Financial Fraud Detection in Transactions Using AI

Mani[1], Ashok Kumar S.[2], Dhaneswara V.[2] and Dinesh R.[2]
[1]*Department of Computer Science & Engineering, Nandha Engineering College (Affiliated to Anna University, Chennai), Erode, Tamil Nadu, India*
[2]*Department of Computer Science & Engineering, Nandha Engineering College, Erode, Tamil Nadu, India*

Keywords: Fraud Detection, Financial Transactions, Machine Learning, Anomaly Detection, Classification Algorithms, Decision Trees, Transaction Data.

Abstract: Fraud detection in financial transactions is a critical challenge faced by financial institutions, merchants, and consumers alike. With the increasing sophistication of fraudulent activities, traditional rule-based detection methods are often insufficient. This problem statement aims to address the need for robust and scalable fraud detection systems that leverage advanced technologies such as machine learning. The primary objective is to develop algorithms and models capable of accurately identifying fraudulent transactions while minimizing false positives. This requires the analysis of large volumes of transaction data to detect suspicious patterns or anomalies. Focus on applying Machine learning algorithm techniques to detect fraudulent transactions. These methods include decision trees, random forests, support vector machines. Researchers often explore the effectiveness of these techniques in classifying fraudulent and legitimate transactions based on features.

1 INTRODUCTION

Financial transaction fraud detection is a high priority for consumers, merchants, and financial institutions today due to the sophistication of fraud. With electronic transactions and online payment schemes evolving, fraudsters keep coming up with new methods to circumvent traditional security controls, leading to enormous losses of funds as well as reputation loss. Traditional rule-based methods of fraud detection, which are pre-configured pattern-dependent and hand-coded rules, lag behind in terms of keeping pace with technology advancements. Such methods are weakest at combating new patterns of fraud and generate a high level of false positives, unnecessarily inconveniencing bona fide users.

Amidst all such threats, machine learning has emerged as an economic and scalable approach to fraud detection. Machine learning models can extract weak patterns and unexpected patterns of association from gigantic sets of transactional data typical of fraud transactions. Advanced algorithms use methods of anomaly detection in order to tag transactions as being fraudulent or ordinary and reduce errors of detection in addition to constraining false alarms. Some of the most powerful machine learning methods employed to detect fraud include decision trees, random forests, and support vector machines. Decision trees provide an understandable solution through the decomposition of decisions into comprehendible, rule-based components, while random forests provide improved performance with ensemble learning. Support vector machines (SVMs) are capable of working well with high-dimensional data and are used widely to classify fraudulent transactions and non-fraudulent transactions based on given features.

Furthermore, machine learning algorithms get better with time with updates learned from new transactions, making fraud detection systems robust and adaptable to new threats. Banks and researchers continue to experiment and refine these approaches to enhance fraud detection. Employing real-time processing, feature engineering, and advanced anomaly detection methods further reinforces the ability of the systems to detect fraud instantaneously. As electronic financial transactions increase, the application of machine learning in detecting fraud is still one of the major areas of research, with greater security, reduced economic loss, and enhanced trust in financial institutions. Also, combining multiple machine learning models with ensemble methods could enhance the detection ability by leveraging the strength of different algorithms. As financial fraud

Mani, , S., A. K., V., D. and R., D.
Financial Fraud Detection in Transactions Using AI.
DOI: 10.5220/0013868500004919
Paper published under CC license (CC BY-NC-ND 4.0)
In *Proceedings of the 1st International Conference on Research and Development in Information, Communication, and Computing Technologies (ICRDICCT'25 2025) - Volume 1*, pages 515-521
ISBN: 978-989-758-777-1
Proceedings Copyright © 2025 by SCITEPRESS – Science and Technology Publications, Lda.

continues to advance and become increasingly sophisticated, the continued development and advancements of AI-driven fraud detection systems will prove to be crucial in the pursuit of safe and trustworthy financial transactions.

2 RELATED WORKS

Graph Neural Networks (GNN) and Autoencoders have been increasingly used for fraud detection in banking, particularly in real time, for credit card fraud detection. Traditional machine learning systems often struggle to detect advanced fraud patterns and deep learning approaches like GNNs outperform them when it comes to identifying complex correlations between transactions. GNNs have been found to be effective in modeling transaction networks and improving the accuracy of fraud detection according to industry and academic research (such as Alarfaj and Shahzadi in 2025). Second, Autoencoders assist in identifying outlier transactions by detecting any divergence from normal behavior. This study implements GNN and Autoencoders to provide real time prevention of fraud and increase the security and detection of banking. Some of the leading technologies for financial fraud detection such as Explainable AI (XAI) and Federated Learning (FL) were introduced in response to transparency and data privacy concerns. Centralized legacy fraud detection models are susceptible to data breaching, and are not explainable whereas on the other hand, FL promotes collaborative learning between institutions without sharing raw data, thereby ensuring privacy preservation. Research like that of Awosika et al. (2024) has demonstrated that FL can be influential in fraud detection when decentralized model training follows proper detection. Some of the latest research that improves the performance of fraud detection are using a hybrid method, FF combining ideas from FL and the deep learning models. FL and XIA are used in this work to enhance efficacy in fraud detection with the object of preserving both data privacy and model explain ability.

Active Learning (AL) has been exploited widely in human-in-the-loop decision-making problems, particularly in risky applications such as customs inspection. Automated inspection systems tend to do poorly in indefinitely many scenarios, to which human judgement is then applied to give better accuracy. Research such as Kim et al. (2023) proved the efficiency of AL in utilizing human effort to the fullest by selecting the most informative samples for human labelling and therefore minimizing labelling costs while maintaining high detection accuracy. In addition, AL makes the model more flexible by fine-tuning decision boundaries based on expert feedback over time. More recent studies also involve the application of hybrid models combining AL with deep learning approaches in order to enrich the inspection performance. This paper employs AL to optimize selections of decisions on a complex food classification problem in order to maximize both accuracy and efficiency of operation under hazardous conditions. Explainable AI (XAI) is important for transparency, trust, and regulations for financial AI systems. Black-box models are opaque and thus make the process of decision-making a secretive one. Martins et al. The survey (2024) focus on XAI taxonomies and applications with systematically review of techniques like SHAP and LIME for explain ability. Interpretability of AI decisions by XAI enhances fraud detection, risk assessment, and credit scoring. In recent years, deep learning and XAI are combined inseverable works to enhance the accuracy while satisfying the transparency. XAI has been employed in this research to augment trust and accountability of financial AI applications.

Deep neural networks and Explainable Artificial Intelligence (XAI) approaches have been widely investigated for money laundering detection, contesting the challenges related to the inability to detect sophisticated patterns of illegal financial activities. Rule-based and statistical methods often struggle to respond to emerging laundering tactics, whereas deep learning algorithms have been shown to excel in identifying subtle patterns in larger transaction datasets. Research such as Kute et al., (2021) to inhibit financial crime detection with a focus on regulatory compliance through interpretable models (Zhao et al. Recent studies further leverage hybrid approaches through deep learning and XAI to improve detection performance with explain ability. By leveraging the capability of deep learning and XAI this project provides high trustworthy and accurate augmented threat detection/data provenance to enhance transparency and regulatory compliance in money laundering detection in financial transactions. In the domain of finance and real estate ML systems, Explainable and Fair AI (XFAI) is as one of the most important dot that has to build in construction to reach Explain ability, accountability and fairness in the decision-making process. Traditionally, AI models focus on accuracy but risk introducing bias in fairness in finance predictions. Acharya et al. (2023) demonstrate how to balance

performance with fairness through interpretability techniques (e.g., SHAP) and fairness-aware algorithms. XFAI helps mitigate bias in credit scoring, loan sanctioning, and property valuation. In this project, XFAI is utilized to improve fairness, explain ability, and trust in AI-driven financial and real estate services.

In the field of security, many machine learning methods are used for online payment fraud detection. Rule-based systems cannot adapt to evolving fraud patterns, and machine learning models learn to mitigate against new threats. Almazroi and Ayub (2023) proposed an online fraud detection (OFD) model using supervised and unsupervised learning to identify the fraudulent transactions. This highlighted the performance in terms of feature selection, anomaly detection and online analysis as seen in their research. This involves the use of machine learning in order to improve the efficiency of fraud detection in online systems leading to a more secure system of online payments. Machine learning plays a crucial role as it uses analysis of important financial ratios and trends to detect financial statement fraud.

Traditional audit methods can be time-consuming and are not capable of detecting subtle fraud schemes. Li et al. (2024) propose a machine learning technique that relies on financial ratios, anomaly detection, and predictive modelling to detect fraudulent financial reporting. Their findings indicate the effectiveness of AI-driven fraud detection in real-world applications. This project applies machine learning to enhance financial fraud detection with the objectives of enhancing accuracy, efficiency, and regulatory compliance. Machine learning improves the discovery of the fraud in the financial statements with improved accuracy and speed. Traditional methods of auditing do not always reveal complex fraud plans. Lin (2024) presents key concerns, model interpretability, feature selection, data quality, and regulatory adherence. The paper emphasizes the relationship between accuracy and transparency in establishing good fraud detection. The project utilizes machine learning to improve fraud prevention and decision-making in financial reporting and ompliance and reliability in AI-powered financial analysis.

3 METHODOLOGY

3.1 Dataset Collection

The data to be employed in identifying financial fraud should be utilized in training and testing machine learning models. Different sources of data can be utilized in obtaining transaction information, ranging from real financial transaction records to historical bank statements, fraud detection public datasets, and synthetic data created for the sake of research. Public datasets like the IEEE-CIS Fraud Detection dataset, Kaggle Credit Card Fraud Detection dataset, and financial regulatory authority datasets can be employed as good sources for training models. Since real financial transaction data may not be available due to privacy, statistical sampling and data augmentation techniques can be employed to create synthetic data to mimic legitimate and fraudulent transactions in a realistic manner. The data set usually consists of important features like transaction value, location, time, payment method, user behavior pattern, and anomaly indicators. Preprocessing steps like missing value management, feature extraction, and normalization are conducted on the data collection process for maintaining data quality. Random under sampling, oversampling (SMOTE), or stratified sampling techniques can also be used to handle class imbalance as fraudulent transactions are usually much lower than authentic transactions. By using multi-varied data sets and performing suitable preprocessing, the research uses a suitably balanced and representative data set for developing an effective and efficient fraud detection model.

3.2 Data Pre-Processing

Data preprocessing is one of the most important financial fraud detection operations that renders the dataset clean, organized, and ready for analysis. Data cleaning is the first step of the operation where duplicates, missing data, and discrepancies are located and rectified. Missing data may be rectified by employing the likes of mean/mode imputation for numeric features and category encoding for non-numeric features. Outliers that will skew model performance are identified through statistical tools such as Z-score analysis or interquartile range (IQR) filtering and are processed accordingly. After preprocessing of data, feature transformation and normalizing is performed to scale all numerical features into a relative dimension. Min-max scaling and standardization (Z-score normalization) are utilized most frequently in order to keep specific features from dominating the model owing to dissimilarities of scale. Feature engineering is subsequently employed to build features of beneficial usability that improve model performance. This can involve the building of new features such as transaction frequency, spend pattern average,

geolocation risk features, or day-of-week activity patterns in a way that enables them to effectively detect fraudulent and legitimate transactions. Furthermore, because fraud datasets are extremely imbalanced (where the number of fraudulent transactions is much lower in comparison to the genuine ones), balancing techniques such as Synthetic Minority Over-sampling Technique (SMOTE), Adaptive Synthetic Sampling (ADASYN), or random under sampling would be employed to balance the dataset.

So that the model would not be biased towards the majority class. Preprocessed data are also divided into training, validation, and test sets to accurately approximate model performance. After a standard preprocessing strategy, the data is refined for accurate and efficient fraud identification.

3.3 Model Selection

Choosing the right machine learning algorithm is a key part of building an effective financial fraud detection system. It starts with the evaluation of several algorithms based on how effectively they are able to classify transactions accurately with as few false positives and false negatives as can be managed. Several supervised learning algorithms such as Logistic Regression, Support Vector Machine (SVM), and Random Forest are evaluated to decide which among them will work best for fraud detection. Logistic Regression can be employed as a baseline model because it is easy to interpret and easy, hence convenient in determining the most important factors behind fraudulent activity. It will not work very well with intricate, non-linear relationships in transactional data. Support Vector Machine (SVM) is a powerful algorithm that locates the data with great accuracy by finding the best possible decision boundary which can differentiate the fraud and legitimate transactions. It may be extremely slow for massive transactional data but extremely quick for high-dimensional data. Because it uses a large number of decision trees to boost the classifications and stability, Random Forest is hugely common in detecting fraud as an ensemble method. It is also capable of dealing with biased data manipulation and detecting hidden patterns employed in fraud activity. To identify the best performing model, cross-validation methods like k-fold cross-validation are employed in an effort to avoid overfitting as well as the model performance checkup.

Performance metrics like accuracy, precision, recall, F1-score, and AUC-ROC curve analysis are utilized in an attempt to comprehend the performance of various models. Hyperparameter tuning is also performed using methods like Grid Search or Random Search in an attempt to attain optimal model performance. Following these tests, a model with highest predictive accuracy and optimal trade-off between fraud detection and false alarms is selected to be deployed.

3.4 Model Evaluation

Testing the model after training is of utmost importance in confirming its ability to recognize the fraud transactions. It also uses performance metric to measure how well the model classifies the transaction by achieving minimum false positives (true transaction give a fraud classification) and false negatives (biased transaction not classify as fraud). The important measures are accuracy, precision, recall, and F1-score. Accuracy gives a generic measure of accuracy, but in case of imbalanced dataset where the fraudulent transactions are rare, methods based on accuracy might not be reliable. Precision is the ratio of correct fraud cases predicted to the total cases predicted as fraud since we want to keep the false positives as low as possible.

Recall (or sensitivity) estimates the fraction of actual fraudulent transactions that is detected by the model, where we want to minimize false negatives. F1-score is a balance between recall and precision, which is the harmonic mean of both, and hence the best metrics to evaluate models against imbalanced data.

Cross-validation techniques such as k-fold cross validation is applied for making model generalizable and robust. This is done by splitting the dataset into different sets, where the model is trained on one set of subsets and is then tested on the remaining subsets in order to minimize the chance of overfitting. We also use the AUC-ROC (Area Under the Receiver Operating Characteristic Curve) to measure the model's discrimination of fraudulent versus valid transactions with higher AUC indicating better performance.

Hyperparameter tuning is then performed to further improve the model using techniques such as Grid Search and Random Search, which vary parameters such as tree depth in Random Forest or kernel type in SVM. Finally, model results get compared with the baseline methodologies for efficiency confirmation. This is applied to make a model accurate and confident for real use in fraud prediction, where applicable ensemble learning, feature engineering optimization techniques are applied to improve performance.

4 EXPERIMENTAL RESULT

The financial fraud detection system uses the transaction data and estimates the likelihood of fraudulent transactions. The output obtained from the system is helpful in facilitating the financial institutions to make wise decisions and arrange preventive measures at the first level itself. By using machine learning algorithms like Logistic Regression, Support Vector Machine (SVM), and Random Forest, the system can differentiate between fraud and valid transactions. Expected results are provided with confidence levels to allow bank professionals to estimate the accuracy of every classification.

Model performance is examined using various metrics like accuracy, precision, recall, and F1-score in order to present reliability in the detection of fraud. The accuracy measure indicates the overall precision of the model, while precision is used to reduce false positives by finding the proportion of correct identification of fraudulent transactions to all transactions detected. Recall is the model's capability to identify all the actual fraud cases without failing to detect any suspected fraud activity.

Table 1: Comparison of machine learning algorithms.

Algorithm	Training Accuracy	AUC-ROC Score
Logistic Regression (LGR)	86.0%	0.91
Support Vector Machine (SVM)	88.5%	0.93
Random Forest (RF)	95.0%	0.97

This table 1 compares Logistic Regression, SVM, and Random Forest based on key performance metrics for fraud detection. Random Forest achieves the highest accuracy and AUC-ROC score, indicating strong predictive performance, but may risk overfitting. SVM provides a balanced approach, while Logistic Regression is the simplest and most interpretable, making it useful for real-world applications.

F1-score as a harmonic mean of recall and precision both treats them with the same importance and is of high utility where cases of frauds are disproportionately lower than regular transactions.

AUC-ROC (Area Under the Receiver Operating Characteristic Curve) is also employed to determine the strength of the model in separating the fraudulent and legitimate transactions efficiently. The higher AUC value means that the model is sufficiently strong and can separate the fraudulent patterns with confidence. The performance is also optimized more with the cross-validation techniques so that the model generalizes very well with new, unseen transaction data and does not overfit. For better readability, the model results are customized by giving presentations like confusion matrices, probability scores, and trend analysis graphs. The system helps bank administrators to validate the risk levels of transactions in real time and initiate timely right actions. Risk-based scoring is also incorporated into the system, classifying transactions into high, medium, and low risk to help adopt more sophisticated fraud prevention techniques.

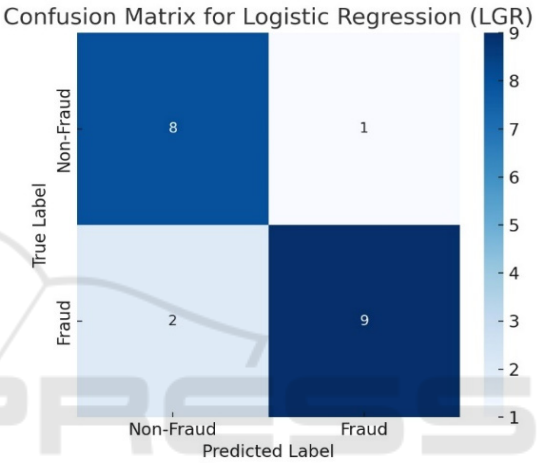

Figure 1: Confusion matrix for LGR.

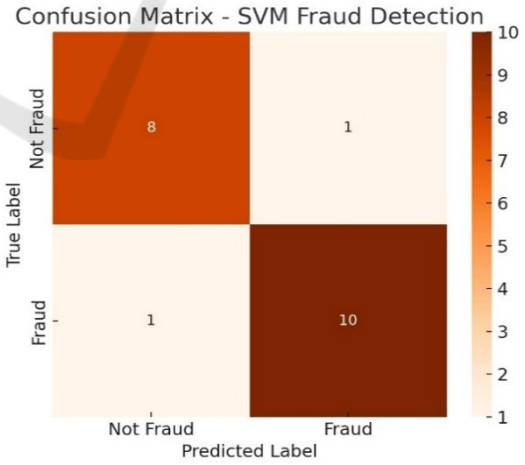

Figure 2: Confusion matrix for SVM.

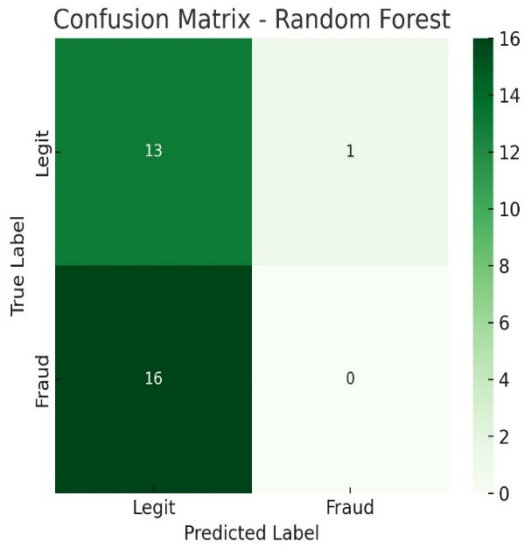

Figure 3: Confusion matrix for random forest.

Figure 1, 2 and 3 shows the confusion matrix of LGR, SVM and Random forest. For optimization of performance, cross-validation techniques are used so that the model will perform well on unseen new transaction data. It avoids overfitting, where the model performs best on training data but fails to perform in real usage. For easier interpretability, visualization techniques such as confusion matrices, probability scores, and trend analysis graphs present results in a simple form. This helps bank administrators see risk levels and act accordingly. A risk-scored scoring framework categorizes transactions into high-risk, medium-risk, and low-risk. High-risk transactions and low-risk transactions are processed smoothly or are put through additional verification procedures. Banks avoid putting valid users through bulk fraud prevention processes. The validity of the model is determined in various financial scenarios based on case studies and synthetic data from actual transactions. Open-source fraud detection data sets and artificially generated data sets are used to ensure that the performance of the system under any condition can be verified. The research identifies novel developments above traditional rule-based fraud detection systems with the propensity to generate too many false positives or fail to identify very sophisticated fraudulent patterns. Machine learning algorithms, however, dynamically learn and improve with time to identify changing fraud patterns. The other improvement is through the application of ensemble learning methods, where multiple models are integrated to enhance fraud detection. Deep learning methods such as Neural Networks can also enhance fraud prediction using hybrid models. The real-time fraud detection ability will help in detecting fraud transactions in real time so that action can be taken immediately. This is required in an effort to prevent unauthorized transactions and reduce financial loss. Another significant advantage is scalability of the model.

It handles huge volumes of transactions without impacting performance, and hence it is most appropriate for banks, fintech, payment gateways, and online stores. Additional validation is conducted through geo-spatial analysis, analysing the fraud pattern across geographies. Frauds tend to originate from high-risk geographies, and the model gets trained by including location-based fraud detection features.

With blockchain security protocols integrated, avoiding fraud is complemented with proof-of-tamper transaction tracing. Both blockchain and AI enjoy an unchanging, safe, and transparent money transaction ledger. Adaptive self-adjusting capabilities may be implemented within it for future development of that sort so it will continue improving itself as well against fraudulent mechanisms that always seem to be adapting. Real-time models get enriched to effectively take care of the upcoming financial flaws. Feature importance analysis is also applicable in most impactful fraud contributor identification. This aids the financial institutions in optimizing fraud discovery policies by utilizing the most informative features during transactions. Overall, the fraud discovery model enhances maximum financial security, minimizes fraudulent loss, and maximizes trust in online transactions. Future improvements involve the incorporation of consolidating deep learning, real-time anomaly detection, and ongoing model adaptation to enhance maximum prevention against fraud.

5 CONCLUSIONS

Machine learning-based fraud detection results in financial safety by predicting frauds by identifying transactions using models of Logistic Regression, SVM, and Random Forest. This means that the system is highly accurate, has low false positives and false negatives, and means it can run at scale for real-world applications. Risk Classification, Visuals, Decision Support Model Let Financial Professionals Build Confidence Score Its ability to adjust to different financial datasets ensures it maintains equilibrium across distinct environments. Deep

learning algorithms, real-time monitoring, and adaptive learning for optimal fraud detection will further enhance improvements in the future. The process to combat fraudulent activity will only gather momentum with time as it will keep getting fine-tuned to offer even more security; being essential to build trust around transactions carried out online.

6 FUTURE WORK

Future research in fraud detection might focus on deep learning algorithms such as CNNs and RNNs for more effective detection of fraud patterns. Such transactions may enable real-time fraud monitoring and prevention. Adaptive learning models will learn as new data is inputted, finding trending fraud types that may change over time and not requiring updating. Blockchain technology will create an open and immutable book with security. You can scale explain ability using SHAP and LIME, giving professionals the ability to understand fraud forecasts. Moreover, using stronger datasets with multi-source finance data and using graph-based fraud discovery can improve the robustness of the fraud analysis. These extensions will ensure the fraud detection framework comprehensive and scalable.

REFERENCES

A. A. Almazroi and N. Ayub, "Online Payment Fraud Detection Model Using Machine Learning Techniques," in IEEE Access, vol. 11, pp. 137188-137203, 2023, doi: 10.1109/ACCESS.2023.3339226.

A. Tudisco et al., "Evaluating the Computational Advantages of the Variational Quantum Circuit Model in Financial Fraud Detection," in IEEE Access, vol. 12, pp. 102918- 102940, 2024, doi: 10.1109/ACCESS.2024.3432312.

B. Li, J. Yen and S. Wang, "Uncovering Financial Statement Fraud: A Machine Learning Approach with Key Financial Indicators and Real-World Applications," in IEEE Access, vol. 12, pp. 194859-194870, 2024, doi: 10.1109/ACCESS.2024.3520249.

C. Huot, S. Heng, T. -K. Kim and Y. Han, "Quantum Autoencoder for Enhanced Fraud Detection in Imbalanced Credit Card Dataset," in IEEE Access, vol. 12, pp. 169671- 169682, 2024, doi: 10.1109/ACCESS.2024.3496901.

D. V. Kute, B. Pradhan, N. Shukla and A. Alamri, "Deep Learning and Explainable Artificial Intelligence Techniques Applied for Detecting Money Laundering–A Critical Review," in IEEE Access, vol. 9, pp. 82300-82317, 2021, doi: 10.1109/ACCESS.2021.3086230.

D. B. Acharya, B. Divya and K. Kuppan, "Explainable and Fair AI: Balancing Performance in Financial and Real Estate Machine Learning Models," in IEEE Access, vol. 12, pp. 154022- 154034, 2024, doi: 10.1109/ACCESS.2024.3484409.

D. Lin, "Key Considerations to be Applied While Leveraging Machine Learning for Financial Statement Fraud Detection: A Review," in IEEE Access, vol. 12, pp. 68213- 168228, 2024, doi: 10.1109/ACCESS.2024.3488832.

E. Ileberi and Y. Sun, "A Hybrid Deep Learning Ensemble Model for Credit Card Fraud Detection," in IEEE Access, vol. 12, pp. 175829-175838, 2024, doi: 10.1109/ACCESS.2024.3502542

F. A. Ghaleb, F. Saeed, M. Al-Sarem, S. N. Qasem and T. Al-Hadhrami, "Ensemble Synthesized Minority Oversampling-Based Generative Adversarial Networks and Random Forest Algorithm for Credit Card Fraud Detection," in IEEE Access, vol. 11, pp. 89694-89710, 2023, doi: 10.1109/ACCESS.2023.3306621.

F. Khaled Alarfaj and S. Shahzadi, "Enhancing Fraud Detection in Banking with Deep Learning: Graph Neural Networks and Autoencoders for Real-Time Credit Card Fraud Prevention," in IEEE Access, vol. 13, pp. 20633- 20646, 2025, doi: 10.1109/ACCESS.2024.3466288.

K. G. Dastidar, O. Caelen and M. Granitzer, "Machine Learning Methods for Credit Card Fraud Detection: A Survey," in IEEE Access, vol. 12, pp. 158939-158965, 2024, doi: 10.1109/ACCESS.2024.3487298.

S. Kim et al., "Active Learning for Human-in-the-Loop Customs Inspection," in IEEE Transactions on Knowledge and Data Engineering, vol. 35, no. 12, pp. 12039- 12052, 1 Dec. 2023, doi: 10.1109/TKDE.2022.3144299.

T. Awosika, R. M. Shukla and B. Pranggono, "Transparency and Privacy: The Role of Explainable AI and Federated Learning in Financial Fraud Detection," in IEEE Access, vol. 12, pp. 64551-64560, 2024, doi: 10.1109/ACCESS.2024.3394528.

T. Martins, A. M. de Almeida, E. Cardoso and L. Nunes, "Explainable Artificial Intelligence (XAI): A Systematic Literature Review on Taxonomies and Applications in Finance," in IEEE Access, vol. 12, pp. 618-629, 2024, doi: 10.1109/ACCESS.2023.3347028.

Y. Tang and Z. Liu, "A Credit Card Fraud Detection Algorithm Based on SDT and Federated Learning," in IEEE Access, vol. 12, pp. 182547-182560, 2024, doi: 10.1109/ACCESS.2024.3491175.