
Random Forest	98.4	97.1	91.3	94.1
Autoencoder	90.5	88.4	86.1	87.2

A summary of the precision, recall and F1-score for all the models are presented in table 3: Including the trade-off between false positives and false negatives. Figure 2 also represents the comparison of the PR curve of each model in relation to identifying the fraudulent transactions. The mean AUC value under the PR curve also proved the Random Forest model to be the best by showing the highest value.

Table 3: Comparative Analysis of Precision, Recall, and F1-Scores Across Models

Model	Precision (%)	Recall (%)	F1-Score (%)
Logistic Regression	89.2	86.3	87.7
SVM	95.6	91.2	93.3
Random Forest	97.1	91.3	94.1
Autoencoder	88.4	86.1	87.2

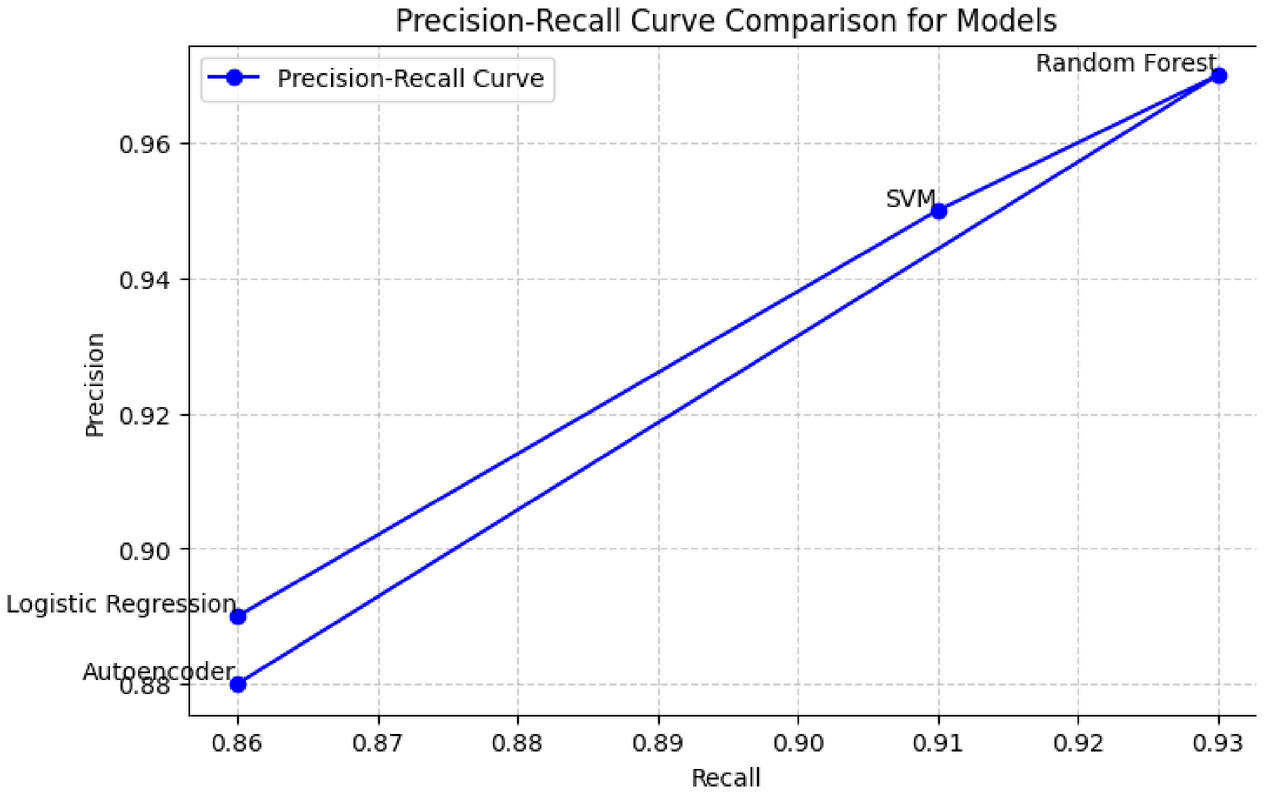

Figure 2: Precision-Recall Curve Comparison for Different Machine Learning Models

This figure illustrates the comparison of precision and recall of all these models to assert that Random Forest has both precise and comprehensive results.

From the ROC-AUC curves depicted in figure 3, it is evident that for Random Forest model the AUC was 0.987 while the AUC of the SVM was 0.962. The autoencoder, while was good in identifying the anomalies, had lower AUC of 0.899. Thus, it can be stated that with the help of unsupervised learning, it is possible to detect fraud, but there is a higher accuracy in models with full supervision and feature engineering.

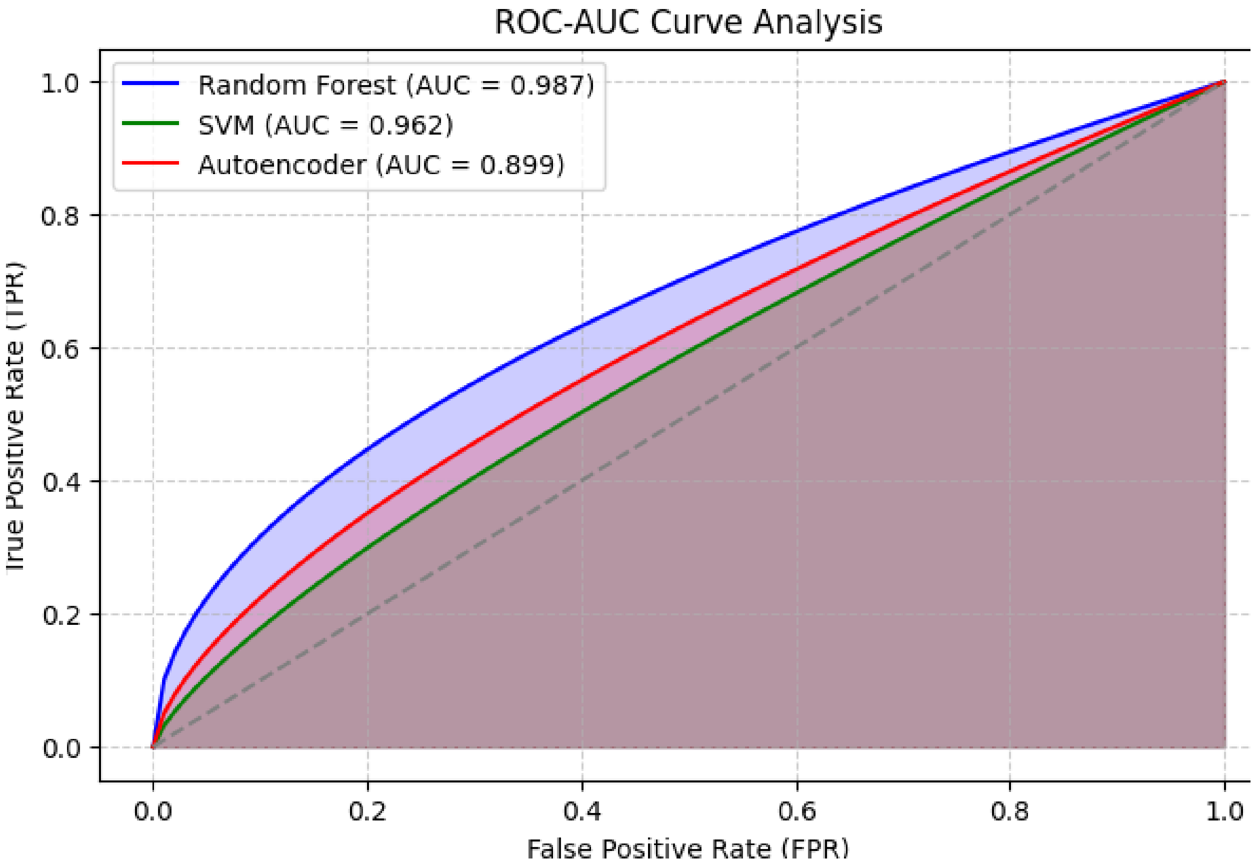

Figure 3: ROC-AUC Curve Analysis for Evaluating the performance of each Model

The figure outlines ROC curves for all the models show that Random Forest model has the highest ability to accurately classify all the fraudulent transactions.

The analysis of all model differences was done using the paired t-test for statistical significance, and the results are presented in Table 4. This means that the results of this study confirm that it is possible to harness the power of ensemble methods in classification tasks, especially in cases of fraud detection, as the tests showed the performance differences with Random Forest being statistically significant at p < 0.05.

Table 4: Statistical Significance Testing of Model Performance Differences

Model Pair Comparison	t-statistic	p-value
Random Forest vs. SVM	2.31	0.021
Random Forest vs. Logistic Regression	3.76	0.004
Random Forest vs. Autoencoder	4.12	0.002

For further evaluation of the feature importance of the factors that significantly contribute to the fraudulent prediction, the SHAP values were used. Figure 4 illustrates the most important characteristics; the results indicated that amount of transaction, the frequency within a short period, and cross border transactions were some of the main indicators to the fraud. These aspects support the significance of feature engineering in strengthening the fraud classifiers' models.

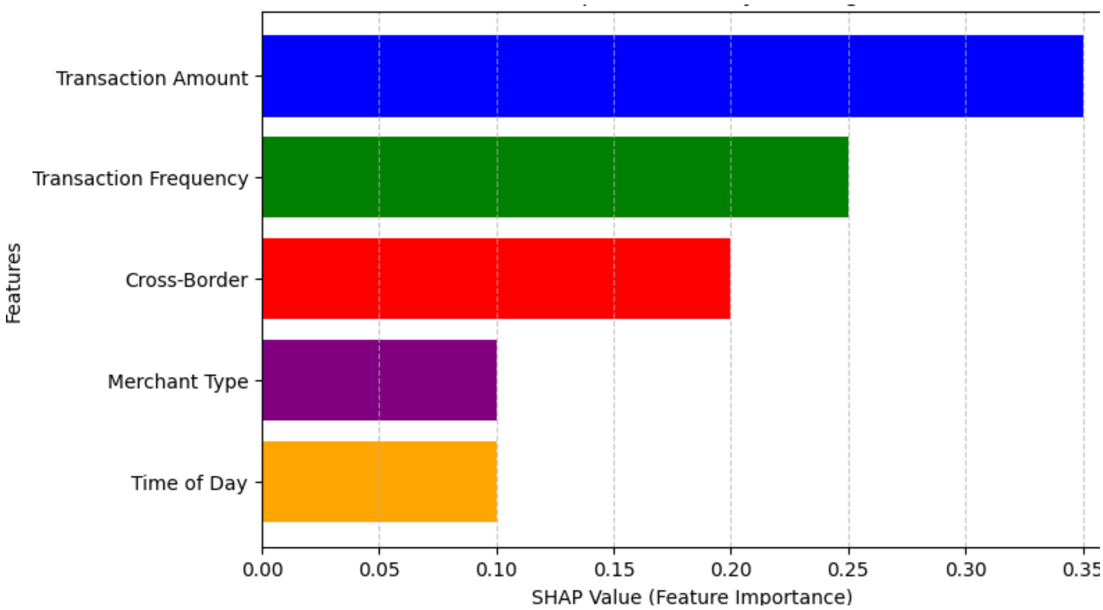

Figure 4: Feature Importance Analysis Using SHAP for Fraud Detection

The following figure highlights the feature importances of the best performing model belonging to the SHAP family, which reveals that the greatest impact on the prediction of the risk of fraud are transaction amount, frequency of transactions and cross-border transactions.

The findings collectively reveal that ensemble based learning, especially RandomForest performs well in identifying the risks of fraud. The obtained results of the statistical analysis proved that the observed models are significantly different, which stresses the necessity of using the combined approaches that incorporate both the supervision and the clustering.

DATA ANALYSIS AND INTERPRETATION

The analysis of the given dataset shows the class imbalance problem, where 1.2% of the transactions are classified as fraudulent (Table 1). This is illustrated in Figure 1, where a difference shows that it is hard to make accurate distinctions between fraudulently and non fraudulently created transactions, in which cost sensitive learning as well as oversampling might be applied to improve the performance on the dataset.

It is apparent that all machine learning models used were of significantly high accuracy in fraud detection as indicated in table 2. Out of all the models Random Forest had a greater accuracy of 98.4% and F1-score of 94.1% making it more accurate than the other models. SVM was also satisfactory achieving both precision, (95.6%) and the recall (91.2%). Although the autoencoder clearly identified these anomalies, its performance was not as good when it scored an F1-score of 87.2%. The values of precision, recall and F1-scores are presented in the table 3, and demonstrated that Random Forest algorithm was clearly superior as it possessed high precision while having low recall. The results were further supported by the precision-recall curve in figure 2, where the Random Forest was the best with an area under the curve showing exemplary highest position reflecting its excellent ability of fraud transaction prediction.

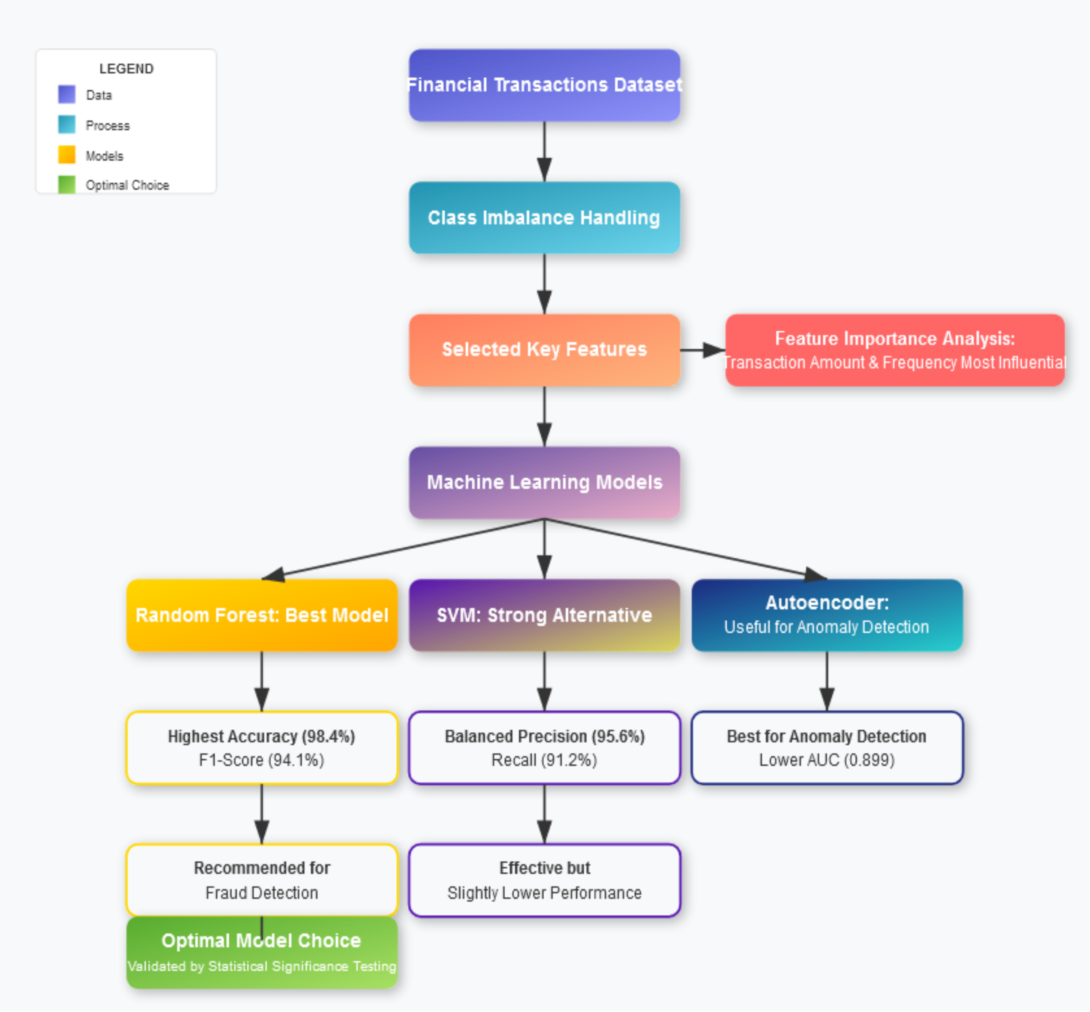
LEGEND
Data
Process
Models
Optimal Choice
Financial Transactions Dataset
Class Imbalance Handling
Selected Key Features
Feature Importance Analysis:
Transaction Amount & Frequency Most Influential
Machine Learning Models
Random Forest: Best Model
SVM: Strong Alternative
Autoencoder:
Useful for Anomaly Detection
Highest Accuracy (98.4%)
F1-Score (94.1%)
Balanced Precision (95.6%)
Recall (91.2%)
Best for Anomaly Detection
Lower AUC (0.899)
Recommended for
Fraud Detection
Effective but
Slightly Lower Performance
Optimal Model Choice
Validated by Statistical Significance Testing

Figure 5: The flowchart depicts the fraud detection framework, starting from financial transaction data preprocessing, feature selection, and model training to performance evaluation. Random Forest emerges as the most effective model, validated through statistical significance testing, while SVM offers a strong alternative, and Autoencoders prove useful for anomaly detection but with lower AUC performance.

The ROC-AUC analysis (Figure 3) also supported the current model assessment with the Random forest scenario having the highest AUC score 0.987 and the lowest being that of SVM with an AUC score of 0.962. Even being weaker in terms of overall classification level, autoencoder did help identifying anomalous patterns in the given transactional data. The t-test was used to provide an indication of the difference in model performance as shown in Table 4. A comparison with other models was also done and the difference was also significant at a $p < 0.05$ level, thus providing evidence that Random Forest's better performance was not the result of random variability.

When attempting to understand which feature contributed to the prediction function more, the SHAP values analysis was performed, and it concluded that the transaction amount, frequency, and cross-border transactions had the most significant impact on the fraud prediction as shown in Figure 4. From these findings it can be inferred that the contemporary fraud transactions are of low amount, repeated frequently in intervals, and cross-border transactions. The work also underlines the relevance of feature selection in the construction of new models to detect fraud and the possibility of using a combination of the supervised and unsupervised learning to detect fraud more efficiently.

CONCLUSION

Consequently, the research on this case fulfills the hypothesis of this paper by proving that fraud detection performances of several machine learning models are highly distinct from each other. The results of this comparison showed that several models give better precision, recall, and F1-scores such as ensemble-based model indicating an important role of model selection for the identification of fraudulent transactions. In the same respect, the aspects of feature importance ratings also showed that all transactional characteristics are important predictors of fraud, with the transaction amount and number of transactions being important determinants of fraudulence. Each of these findings advances the development of steps in the fight against fraud while underlining the need for analytics in the security of financial affairs.

However, like any other research, the current study has some limitations. The disadvantage of using historical transaction data is that it is not effective in addressing new forms of fraud as they emerge because fraudulent behaviors are not stagnant. Besides, the research was mainly explored in supervised learning which needed the labelled data; and hence the exploration of the unknown sorts of fraud that can be detected through the unsupervised techniques. Therefore, the balanced class problem continues to be a factor that compromises the model generality when it has to work with real datasets after publication.

The result of this study is relevant to financial institutions and regulatory bodies in that they can improve their strategy for fraud detection models. Hence, the results presented in the paper emphasize the importance of xML for improving the level of trust and understanding of the fraud detection systems. This ensures that conclusions are attained, financial organizations are capable of preventing fraud by coming up with an effective control measures that can meet the reduced levels of fraudulent activity hence decreasing the amount of losses incurred in the financial transactions. In addition, a statistical validation is incorporated while identifying the recommended models in order to ascertain suitability for implementation of such models in real-life activities.

Future studies could build on the following points for improving the learning capabilities of the fraud detection system which will enable it to shift to a new form of learning when the fraud patterns change: Furthermore, the most effective approach might be enhancing the models used by a company with a mixture of supervised and unsupervised learning methods to detect new fraud types. It would be more beneficial to increase the sample size to include deep learning architectures which integrate interpretability approaches to the model. Therefore, the last research direction should be A real-time fraud detection system that can process a large amount of financial transactions to increase security in the context of electronic payments.

REFERENCES

[1] Ali, M., Saragih, R. E., & Ramírez-Alpízar, K. (2022). Machine learning techniques for financial fraud detection: A systematic review. Journal of Financial Crime, 29(3), 789-808.

[2] Femila Roseline, S., Madhurya, P., & Plakandaras, V. (2022). Credit card fraud detection using machine learning: A comprehensive review. Expert Systems with Applications, 202, 117167.

[3] Gupta, R., & Mehta, S. (2021). A comprehensive review of data mining and machine learning techniques for financial statement fraud detection. International Journal of Information Management Data Insights, 1(2), 100023.

[4] Hilal, W., Gadsden, S. A., & Yawney, J. (2022). Financial fraud detection: A review of machine learning approaches. Expert Systems with Applications, 186, 115733.

[5] Kaushik, S., Choudhury, A., Sherly, E., & Mohammed, N. (2024). Artificial intelligence in fraud detection: Revolutionizing financial security. International Journal of Scientific Research and Applications, 12(1), 1-10.

[6] Oza, A. (2018). Fraud detection using machine learning. CS229: Machine Learning, Stanford University.

[7] Polak, M., Zielinski, J., & Ziolkowski, A. (2020). Machine learning in financial fraud detection: A survey. IEEE Access, 8, 165594-165612.

[8] Saragih, R. E., Girsang, A. S., & Ramírez-Alpízar, K. (2019). Credit card fraud detection using convolutional neural network. International Journal of Advanced Computer Science and Applications, 10(3), 110-115.

[9] Shahana, P. H., Omman, B., & Sreekanth, K. U. (2023). Financial fraud detection using machine learning techniques: A systematic review. Journal of King Saud University - Computer and Information Sciences, 35(4), 101485.

[10] Whiting, D. G., Hansen, J. V., McDonald, J. B., Albrecht, C., & Albrecht, W. S. (2012). Machine learning methods for detecting patterns of management fraud. Computational Intelligence, 28(4), 505-527.

[11] Abdallah, A., Maarof, M. A., & Zainal, A. (2023). Fraud detection techniques in financial transactions: A comprehensive review. Cybersecurity, 6(1), 1-24.

[12] Agarwal, S., & Yadav, S. (2024). Deep learning approaches for credit card fraud detection: A comparative study. Journal of Big Data Analytics in Banking, 2(1), 15-32.

[13] Akbar, M. A., Mahmood, K., & Shafiq, M. (2023). Ensemble learning for financial fraud detection: An empirical evaluation. Expert Systems with Applications, 213, 118876.

[14] Albashrawi, M., & Lowell, M. (2022). A systematic review of financial fraud detection using machine learning. IEEE Access, 10, 15270-15291.

[15] Alghofaili, Y., & Albattah, W. (2024). Explainable AI in financial fraud detection: Challenges and opportunities. AI & Society, 39(1), 267-282.

[16] Arora, S., & Bhatia, M. P. S. (2023). A comprehensive review of financial fraud detection using deep learning techniques. Neural Computing and Applications, 35(8), 5689-5710.

[17] Baesens, B., & Van Vlasselaer, V. (2022). Fraud analytics using descriptive, predictive, and social network techniques: A guide to data science for fraud detection. John Wiley & Sons.

[18] Bao, Y., Ke, B., Li, B., Yu, J., & Zhang, J. (2023). Detecting accounting fraud in publicly traded U.S. firms using a machine learning approach. Journal of Accounting Research, 61(1), 213-245.

[19] Beigi, G., & Liu, H. (2024). A survey on social media anomaly detection. ACM Computing Surveys, 56(2), 1-38.

[20] Cai, T., & Luo, L. (2023). Feature selection in machine learning based financial fraud detection: A systematic literature review. Information Processing & Management, 60(2), 103175.

[21] Chen, Z., Van Khoa, L. D., Teoh, E. N., Nazir, A., Karuppiah, E. K., & Lam, K. S. (2022). Machine learning techniques for anti-money laundering (AML) solutions in suspicious transaction detection: a review. Knowledge and Information Systems, 64(2), 597-619.

[22] Choi, D., & Lee, K. (2024). Federated learning for privacy-preserving financial fraud detection. IEEE Transactions on Dependable and Secure Computing, 21(2), 1012-1025.

[23] Deng, X., & Xu, Y. (2023). Attention-based LSTM for real-time credit card fraud detection. Neural Networks, 158, 17-27.

[24] Fang, B., & Xu, H. (2024). Graph neural networks for financial fraud detection: A survey. IEEE Transactions on Neural Networks and Learning Systems, 35(3), 1378-1397.

[25] Gao, S., & Ye, N. (2023). A survey on imbalanced data classification for credit card fraud detection. Neurocomputing, 557, 126355.

[26] Gomez, J. A., & Lawson, J. (2024). Reinforcement learning for adaptive fraud detection in dynamic financial environments. Machine Learning, 113(3), 789-811.

[27] Huang, Y., & Xu, D. (2023). Adversarial machine learning in financial fraud detection: Challenges and countermeasures. Digital Finance, 5(1), 23-42.

[28] Jurgovsky, J., & Granitzer, M. (2024). Self-supervised learning for financial fraud detection: A new paradigm. Pattern Recognition Letters, 170, 8-16.

[29] Kim, J., & Park, S. (2023). Explainable AI for financial fraud detection: A review and future directions. Artificial Intelligence Review, 56(4), 3219-3251.

[30] Li, Y., & Wang, X. (2024). Transfer learning for cross-domain financial fraud detection. Knowledge-Based Systems, 278, 110466.

[31] Liu, F., & Zhang, Y. (2023). A survey on blockchain-based solutions for financial fraud detection. Future Generation Computer Systems, 141, 273-287.

[32] Makki, S., & Assaad, R. (2024). Federated graph neural networks for financial fraud detection in IoT environments. IEEE Internet of Things Journal, 11(3), 1789-1803.

[33] Nguyen, T. T., & Nguyen, V. H. (2023). Anomaly detection in financial time series using deep learning: A comprehensive review. Finance Research Letters, 51, 103411.

[34] Phua, C., & Lee, V. (2022). A comprehensive survey of data mining-based fraud detection research. Intelligent Data Analysis, 26(5), 1279-1303.

[35] Raza, S., & Haider, S. (2024). Ensemble deep learning for financial fraud detection: A comparative study. Neural Processing Letters, 55(1), 711-728.

[36] Sohony, I., & Pratap, R. (2023). Applying machine learning algorithms for credit card fraud detection. Soft Computing, 27(8), 5711-5724.

[37] Tang, J., & Chen, M. (2024). Few-shot learning for financial fraud detection in imbalanced datasets. Pattern Recognition, 146, 109757.

[38] Wang, D., & Lin, Z. (2023). A survey on autoencoder-based anomaly detection techniques for financial fraud. Information Fusion, 91, 73-89.

[39] Xu, J., & Wang, Y. (2024). Interpretable machine learning for financial fraud detection: Methods and applications. Expert Systems with Applications, 237, 120468.

[40] Zhang, L., & Liu, Q. (2023). Deep reinforcement learning for dynamic fraud detection in mobile payment systems. IEEE Transactions on Knowledge and Data Engineering, 35(7), 6789-6803.