International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 – 5161
©2025 INPRESSCO®, All Rights Reserved
Available at http://inpressco.com/category/ijcet

Research Article

Enhancing Financial Security Based on Machine Learning Techniques for Anomaly Detection in Fraud Transactions

Mani Gopalsamy*

Independent Researcher

Received 25 March 2025, Accepted 10 April 2025, Available online 12 April 2025, **Vol.15, No.2 (March/April 2025)**

Abstract

Financial organizations face growing threats to their security because of digital banking along with online financial transactions. The research demonstrates a method to boost financial security that implements machine learning anomaly detection algorithms on fraudulent payment systems. The research utilizes the Credit Card Fraud (CCF) dataset with substantial discrepancy between authentic and fraudulent records while executing comprehensive data preprocessing techniques that utilize outlier identification methods in addition to random under-sampling strategies. The important features are comprised of 31 attributes that include anonymized variables (V1–V28) and transaction parameters (time and amount) with their assigned class label. The data has been partitioned into training, which takes up 70%, and testing, which occupies 30%. The method known as Isolation Forest (iForest) turns out to be the most effective classifier when tested on anomalous transactions with 98.65% accuracy coupled with 98.20% precision along with 98.64% recall and 98.52% F1-score performance. Anomaly detection-based machine learning methods indicate their clear ability to detect fraudulent transactions through both precise and high-recall manner. The results prove that sophisticated machine learning systems function as effective security instruments to stop financial system fraud.

Keywords: *Credit Card Fraud Detection, Anomaly Detection, Machine Learning, Isolation Forest, Financial Security, Fraudulent Transactions*

1. Introduction

The financial sector presents a substantial fraud problem due to both its expanding transaction numbers and its sectoral diversification. Such fraudulent practices put financial institutions together with client consumers in serious danger. Efficient systems to detect and prevent fraud have become essential due to the current situation [1]. Conventional fraud detection methods have played an essential role over the past decades, but current fraudulent tactics, alongside the rapid increase in data, have made their operational boundaries more evident [2].

Financial transaction crimes are serious offenses that exploit monetary systems to harm people and corporate entities or such organizations. Money loss is only one consequence of financial transaction fraud [3], The financial market stability along with its integrity faces significant risks by these acts. Financial transaction fraud has evolved because of new technology, which has also enabled the global expansion of financial systems [4].

The primary foundation of using conventional fraud detection methods requires establishing several thresholds which become warning signs for detecting unusual transaction behaviors. Standard statistical detection approaches carry their own disadvantages for fraud prevention purposes [5]. The traditional approaches generally demonstrate inferior learning capabilities compared to modern ML algorithms, which leads to efficiency problems during large data processing [6][7]. The financial industry transformed client relationships concerning service delivery usage and access to financial products [8][9]. The development of information technology led to operational streamlining of financial services to enhance the simplicity of consumer transactions and banking account management and institutional communication [10]. Digital innovation introduces major security risks because fintech services process confidential financial information, which scammers exploit as targets.

AI technologies in ML facilitate the overview of trends and adaptation to new risks by processing existing data so organizations can benefit from enhanced security measures [11]. Real-time hazard identification occurs through continuous ML model

*Corresponding author's ORCID ID: 0000-0002-7847-6928
DOI: https://doi.org/10.14741/ijcet/v.15.2.10

development from analysis of large data sets, while existing security systems require predetermined rules. The financial industry finds great value in this adaptable feature [12], where fraud and anomaly detection [11] A platform security system requires essential protection through intrusion detection together with vulnerability assessment approaches. ML functions to predict risks while simultaneously strengthening security measures against fraud attempts [13], facilitating financial organizations' proactive vulnerability management as opposed to their reactive approach [14].

In order to realize the system, it is necessary to create an effective intrusion detector that can monitor harmful activity. Infact an anomaly detection technique can be employed to identify deviations of known use patterns as intrusion [15]. The known hostile activity is better addressed with automated detection. Automatic detection can be done via methods based on ML [16] [17]. The practice of identifying items or events that deviate from the anticipated pattern or other components of a collection is known as anomaly detection [18]. While some anomalies may just be accidents, others may be purposefully created by malevolent invaders [19].

The ML provides a dynamic, adaptable, and intelligent way to improve security as the financial sector expands and cyber threats become more complex, preserve client information, and guarantee legal compliance [20]. Transcending conventional, static security methods [21], Fintech businesses may use ML to create more secure and robust systems that can survive the constantly changing cyberthreat scenario [22].

A. Structure of paper

This is the structure of the paper: A thorough analysis of the research on ML-based methods for identifying irregularities in financial transactions is provided in Section II. The approach, including data collection, preprocessing, feature selection, dataset splitting, and the Isolation Forest algorithm-based classification phase, is described in Section III. The findings and performance evaluation are covered in Section IV. The study is concluded in Section V, which also makes recommendations for future improvements to fraud detection systems in financial contexts.

2. Literature Review

This section presents earlier studies on financial security using machine learning techniques for identifying anomalies in fraudulent transactions.

Rani and Mittal (2023) the research on AI-inspired deception identification with digital payment security hinges on secondary data sources, including publications and academic papers, to provide an understanding of their development, effectiveness, and challenges. This analysis attempts to provide interesting views by looking at and comparing the results from past studies, which are towards the improvement of electronic transaction systems by financial institutions, businesses and the policy makers. The two main facets of digital payment security that are the subject of this study are anomaly detection and real-time transaction monitoring. The purpose of this research is to conduct a thorough examination of deception detection systems driven by AI [23].

Vynokurova et al. (2020) a hybrid ML system is presented for solving anomaly detection jobs. The anomaly detection subsystem, which employs unsupervised learning, and the anomaly type interpretation subsystem, which is based on a supervised system, make up this hybrid system. The advantage of the proposed hybrid system is that it can process data rapidly when it is supplied in real time. When solving the anomaly detection problem using actual data streams, the efficacy of the suggested method was validated [24].

Boutaher et al. (2020) explain the basic principles of fraud detection, the systems in place for detecting fraud, the problems and difficulties associated with banking-related frauds, and the machine learning-based solutions now in use. Big Data technologies affect a number of important industries, including manufacturing, transportation, healthcare, finance, and e-commerce. The rise of e-commerce transactions and the digitization of services have an impact on financial services, they are thus essential to the financial industry. Consequently, a number of problems that affect the banking industry have been brought about by the rise in credit card usage and the rise in fraudsters. These problems, regrettably, undermine the effectiveness of fraud control systems (fraud detection and prevention systems) and exploit the openness of online payments [25].

Kumar, Dua and Rastogi (2023) investigate and contrasts several methods for deep learning and machine learning. For several reasons, such as severely unbalanced datasets, a lack of information on real frauds, and the unpredictability of the issue, anomaly identification may be a challenging undertaking. The issue is also contextual because the transaction in question does not have to be an anomaly. By doing fraud detection on datasets related to healthcare provider and credit card fraud, they have been able to make some conclusions about which algorithms perform better in certain situations. Finding data points that don't follow the typical patterns that the rest of the dataset follows is known as anomaly detection [26].

Thilagavathi et al. (2024) propose an innovative system that improves fraud detection by fusing anomaly detection methods with GNNs. Transactions are represented as graphs, allowing GNNs to capture intricate fraud patterns. Anomaly detection methods flag suspicious transactions. Ablation studies underscore the significance of graph-based representations and anomaly detection mechanisms.

Only 0.172% of all transactions are fraudulent, making the sample very imbalanced. Their approach surpasses the cutting-edge Gradient Boosting Classifier by 10% with a 2% false positive rate and a 95% detection rate [27].

Sharma and Sharma (2024) provided by the development of the integration of unsupervised learning models and methods for Real-time fraud detection will allow for the future development of more advanced fraud detection systems. Improving the capacity to identify fraud inside digital financial infrastructures: a comparison of the efficacy of DL and ML models, namely CNNs and RNNs. With an AUC of 0.972, an astounding 95.8% precision, 93.7% sensitivity, and 97.5% specificity, the research reveals that the RNN architecture outperforms the CNN model. The models' constant good performance across different transaction amounts, as shown in the investigation, further points to their resilience and versatility [28].

Table I summarizes recent studies on anomaly detection in fraud transactions. It compares methodologies, datasets, performance, and limitations and highlights advancements in AI, DL and algorithms for detecting fraud in real time.

Table 1 Comparative table for literature review on Anomaly detection in fraud transactions

Reference	Methodology	Dataset	Performance	Limitations & Future Work
Rani and Mittal (2023)	AI-based anomaly detection using secondary data; focuses on real-time surveillance.	Research papers and articles	Qualitative insights; highlights AI's role in digital payment security.	No real-world ML implementation; lacks empirical validation. Future work: empirical AI studies.
Vynokurova et al. (2020)	Hybrid model with unsupervised + supervised learning for real-time detection.	Real-time transaction streams	High-speed processing; effective anomaly detection.	Needs scalability testing; explore DL for fraud classification.
Boutaher et al. (2020)	ML-based fraud detection in various sectors using Big Data.	Financial sector Big Data	Identifies key challenges; emphasizes AI solutions.	No real-world validation; explore real-time AI solutions.
Kumar, Dua and Rastogi (2023)	Comparative study of ML/DL models; addresses data imbalance.	Credit card & healthcare fraud datasets	Evaluates model performance on imbalanced data.	Struggles with anomalies not being outliers; suggests data augmentation, self-supervised learning.
Thilagavathi et al. (2024)	Graph-based transaction modelling and anomaly-detecting graph neural networks (GNNs).	Imbalanced dataset (0.172% fraud)	95% detection rate; outperforms traditional models.	Needs real-time optimization; improved deployment scalability.
Sharma and Sharma (2024)	CNNs + RNNs for real-time detection; integrated anomaly framework.	Digital transaction data	95.8% accuracy; robust across transaction types.	Reduce false positives; explore federated learning for scalability.

3. Methodology

This study follows a structured methodology for ML algorithms for detecting credit card fraud. There is a considerable class imbalance in the dataset, which comprises 284,807 transactions, of which 284,315 are valid and just 492 are fraudulent. Each record is represented by 31 features, including anonymized principal components (V1–V28), Time, Amount, and Class. During data preprocessing, outlier mitigation and random under-sampling were applied to address extreme values and class imbalance. The most important features were kept in the feature selection process, improving the model's accuracy and interpretability while reducing duplication. A correlation matrix confirmed that most features have low correlation with one another, indicating minimal multicollinearity. In order to guarantee effective model learning and trustworthy performance evaluation, the dataset was then divided into 70% for training and 30% for testing, as seen in Figure 1. The Isolation Forest (iForest) algorithm was employed for classification, leveraging random binary trees to isolate anomalies based on path length. The model was assessed using performance indicators such as F1-Score, Accuracy, Precision, and Recall. These metrics provided insight into different aspects of categorization quality.

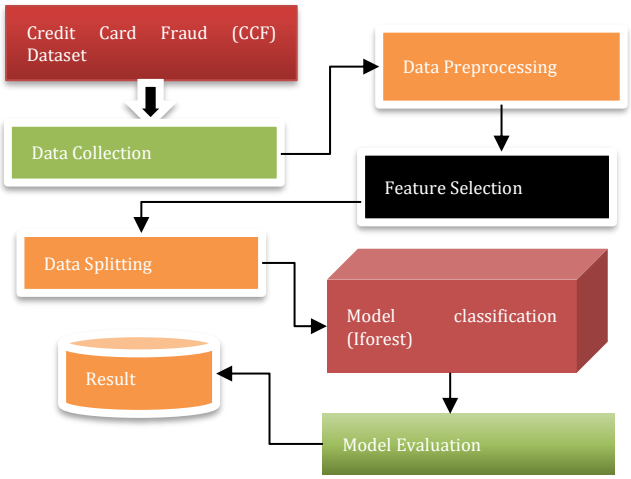

Figure 1 Workflow Diagram

Data Collection

The dataset for credit card fraud, or CCF, which comprises 284,807 transaction records in total, is used in this study. There is a notable class disparity among these, with 284,315 transactions classified as valid and only 492 as fraudulent. The dataset is divided into two categories, fraudulent and valid transactions, and is organized for binary classification tasks. Each record is

represented by 31 features (V1 to V28, Time, Amount, Class) that record different behavioral and transactional characteristics that are essential for detecting fraud.

Data Preprocessing

The preparation procedure also involved resampling the data to address class imbalance, which is typically a critical issue with relation to fraud data, and using an outlier mitigation technique to handle high values within the dataset. The initial unbalanced dataset and the balanced one following random under-sampling are displayed in Figure 2. One popular technique for dealing with uneven data of a comparatively big magnitude is random under-sampling.

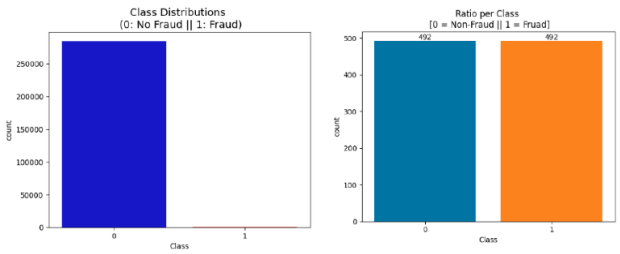

Figure 2 Class Distribution Before and After Resampling for Fraud Detection

Feature Selection & Important

The feature selection procedure enhanced the model's performance and efficiency. Table II lists the anonymized principal components (V1-V28) obtained via PCA transformations, transaction Time, target variable, and the amount. Key characteristics include class, which reflects the fraud status. Due to their capacity to identify crucial trends in transaction behavior and differentiate between authentic and fraudulent activity, these properties were crucial. By concentrating on these factors, the technique achieved maximum operating efficiency, improved interpretability, and preserved model accuracy while reducing dimensionality.

Table 2 Features Used for Fraud Detection Analysis

No.	Feature
1	V1-V28
2	Time
3	Amount
4	Class

Figure 3, illustrates the correlation between features V1 to V28 in the fraud detection dataset. Lighter colors indicate stronger correlations, while darker shades represent weaker or negative correlations. Most features show low correlation with each other, suggesting minimal multicollinearity, which is beneficial for model performance and interpretation.

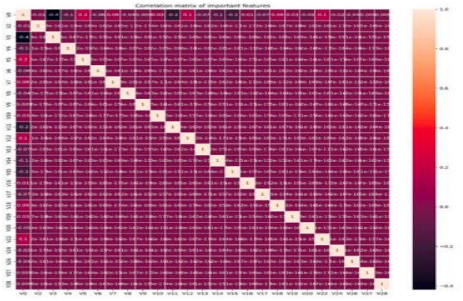

Figure 3 Correlation Matrix of Important Features

Dataset Split

The model for detecting credit card fraud was constructed using 70% of the dataset for training and 30% for testing. This division ensured that the model had enough data to assess its performance appropriately and discover trends.

Classification Phase

A subfield of AI called ML enables computers to understand and learn from data without the need for explicit programming. ML enables self-sufficient solutions for a variety of computational issues.

Isolation Forest (iForest)

A group of independent, random trees (itrees) utilised in this approach is called a random forest. Using every tree in the forest, IForest creates a score for every piece of data. Two input parameters are used by IForest to determine the data score [29]. The parameters are ψ, the size of the randomly selected sample from the complete dataset, and t, the number of trees in the forest. Since each tree is created separately by sampling the dataset, the number of trees and samples is equal.

Binary trees make up the isolation tree (itree). The following is how the tree's construction is accomplished: All of the sample data is initially included in the root node. Every internal node is divided into two subnodes (left and right) during the tree-building process until all data is isolated or the maximum tree depth is reached (Equation 1):

$$max\_depth = log2(\psi) \quad (1)$$

As seen in Figure 4, when X0 and Xi are isolated after three and eleven splits, respectively, data is said to be isolated when it is alone in its node.

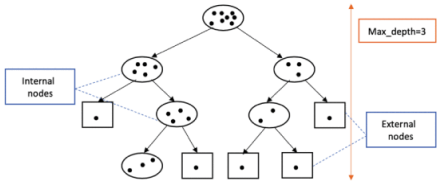

Figure 4 Isolation Forest (IForest)

Performance Matrix Model Evaluation

To choose the evaluation metric that will best evaluate the model, one must be aware of how each metric measures. The aim was to evaluate all of these. The effectiveness of ML algorithms is assessed using performance measures, including F1-Score, Accuracy score, Precision, and Recall.

Accuracy

The percentage of cases the model properly classifies and the overall error in class prediction are known as accuracy. The model's performance across classes is summed up by this metric. However, performance may be misrepresented by biased data [30]. It is possible for a classifier that mostly predicts the majority class to be correct while misclassifying instances of the minority class (Equation 2).

$$Acuracy = \frac{TP+TN}{TP+TN+FN+FP} \quad (2)$$

Precision

The percentage of instances that are accurately allocated to a class after all the data has been categorized is known as precision [31]. In this instance, it shows the proportion of corona cases that actually are corona cases. The one-vs-all method is used to compute it for every class (Equation 3):

$$Precision = \frac{TP}{TP+FP} \quad (3)$$

Recall

The number of cases correctly categorized into a class is determined by sensitivity or recall [32]. This context is a measure of the proportion of properly representing instances by the classifier over the sum of all carriers of the illness. Recall is computed according to the one-vs-all method, the same as precision (Equation 4).

$$Recall = \frac{TP}{TP+FN} \quad (4)$$

F1-score

The F1-score, often called the weighted harmonic mean of recall and accuracy is called the F-measure [33]. This metric is best suited for usage when the dataset is very unbalanced. A more thorough evaluation is possible when a wider view point is used (Equation 5).

$$F1 - score = 2 * \frac{precision*recall}{precision+recall} \quad (5)$$

Where,

TP (True Positive): The result was positive, as the model had projected.

TN (True Negative): In contrast to what the model had predicted, the value was really negative.

FP (False Positive): Although A negative number was returned, even though the model had predicted a positive one.

FN (False Negative): In contrast to the model's forecast, the real outcome was favorable.

4. Results And Discussion

In this section, it gets a description of simulated outcomes of ensemble learning techniques to detect credit card data anomalies having overlapping classes and imbalanced classes, respectively. Results This concludes the dataset evaluation results of the study carried out on this dataset and includes classifier statistics, performance metrics, and results.

Model Performance

In this section, since the classes that are part of an ensemble learning technique to detect anomalies in these classes are unbalanced and overlapping, the findings of using the Iforest model in the identification of anomalies in credit card data with unbalanced and overlapping classes are provided.

Table 3 Performance Metrics of Iforest Classifier for Fraud and Non-Fraud Detection

Classifier	Accuracy		Precision		Recall		F1 Score	
	Fraud	***Non-fraud***	***Fraud***	***Non-fraud***	***Fraud***	***Non-fraud***	***Fraud***	***Non-fraud***
Iforest	96.34	98.70	96.32	98.09	97.31	98.47	95.06	98.21

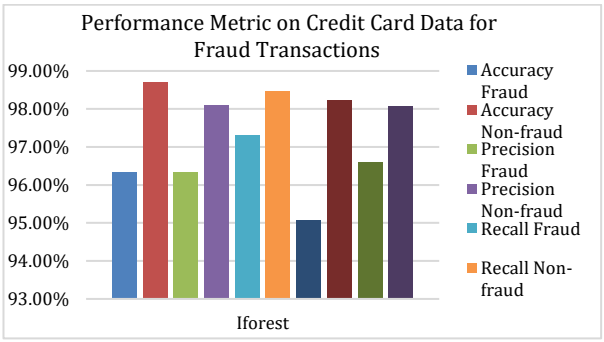

Figure 5. ML-Based Fraud Detection: Performance Evaluation

The above is illustrated with numbers in Table III and Figure 5. Noise had positively affected the model's precision at 96.32% for fraud and 98.09% for non-fraud, which contributed a small number of misconfirmed cases in both groups. Equally striking were the recall rates, namely 97.31% for fraud and 98.47% for non-fraud, implying the model's remarkable ability to spot actual fraud situations while, at the same time, reducing the number of cases that were not fraud but were misclassified. Given the F1-score of 95.06% and 98.21%, which was the product of precision and recall, it was evident that the model responded well to both categories.

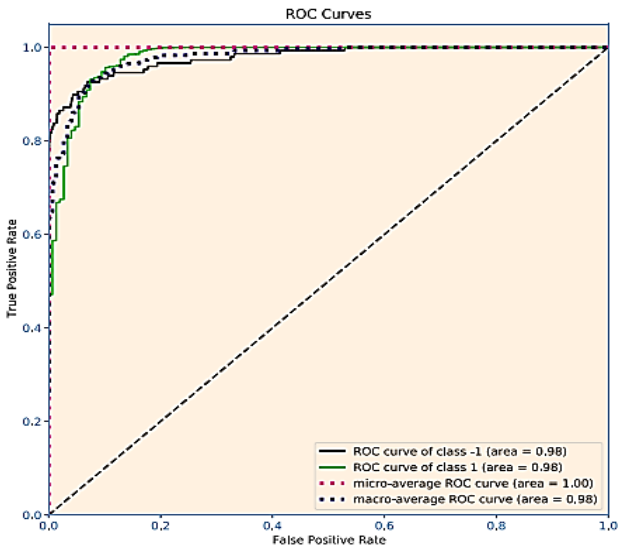

Figure 6 ROC Curve for Fraud Detection Using Machine Learning

Figure 6, illustrates the effectiveness of the model in differentiating between transactions that are fraudulent and those that are not. The impressive AUC of 0.98 for both class -1 and class 1 on the ROC curve indicates strong classification skills. The model's resilience and dependability in managing unbalanced fraud detection scenarios are demonstrated by the micro-average ROC curve's flawless AUC = 1.00 and the remarkable AUC of 0.98 for the macro-average ROC curve.

Comparative analysis and Discussion

A comparative analysis of several anomaly detection methods. The following Table IV compares and evaluates a number of machine learning models for ransomware detection prediction based on performance measures.

Table 4 Comparative Performance Analysis of Machine Learning Models for Enhanced Security

Model (%)	Accuracy	Precision	Recall	F1 Score
AdaBoost [34]	75	78	40	83
RF+AB[35]	94.14	94.61	93.72	94.00
Iforest	98.65	98.20	98.64	98.52

Table IV, presents a comparison of several ML models for predicting Android malware using anomaly detection. The models—AdaBoost, RF combined with AdaBoost (RF+AB), and Isolation Forest (Iforest)—are evaluated according to crucial metrics for performance, comprising Recall, Accuracy, Precision, and F1 Score. With a 98.65% accuracy rate, the highest among them, Iforest performs better than the others, demonstrating its exceptional capacity to detect ransomware abnormalities.

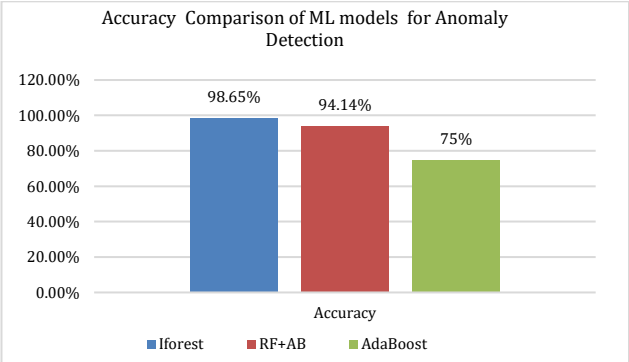

Figure 7 Accuracy Comparison of ML models for Anomaly Detection

Figure 7 compares the anomaly detection accuracy of four machine learning models (Iforest, RF+AB, and AdaBoost). With an accuracy of 98.65%, iforest earned the highest accuracy, followed by RF+AB, while AdaBoost had the lowest accuracy at 75%.

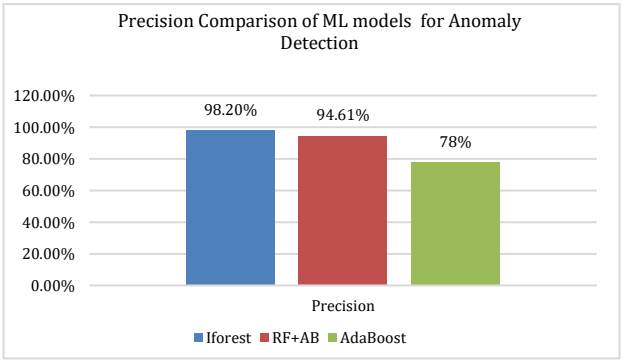

Figure 8 Precision Comparison of ML Models for Anomaly Detection

Figure 8 compares the accuracy of four ML models for anomaly detection (Iforest, RF+AB, and AdaBoost). With the highest precision of 98.20%, iforest was followed by RF+AB, while AdaBoost had the lowest accuracy of 78%.

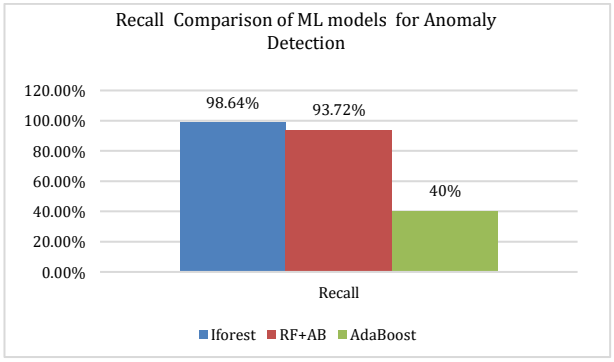

Figure 9 Recall Comparison of ML Models for Anomaly Detection

Figure 9 compares the accuracy of four ML models for anomaly detection (Iforest, RF+AB, and AdaBoost).

With Iforest was followed by RF+AB with an accuracy of 98.64%, and AdaBoost had the lowest accuracy of 40%.

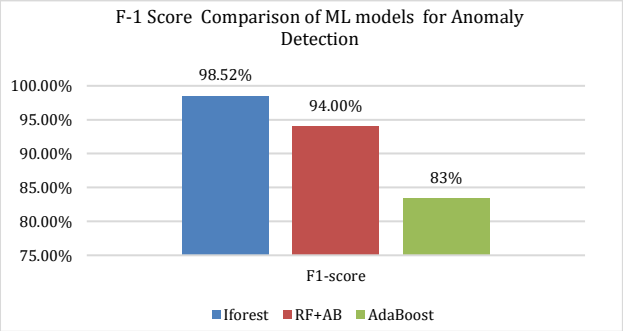

Figure 10 F-1 Score Comparison of ML Models for Anomaly Detection

An accuracy comparison of four ML models: Iforest, RF+AB and AdaBoost, in Figure 10 for the anomaly detection. Accuracy of AdaBoost was 83%, while that of RF+AB and iforest was 98.52%.

Conclusion And Future Work

The main contribution of this study is to demonstrate that the use of ML methods to increase bank security is essential by successfully identifying fraudulent transactions. It was decided to process the dataset on credit card fraud in a way that evolved a range of preprocessing methods to address class imbalance and improve model performance, such as data resampling and outlier reduction. Isolation Forest was one of the top models in terms of F1 score, recall, accuracy, and precision to identify irregularities in financial fraud. It is confirmed in the research that ML based anomaly detection methods can provide a significant contribution to reducing financial risk and improving transaction security in real-time systems.

That said, future research can be performed with more diverse and validation of the suggested models' generalizability using real-world transactional datasets based on a single financial institution's population. Investigating sophisticated ensemble methods and meta-learning strategies may help improve the precision and robustness of systems for detecting fraud. Including contextual information like device ID, geolocation, or Patterns of user behavior might enhance the system's ability to identify intricate fraud efforts. Additionally, federated learning and other privacy-preserving ML approaches may be used to enable cross-institutional collaborative model training while guaranteeing the security of sensitive client data. Lastly, to accommodate the ever-changing nature of fraudulent activity, ongoing observation and recurring model upgrades must be taken into account.

References

[1] M. Shah, P. Shah, and S. Patil, "Secure and Efficient Fraud Detection Using Federated Learning and Distributed Search Databases," in 2025 IEEE 4th International Conference on AI in Cybersecurity (ICAIC), IEEE, Feb. 2025, pp. 1–6. doi: 10.1109/ICAIC63015.2025.10849280.

[2] R. P. Mahajan, "Improvised Diabetic Retinopathy Detection Accuracy in Retinal Images Using Machine Learning Algorithms," TIJER – Int. Res. J., vol. 12, no. 03, pp. b155–b161, 2025.

[3] S. Tyagi, "Analyzing Machine Learning Models for Credit Scoring with Explainable AI and Optimizing Investment Decisions," vol. 5, no. 01, pp. 5–19, 2022, [Online]. Available: http://arxiv.org/abs/2209.09362

[4] V. Pillai, "System And Method For Intelligent Detection And Notification Of Anomalies In Financial And Insurance Data Using Machine Learning," 202421099024, 2025

[5] Suhag Pandya, "A Machine and Deep Learning Framework for Robust Health Insurance Fraud Detection and Prevention," Int. J. Adv. Res. Sci. Commun. Technol., pp. 1332–1342, Jul. 2023, doi: 10.48175/IJARSCT-14000U.

[6] E. Pan, "Machine Learning in Financial Transaction Fraud Detection and Prevention," Trans. Econ. Bus. Manag. Res., vol. 5, pp. 243–249, 2024, doi: 10.62051/16r3aa10.

[7] M. S. Akaash Vishal Hazarika, "Blockchain-based Distributed AI Models: Trust in AI model sharing," Int. J. Sci. Res. Arch., vol. 13, no. 2, pp. 3493–3498, 2024.

[8] V. Prajapati, "Blockchain-Based Decentralized Identity Systems : A Survey of Security , Privacy , and Interoperability," vol. 10, no. 3, 2025.

[9] V. Pillai, "Anomaly Detection for Innovators: Transforming Data into Breakthroughs," Lib. Media Priv. Ltd., 2022.

[10] K. Rajchandar, M. Ramesh, A. Tyagi, S. Prabhu, D. S. Babu, and A. Roniboss, "Edge Computing in Network-based Systems: Enhancing Latency-Sensitive Applications," in 2024 7th International Conference on Contemporary Computing and Informatics (IC3I), IEEE, Sep. 2024, pp. 462–467. doi: 10.1109/IC3I61595.2024.10828607.

[11] N. Malali, "Adversarial Robustness of AI-Driven Claims Management Systems," Int. J. Adv. Res. Sci. Commun. Technol., 2025.

[12] S. Chatterjee, "Risk Management in Advanced Persistent Threats (APTs) for Critical Infrastructure in the Utility Industry," 2021, doi: https://doi.org/10.36948/ijfmr.2021.v03i04.34396.

[13] A. V. Hazarika, M. Shah, S. Patil, and N. Carolina, "Risk Management for Distributed Arbitrage Systems : Integrating Artificial Intelligence," no. 2025.

[14] V. S. Thokala, "Improving Data Security and Privacy in Web Applications: A Study of Serverless Architecture," TIJER – Int. Res. J., vol. 11, no. 12, 2024, [Online]. Available: https://tijer.org/tijer/papers/TIJER2412011.pdf

[15] V. Pillai, "Anomaly Detection Device for Financial and Insurance Data," 2025.

[16] A. & A. Vishal Hazarika, "Extreme Gradient Boosting using Squared Logistics Loss function," Int. J. Sci. Dev. Res., vol. 2, no. 8, pp. 54–61, 2017, [Online]. Available: www.ijsdr.org

[17] M. Gopalsamy and K. B. Dastageer, "The Role of Ethical Hacking and AI in Proactive Cyber Defense : Current Approaches and Future Perspectives," vol. 10, no. 2, 2025.

[18] N. Malali, "AI Ethics in Financial Services : A Global Perspective," vol. 10, no. 2, 2025.

[19] M. Das Nath and T. Bhattasali, "Anomaly detection using machine learning approaches," Azerbaijan J. High Perform. Comput., vol. 3, pp. 196–206, 2020, doi: 10.32010/26166127.2020.3.2.196.206.

[20] S. Arora, S. R. Thota, and S. Gupta, "Data Mining and Processing in the Age of Big Data and Artificial Intelligence -

Issues, Privacy, and Ethical Considerations," in 2024 4th Asian Conference on Innovation in Technology (ASIANCON), IEEE, Aug. 2024, pp. 1–6. doi: 10.1109/ASIANCON62057.2024.10838087.

[21] H. S. Chandu, "A Review of IoT-Based Home Security Solutions: Focusing on Arduino Applications," TIJER – Int. Res. J., vol. 11, no. 10, pp. a391–a396, 2024, [Online]. Available: https://tijer.org/tijer/papers/TIJER2410044.pdf

[22] J. Joseph, O. Irekponor, N. Aleke, and L. Yeboah, "Machine learning techniques for enhancing security in financial technology systems," Int. J. Sci. Res. Arch., vol. 13, pp. 2805–2822, 2024, doi: 10.30574/ijsra.2024.13.1.1965.

[23] S. Rani and A. Mittal, "Securing Digital Payments a Comprehensive Analysis of AI Driven Fraud Detection with Real Time Transaction Monitoring and Anomaly Detection," in Proceedings of International Conference on Contemporary Computing and Informatics, IC3I 2023, 2023. doi: 10.1109/IC3I59117.2023.10397958.

[24] O. Vynokurova, D. Peleshko, O. Bondarenko, V. Ilyasov, V. Serzhantov, and M. Peleshko, "Hybrid machine learning system for solving fraud detection tasks," in Proceedings of the 2020 IEEE 3rd International Conference on Data Stream Mining and Processing, DSMP 2020, 2020. doi: 10.1109/DSMP47368.2020.9204244.

[25] N. Boutaher, A. Elomri, N. Abghour, K. Moussaid, and M. Rida, "A Review of Credit Card Fraud Detection Using Machine Learning Techniques," in Proceedings of 2020 5th International Conference on Cloud Computing and Artificial Intelligence: Technologies and Applications, CloudTech 2020, 2020. doi: 10.1109/CloudTech49835.2020.9365916.

[26] S. Kumar, S. Dua, and S. Rastogi, "Anomaly Detection: A Machine Learning and Deep Learning Perspective," in 2023 International Conference on Computer, Electronics and Electrical Engineering and their Applications, IC2E3 2023, 2023. doi: 10.1109/IC2E357697.2023.10262460.

[27] M. Thilagavathi, R. Saranyadevi, N. Vijayakumar, K. Selvi, L. Anitha, and K. Sudharson, "AI-Driven Fraud Detection in Financial Transactions with Graph Neural Networks and Anomaly Detection," Proc. 2024 Int. Conf. Sci. Technol. Eng. Manag. ICSTEM 2024, pp. 2024–2025, 2024, doi: 10.1109/ICSTEM61137.2024.10560838.

[28] R. Sharma and A. Sharma, "Combatting Digital Financial Fraud through Strategic Deep Learning Approaches," in 2024 2nd International Conference on Sustainable Computing and Smart Systems (ICSCSS), 2024, pp. 824–828. doi: 10.1109/ICSCSS60660.2024.10625249.

[29] S. Li, K. Zhang, P. Duan, and X. Kang, "Hyperspectral Anomaly Detection with Kernel Isolation Forest," IEEE Trans. Geosci. Remote Sens., 2020, doi: 10.1109/TGRS.2019.2936308.

[30] Á. Horváth, E. Ferentzi, K. Schwartz, N. Jacobs, P. Meyns, and F. Köteles, "The measurement of proprioceptive accuracy: A systematic literature review," 2023. doi: 10.1016/j.jshs.2022.04.001.

[31] A. Letai, P. Bhola, and A. L. Welm, "Functional precision oncology: Testing tumors with drugs to identify vulnerabilities and novel combinations," 2022. doi: 10.1016/j.ccell.2021.12.004.

[32] P. Wollburg, M. Tiberti, and A. Zezza, "Recall length and measurement error in agricultural surveys," Food Policy, 2021, doi: 10.1016/j.foodpol.2020.102003.

[33] K. Takahashi, K. Yamamoto, A. Kuchiba, and T. Koyama, "Confidence interval for micro-averaged F 1 and macro-averaged F 1 scores," Appl. Intell., 2022, doi: 10.1007/s10489-021-02635-5.

[34] I. Aruleba and Y. Sun, "Effective Credit Risk Prediction Using Ensemble Classifiers With Model Explanation," IEEE Access, vol. 12, no. August, pp. 115015–115025, 2024, doi: 10.1109/ACCESS.2024.3445308.

[35] X. Feng and S. K. Kim, "Novel Machine Learning Based Credit Card Fraud Detection Systems," Mathematics, vol. 12, no. 12, 2024, doi: 10.3390/math12121869.