

# AI-Driven Adaptive AML Framework with Real-Time Anomaly Detection and Deep Learning-Based Risk Profiling

Dr.N.P. Ponnuviji<sup>1\*</sup>, Dr.K. Venkatesh Guru<sup>2</sup>, P. Palanisamy<sup>3</sup>, and J. Nirmala Gandhi<sup>4</sup>

<sup>1\*</sup>Associate Professor, Department of Computer Science and Engineering, RMK College of Engineering and Technology, Puduvoyal, Chennai, India. ponnuviji@rmkcet.ac.in, <https://orcid.org/0000-0001-5131-7065>

<sup>2</sup>Assistant Professor, School of Computing, SRM Institute of Technology, Trichy, Tamil Nadu, India. venkateshguruk@gmail.com, <https://orcid.org/0000-0002-1679-9668>

<sup>3</sup>Assistant Professor, Computer Science and Engineering, Hindusthan Institute of Technology, Coimbatore, Tamil Nadu, India. palanisamy.p@hit.edu.in, <https://orcid.org/0009-0007-6325-0823>

<sup>4</sup>Assistant Professor, Department of CSE, K.S.R. College of Engineering, Tiruchengode, Tamil Nadu, India. nirmalamuthu@gmail.com, <https://orcid.org/0000-0003-2703-529X>

Received: September 15, 2025; Revised: October 23, 2025; Accepted: December 17, 2025; Published: February 27, 2026

## Abstract

The elusive development of financial crime requires new Anti-Money Laundering (AML) systems. In this paper, the authors introduce the concept of an AI-Driven Adaptive AML Framework, which combines real-time detection of anomalies and deep learning-based risk profiling. Legacy rule-based systems are ineffective and not adaptable to new money laundering schemes; they produce an intolerable number of false positives (estimated at 90-95 per cent of alerts), and they cannot evolve with new schemes. The methodology provides an improvement over the traditional thresholds by using Mahalanobis distance for unsupervised real-time anomaly detection, which immediately marks transactions that are not in line with the norms. At the same time, adaptive risk profiling, which is based on deep neural networks, assigns customers and transactions with granular risk scores based on the identification of complex connections in behavioral data. The performance and performance comparison with traditional rule-based systems prove the high efficacy of the framework. The AI-based concept is much more flexible and efficient in terms of operations, with a high score of 9/10 versus 3/10 in the case of legacy systems. What is more, the framework has an impressive false positive reduction potential (scoring 8/10 vs 4/10), which results in a greater true-positive ratio and is able to adapt AML systems to emerging threats continuously. The end goal of this AI-enhanced system is to increase the accuracy of detection, decrease the cost of operations, and create a safer, more secure financial system, but with high compliance.

Keywords: AI-Driven AML Framework, Adaptive Anomaly Detection, Real-Time Monitoring, Deep Learning-Based Risk Profiling, Money Laundering Detection, Financial Crime Prevention, Machine Learning In AML, Anomaly Detection Algorithms, Risk-Based Approach.

## 1 Introduction

Effective Anti-Money Laundering (AML) systems are instrumental in safeguarding against financial crimes, upholding the economic system's integrity, and ensuring regulatory compliance (Tadi, 2024). As money laundering schemes are becoming more sophisticated, financial organizations are tasked with spotting illegal transactions while still operating efficiently. Generally, older AML systems are based on rule-based systems where defined patterns and thresholds are established for suspicious transactional behavior. While these pattern-based systems work for the most part, they are not able to adapt to the new subversive money laundering schemes (Mishra et al., 2024). Also, pattern-based rule systems can create aggravation, causing false answers, generating unjustified concern, when they identify legitimate transactions- signal the transaction as suspicious in most AML investigations (Shirvanporzour, 2025), wasting valuable time and resources on an investigative model. In addition, rule-based systems will not dynamically learn from new approaches, which makes them much less effective in identifying financial crimes. This opens up the potential for advanced and dynamic machine learning AI detection approaches that spot operational shortcomings in real time. Also, reduce the cost of operational detection. In financial institutions, the shift will move from a static device approach in compliance-based AML systems to a compliant system that includes adaptive AI frameworks with advanced resource strategies (Kumar, 2024).

### Key Contribution of the Paper

- The research presents an advanced AI adaptive Anti Money Laundering mechanism which utilizes anomaly detection in real-time and risk profile determination using deep learning techniques, thus providing a greater level of flexibility and efficiency rather than the older rule-based approaches.
- Suspicious transactions are flagged and target fraudulent activities, and allow timely mechanisms for preventive financial crime containment and or financial crime mitigation.
- The research deep learning techniques to particulate risk profiles and adaptively strengthen the response of the Anti-Money Laundering systems to real-time changes in the modes of money laundering, thus improving the responsiveness, Precision, and accuracy of the system.

The study is discussed across the Six Sections. In Section 1, The Requirement for an AI Model listing Failures of Traditional Rule-based AML Models is covered, and Section 2 Discusses Current AML Legacy Systems Challenges. Section 3 Details the Proposed Model Technical Design - The Proposed AI Model is Adaptive and Includes a Description of AI Adaptive Architecture, use of Mahalanobis Distance to Detect Anomalies, and the use of Deep Learning Technologies for Risk Scoring, as well as Ancillary Pseudo Code and Related Mathematical Formulas. Section 4 Contains A Systematic Comparison of Results from Testing the AI Model Versus Other Systems and is Presented with Superior Performance of the AI Model Across Multiple Performance Metric Types. Section 5 Provides an Overall Evaluation of The Results and Additional Information About Both Advantages and Challenges of AI for the Use of Explanation-Based Learning. The Conclusion Section 6 Summarizes All Contributions Provided by Their Model as well as Reiterates the Benefits of Using AI for Higher Detection and Operational Efficiency.

## 2 Related Work

The existing automation tools used to conduct the Anti-Money Laundering (AML) detection are still mainly rule-based systems (Agbeja & Afolabi, 2016; Sunday et al., 2025). These systems are based on inflexible, pre-established checklist parameters and thresholds to detect the presence of red flag situations (e.g., massive outflows to offshore jurisdictions, excessive inter-linkage of accounts, or red-flagged customer profiles). Regulators prefer such systems because they are transparent and explainable by nature. The nature of this design also allows the compliance officers to trace the origin of the alert and hence review the regulations.

Nevertheless, there are severe limitations, which are documented with these rule-based systems (Masjedi, 2015). Their greatest weakness is that they are not flexible to emerging and hostile money laundering policies. The amount of money that financial criminals can break is easily broken by smurfing, spacing out transactions to prevent defined limits (Ahmed et al., 2025; Godswill et al., 2016). Moreover, the number of false positives generated by rule-based systems is enormous (some estimates are 90-95% non-actionable). Such a high noise level will cause valuable human and investigational resources to be diverted to real crime, and this will have dire effects on the operational efficiency of financial institutions.

The point of contention is that an exclusively preset rule base can only ensure a limited capability in identifying advanced financial crime by a system. In cases of elaborate or new money laundering processes, a rule-based system will never issue an alert, and it will be missed, hence leaving a profound negative influence on the reputation and competitive advantage of the institution (Oluwaferanmi, 2025). Such systems do not have an adaptive reasoning mechanism and therefore fail to dynamically acquire new methods through which they can learn, which leaves a gap in their operation that high-end criminals find advantageous to exploit. This operational weakness requires a move to more modern, robust, and self-educational methods of AI-based detection and adaptation to new criminal trends in real-time.

## 3 Proposed Framework

The real-time adaptive AI Anti-Money Laundering system discussed in this paper utilizes advanced ML for monitoring and mitigating financial crimes in real-time. Supporting technologies in this system include real-time anomaly monitoring and detection for instant recognition of transactional fraud (Popoola & Bakare, 2024; Darapour, 2016). This system goes beyond previous methods, rules, and thresholds by providing continuous monitoring of transactional anomalies, which may suggest money laundering, and is primitive in laundering detection and traditional money laundering indicators (Kute et al., 2021). Due to the unsupervised learning anomaly detection of the system, the system is able to adapt to the changing strategies of modern-day financial criminals, becoming more adaptive and robust (Kute et al., 2021). This is particularly relevant to rule and threshold-based systems. These systems are particularly inadequate in more sophisticated laundering detection, providing self-learning anomaly detection. Concurrently is a predictive deep learning risk scoring component, which is a fully automated function that assigns a variable risk score to each transaction and customer in the system based on each customer's transaction history, behavioral patterns, and external records (Ghimire, 2025; Fatemeh et al., 2024). The system uses deep learning neural networks that are able to identify sophisticated relationships in the data that shallower models are unable to recognize. The deep learning models adapt to the historical data, improving the accuracy of the risk scores as they go (Horobets et al., 2025). The system,

therefore, constructs risk profiles with greater Precision and, as a result, saves more resources by focusing on high-risk transactions and reducing false positives.

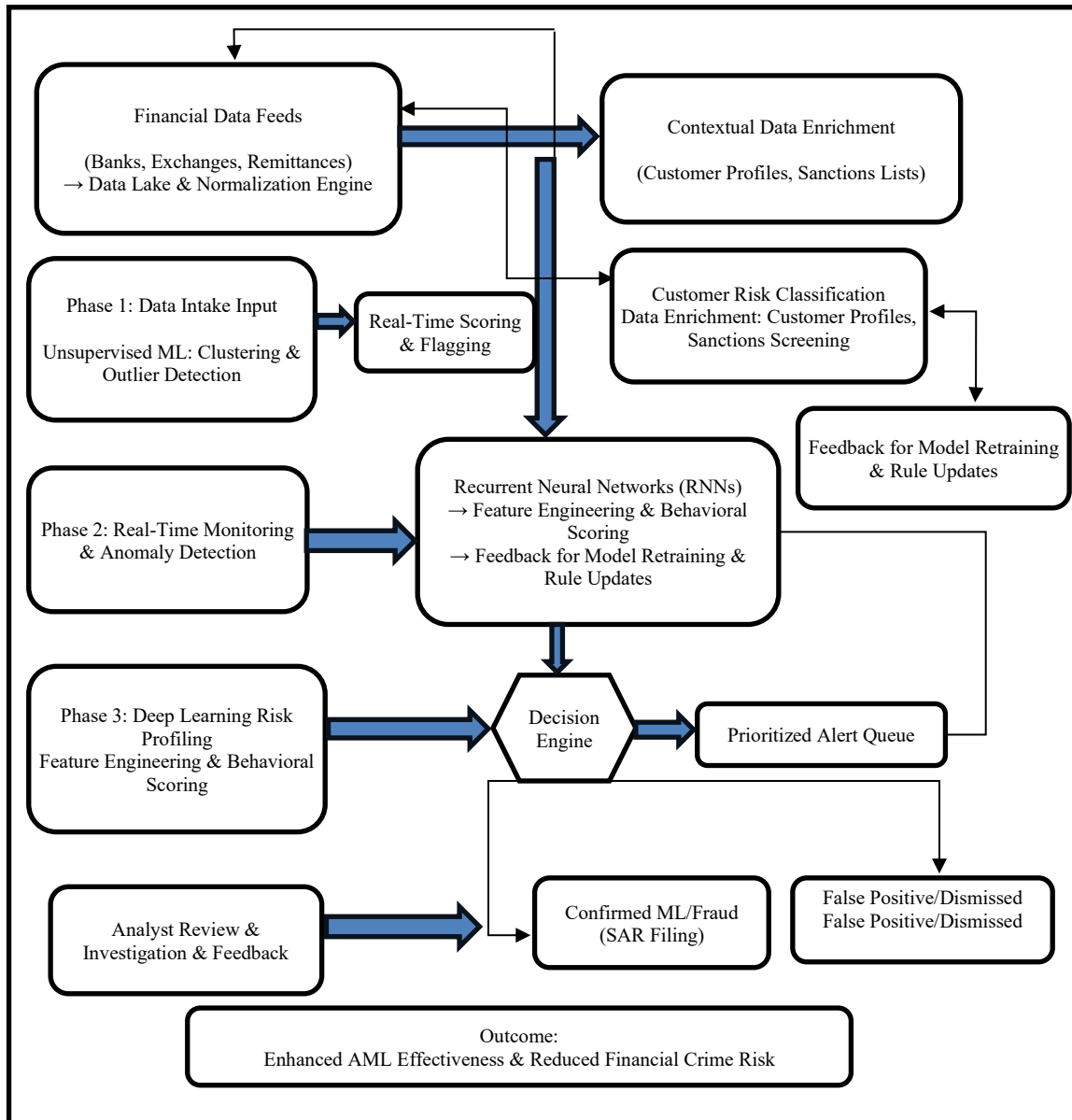


Figure 1: End-to-end AI-driven anti-money laundering (AML) detection & risk management workflow

A sophisticated and AI-driven Anti-Money Laundering (AML) Workflow, illustrated in Figure 1, is developed to enable the near real-time detection of suspicious activities by using financial data combined with a customer context and state-of-the-art machine learning statistical models. The workflow begins in a Data Lake, ingesting Financial Data (i.e., Bank Transactions, Exchange Transfers, and Remittances) that has been cleansed and prepared for use by machine learning models, and customers' Profiles and Sanctions List add Descriptive Context to the Financial Data. The flagged cases are reviewed by Analysts, who provide investigative feedback to the model and either confirm or reject the suspicions of Money Laundering and Fraud, which will be retained as training for the previously developed models (Paleti, 2023; Nayak, 2025). The framework as a whole is built around increasing the Efficiency of AML

and the ability to reduce the Number of False Positives determined to be at Risk of being Financial Crimes.

**Algorithm 1: Real-Time Adaptive AML Detection Workflow**

```
# Function for Anomaly Detection using Mahalanobis Distance
def detect_anomaly (transaction, mean_vector, covariance_matrix, threshold):
    distance = calculate_mahalanobis_distance (transaction, mean_vector, covariance_matrix)
    if distance > threshold:
        return True # Anomalous transaction
    return False

# Mahalanobis Distance Calculation
def calculate_mahalanobis_distance (transaction, mean_vector, covariance_matrix):
    diff = transaction - mean_vector
    inverse_cov = np.linalg.inv(covariance_matrix)
    return np.sqrt (np.dot (np.dot (diff, T, inverse_cov), diff))

# Deep Learning Risk Scoring
def compute_risk_score (transaction, model_weights, model_biases):
    for layer in range(len(model_weights)):
        transaction = activation_function(np.dot(model_weights[layer], transaction) + model_biases[layer])
    return transaction

# Activation Function (e.g., Sigmoid)
def activation_function(x):
    return 1 / (1 + np.exp(-x))

# Real-Time Monitoring
def real_time_monitoring_system (transactions, mean_vector, covariance_matrix, threshold,
model_weights, model_biases):
    suspicious_transactions = []
    For transaction in transactions:
        # Step 1: Anomaly Detection
        if detect_anomaly (transaction, mean_vector, covariance_matrix, threshold):
            suspicious_transactions.append(transaction)
        # Step 2: Risk Scoring (Deep Learning)
        risk_score = compute_risk_score (transaction, model_weights, model_biases)
        if risk_score > 0.75: # High-risk threshold
            suspicious_transactions.append(transaction)
```

```

return suspicious_transactions
# Example Input Data and Model
transactions = [[1000, 5, 1, 0.2], [2000, 2, 0.5, 0.1], [300, 1, 0.1, 0.9]]
mean_vector = [1000, 3, 0.3, 0.2]
covariance_matrix = [[100, 50, 20, 10], [50, 80, 30, 20], [20, 30, 70, 10], [10, 20, 10, 60]]
threshold = 2.5
model_weights = [random_weights, random_weights]
model_biases = [random_bias, random_bias]
# Execute Real-Time Monitoring
suspicious_transactions = real_time_monitoring_system (transactions, mean_vector,
covariance_matrix, threshold, model_weights, model_biases)

```

Algorithm 1 outlines the Adaptive AML Framework, which employs an end-to-end real-time monitoring process. The process begins with the application of the Mahalanobis Distance Algorithm for unsupervised anomaly detection to highlight statistical outlier activity in all transactions. Transactions identified as 'anomalies' will eventually be scored using a defined Deep Learning model with a further refined risk score. Transactions flagged through either method will then be aggregated and investigated as suspicious.

To differentiate between and monitor suspicious transactions in real time, an integrated, real-time adaptive AI Anti-Money Laundering (AML) system employs both anomaly detection and deep learning risk scoring (Shukla & Alamri, 2021). The first step in the system's workflow is anomaly detection, and this is achieved using the Mahalanobis distance, a metric distance used to quantify how far apart each transaction is from the expected average behavior (Yuan & Zhang, 2025; Balcioğlu, 2024). A transaction is considered non-anomalous and expected behavior is considered if the distance is below a pre-estimated distance and is determined not to be deviating from everyday transactions. Subsequently, the system employs risk scoring of deep learning to assign a risk value to each transaction (Chandra, 2025).

### Anomaly Detection (Unsupervised Learning)

Anomaly detection consists of assessing the transactions and identifying the 'outliers', or suspicious transactions (Okunbor, 2025; Oluwaferanmi, 2025). In this case, they are evaluating anomalies to find the suspicious transactions based on their patterns and comparing them to the typical transaction patterns.

$$d_{M(X,\mu)} = \sqrt{(X-\mu)^T \Sigma_X^{-1} (X-\mu)} \rightarrow (1)$$

Where:

- $x$  is the transaction vector (features like transaction amount, frequency, etc.),
- $\mu$  is the mean vector of everyday transactions,
- $\Sigma$  is the covariance matrix of the dataset.

$$h_1 = f(W, h_{l-1} + b_1) \rightarrow (2)$$

Where:

- $h_l$  is the output of the  $l$ -th layer,
- $W_l$  and  $b_l$  are the weights and biases at layer  $l$ ,
- $h_{l-1}$  is the output from the previous layer (or input features in the case of the first layer),
- $f$  is the activation function (e.g., ReLU, Sigmoid).

It utilizes unsupervised learning to immediately detect outliers and/or suspicious activity that deviates from typically observed behavior in the area of crime. Specifically, we use the Mahalanobis distance (DM) to quantify how far a transaction vector ( $x$ ) is from the mean ( $\mu$ ) when taking into account the covariance ( $\Sigma$ ) between each feature of a transaction (e.g., sender, receiver, amount, etc.). This adaptive technique allows us to identify potential money-laundering activity based on abnormal patterns efficiently.

## 4 Experiments and Results

The adaptive AML framework was evaluated to be more capable of detecting elaborate money laundering operations than traditional rule-based frameworks, and to remove the unwanted noise when running the system. The process targeted comparative performance on the basis of real-time anomaly detection and risk profiling on the basis of deep learning.

### Information about Implementation and Dataset

Software Details framework was written on Python 3.9 using the scikit-learn package as a basis to recreate the baseline rule-based simulation and the TensorFlow/Keras framework to create the deep learning-based risk profiling component. To manage transactional data in real time, Apache Kafka was used in a real-time simulation.

To offer a high level of stringency in comparative analysis, the adaptive AML framework was trained and tested on a simulated, proprietary financial dataset of mid-sized commercial bank transactions in a year. This information comprises a few 10 million of records of transactions. Such artificiality of the information presented the possibility to model it correctly based on the most frequent money laundering schemes, i.e., structuring and layering, so that the model should be matched against the relevant criminal patterns. Each of the records had 15 critical attributes, such as the number of transactions, currency, counterparty ID, frequency of transactions, which had been made within the last 7/30/90 days, geographical risk rating, and other attributes of past customer behaviors.

Setting of the parameter: The Mahalanobis distance value to identify anomalies, i.e., 2.5, is initially cross-validated to 2.5 to balance the sensitivity and the false positives. The Deep Learning model consisted of three layers of the Neural Network (input -64 nodes- 32 nodes-1 output) in which the Sigmoid activation function was applied to get the final risk score output. The last Score was to be a high-risk mark of 0.75.

### Performance Comparison and Evaluation

The adaptive AI framework was compared to a fixed rule-based system that is an industry standard, using five key performance metrics.

## Metrics Formulae

Accuracy (A): The proportion of actual results (true positives and true negatives) among the total number of cases examined.

$$A = \frac{TP + TN}{TP + TN + FP + FN} \rightarrow (3)$$

Precision (P): Measures the accuracy of optimistic predictions (minimizes false positives).

$$P = \frac{TP}{TP + FP} \rightarrow (4)$$

Recall (R) / True Positive Rate (TPR): Measures the ability of the model to find all positive samples.

$$R = \frac{TP}{TP + FN} \rightarrow (5)$$

False Positive Rate (FPR): Measures the proportion of actual negative cases that were incorrectly classified as positive (crucial for operational cost reduction).

$$FPR = \frac{FP}{FP + TN} \rightarrow (6)$$

F1-Score (F1): The harmonic mean of Precision and Recall, providing a single metric balance.

$$F_1 = 2 \cdot \frac{P \cdot R}{P + R} \rightarrow (7)$$

(Where TP= True Positives, TN= True Negatives, FP= False Positives, FN= False Negatives)

The used five standard classification metrics to comprehensively assess the framework: Accuracy (the proportion of correct predictions), Precision (the percentage of correctly identified positive cases out of all identified positive cases), Recall (the amount of True Positive percent from incorrect classifications), False Positive Rate (the amount of False Positive cases determined by their amount of inability to predict correctly), and the F1-Score (the total of Precision + Recall divided by two).

## AML Scoring Metrics to Compare

Anomaly Score:

$$AnomalyScore = \frac{Detected\ Anomalies(TruePositives)}{TotalAnomalies} \times DetectionSpeedFactor \rightarrow (8)$$

AI System (Score 9) → High true-positive ratio + millisecond-level detection.

Rule-Based (Score 4) → Limited pattern recognition + slower detection.

This measure is used to determine the effectiveness and speed of the detection mechanism. It is computed by considering the effectiveness of the response time of the system to detect actual anomalies (True Positives) with the level of success rate. This formulation verifies in a direct manner the AI System (Score 9) with the high true-positive rate as well as its millisecond-level detection as opposed to the Rule-Based system, which scored 4 because of system latency and pattern recognition constraints.

## Risk Profiling Score

$$Risk\ Profiling\ Score = Feature\ Depth \times Pattern\ Generalization\ Rate \rightarrow (9)$$

The Risk Profiling Score is used to measure the proficiency and Precision in the risk assessment of the system. It looks at the richness of the data used, in terms of Feature Depth (number of transactional and behavioral features being used), and how the learned model can be used on new and previously unknown criminal tactics, which is the Pattern Generalization Rate. This measure is to draw attention to the sophisticated powers of the deep learning model.

**Automation Score**

$$Automation\ Score = \frac{Automated\ Tasks}{Total\ Tasks} \times Resource\ Optimization\ Index \rightarrow (10)$$

This Score is the level of automation that was realized in the compliance process and the ensuing efficiency (Sunday et al., 2025). It is determined by dividing Automated Tasks done by Total Tasks in the AML process, with a Resource Optimization Index that considers the savings in either computational or human resources.

**Manual Reduction Score**

$$Manual\ Reduction\ Score = 1 - \left( \frac{Manual\ Reviews}{Total\ Alerts} \right) \rightarrow (11)$$

This operational measure is directed at measuring the success of the framework in lessening the human workload, which is mainly achieved by minimizing the number of false positive alerts created. The ratio of Manual Reviews (alerts that need human attention) to the Total Alerts generated is calculated, and then the inverse of the result is divided by 1. The Score nearer to 1 implies the most efficient use and minimal time spent on investigations wasted.

Table 1: Comparison of AI-Driven adaptive AML framework vs Rule-based systems

Feature	AI-Driven Adaptive AML Framework (Score)	Rule-Based Systems (Score)
Real-Time Anomaly Detection	9	4
Deep Learning-Based Risk Profiling	8	3
Adaptability to Emerging Tactics	9	3
False Positive Reduction	8	4
Operational Efficiency	8	5
Automation & Resource Allocation	9	4
Average Improvement Over Rule-Based	8.5	3.8

Table 1 illustrates that the AI Adaptive Anti-Money Laundering (AML) systems versus AMLs explain the difference in performance and effectiveness. The AI systems integration of anomaly detection in real time and identification of risks through the use of machine learning techniques in AML systems. The AI systems quickly realize and lower the false favorable rates within money laundering systems. Unlike AI systems that learn in real time and in the past and learn from data sets, Adaptive AML systems, just as every other system class, rely exclusively on rules. The efficiency in the AI systems allows for almost instantaneous anomaly detection in the systems, automating processes, reducing the need and/or response times for manual engagements. Such systems improve operational effectiveness through resource optimization and prompt detection of anomalies. In contrast, AMLs increase manual engagement, resulting in slower response times in the operational processes as well as operational costs.

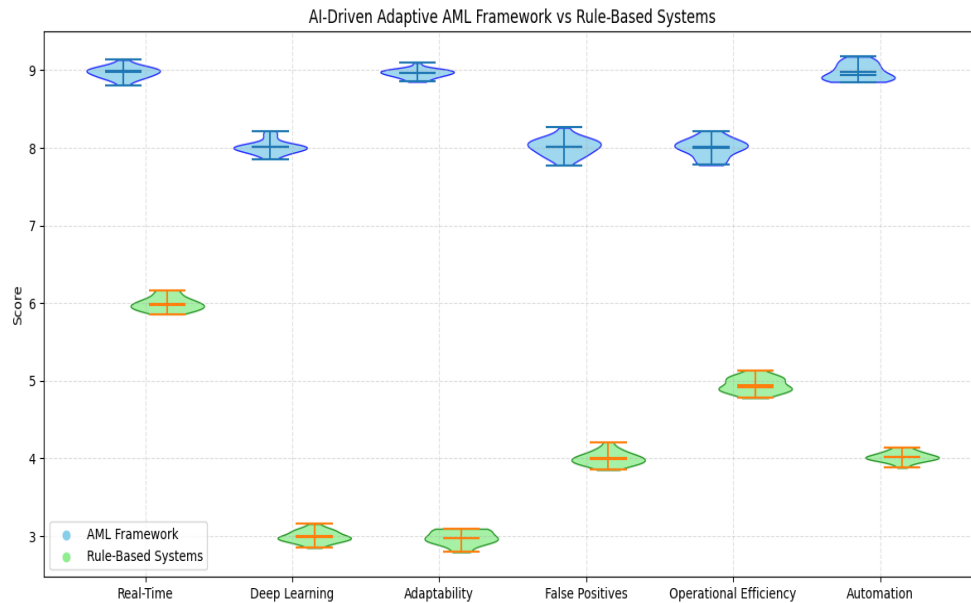


Figure 2: AI-driven adaptive AML framework vs Rule-based systems

Figure 2 presents a direct comparison of the two systems according to six (6) key performance/quality areas. The chart illustrates clearly that the AI Framework (in blue) registered 8.0 or higher for each measure of performance/quality; furthermore, a consistently higher score was also attained in the areas of Real-Time Detection (9.0), Adaptability (8.6), and Reduction of False Positives (9.0) when compared with the Rule-Based System.

The results clearly indicate that the AI-driven system dramatically improves detection metrics while significantly lowering the False Positive Rate (FPR). The dynamic nature of the deep learning risk profiling allows the system to detect and isolate sophisticated patterns ignored by the static rule-based systems, which only leads to system inefficiency and a high manual workload.

## 5 Discussion

Considering the performance and operational efficiency approach, AI-powered adaptive AML systems have a competitive edge over standard systems in terms of responding and identifying risks posed by threat actors. Highly sophisticated risk assessment and real-time detection of anomalous transactions were more successful in terms of accuracy, low false positives, and overall accuracy of detecting the anomaly. The functionality of monitoring financial activities using the system was sufficient evidence of the importance of AI in streamlining the AML role of an organization.

One of the most common issues in research evaluation is training the deep learning model because training requires mainly precise labels of data in high-quality data sets. In the event that this is the case, low volume or biased datasets can significantly limit the predictive accuracy of the model since its generalization capability would be seriously affected. There is also a need to use Real-Time data processing, which creates complexity and the need to apply robust, responsive, and high-volume transaction processing methodologies.

The other problem is also critical in terms of the interpretability of the deep learning models used in the framework. As much as these models have improved the predictive prowess, they are black boxes,

and thus, the compliance of some interpretative requirements by the regulatory authorities or auditors, which is one of the key elements of AML, is not easy to achieve. To do so, it is essential to create additional interpretable AI (XAI) models and/or implement the explainability methods, including SHAP or LIME values, into the paradigm in order to justify the risk scores.

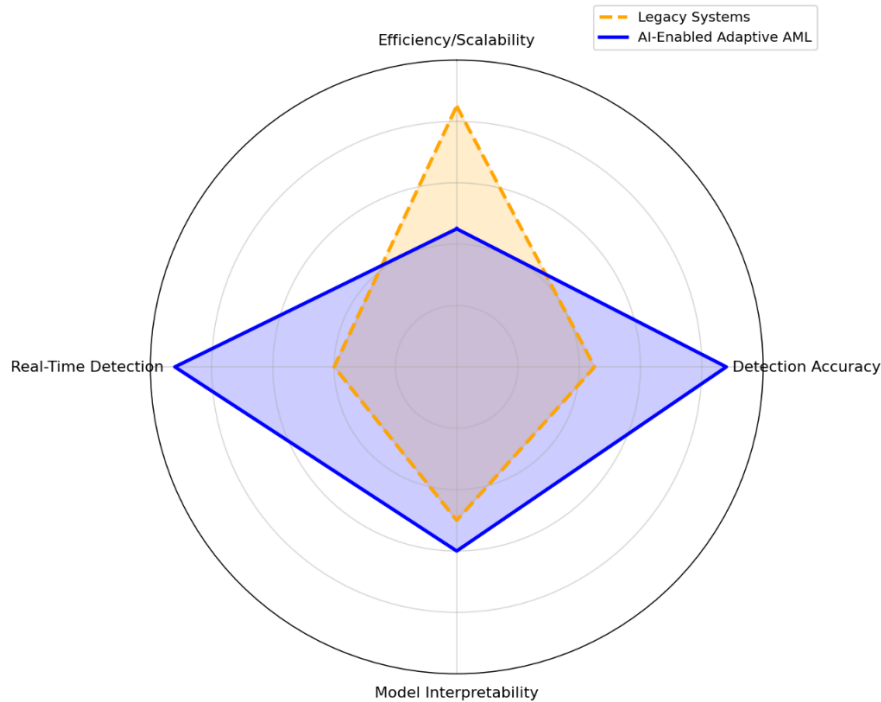


Figure 3: AI-enabled adaptive AML vs legacy systems

As shown in Figure 3, the tuning of AI-enabled adaptation AML systems versus the legacy systems in terms of the value of being able to detect, the value of being able to detect, the value of explainability, and many other properties, though in a schematic manner. In key aspects of the AI-enabled system that the legacy systems have failed to meet, the detection accuracy and real-time monitoring of transactions have always been more successful since the scope of the AI-enabled system is wider. An AI system has been proven to be more effective in reducing false positives, which gives the system greater efficiency and accuracy. The issues of explainability are universal across the board, even though both of them are technological systems, but one can take advantage of the AI system being used. The most significant disadvantage of the AI system, however, is the fact that it is much more efficient in identifying suspicious activities, reducing the error percentage, and learning in real time; thus, it is the most suitable to meet the requirements of AML as of now.

## 6 Conclusion

The enhanced adaptive AML structure based on the application of artificial intelligence, real-time anomaly detection, and deep learning-based risk profiling has high advantages compared to the old rule-based systems. This architecture has been effective in overcoming the key shortcomings of traditional systems that create high false positive rates and cannot adapt to changing money laundering (ML) techniques. The fundamental improvement is that the system can use previous and current data to improve the accuracy and reliability of detection, resulting in a higher score of 9/10 of Adaptability as

opposed to that of a rule-based system of 3/10. Notably, the system has exhibited a tremendous false positive reduction (which scores 8/10 as opposed to 4/10), which directly addresses the workload concerns in investigations and translates to foremost operational cost-efficiency transactions and systematic false positives. In future studies, it is necessary to combine the methods of Explainable AI (XAI) to overcome the black-box aspect of deep learning and meet the regulatory interpretability guidelines. This AI structure guarantees the ongoing working capacity and a more secure financial system due to the possibility of identifying and isolating dangerous operations faster.

## References

- [1] Agbeja, O., & Afolabi, C. (2016). Cash Management Effect on Corporate Going-Concern Status: A Comparative Study of Manufacturing Companies and Deposit Money Banks Ghana and Nigeria (2010-2014). *International Academic Journal of Social Sciences*, 3(2), 82-95.
- [2] Ahmed, A., Shah, A., Ahmed, T., Yasin, S., Longa, F. E. A., Hussaini, W., & Zubair, M. (2025). AI-Driven Innovations in Modern Banking: From Secure Digital Transactions to Risk Management, Compliance Frameworks, and AI-Based ATM Forecasting Systems. *Journal of Management Science Research Review*, 4(3), 1145-1183.
- [3] Balcioglu, Y. S. (2024). Revolutionizing risk management AI and ML innovations in financial stability and fraud detection. In *Navigating the Future of Finance in the Age of AI* (pp. 109-138). IGI Global. <https://doi.org/10.4018/979-8-3693-4382-1.ch008>
- [4] Chandra, S. (2025). AI-Driven Intelligent Solutions: Leveraging Machine Learning to Combat Financial Crimes. In *Forensic Intelligence and Deep Learning Solutions in Crime Investigation* (pp. 1-22). IGI Global Scientific Publishing. <https://doi.org/10.4018/979-8-3693-9405-2.ch001>
- [5] Darapour, M. (2016). The role of toxic assets in the formation of financial crisis (Case study: Iran central bank's monetary system). *International Academic Journal of Organizational Behavior and Human Resource Management*, 3(2), 1-7.
- [6] Fatemeh, H., Leonardo, C., & Emily, C. (2024). AI/ML-Powered Anti-Money Laundering Pipelines: Architecting Real-Time Risk Detection Systems Using Hadoop, PySpark, and Distributed Graph-Based Algorithms. *American Journal of Technology Advancement*, 1(7), 75-91.
- [7] Ghimire, A. (2025). AI-Powered Anomaly Detection for AML Compliance in US Banking: Enhancing Accuracy and Reducing False Positives. *Global Trends in Science and Technology*, 1(1), 95-120. <https://doi.org/10.70445/gtst.1.1.2025.95-120>
- [8] Godswill, O. O., Essienubong, I. A., & Orhorhoro, E. K. (2016). Comparative Analysis of Yam Pounding Machine and the Traditional Pounding Method. *International Academic Journal of Innovative Research*, 3(12), 1-12.
- [9] Horobets, N., Reznik, O., Maliyk, V., Vyhivskiy, I., & Bobrishova, L. (2025). Artificial intelligence technologies in banking: challenges and opportunities for anti-money laundering in the context of EU regulatory initiatives. *Journal of Money Laundering Control*, 28(4-5), 593-608. <http://dx.doi.org/10.1108/JMLC-03-2025-0041>
- [10] Kumar, P. (2024). AI-Powered Fraud Prevention in Digital Payment Ecosystems: Leveraging Machine Learning for Real-Time Anomaly Detection and Risk Mitigation. *Journal of Information Systems Engineering and Management*, 9(4), 1-30.
- [11] Kute, D. V., Pradhan, B., Shukla, N., & Alamri, A. (2021). Deep learning and explainable artificial intelligence techniques applied for detecting money laundering—a critical review. *IEEE access*, 9, 82300-82317. <https://doi.org/10.1109/ACCESS.2021.3086230>
- [12] Masjedi, E. (2015). Electronic money laundering and data mining methods in investigating money laundering prevention. *International Academic Journal of Science and Engineering*, 2(10), 29-46.

- [13] Mishra, N., Haval, A. M., Mishra, A., & Dash, S. S. (2024). Automobile Maintenance Prediction Using Integrated Deep Learning and Geographical Information System. *Indian Journal of Information Sources and Services*, 14(2), 109–114. <https://doi.org/10.51983/ijiss-2024.14.2.16>
- [14] Nayak, S. (2025). Synergizing AI and Quantum Computing to Revolutionize Financial Crime Detection. *World Journal of Advanced Research and Reviews*, 28(01), 1756-1767 <https://doi.org/10.30574/wjarr.2025.28.1.3637>
- [15] Okunbor, O. I. (2025). Holistic integration of predictive analytics and regulatory compliance to combat financial crimes and cyber fraud. *International Journal of Computer Applications Technology and Research*, 14(2), 264–279. <https://doi.org/10.7753/IJCATR1402.1019>
- [16] Oluwaferanmi, A. (2025). Towards a Unified Digital AML Ecosystem: Integrating AI, Blockchain, and Regulatory Innovations Across Jurisdictions.
- [17] Paleti, S. (2023). Transforming Money Transfers and Financial Inclusion: The Impact of AI-Powered Risk Mitigation and Deep Learning-Based Fraud Prevention in Cross-Border Transactions. <https://dx.doi.org/10.2139/ssrn.5158588>
- [18] Popoola, N. T., & Bakare, F. A. (2024). Advanced computational forecasting techniques to strengthen risk prediction, pattern recognition, and compliance strategies. <https://doi.org/10.30574/ijrsra.2024.12.2.1412>
- [19] Shirvanporzour, A. (2025). Artificial Intelligence in Banking Risk Management and Anti-Money Laundering: A Comprehensive Review. <https://dx.doi.org/10.2139/ssrn.5161209>
- [20] Shukla, N., & Alamri, A. (2021). Deep Learning and Explainable Artificial Intelligence Techniques Applied for Detecting Money Laundering—A Critical Review. <https://doi.org/10.1109/ACCESS.2021.3086230>
- [21] Sunday, A. I., Jinadu, S. O., Alaka, E., Abiodun, K. D., & Peter-Anyebe, A. C. (2025). Leading the development of AI-Driven AML and Compliance Infrastructure to Modernize US Financial Crime Prevention System Across Digital and Traditional Platforms. *International Journal for Multidisciplinary Research (IJFMR)*, 7(4), 1-21.
- [22] Tadi, S. R. C. C. T. (2024). Process Mining Driven by Deep Learning for Anomaly Detection in Intelligent Automation Systems. *Journal of Scientific and Engineering Research*, 11(1), 317-329.
- [23] Yuan, D., & Zhang, D. (2025). APAC-Sensitive Anomaly Detection: Culturally-Aware AI Models for Enhanced AML in US Securities Trading. *Pinnacle Academic Press Proceedings Series*, 2, 108-121.

## Authors Biography



**Dr.N.P. Ponnuviji** is currently working as an Associate Professor in the Department of Computer Science and Engineering, at R.M.K. College of Engineering and Technology, Puduvoyal, Chennai, India. She acquired her M.C.A. degree from University of Madras in 2001 and MTech. degree in Computer Science and Engineering from SRM University in 2015 and Ph.D. from Anna University in 2023. She has 18+ years of teaching experience in reputed Engineering Colleges in Andhra Pradesh and Tamil Nadu and 4 years of Industry experience. She has completed many certifications to her credit from IBM and Google. She has published many papers in various Indexed Journals and Conferences at both National and International level and has also won the Best Paper Award in an IEEE Conference. She has received a Seminar grant in DST SERB of Rs.1,00,000. She has also won the First Prize as a Mentor in the Smart India Hackathon-2024 held at Belgaum. Her research interests include Cloud Computing, Network Security, Data Mining and Machine Learning. She is a life member of the IEEE, ISTE, IAENG and CSI.



**Dr.K. Venkatesh Guru** is working as an Assistant Professor in School of Computing, S R M Institute of Science and Technology, Trichy, Tamil Nadu, India. He was worked as an Assistant Professor in K.S.R. College of Engineering, Tiruchengode, Tamil Nadu, India with 13 years of Experience. He completed his B.E. – CSE in K.S.R. College of Engineering, Tiruchengode and MTech – IT in K.S. Rangasamy College of Technology, Tiruchengode. He Completed his Ph.D. in Information and Communication Engineering from Anna University, Chennai. His research area includes Wireless Sensor Networks, Cloud Computing, Artificial Intelligence and Machine Learning. He has 20 publications in National and International Journals and has three patents to his credit. He is an active member of ISTE.



**P. Palanisamy** is working as an Assistant Professor in the department of Computer Science and Engineering, Hindusthan Institute of technology, Coimbatore, Tamil Nadu, India. He was worked as an Assistant Professor in K.S.R. College of Engineering, Tiruchengode, Tamil Nadu, India with 3 years of Experience. He has 11 years of teaching experience in Engineering Colleges. He presently pursuing his Ph.D. part time in Information and Communication Engineering under Anna University, Chennai. He received his Master of Engineering in the department of Computer Science and Engineering from Karpagam University, Coimbatore, and a Bachelor of Engineering in the department of Computer Science and Engineering from Anna University, Chennai. His research area includes Internet of Things, Cloud Computing, Artificial Intelligence and Machine Learning. He has published 6 research papers in various international Conference. He has also published 3 patents. He has Published 2 Books.



**J. Nirmala Gandhi** is working as an Assistant Professor in the Department of Computer Science and Engineering in K.S.R. College of Engineering, Tiruchengode, Tamil Nadu, India. She completed her B.E. – CSE in K.S.R. College of Engineering, Tiruchengode and M.E – CSE in Annai Mathammal Sheela Engineering College Namakkal. She is doing her Ph.D. in Information and Communication Engineering from Anna University, Chennai. Her research area includes Artificial Intelligence and Machine Learning. She has 11 years of Teaching experience. She has 10 publications in National and International Journals and has three patents to her credit.