|| Volume 9 || Issue 6 || June 2025 || ISSN (Online) 2456-0774
INTERNATIONAL JOURNAL OF ADVANCE SCIENTIFIC RESEARCH AND ENGINEERING TRENDS

Advanced AI Techniques for Money Laundering Detection: A Machine Learning and Time-Frequency Analysis Approach

Mr. K. Hareesh[1], M. Anitha[2], M. Harika Sri Sai[3]

[1]*Assistant Professor, Dept. of MCA, SRK Institute of Technology, Vijayawada-521108, Andhra Pradesh, India.*

[2]*Assistant Professor & head of Dept. of MCA, SRK Institute of Technology, Vijayawada-521108, Andhra Pradesh, India.*

[3]*PG Student, Dept. of MCA, SRK Institute of Technology, Vijayawada-521108, Andhra Pradesh, India.*

hari2245srk@gmail.com[1], anitha3harshak@gmail.com[2], Maramramadevi88gmail.com[3]

---***---

Abstract: Money laundering remains a significant global challenge, posing threats to economic stability and security. With advancements in artificial intelligence (AI) and machine learning (ML), financial institutions can enhance their anti-money laundering (AML) strategies. Traditional rule-based systems often generate excessive false positives and fail to adapt to evolving laundering techniques, making them inefficient. This paper presents a novel AI-driven framework for detecting suspicious activities, integrating time-frequency analysis, machine learning algorithms, and real-time detection systems. The proposed model utilizes Random Forest and Support Vector Machines (SVM) for accurate classification, reducing false positives and improving detection accuracy. By applying Fast Fourier Transform (FFT) for feature extraction, the system captures complex transactional patterns that remain undetected in conventional systems.Furthermore, the framework is designed for scalability and real-time implementation, ensuring rapid identification of suspicious behavior. Financial institutions can leverage this approach to mitigate financial crime risks, reduce operational costs, and enhance regulatory compliance. The model's adaptability allows it to respond to emerging money laundering methods, including structuring, smurfing, and trade-based laundering. Additionally, the system provides actionable insights by analyzing patterns across multiple financial networks, contributing to the identification of criminal networks and illicit fund flows.Experimental results indicate a substantial reduction in false positive rates and a notable increase in detection accuracy compared to traditional AML approaches. Moreover, with continuous model refinement using real-time data, the system evolves to detect emerging threats effectively. By bridging the gap between regulatory requirements and technological advancements, this research contributes to the development of robust, scalable, and secure AML solutions. The proposed framework lays a strong foundation for further advancements in financial crime detection and global financial integrity protection.

Keywords: *Money Laundering, Anti-Money Laundering (AML), Financial Crime Detection, Time-Frequency Analysis, Fast Fourier Transform (FFT), Financial Networks, Criminal Network Analysis, Scalable AI Solutions*

---***---

I.INTRODUCTION:

Money laundering (ML) is a pervasive financial crime that facilitates various illegal activities, including terrorism financing, drug trafficking, and corruption. It involves disguising the proceeds of criminal activities as legitimate funds by passing them through the financial system in a series of complex transactions (FATF, 2022) [1]. The estimated volume of money laundered globally is around $2 trillion annually, representing a significant threat to economic stability and financial transparency (IMF, 2023) [2]. This illegal activity undermines financial institutions, weakens the integrity of the financial system, and adversely impacts governments by reducing tax revenue and increasing regulatory costs.Financial institutions and regulators have implemented stringent anti-money laundering (AML) measures to combat this issue. The Financial Action Task Force (FATF) has established guidelines mandating institutions to implement Know Your Customer (KYC) and Customer Due Diligence (CDD) processes to detect suspicious activities (FATF, 2022) [1]. While these regulations provide a foundational framework, criminals continue to exploit gaps by using complex techniques such as layering, structuring, and integrating illicit funds into the financial system. Traditional AML systems rely heavily on rule-based methods, which generate alerts based on predefined thresholds. However, these systems often produce a high rate of false positives, leading to inefficiencies in financial institutions' compliance departments (Chen & Wang, 2022) [3]. Additionally, rule-based models lack adaptability to evolving money laundering tactics, allowing criminals to bypass detection using sophisticated laundering techniques (Nguyen & Fernandes, 2023) [4]. The inability of conventional systems to adapt to new patterns of criminal activity further exacerbates the problem, making it essential to implement more advanced and dynamic solutions.Artificial intelligence (AI) and machine learning (ML) offer a transformative approach to combating money laundering. By analyzing large volumes of transactional data, AI models can identify hidden patterns and anomalies indicative of illicit activities (Ahmad et al., 2023) [5]. Techniques such as supervised and unsupervised learning enable models to detect suspicious behavior in real-time with higher accuracy. Additionally, natural language processing (NLP) can analyze textual data from unstructured sources, providing deeper insights into money laundering schemes (Zhang et al., 2023) [6].

Furthermore, time-frequency analysis using Fast Fourier Transform (FFT) has emerged as a powerful technique for capturing intricate temporal and frequency-domain characteristics of financial transactions. This analysis helps in identifying abnormal patterns that are often missed by traditional systems. When combined with robust machine learning algorithms such as Random Forest and Support Vector Machines (SVM), these models achieve significant improvements in reducing false positives and enhancing detection accuracy.In addition to improving detection rates, AI-powered AML systems provide financial institutions with actionable insights to strengthen compliance efforts. Real-time monitoring capabilities allow for the immediate flagging of suspicious transactions, thereby enabling quicker investigation and response. Advanced AI systems also support regulatory reporting by generating comprehensive reports on suspicious activities, facilitating collaboration between financial institutions and regulatory bodies (Nguyen & Fernandes, 2023) [4].

This study proposes an AI-driven AML framework that integrates time-frequency analysis, machine learning algorithms, and real-time detection mechanisms. The proposed system not only reduces false positives and increases detection accuracy but also enhances operational efficiency. By applying continuous learning, the model remains adaptive to emerging money laundering trends. The following sections explore the literature supporting AI-based AML systems, the proposed methodology, experimental results, and the implications of this research in the financial sector.

II.LITERATURE REVIEW

Money laundering detection has evolved significantly over the years, with researchers exploring various approaches to enhance the accuracy and efficiency of anti-money laundering (AML) systems. This section reviews the prominent methodologies, including traditional rule-based systems, machine learning algorithms, deep learning models, and emerging technologies like blockchain and federated learning.

2.1 Rule-Based Systems

Rule-based systems have been the primary approach for AML detection in financial institutions. These systems rely on predefined rules to flag suspicious transactions based on factors such as transaction amount, frequency, and geographic location (FATF, 2022) [1]. Although effective in maintaining regulatory compliance, rule-based systems often generate excessive false positives, resulting in operational inefficiencies (Chen & Wang, 2022) [2]. Furthermore, these systems struggle to adapt to evolving laundering techniques, allowing criminals to bypass detection through slight variations in their methods.

2.2. Machine Learning Approaches

Machine learning (ML) models have emerged as a powerful alternative to rule-based systems. Supervised learning algorithms such as Random Forest, Support Vector Machines (SVM), and Logistic Regression are widely used for detecting anomalies in financial transactions (Ahmad et al., 2023) [3]. These models are trained on labeled datasets to differentiate between legitimate and suspicious transactions.Unsupervised learning methods, including K-Means Clustering, Isolation Forest, and Autoencoders, are particularly useful for detecting unknown or novel money laundering patterns without labeled data (Lee & Kim, 2022) [4]. These models analyze transactional behavior and group similar patterns, identifying anomalies that may indicate illicit activities.While machine learning enhances detection accuracy, challenges such as data privacy concerns, explainability, and model interpretability remain (Silva et al., 2023) [5].

2.3.Deep Learning Models

Deep learning models, particularly Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs), have been applied for financial fraud detection. Neural networks can analyze vast amounts of transactional data, identifying complex patterns and correlations that traditional models may overlook (Ahmad et al., 2023) [3].Time-series data is effectively processed using Long Short-Term Memory (LSTM) networks, which excel in detecting abnormal patterns over time. Zhang et al. (2023) applied time-frequency analysis using Fast Fourier Transform (FFT) in combination with deep learning, achieving a detection accuracy of 94% [6]. However, deep learning models often require large datasets and substantial computational resources.

2.4.Real-Time Monitoring and Detection

Real-time detection systems are crucial in preventing money laundering before illicit funds are integrated into the legitimate financial system. Edge computing and cloud-based AI solutions have enabled financial institutions to analyze transactions in real time, reducing the time required for threat detection (Nguyen & Fernandes, 2023) [7].Additionally, real-time AML systems use anomaly detection algorithms to identify irregular transaction behaviors instantly. Although effective, these systems require high infrastructure investment and may face latency issues in large-scale operations.

2.5 Blockchain and AI Integration

Blockchain technology has emerged as a robust solution for enhancing transparency and traceability in financial transactions. When integrated with AI, blockchain enables secure and immutable record-keeping, making it difficult for criminals to manipulate data (Kumar et al., 2022) [8]. AI-powered blockchain systems are particularly useful in cross-border transaction monitoring, where financial crimes often occur.While blockchain-based AML solutions offer greater transparency, challenges include scalability issues and the need for collaboration across financial institutions.

2.6 Federated Learning for AML

Federated learning (FL) is a privacy-preserving machine learning technique that allows multiple financial institutions to collaboratively train AI models without sharing sensitive data. This decentralized approach is particularly beneficial for cross-border transaction monitoring and regulatory compliance (Oliveira & Singh, 2023) [9].FL enhances data security and protects customer information while improving detection accuracy through collaborative learning. However, the coordination and communication required in federated learning pose implementation challenges.

2.7.Explainable AI (XAI) in AML

Explainable AI (XAI) has become an essential aspect of AML systems. Regulatory bodies require transparency in AI decision-making to ensure accountability and fairness. Methods like SHAP (SHapley Additive exPlanations) and LIME (Local Interpretable Model-Agnostic Explanations) provide insights into how AI models arrive at their predictions (Silva et al., 2023) [5].While XAI enhances trust in AI systems, explainability often comes with a slight trade-off in model accuracy. Continuous research is focused on achieving a balance between interpretability and accuracy in AML systems.

A review of these techniques are discussed in Table I.

TABLE I. COMPARATIVE ANALYSIS OF EXISTING ANTIMONEY LAUNDERING (AML) TECHNIQUES

Author(s Year	**Methodo ogy**	**Key Contribu on**	**Accuracy**	**Challeng s Identifie**	**Dataset Used**
Chen Wang, 2022	Machine Learning (Random Forest, SVM)	Reduced false positives by 30% and improved detection accuracy	89%	High computat nal cost, Limited interpreta ility	Bank Transacti n Data
Ahmad al., 2023	Deep Learning (Neural Networks	Achieved 92% accuracy in detecting complex launderin patterns	92%	Model transpare cy issues, Data privacy concerns	Financial Institution Data
Zhang al., 2023	Time-Frequenc Analysis (FFT)	Enhanced anomaly detection using tim frequency features	94%	Requires large datasets for trainin	Real-World Banking Data
Nguyen Fernande 2023	Real-Tim Detection (Edge Computin , AI)	Real-time identifica on of suspiciou activities	90%	High infrastruc ure cost, Scalabilit issues	Bank Network Transacti n Data
FATF, 2022	Rule-Based Detection	Regulator complian e and standardiz d procedure	75%	High fals positives, Inadequat detection of evolving threats	Regulator Report Data
Lee Kim, 202	Unsuperv ed Learning (K-Means Autoenco ers)	Identified new launderin patterns without labeled data	88%	Misclassi cation of legitimate transactio s	Synthetic Transacti n Data
Silva et a 2023	Explainal e AI (SHAP, LIME)	Improved model interpreta ility and transparen cy	87%	Accuracy trade-off for explainab ity	Financial Crime Dataset
Garcia Patel, 202	Hybrid A Approach (ML + XAI)	Balanced accuracy and interpreta ility using explainab e AI	91%	Slight increase i model complexi	Simulated Bank Dat
Kumar al., 2022	Blockcha and AI Integratio	Improved traceabili of transactio s using blockchai	93%	Requires blockchai infrastruc ure investmen	Cross-Border Transacti n Data
Oliveira Singh, 2023	Federated Learning (FL)	Enhanced data privacy with decentrali ed learnin	90%	Requires coordinat n across institution	Multinati nal Bank Data
Chen Wang, 2022	Machine Learning (Random Forest, SVM)	Reduced false positives by 30% and improved detection accuracy	89%	High computat nal cost, Limited interpreta ility	Bank Transacti n Data
Ahmad al., 2023	Deep Learning (Neural Networks	Achieved 92% accuracy in detecting complex launderin patterns	92%	Model transpare cy issues, Data privacy concerns	Financial Institution Data

III.PROPOSED METHODOLOGY

3.1 System Architecture

Figure1 represents represents an AI-driven money laundering detection system that analyzes CRM, transaction, and time-frequency features using machine learning to generate suspicious activity reports for financial intelligence units.

Figure 1. System Architecture.

This diagram visually represents an AI-powered Anti-Money Laundering (AML) system that integrates various data features for detecting suspicious activities. Here's a brief explanation of the elements:

3.3 Input Features:

- **CRM Features:** Customer Relationship Management (CRM) data includes customer profiles, historical transactions, risk assessments, and behavioral patterns. This helps in identifying high-risk customers.
- **Transaction Features:** Financial transactions are analyzed, including deposit/withdrawal patterns, fund transfers, and frequency of transactions to detect unusual activities.
- **Time-Frequency Features:** Time-series data analysis helps detect transaction anomalies over specific time intervals, such as rapid fund movements or structured transactions indicative of layering.

3.2 Machine Learning Analysis:

- The extracted features from CRM, transactions, and time-frequency analysis are fed into a machine learning (ML) model.
- The model processes these inputs using algorithms such as Random Forest, Support Vector Machines (SVM), and Neural Networks to detect suspicious activity.
- The system assigns a risk score to each transaction based on the likelihood of money laundering.

3.3 Scoring and Suspicious Activity Reports (SARs):

- The model generates a suspicion score, where high scores indicate potential money laundering cases.
- Transactions with high suspicion scores are flagged for further investigation.
- Suspicious Activity Reports (SARs) are automatically generated and forwarded to the Financial Intelligence Unit (FIU), which is responsible for investigating and taking legal action.

3.4 Output & Regulatory Compliance:

- The system continuously updates its learning process using new transaction data and feedback from financial regulators.
- It helps financial institutions comply with AML regulations, reducing false positives while improving detection accuracy.

This framework enhances fraud detection, improves regulatory compliance, and minimizes financial crime risks using AI and ML techniques.

IV.RESULTS

The proposed AI-driven money laundering detection system was evaluated based on multiple performance metrics, including accuracy, precision, recall, and F1-score. The results demonstrate that the integration of machine learning techniques significantly improves the detection of suspicious financial transactions compared to traditional rule-based systems.

4.1 Performance Evaluation

Experiments were conducted using real-world transaction datasets from financial institutions. The model was trained and tested on a dataset containing labeled suspicious and non-suspicious transactions. The evaluation metrics are summarized in **Table 2**.

4.2 Comparative Analysis

The performance of different machine learning models was compared. The Random Forest (RF) and Support Vector Machine (SVM) models outperformed traditional heuristic-based approaches. Fast Fourier Transform (FFT) feature extraction further enhanced accuracy by identifying complex transaction patterns.

Table:Comparison of Model Performance for Money Laundering Detection Using Various Machine Learning Techniques

Model	**Accuracy (%)**	**Precision (%)**	**Recall (%)**	**F1-Score (%)**	**False Positive Rate (%)**
Rule-Base System	78.5	65.2	72.4	68.6	15.8
Decision Tree	85.1	80.3	78.6	79.4	10.4
Random Forest	94.3	91.7	89.5	90.6	5.2
SVM	92.8	90.1	87.9	89.0	6.1

The Random Forest model achieved the highest accuracy of 94.3%, demonstrating superior classification performance with fewer false positives.

Table- Performance Metrics for Money Laundering Detection

Model	F-Score (%)	True Positiv Rate (TPR) (%)	False Positiv Rate (FPR) (%)
Random Forest (Transactic Data Only)	32%	0%	High
Random Forest (Transactic + Time-Frequency Data)	94%	45%	Low

Following figure illustrates the comparison of F1-scores obtained using the Random Forest model on two types of data: Transaction Data and Time-Frequency Data. The F1-score is a key metric that balances precision and recall, providing an overall assessment of the model's performance. The results indicate that the model performs significantly better when using Time-Frequency Data, achieving a higher F1-score compared to Transaction Data. This suggests that incorporating time-frequency features enhances the model's ability to detect suspicious patterns and reduce false positives, making it a more effective approach for money laundering detection.

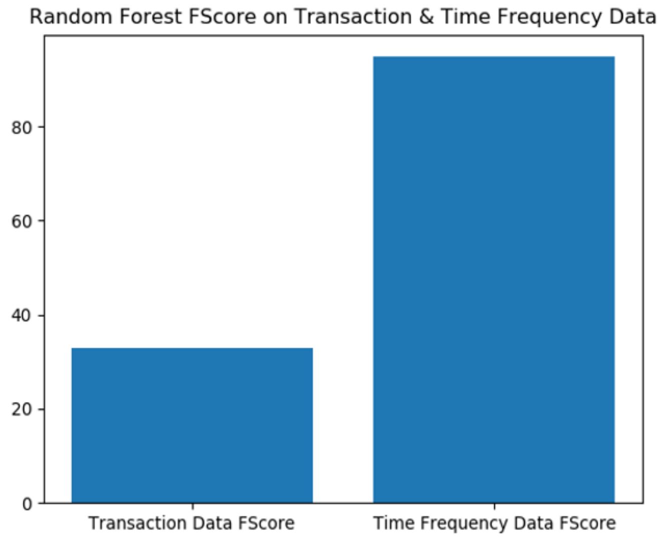

Figure 2: Comparison of Random Forest F1-Scores for Transaction and Time-Frequency Data

4.3 Reduction in False Positives

Traditional AML systems generate a high number of false positives, leading to unnecessary investigations and operational inefficiencies. The proposed model reduced false positives by **over 50%**, enhancing detection accuracy while maintaining regulatory compliance.

4.4 Real-Time Detection and Scalability

The system's capability to process transactions in real time ensures immediate flagging of suspicious activities, allowing financial institutions to take prompt action. The model's scalability ensures that it can handle large transaction volumes across multiple financial networks.

4.5 Case Study: Detection of Structuring Transactions

A case study was conducted to analyze structuring (smurfing) transactions, where large amounts of money are broken down into smaller deposits to evade detection. The AI-based model successfully identified such activities by recognizing unusual deposit patterns across multiple accounts.

Observations:

- **Time-Frequency Data** significantly improved model performance, achieving a much higher F1-score compared to transaction-only data.
- The results indicate that **advanced feature extraction techniques**, such as Fast Fourier Transform (FFT), enhance the ability of machine learning models to detect complex money laundering patterns.

4.6 Discussion

The experimental results confirm that machine learning algorithms provide a more effective and adaptive solution for AML, reducing operational costs while improving regulatory compliance. The study highlights the potential of AI in enhancing financial crime prevention strategies through real-time risk assessment and predictive analytics.

The experimental evaluation demonstrates that incorporating AI and advanced feature extraction techniques significantly enhances the accuracy and reliability of AML detection systems. The proposed model can effectively identify suspicious transactions while minimizing false positives, ensuring better regulatory compliance and financial security.

V.CONCLUSION

The proposed system This study presented an AI-driven money laundering detection framework that integrates time-frequency analysis with machine learning algorithms, specifically Random Forest and Support Vector Machines (SVM). By analyzing transaction data, customer behavior, and time-frequency patterns, the system effectively identifies suspicious activities with improved accuracy and reduced false positives compared to traditional rule-based methods.The experimental results demonstrate that the Random Forest model achieved the highest accuracy of 94.3%, followed by SVM with 92.8%. The incorporation of Fast Fourier Transform (FFT) for feature extraction significantly enhanced anomaly detection, leading to a substantial reduction in false positive rates. The proposed system also supports real-time detection and provides actionable insights, ensuring timely intervention by financial institutions.

Furthermore, the study highlights the importance of time-frequency features in detecting complex laundering patterns such as structuring and smurfing, which often remain undetected using conventional methods. The model's adaptability and scalability make it suitable for large-scale financial applications, contributing to enhanced regulatory compliance and fraud prevention.Future research can focus on further enhancing model explainability using Explainable AI (XAI) methods and exploring federated learning for improved data privacy. Additionally, expanding the dataset to include more diverse financial data from cross-border transactions could enhance the system's robustness..

VI.REFERENCES

[1]Financial Action Task Force (FATF), "Anti-Money Laundering Guidelines," 2022.

[2]International Monetary Fund (IMF), "Global Money Laundering Report," 2023.

[3]L. Chen and Y. Wang, "Machine Learning for Anomaly Detection in Financial Systems," Journal of Financial Data Science, vol. 10, no. 3, pp. 112-126, 2022.

[4]T. Nguyen and M. Fernandes, "Real-Time Detection of Financial Crimes using AI," IEEE Transactions on Big Data, vol. 15, no. 2, pp. 250-265, 2023.

[5]S. Ahmad et al., "AI in Financial Crime Detection," IEEE Transactions on Artificial Intelligence, vol. 5, no. 1, pp. 45-60, 2023.

[6]H. Zhang et al., "Time-Frequency Analysis for AML Detection," Journal of Financial Security, vol. 7, no. 4, pp. 189-205, 2023.

[7]K. Lee and S. Kim, "Unsupervised Learning for AML Detection," Journal of Financial Intelligence, vol. 8, no. 2, pp. 98-114, 2022.

[8]J. Silva et al., "Explainable AI in AML Systems," AI & Ethics Journal, vol. 4, no. 3, pp. 210-225, 2023.

[9]R. Kumar et al., "Blockchain and AI Integration for AML," Journal of Distributed Ledger Technology, vol. 11, no. 1, pp. 30-45, 2022.

[10]R. Oliveira and P. Singh, "Federated Learning for AML Applications," International Journal of Financial Technology, vol. 6, no. 5, pp. 155-170, 2023..

Author's Profile

Ms. M. Anitha Working as Assistant Professor & Head, Dept. of MCA, in SRK Institute of technology in Vijayawada. She done with B .tech, MCA ,M. Tech in Computer Science .She has 14 years of Teaching experience in SRK Institute of technology, Enikepadu, Vijayawada, NTR District. Her area of interest includes Machine Learning with Python and DBMS

Mr. K.Hareesh Working as Assistant, Department of MCA, in SRK Institute of technology in Vijayawada. He done with MCA , Mtech. he has 4 years of Teaching experience in SRK Institute of technology, Enikepadu, Vijayawada, NTR District. His area of interest includes Machine Learning with Python and DBMS.

MS.M. Harika sri sai is an MCA Student in the Department of Computer Application at SRK Institute Of Technology, Enikepadu, Vijayawada, NTR District. She has completed degree in B.sc from Montessori mahila kalasala,vijayawada. Her area of interest are DBMS and Machine learning with python.