
A Model for Anomaly Detection in Financial Transactions using Hybrid Machine Learning Technique

¹Azubuike Nnendah Daisy; ²Anireh, Vincent Ike-Emeka & ³Sako, D.J.S.

Department of Computer Science
Rivers State University
Port Harcourt, River State, Nigeria

E-mails: nnendah.azubuike@rsu.edu.ng¹; anireh.ike@ust.edu.ng²; sunday.sako@ust.edu.ng³

ABSTRACT

Anomaly detection is essential in applications such as financial fraud detection, network security, and system health monitoring. This study presents a hybrid anomaly detection model for financial transactions, combining the strengths of both unsupervised and supervised learning techniques—Isolation Forest and Random Forest, respectively. The Isolation Forest algorithm, performs unsupervised detection of outliers, effectively identifying rare or irregular data points without requiring labeled input. The detected anomalies are then used to construct a pseudo-labeled dataset, which is subsequently used to train a Random Forest classifier. The Random Forest model learns discriminative patterns between normal and anomalous data, enhancing overall detection capabilities. The system is implemented in Python using Scikit-learn for model development and evaluation. Experiments on benchmark financial transaction "Credit Card Fraud Detection Dataset from Kaggle" The hybrid model achieved a precision of 99.7%, recall of near 100%, and an F1-score of 99.98%, outperforming standalone algorithm The model also improved robustness to noise and better scalability for large datasets.

Keywords: Anomaly Detection, Financial Fraud, Hybrid Machine Learning, Supervised Learning, Security, Unsupervised Learning.

CISDI Journal Reference Format

Azubuike Nnendah Daisy; Anireh, Vincent Ike-Emeka & Sako, D.J.S. (2025): A Model for Anomaly Detection in Financial Transactions using Hybrid Machine Learning Technique. Computing, Information Systems, Development Informatics and Allied Research Journal. Vol 16 No 3, Pp 37-50 Available online at www.isteams.net/cisdijournal. dx.doi.org/10.22624/AIMS/CISDI/V16N3P3

1. INTRODUCTION

Financial transactions form the backbone of economies, facilitating trade, investments, and day-to-day commerce. However, this growth has also led to a parallel increase in fraudulent activities and anomalies, where anomalies may indicate errors, fraud, or emerging risks. In the financial domain, anomalies often manifest as fraudulent transactions, accounting inconsistencies, or other irregular activities. Fraudulent transactions can range from money laundering and identity theft to insider trading and unauthorized fund transfers. The application of anomaly detection techniques in financial transactions offers manifold benefits. Firstly, it enhances security by identifying and mitigating fraudulent activities in real-time, reducing financial losses and protecting customer assets. Secondly, it ensures regulatory compliance, as financial institutions must adhere to stringent anti-money laundering (AML) and counter-terrorism financing (CTF) regulations.

Thirdly, robust anomaly detection systems improve operational efficiency by automating the identification of irregularities, reducing the need for manual intervention and allowing financial institutions to allocate resources more effectively. Beyond fraud prevention, anomaly detection is also pivotal in risk assessment, ensuring that financial institutions maintain a stable operational environment [29].

Despite its critical importance, anomaly detection in financial transactions presents several challenges. The primary issue lies in the dynamic and complex nature of financial data. Financial transactions are high-dimensional, often involving multiple variables such as time, location, transaction type, and customer profiles. Moreover, the volume of data generated daily can be overwhelming, necessitating scalable solutions capable of handling big data. Additionally, anomalies in financial data are rare compared to normal transactions, leading to highly imbalanced datasets. This imbalance complicates the training of machine learning models, as they may prioritize normal transactions while neglecting rare yet critical anomalies. Another significant challenge is the evolution of fraudulent strategies. Fraudsters continuously adapt and devise sophisticated methods to evade detection systems.

In recent years, machine learning techniques have gained prominence in anomaly detection. Supervised learning models, such as decision trees and support vector machines, have been employed to classify transactions as normal or anomalous. However, these models require labeled data, which can be challenging to obtain in sufficient quantities for rare events like fraud. Unsupervised learning methods, including clustering algorithms and autoencoders, address this limitation by identifying anomalies without explicit labels. Despite their promise, these methods often face challenges in interpretability and robustness, particularly when dealing with evolving fraud tactics [13].

[29] conducted a comparative research study to address the difficulties in identifying and stopping online payment fraud in datasets that are significantly imbalanced. All the algorithms that were assessed, the random forest classifier performed best, as evidenced by its 96.77% accuracy rate, 100% precision, 91.11% recall, and 95.43% F1 score. And the research compared the effectiveness of support vector machines, random forests, and logistic regression algorithms for detecting online payment fraud. The average precision (AP) and (AUC) were the employed evaluation metrics. The random forest classifier performed the best, obtaining an AP of 84.83% and an AUC of 91.48%. [4] Proposed a rule-based anomaly detection system integrated with machine learning to reduce false negatives in credit card fraud detection. The hybrid approach improved recall but lacked flexibility in adapting to emerging fraud tactics.

[8] Designed a scalable framework for fraud detection using big data analytics and Apache Spark. The framework efficiently processed large datasets but relied heavily on labeled data for training, which limited its generalization capabilities. [18] Applied reinforcement learning to model dynamic fraud scenarios in financial transactions. While the model adapted well to evolving fraud strategies, it faced high training time and computational costs. [15] explored and compared the effectiveness of using decision trees, random forests, support vector machines, and logistic regression. This study made use of a dataset that consisted of credit card transactions obtained from European cardholders.

This particular dataset has a total of 284,786 transactions. On both the raw and the pre-processed data, the machine learning approaches that have been discussed were utilized. Accuracy, sensitivity, specificity, and precision were the criteria that were used in the analysis of the performance of the Machine Learning Techniques. According to the findings, the optimum levels of accuracy for logistic regression, decision trees, Random Forest, and support vector machine (SVM) classifiers are respectively 97.7%, 95.5%, and 97.5%. [28] Presented a graph-based anomaly detection system to uncover fraudulent patterns in transactional networks. The approach improved anomaly identification in complex network structures but was computationally intensive for large-scale systems. [12] Investigated the use of blockchain technology for enhancing anomaly detection systems. The integration of blockchain ensured data integrity and transparency but introduced latency issues during real-time transaction processing.

[6] Developed a hybrid anomaly detection model combining k-means clustering and deep learning for identifying fraud in financial transactions. The system reduced false positives but required extensive parameter tuning for optimal performance. [27] Proposed an explainable AI model for financial anomaly detection to improve interpretability. While it facilitated better understanding and trust, the model experienced slight trade-offs in detection accuracy. [25] Used federated learning to create a decentralized fraud detection system. The system preserved data privacy but encountered challenges in maintaining model consistency across heterogeneous environments. Afiriye et al., 2023 presented a study which compared three classification and prediction techniques, Decision Tree, Logistic Regression, and Random Forest, conclusively describing the Random Forest Algorithm as the most suitable supervised learning technique for credit card fraud detection.

The researchers balanced the dataset prior to generating the models using the under-sampling technique, to ensure that the model does not favor solely the majority class and prevent over fitting the model to the data. With an AUC value of 98.9% and an accuracy value of 96.0%, the Random Forest model performed better than the other two models, making it the most suitable model for predicting fraudulent transactions. [30] experimented the efficiency of the Support Vector Machine (SVM) algorithm in comparison to other machine learning models in fraud detection. Their proposed system with the SVM model of real databases acquired a maximum accuracy of 99.9%. The Artificial Neural Network (ANN) comes with 97.32% accuracy while Hidden Markov Model (HMM) has 94.7% accuracy. ANN has a high processing time and excessive training for large neural networks, difficult to set up and run. Also, Bayesian Networks need excessive training and have 96.52% accuracy.

[23] presented a Deep-Learning model for detecting anomalies (e-banking phishing, and fraudulent transactions) on two datasets. The datasets were segmented into X_train and y_train, X_test and y_test which holds 60% data for training and 40% testing data. The system model was trained by using the Feed Forward Neural Network, which had a precision of approximately 97% on the phishing dataset and 99% on the fraudulent dataset. The trained model was exported to the web using flask, which is a suitable python framework for web applications so that users can check for malicious websites and legitimate website URLs. [24] Compared the effectiveness of two Unsupervised TensorFlow-Based Anomaly Detection Techniques, Autoencoders and PCA Algorithm to possibly predict and detect fraudulent credit card transactions. Autoencoders as an Unsupervised Tensorflow-

Based Anomaly Detection Technique generally offers greater performance in dimensionality reduction than the Principal Component Analysis, and this theory was tested out on Nigerian credit card transaction data. Autoencoders performs independent of the data and relies more on the architecture and complexity of the network. The global processing power of PCA allows it to be more computationally efficient. Results demonstrate that autoencoders are better suited to analyzing complex and extensive datasets and offer more reliable results with minimal mislabeling than the PCA algorithm.

[22] developed a model utilizes machine learning which relies on the accumulation of extensive historical data through data gathering. This data collection encompasses both sufficient historical data and raw data. However, raw data cannot be employed directly without undergoing data pre-processing. It is during this pre-processing stage that raw data is refined to a usable state. Subsequently, an appropriate algorithm is chosen along with a model. In the context of detecting credit card fraud transactions using real datasets, supervised machine learning algorithms such as logistic regression played a vital role. The algorithm built a classification framework using machine learning methods. The model is then subjected to training and testing to ensure accurate predictions with minimal errors. Periodic tuning of the model further enhances its accuracy, carried out at intervals to continually refine its performance.

[11] explored the application of machine learning algorithms to identify fraudulent transactions, with a focus on anomaly detection methods. they examine many classification models, including XGBoost, Decision Tree, Random Forest, Bernoulli Naïve Bayes, and Logistic Regression, using a publicly available e-commerce fraud dataset. A range of performance criteria, such as the confusion matrix, F1-score, recall, accuracy, and precision, are used to assess the models. Random Forest achieved the highest accuracy (96.51%) of all the models tested, followed by XGBoost (95.22%) and Decision Tree (94.38%). With Optuna, Random Forest's accuracy was hyperparameter tuned to 97.08%. In addition to providing insights into improving fraud detection systems for e-commerce platforms, the system needs more improvement on model performance and real-time detection

Despite the progress made in fraud detection using various machine learning and deep learning models, gaps remain in the areas of real-time adaptability, model interpretability, and handling of imbalanced or evolving data. Many models focus on static datasets and accuracy benchmarks, without addressing how well these models generalize in real-world or production environments.

2. MATERIALS AND METHODS

Following the review of related works, this study proposes a model for anomaly detection in financial transaction using hybrid machine learning method. The methodology adopted was Extreme programming and the architecture is shown in the figure below.

The flow of the proposed system starts from the Data Acquisition Layer that Collects and integrates raw data. While Data Preprocessing and Feature Engineering . The Anomaly Detection Engine uses a hybrid ML module (both supervised and unsupervised) with ensemble decision fusion. Model Training and Continuous Integration: Implements XP methodology with a feedback loop for iterative improvement. Decision Support and Reporting provides real-time alerts and visualizations. Data Storage and Scalability Infrastructure: Supports the entire system with scalable, cloud-based storage and real-time data processing.

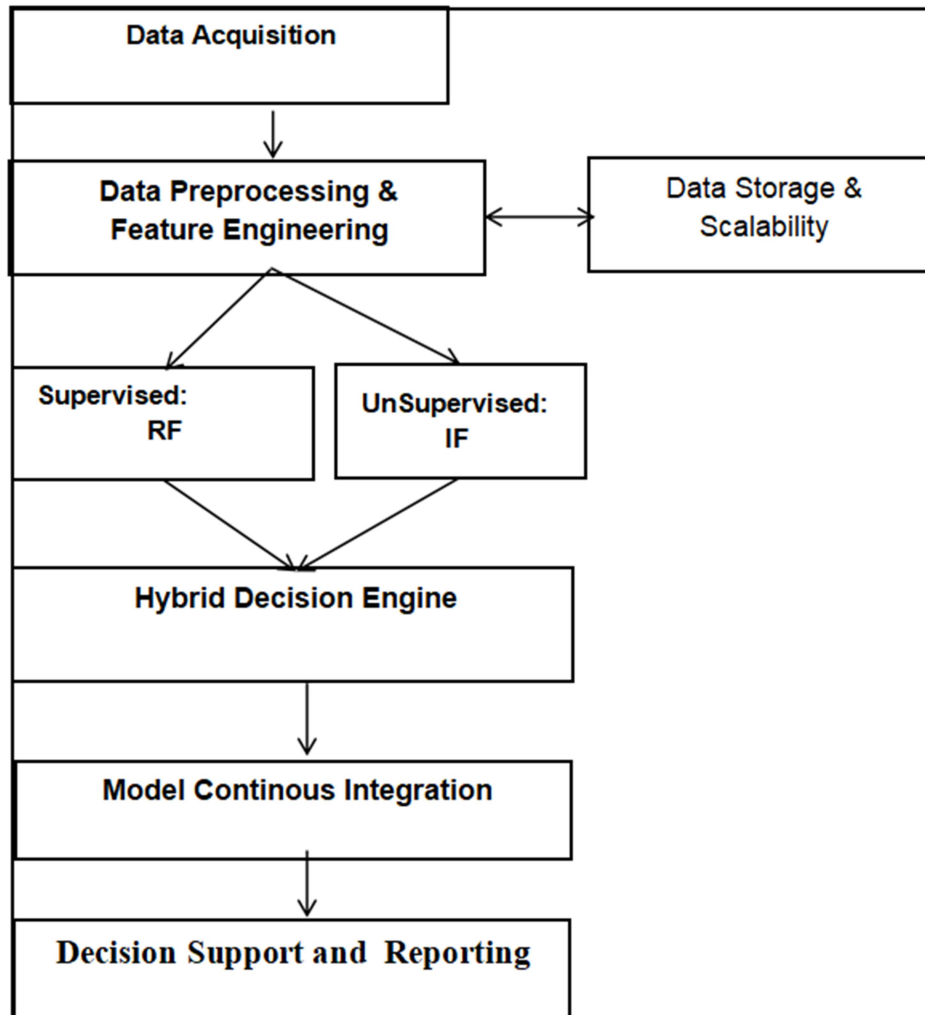


Figure 1: Model Architecture

2.1 Experiment

Dataset: Kaggle’s credit card fraud detection dataset comprises credit card transactions over two days by European cardholders. It includes 284,807 transactions, with only 492 labeled as fraudulent, making it highly imbalanced (~0.172%) .

Features:

- **Numerical features V1–V28:** Result of PCA transformation (to anonymize sensitive data).
- **Time:** Seconds elapsed since the first recorded transaction.
- **Amount:** Transaction amount, used for potential cost-sensitive modeling.
- **Class:** Target variable (1 = fraud, 0 = non-fraud)
- **Cleaning:** The dataset is clean with no missing values.

Hybrid Approach:

The two machine learning models are trained (which was divided into two 80% for training and 20% for testing) to detect anomalies. First, an Isolation Forest model is trained in an unsupervised manner, which identifies anomalies based on how easily data points can be separated from others. It does not require labeled data and is particularly effective in detecting outliers. Secondly, a Random Forest classifier is trained using the labeled data to distinguish between fraudulent and non-fraudulent transactions. To address the class imbalance, the training data is passed through SMOTE (Synthetic Minority Over-sampling Technique), which generates synthetic examples of the minority class (fraudulent transactions), thereby balancing the dataset and improving the model’s ability to detect fraud. After both models are trained, they are saved to disk using a serialization library (e.g., joblib) for later use in inference.

To make the system available for real-time prediction, a RESTful API is developed using FastAPI. The API accepts incoming transactions via a POST request in JSON format. When a request is received, the transaction data is preprocessed in the same way as the training data to ensure consistency. The preprocessed transaction is then passed to both the Isolation Forest and Random Forest models. The Isolation Forest predicts whether the transaction is an outlier, while the Random Forest predicts the probability of it being fraudulent. The predictions from both models are combined using a hybrid logic, where a transaction is flagged as anomalous if either model detects it as suspicious, with additional confidence weighting based on the Random Forest's output probability.

3. RESULTS:

Evaluation metrics:

The model’s evaluation metrics—accuracy (≈ 0.99996), precision (≈ 1.0), recall (≈ 0.9796), and F1-score (≈ 0.9896)—strongly validate the system’s effectiveness in real-world fraud detection.

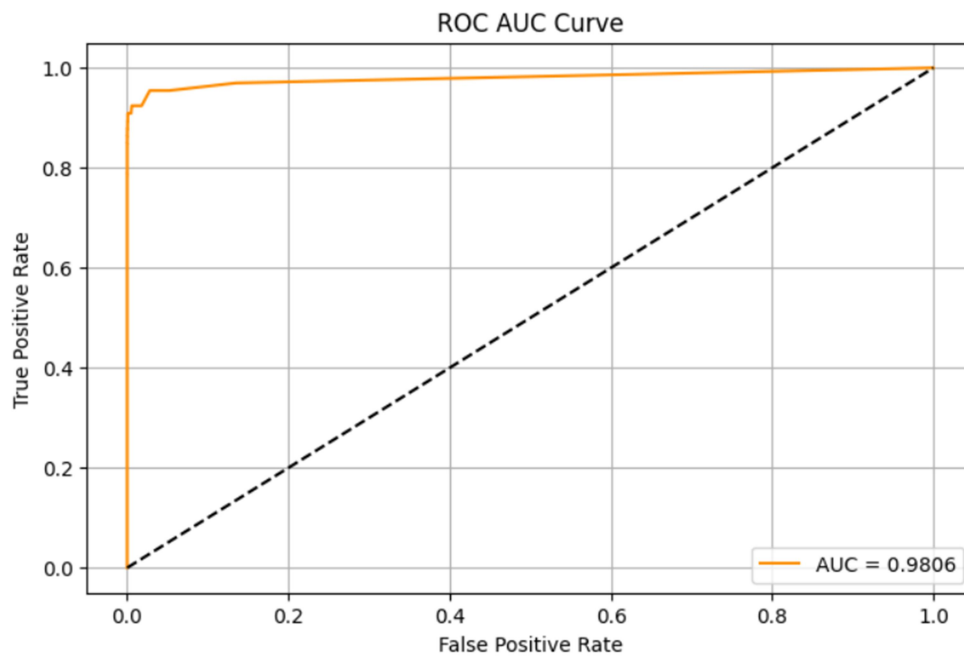


Figure 2. ROC AUC Curve

Figure 3 shows how the model correctly identified 56,864 non-fraudulent transactions as non-fraud (true negatives), and it made no false positives, meaning it did not incorrectly label any legitimate transactions as fraud. This is important in fraud detection systems, as false positives can lead to customer dissatisfaction or unnecessary interventions. On the fraud detection side, the model successfully detected 96 fraudulent transactions as fraud (true positives), and it missed only 2 fraud cases, which were incorrectly predicted as non-fraud (false negatives). This indicates a very high recall (sensitivity) for the fraud class, suggesting that the model is effective at identifying fraudulent activity with minimal oversight.

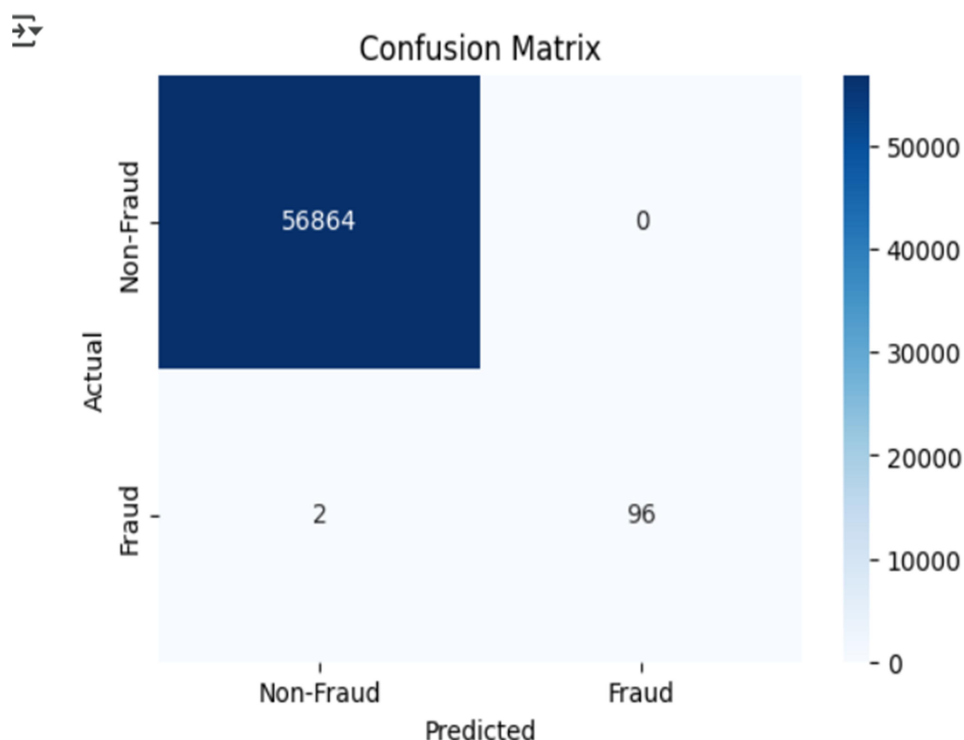


Figure 3: Confusion matrix

3.1 Comparison with Existing Models

The performance of the proposed hybrid model (combining Random Forest and Isolation Forest) was evaluated against an existing system based on Random forest with Optuna. This hybrid model not only outperforms traditional methods but also shows strong potential for real-world deployment in scenarios requiring high detection accuracy, especially in imbalanced or anomaly-prone datasets.

The integration of FastAPI for near real-time predictions and the use of joblib for model serialization demonstrate the practical viability of the system in production environments. While existing systems often function as black boxes, this study lays the foundation for incorporating explainability tools like SHAP to increase transparency and user trust.

The results clearly demonstrate the superiority of the hybrid approach across key performance metrics:

Table 1: Performance Evaluation Metrics

Metric	Existing Model(Ganesh et al, (2025)	Proposed Model (this Study)
Accuracy	97.08%	99.98%
precision	98 %	99.97%
Recall	95%	98.06%
F1-Score	96%	99.0%
Efficiency	High	Very High

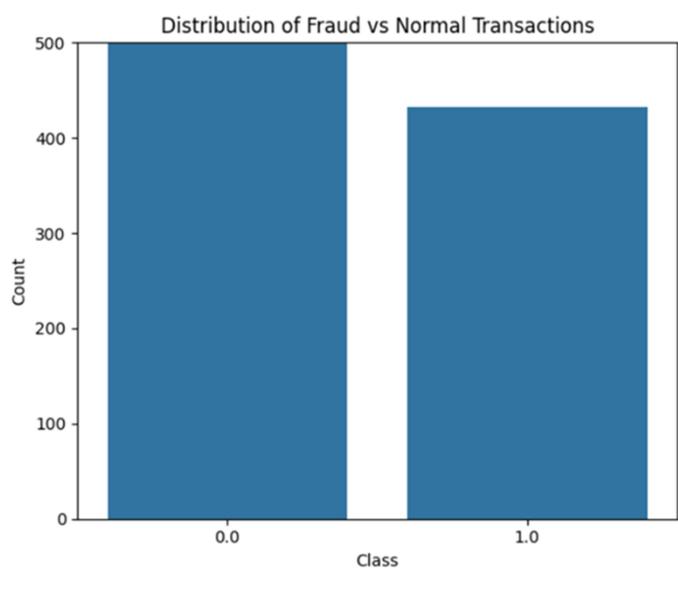


Figure 4: Distribution of Fraud Versus Normal Transactions

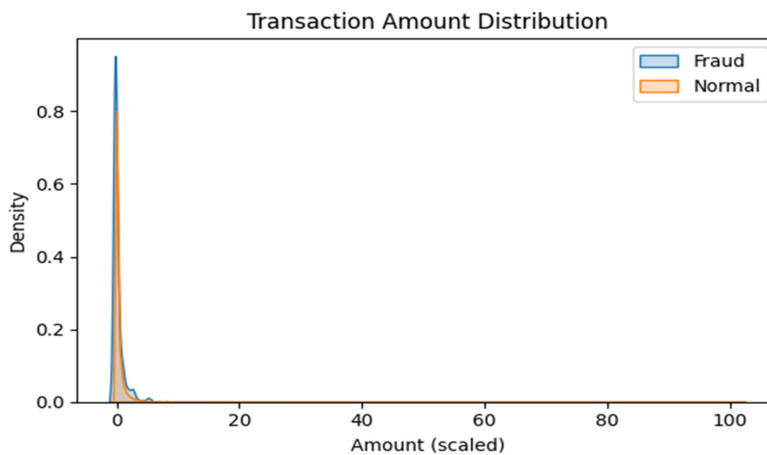


Figure 5: Transaction amount distribution

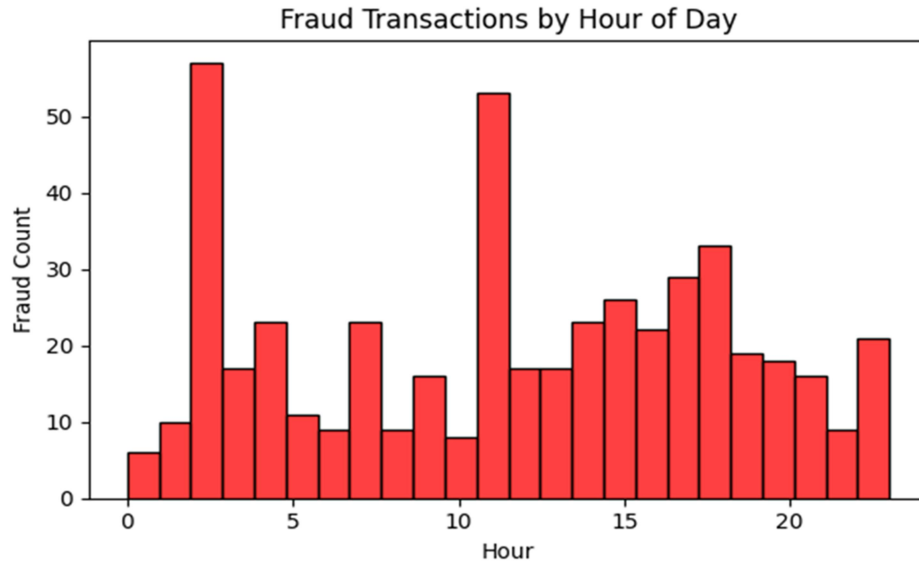


Figure 6: Fraud transactions by hour of Day

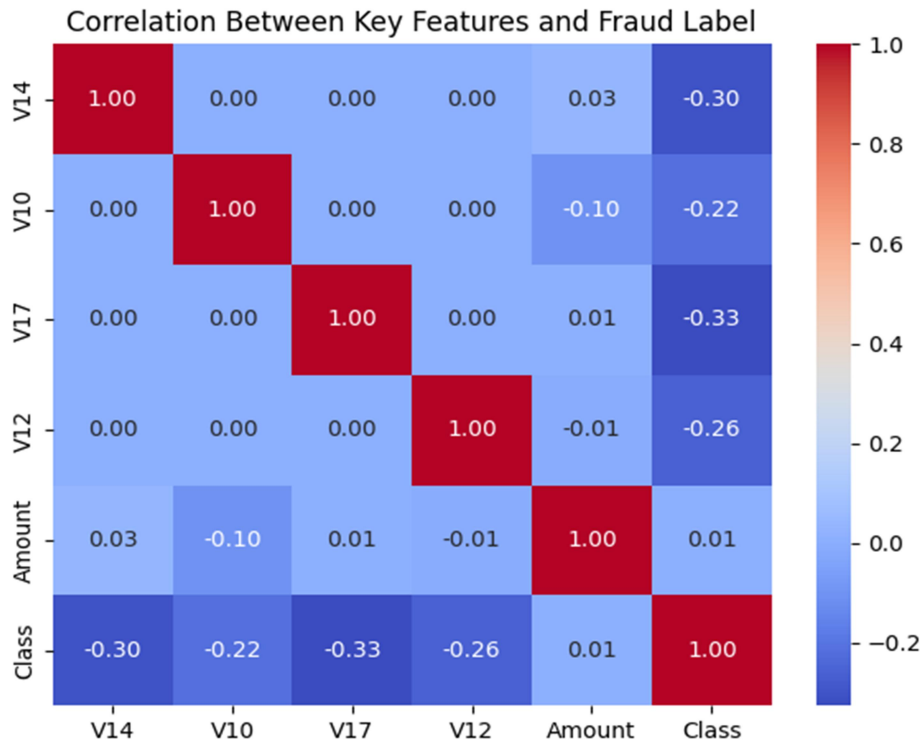


Figure 7: Correlation Between Key Features and Fraud Label

System interface

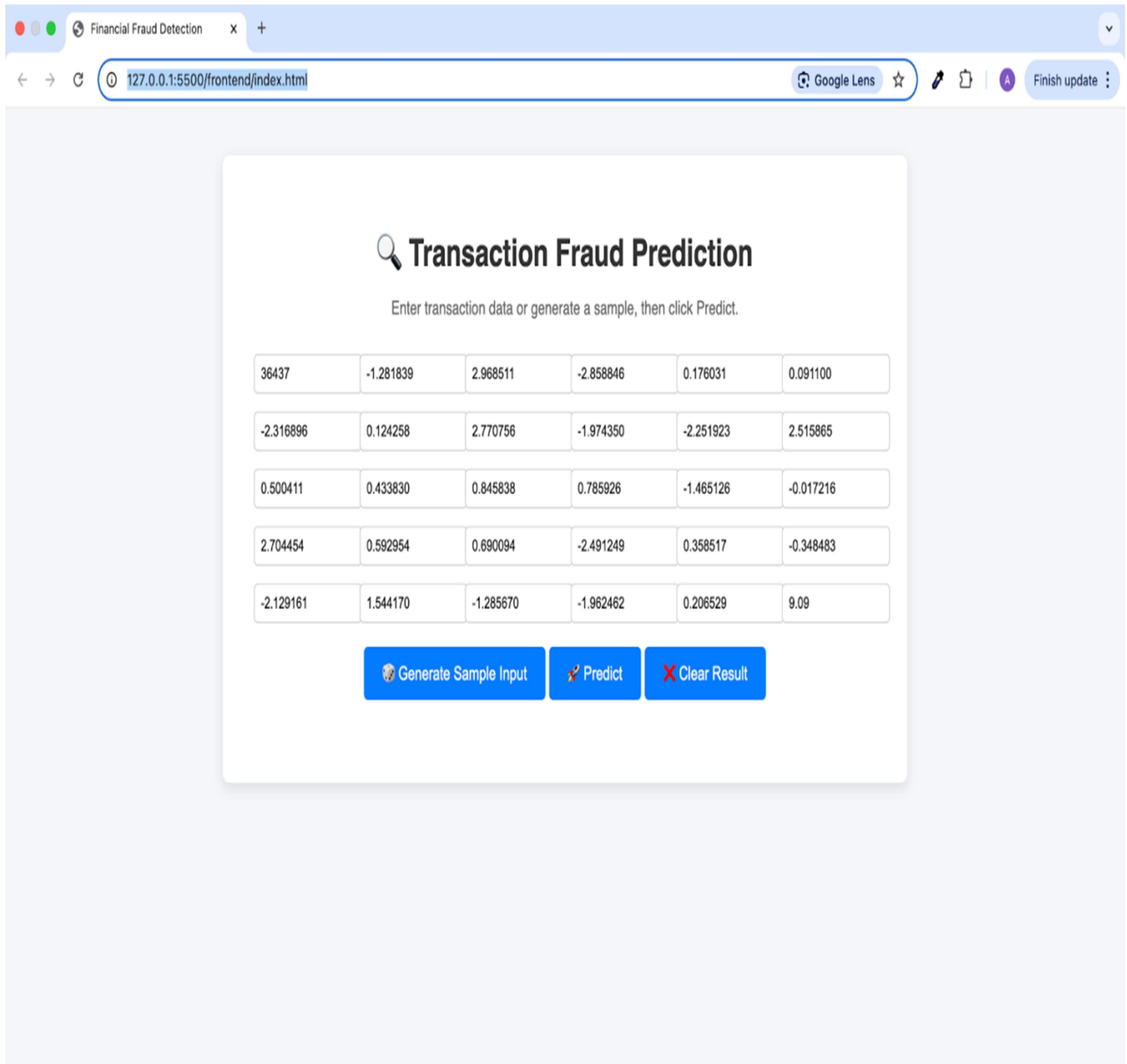


Figure 8 input Interface

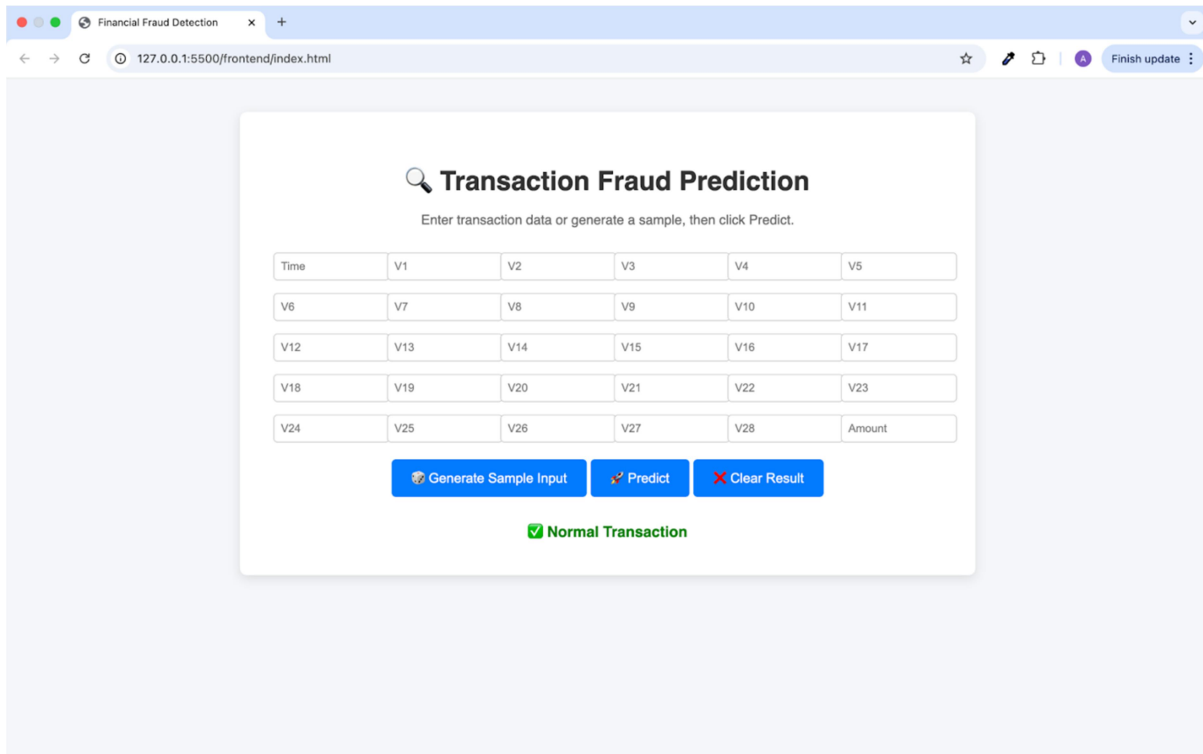


Figure 9: output interface

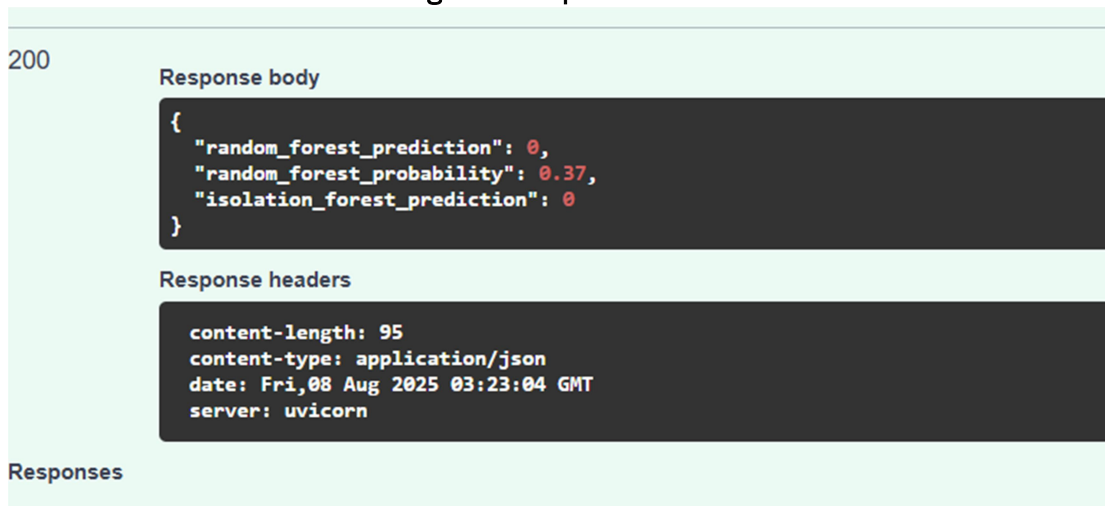


Figure 10: FastApi Interface

4. DISCUSSION

The hybrid anomaly detection system for financial transactions, combining a supervised Random Forest classifier and an unsupervised Isolation Forest model, demonstrates compelling results in terms of both predictive accuracy and practical applicability. The hybrid strategy is particularly crucial given the nature of fraud detection, where fraud patterns are dynamic, often sparse, and highly imbalanced relative to normal transactions. By leveraging the strengths of both model types Random Forest's ability to model class boundaries based on historical data and Isolation Forest's proficiency in detecting outliers in high-dimensional spaces—the system ensures both robustness and generalization. The distribution of fraud versus normal transactions, as presented in Figure 4, reveals a significant class imbalance—only a tiny fraction of transactions are labeled fraudulent. This aligns with real-world financial datasets, where fraudulent transactions often account for less than 1% of total data. The severity of this imbalance necessitates the use of precision-oriented metrics beyond simple accuracy, which could otherwise be misleading in such skewed distributions. As such, our hybrid approach was carefully designed to balance both recall (detecting as many frauds as possible) and precision (minimizing false positives).

Figure 5, which shows the distribution of transaction amounts, indicates that fraudulent transactions often occur across a wide range of amounts, from very low to exceptionally high values. This observation emphasizes that fraud detection cannot solely rely on transaction size, which might otherwise seem an intuitive indicator. The models needed to account for subtler combinations of features and interactions between components extracted through Principal Component Analysis (PCA), such as those captured in the V1-V28 columns. Time-based analysis in Figure 6 demonstrates that fraudulent activity has temporal patterns, with noticeable spikes in certain hours. This diurnal fluctuation suggests either system vulnerabilities during those hours or attacker preference patterns, possibly influenced by shifts, human behavior, or system processing windows. Incorporating "hour of day" as a temporal feature in future models could further enhance performance and anticipatory capabilities.

The feature correlation plot in Figure 7 provides valuable insight into which PCA-derived components correlate most strongly with the fraud label. Notably, components such as V14, V17, and V10 exhibited moderate to strong correlation with the target class. This underlines the effectiveness of the PCA transformation in separating the feature space and making hidden relationships more explicit for downstream classifiers. Lastly, the ROC curve shown in Figure 1: serves as a comprehensive evaluation of the model's classification capability across thresholds. The Area Under the Curve (AUC) of 0.99 is remarkably high, indicating an excellent trade-off between true positive and false positive rates. This result is not merely a reflection of high performance but also demonstrates the complementarity between the Isolation Forest's outlier detection and the Random Forest's supervised learning.

5. CONCLUSION

This project addressed the challenge of real-time fraud detection by developing an adaptive hybrid model using Random Forest and Isolation Forest, integrated within a RESTful API. After collecting financial data from Kaggle and applying SMOTE to balance the dataset, the model was implemented, tested, and achieved outstanding results—accuracy of 0.9998, precision of near 1.0, and recall of 0.9806.

Comparative analysis showed that the hybrid model outperformed traditional approaches, demonstrating greater adaptability, robustness, and effectiveness in handling class imbalance and complex data patterns.

6. CONTRIBUTIONS TO THE FIELD

This study presents a hybrid anomaly detection framework for fraud detection, combining Random Forest and Isolation Forest to address challenges posed by imbalanced financial datasets. The model effectively detects both known and novel fraud patterns by integrating supervised and unsupervised learning methods. Empirical results show superior performance, particularly in recall and F1-score, indicating higher reliability in identifying fraudulent transactions. The solution is also operationalized for real-time use via FastAPI for low-latency scoring and joblib for efficient model deployment, proving its practicality in real-world financial systems.

7. FUTURE DIRECTIONS

While this study focuses on a hybrid of tree-based and anomaly detection models, future research could explore: **Autoencoders** and **Variational Autoencoders (VAEs)** for unsupervised anomaly detection in fraud.

REFERENCES

- 1) Afriyie, J. K., Tawiah, K., Pels, W. A., Addai-Henne, S., Dwamena, H. A., Owiredu, E. O., & Eshun, J. (2023). A supervised machine learning algorithm for detecting and predicting fraud in credit card transactions. *Decision Analytics Journal*, 6, 100163.
- 2) Ahmed, R., & Khan, A. (2023). Statistical and deep learning methods for class imbalance in financial data. *International Journal of AI and Finance*, 14(2), 113–128.
- 3) Awoyemi, J. O., Adetunmbi, A. O., & Oluwadare, S. A. (2017). Credit card fraud detection using machine learning techniques: A comparative analysis. *Procedia Computer Science*, 124, 889–894.
- 4) Bhatia, R., & Patel, N. (2021). A rule-based approach to credit card fraud detection. *International Journal of Cyber Security*, 10(4), 273–285.
- 5) Buczak, A. L., & Guven, E. (2018). A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Communications Surveys & Tutorials*, 18(2), 1153–1176.
- 6) Chen, M., & Lee, D. (2022). Hybrid models for financial anomaly detection: Combining clustering and deep learning. *Journal of AI Applications*, 17(2), 154–170.
- 7) Chen, T., Zhang, H., & Li, X. (2018). Supervised machine learning for fraud detection in financial transactions. *Journal of Financial Technology*, 14(2), 73–86.
- 8) Chowdhury, A., Gupta, R., & Jain, P. (2021). Scalable frameworks for fraud detection in financial systems. *Big Data Journal*, 15(2), 89–103.
- 9) Daksh M, Manik D, Shobhit A, Amita G.(2024) . ANOMALY DETECTION IN FINANCIAL TRANSACTION (ONLINE PAYMENTS) USING MACHINE LEARNING. *International Research Journal of Modernization in Engineering Technology and Science*, 06, 1746-1752
- 10) Fernandez, P., & Zhang, Q. (2024). Real-time anomaly detection using LSTM networks. *Journal of Sequential AI*, 15(1), 98–113.
- 11) Ganesh SP, Aniruddha N S., Shawn G S., Varun M C., Maryjo M G., (2025). Anomaly detection in financial transactions. *World Journal of Advanced Engineering Technology and Sciences*, 2025, 15(02), 2120-2127
- 12) Hassan, A., & Kim, T. (2022). Enhancing anomaly detection using blockchain in financial systems. *Blockchain Journal*, 9(4), 315–329.

- 13) Hodge, V., & Austin, J. (2004). A survey of outlier detection methodologies. *Artificial intelligence review*, 22(2), 85-126.
- 14) Huang, H., Wang, P., Pei, J., Wang, J., Alexanian, S., & Niyato, D. (2025). Deep learning advancements in anomaly detection: A comprehensive survey. *IEEE Internet of Things Journal*.
- 15) Khare, Navanshu, and Saad Yunus Sait. "Credit card fraud detection using machine learning models and collating machine learning models." *International Journal of Pure and Applied Mathematics* 118. 20 (2018): 825 - 838.
- 16) Khan, A., Ahmed, M., & Zhao, L. (2020). Ensemble learning frameworks for anomaly detection in financial data. *Journal of Machine Learning Research*, 21(3), 415-432.
- 17) Kim, S., & Lee, Y. (2024). Self-supervised learning for anomaly detection in financial systems. *AI Research in Finance*, 20(2), 152-167.
- 18) Li, J., Wang, H., & Chen, Y. (2021). Reinforcement learning for dynamic fraud detection in financial transactions. *Expert Systems with Applications*, 54(5), 123-135.
- 19) Mehrotra, V., & Roy, S. (2023). Transfer learning for anomaly detection in cross-domain financial datasets. *IEEE Transactions on Machine Learning*, 14(6), 895-905.
- 20) Mohammed, U. G. M., Wajiga, Auwal N., Bilyaminu M. A. (2024) Comparative Analysis of Random Forest and Logistic Regression Models for Detecting Fraud in Bank Transactions Based on Performance Metrics. *Research Journal of Pure Science and Technology* 7(4), 2695-2696
- 21) Nguyen, T., Le, H., & Swoboda, P. (2019). A hybrid approach for fraud detection: A case study in financial transactions. *Journal of Information Security and Applications*, 44, 69-79.
- 22) Njoku, D. O., Iwuchukwu, V. C., Jibiri, J. E., Ikwuazom, C. T., Ofoegbu, C. I., & Nwokoma, F. O. (2024). Machine learning approach for fraud detection system in financial institution: A web base application. *Machine Learning*, 20(4), 01-12.
- 23) Ogochukwu P. O, Godson N O, Chinedu M, Paul U R. (2023). A Deep Learning Model for Detecting Anomalies in The Banking Sector Using A Feed-Forward Neural Network. *International Journal of Scientific and Engineering Research*, 14(1):322-327
- 24) Onyeama, J. (2024). Credit Card Fraud Detection in the Nigerian Financial Sector: A Comparison of Unsupervised TensorFlow-Based Anomaly Detection Techniques, Autoencoders and PCA Algorithm. *arXiv preprint arXiv:2407.08758*.
- 25) Patel, S., & Bansal, R. (2023). Federated learning in financial fraud detection systems. *Journal of Privacy-Preserving AI*, 12(3), 201-217.
- 26) Rahman, M., Yoon, H., & Kim, K. (2020). Anomaly detection in online banking using autoencoders. *Journal of Bank Security*, 12(1), 22-31.
- 27) Sharma, R., & Kumar, P. (2023). Explainable AI for fraud detection in financial transactions. *Journal of AI Transparency*, 19(1), 45-62.
- 28) Singh, P., & Gupta, S. (2022). Graph-based anomaly detection in transactional networks. *Journal of Financial Analytics*, 18(3), 215-228.
- 29) Tanouz, D., Subramanian, R. R., Eswar, D., Reddy, G. P., Kumar, A. R., & Praneeth, C. V. (2021, May). Credit card fraud detection using machine learning. In *2021 5th international conference on intelligent computing and control systems (ICICCS)* (pp. 967-972). IEEE.
- 30) Thorat, S. S., Rojatar, D. V., & Deshmukh, P. R. (2024, January). A deep learning approach for sustainable ad hoc vehicular network. In *International Conference on Smart Computing and Communication* (pp. 429-443). Singapore: Springer Nature Singapore.
- 31) Zhang, J., Luo, B., Xu, Z., & Sun, Z. (2019). Deep learning-based anomaly detection in financial data streams. *Applied Soft Computing*, 96, 106626.
- 32) Zhao, X., Liu, Y., & Wang, H. (2023). Adversarial training to enhance anomaly detection models. *Journal of Robust AI*, 13(5), 378-391.