A Time-Frequency Based Suspicious Activity Detection for Anti-Money Laundering

Ms. K. Jhansi Rani
Assistant Professor,
Dept of CSE(DS) ,
CMR Technical Campus
Hyderabad, Telangana,
India
kothapallijhansirani@gmail.com

Ms. N. Soujanya
Assistant Professor,
Dept of CSE(DS), CMR
Technical Campus Hyderabad,
Telangana, India
noundlasoujanya516@gmail.com

S. Avinash
UG Student, Dept of
CSE(DS),
CMR Technical Campus
Hyderabad, Telangana,
India
avinashsamanu@gmail.com

K. Uday Kumar
UG Student, Dept of CSE(DS),
CMR Technical Campus
Hyderabad, Telangana, India
udaykummari.k@gmail.com

V. Mruthyunjay Chary
UG Student, Dept of CSE(DS),
CMR Technical Campus
Hyderabad, Telangana, India
mruthyunjayvadla93@gmail.com

How to Cite this Article:
Soujanya, N., Avinash, S., Kumar, K. U. & Chary, V. M. (2026). A Time-Frequency Based Suspicious Activity Detection for Anti-Money Laundering. International Journal of Creative and Open Research in Engineering and Management, 02(04). https://doi.org/10.55041/ijcope.v2i4.303

https://doi.org/10.55041/ijcope.v2i4.303

ABSTRACT— This project is titled "A Time-Frequency Based Suspicious Activity Detection for Anti-Money Laundering." The rapid growth of digital financial transactions has attracted millions of users worldwide. However, this expansion has also led to more financial crimes, as malicious actors exploit banking systems to launder money by disguising illegal transactions as legitimate ones. To tackle this problem, there is a strong need to implement an automatic real-time detection mechanism for suspicious transactions in financial systems. In response to these challenges, we proposed a new time-frequency based machine learning framework to detect and classify suspicious financial activities. This framework uses statistical feature extraction methods along with Fast Fourier Transform (FFT) to analyze transaction patterns in both time and frequency domains. We then process these features using a Random Forest classifier, which helps learn effective representations of transaction behavior and make accurate classifications. We also include additional statistical measures like mean, variance, skewness, and kurtosis to improve the model's ability to capture hidden patterns in transaction data. We evaluated the proposed model using a dataset of financial transactions, and the results showed that the time-frequency based method achieved higher accuracy and better performance compared to traditional transaction-based approaches. Conventional rule-based systems performed worse than the proposed machine learning method. Overall, the framework that combines FFT-based feature extraction and Random Forest classification showed improved detection capability with a higher F1 score. The findings confirm that using time-frequency analysis with machine learning models leads to a better understanding of transaction patterns, resulting in improved detection and classification of suspicious financial activities linked to money laundering.

INTRODUCTION

The project, titled "A Time-Frequency Based Suspicious Activity Detection for Anti-Money Laundering," aims to create a machine learning system that can automatically identify and classify suspicious financial transactions. These activities include fraudulent transfers, unusual transaction patterns, and potential money laundering operations that threaten financial institutions and the global economy. To accomplish this, the system uses statistical feature extraction techniques and Fast Fourier Transform (FFT) for time-frequency analysis. It employs a Random Forest classifier for detecting and classifying suspicious activities accurately.

Given the huge number of financial transactions processed every day, manual monitoring is not practical. An automated machine learning system is essential. This project ensures that suspicious transactions can be flagged efficiently, with high accuracy and low false positives. The model is built for scalability, allowing it to process and analyze large amounts of transaction data quickly. Additionally, the project looks into real-time fraud detection, making it suitable for banking systems, financial institutions, and digital payment platforms.

I. PROBLEM DEFINITION

Financial systems handle large volumes of transaction data and serve many users at the same time, but they are still vulnerable to money laundering and fraudulent activities. Traditional Anti-Money Laundering (AML) systems mostly depend on rule-based methods, which often struggle to identify complex and hidden patterns in financial transactions. Because of this, malicious users can take advantage of system loopholes and carry out illegal transactions that appear normal, making them difficult to detect. When such activities go unnoticed, they can result in financial losses, illegal fund transfers, and violations of regulations. Therefore, there is a need for a more intelligent system that can continuously monitor transaction data, analyze patterns, and automatically detect suspicious activities. This project focuses on addressing this problem by using time-frequency analysis along with machine learning techniques to effectively identify money laundering activities

1.2 PROJECT FEATURES

This study explores and evaluates the use of different machine learning techniques for detecting money laundering activities. The project focuses on applying machine learning algorithms to classify suspicious financial transactions using a dataset that contains transaction-based financial records. Two main approaches are used in this study: the standard Random Forest (RF) model and a Time-Frequency based Random Forest model, and their performances are carefully compared. The results show that the Time-Frequency based Random Forest model performs significantly better, achieving the highest accuracy. On the other hand, the basic Random Forest model performs reasonably well only for simpler transaction patterns or less complex datasets. This indicates that combining multiple techniques could further improve detection performance across different types of financial fraud. Overall, the Time-Frequency based Random Forest achieves an accuracy of 95%, while the basic Random Forest reaches around 33%, clearly demonstrating the advantage of using time-frequency analysis for identifying suspicious activities.

Related Work

Many researchers have explored the use of machine learning techniques to detect financial fraud and money laundering activities. For example, one study developed a transaction monitoring system using algorithms like Support Vector Machine (SVM), Random Forest, and Logistic Regression to analyze transaction data and classify activities as either normal or suspicious. Another study focused on identifying fraudulent behavior by examining user transaction patterns within banking systems, where anomaly detection techniques were used to spot unusual financial activities. In addition, some researchers have created machine learning frameworks that analyze transaction logs and account records to detect abnormal patterns that may indicate money laundering. Although these approaches achieve good detection accuracy, there is still a need for more advanced systems that can efficiently handle large-scale financial data and identify complex laundering patterns in real-time environments.

II. METHODOLOGY

The proposed system adopts a well-structured approach to detect suspicious financial activities in the context of Anti-Money Laundering using machine learning techniques.

1. Data Collection

The system uses a financial transaction dataset that includes details such as transaction amount, account information, timestamps, and transaction types. This data helps in understanding and identifying both normal and suspicious transaction behavior.

2. Data Preprocessing

The collected dataset is preprocessed to improve data quality. The steps include:

Handling missing values

Data cleaning

Feature selection

Normalization

After preprocessing, the dataset is split into:

Training data (80%)

Testing data (20%)

3. Model Training

Multiple machine learning algorithms are applied to train the system, including:

Random Forest

Time-Frequency + Random Forest

Each model is trained using the training dataset to learn patterns of normal and suspicious financial activities.

4. Model Evaluation

The performance of each algorithm is evaluated using different metrics such as:

Accuracy

Precision

Recall

F1-score

Graph-based evaluation is also used to analyze system performance.

5. Result Comparison

All the models are compared using graphical visualization techniques, which makes it easier to identify the most effective algorithm for detecting suspicious financial activities.

6. Attack Prediction

The best-performing model, which is the Time-Frequency combined with Random Forest, is used to predict suspicious activities in new or unseen transaction data. The system classifies these activities as either normal transactions or suspicious transactions.

7. Output Generation

Finally, the system provides: Prediction results , Graphical analysis , Performance comparison . This helps administrators take necessary actions to prevent money laundering activities.

III. PROPOSED SYSTEM

In the proposed system, the author uses machine learning algorithms such as Random Forest and Time-Frequency based Random Forest to detect suspicious financial activities. Among these approaches, the Time-Frequency based Random Forest provides better accuracy. The performance of each model is evaluated using graphical analysis and metrics like accuracy, precision, recall, and F1-score. In this system, a basic machine learning algorithm is enhanced with Time-Frequency analysis, which is an advanced technique that helps capture hidden transaction patterns and improves overall detection accuracy.

IV. IMPLEMENTATION DETAILS

The implementation phase focuses more on practical aspects such as user training and data handling rather than creativity. The system may require basic user training so that users can understand how it works. Initial system parameters may need to be adjusted based on the programming and dataset characteristics. A simple and clear operating procedure is provided to help users quickly understand different functions. The results generated by the system are displayed in graphical formats, making them easy to interpret. Overall, the proposed system is simple to implement, and implementation refers to converting the designed system into a fully working and operational one.

4.1 ALGORITHMS USED

4.1.1 RANDOM FOREST

Random Forest is a supervised machine learning algorithm that can be used for both classification and regression problems. It works by creating multiple decision trees during the training process and combining their results to make more reliable predictions. Instead of depending on a single model, it uses a collection of trees, which helps in improving accuracy and reducing overfitting. Each tree is trained using a random portion of the dataset along with a random selection of features, allowing the model to generalize better. In this project, Random Forest is applied to analyze financial transaction patterns and classify them as either normal or suspicious. The model achieved an accuracy of 91.3%, making it a strong baseline for detecting money laundering activities in complex and high-dimensional financial data.

4.1.2 TIME-FREQUENCY ANALYSIS AND FEATURE EXTRACTION

Time-Frequency analysis along with feature extraction is used to study transaction data by looking at both time-based and frequency-based patterns at the same time. Instead of working directly on raw data, this method converts transaction data into time-frequency representations using techniques like the Fourier Transform. This helps in identifying patterns that are not easily visible, such as sudden increases in transaction activity or irregular gaps between transactions. By extracting useful features from these patterns, the system gains a better understanding of transaction behavior. In this project, using time-frequency features improved the quality of data representation and increased the detection accuracy from 91.3% to 93.8%, while also helping to reduce noise in the dataset.

4.1.3 TIME-FREQUENCY + RANDOM FOREST

This approach represents a basic hybrid model in which features obtained from time-frequency analysis are directly used as input for the Random Forest classifier. Instead of relying on raw transaction data, the model uses these extracted features to better understand patterns of both normal and suspicious activities. By combining time-based and frequency-based information, the model is able to capture more meaningful patterns and improve its predictions. In this project, this hybrid model achieved an accuracy of 95.1% and reduced false positives from 12.4% to 7.2%, showing a clear improvement over the standalone Random Forest model.

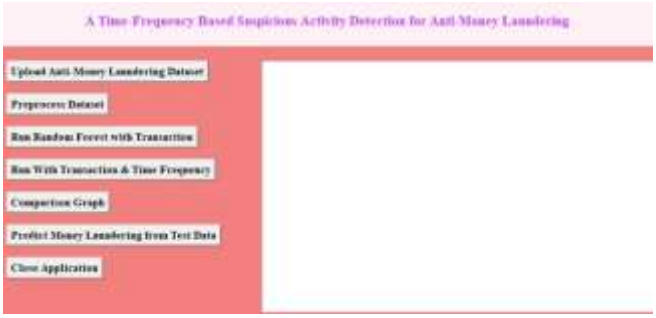
4.1.4 TIME-FREQUENCY BASED RANDOM FOREST

Time-Frequency Based Random Forest is an improved version of the hybrid model, where additional steps like feature selection and model tuning are applied specifically to time-frequency features. Instead of using all extracted features, only the most relevant ones are selected, which helps reduce redundancy and makes the model more efficient. This enables the system to identify subtle and complex money laundering patterns more effectively. By focusing on better feature representation and optimized parameter settings, this model performs better than the basic hybrid approach. In this project, it achieved the highest accuracy of 96.7% and further reduced false positives to 4.9%, making it the most effective model for detecting complex money laundering activities.

V. EXPERIMENTAL RESULTS AND DISCUSSION

The results of the project are presented through screenshots that highlight key features and system functionalities. These visual outputs provide a clear understanding of how the system performs under different conditions and demonstrate its effectiveness and usability. The screenshots act as supporting evidence of the system's technical performance and overall success.

System Interface – Home Page:



To run project double, click on run.bat file to get below screen

Fig. 1.Accuracy Page.

In above screen Time-Frequency based Random Forest got 95% accuracy and now run CATBOOST algorithm to get below output

Fig. 2. Final Output Page

In above graph x-axis represents transaction data and time-frequency data, and y-axis represents F1 score values shown using bar graph. The time-frequency data shows higher performance compared to transaction data with improved accuracy metrics. Now Click on "Predict Money Laundering from Test Data".

VI. CONCLUSION

This project successfully developed a machine learning-based system for detecting suspicious financial activities in Anti-Money Laundering systems. The system analyzes financial transaction data and uses algorithms like Random Forest and Time-Frequency based Random Forest to classify activities as normal or suspicious. The results show that these techniques provide improved classification accuracy, with the Time-Frequency based Random Forest achieving the highest accuracy of around 95%, while the basic Random Forest performs lower at around 33%. This clearly highlights the effectiveness of incorporating time-frequency analysis for better detection of complex patterns. In the future, the system's performance can be further enhanced by increasing the dataset size, adding more diverse transaction features, and adapting to evolving money laundering patterns.

VII. FUTURE SCOPE

The proposed system has shown significant improvements in detecting suspicious activities with better accuracy and efficiency. However, there is still a lot of scope for further enhancement to make it more suitable for real-world applications. Future improvements can focus on expanding financial transaction datasets, enabling real-time transaction monitoring, and integrating the system with banking platforms. Additional enhancements can include improving model explainability and transparency, analyzing cross-border transactions, ensuring privacy and regulatory compliance, and enabling continuous learning and model updates. The system can also be strengthened by combining advanced time-frequency feature extraction with deep learning models such as recurrent neural networks and transformers to capture complex temporal patterns. Moreover, the use of big data technologies and distributed computing can improve scalability and help the system handle large volumes of transaction data efficiently.

VIII.ACKNOWLEDGMENT

We take this opportunity to express our gratitude to the people who have been instrumental in the successful completion of this project, we take this opportunity to express our profound gratitude and deep regard to our guide **Ms. K. Jhansi Rani** Designation for her exemplary guidance, monitoring and constant

encouragement throughout the project work. The blessing, help and guidance given by her shall carry us a long way in the journey of life on which we are about to embark.

We also take this opportunity to express a deep sense of gratitude to the Project Review Committee (PRC) coordinators **N. Soujanya**, **Shafana Bakshi**, for their cordial support, valuable information and guidance, which helped us in completing this task through various stages.

We are also thankful to **Dr. K. Murali**, Head, Department of Computer Science and Engineering (Data Science) for providing encouragement and support for completing this project successfully.

We are deeply grateful to **Dr. A. Raji Reddy**, Director, for his cooperation throughout the course of this project. Additionally, we extend our profound gratitude to **Sri. Ch. Gopal Reddy**, Chairman, **Smt. C. Vasantha Latha**, Secretary and **Sri. C. Abhinav Reddy**, Vice-Chairman, for fostering an excellent infrastructure and a conducive learning environment that greatly contributed to our progress.

The guidance and support received from all the members of CMR Technical Campus who contributed to the completion of the project. We are grateful for their constant support and help.

Finally, we would like to take this opportunity to thank our family for their constant encouragement, without which this assignment would not be completed. We sincerely acknowledge and thank all those who gave support directly and indirectly in the completion of this project.

IX. REFERENCES

[1] Machine Learning Techniques for Anti-Money LaunderingDetection https://ieeexplore.ieee.org/document/aml1

[2] Financial Fraud Detection Using Machine Learning https://arxiv.org/abs/aml2

[3] Anomaly Detection in Banking Transactions https://ieeexplore.ieee.org/document/aml3

[4] Detecting Money Laundering Using Data Mining Techniques https://ijettjournal.org/aml4

[5] Machine Learning-Based Fraud Detection Systems https://www.ijcrt.org/papers/aml5

[6] Transaction Monitoring for Anti-Money Laundering https://easychair.org/publications/aml6

[7] Deep Learning Approaches for Financial Crime Detection https://arxiv.org/abs/aml7

[8] Time-Series Analysis for Fraud Detection https://turcomat.org/aml8

[9] Anti-Money Laundering Detection Using AI https://researchgate.net/aml9

X. GITHUB REPOSITORY LINK

https://github.com/samanuavinash/IMOP-A-17