Machine Intelligence Research
www.mi-research.net

22(5), October 2025, 929-940
DOI: 10.1007/s11633-025-1550-8

Anti-Money Laundering (AML) & Compliance: Enhancing Transaction Monitoring and Fraud Detection Using AI Algorithms

Sukumar Reddy Beereddy[1*], Kiran Kumar K[2]

[1*] Treasury and Financial Risk Management Lead (SAP)

[2] Treasury and Financial Risk Management and Banking Lead (SAP)

*Corresponding Author Email: sbeereddy1120@gmail.com

Abstract: Traditional rule-based anti-money laundering (AML) systems struggle to detect modern financial fraud exploiting transaction sequences, structures, and behavioural patterns. This study proposes a hybrid framework combining XGBoost, Long Short-Term Memory (LSTM) networks, and Graph Neural Networks (GNNs) for AML detection, evaluated using the IBM AML Transactions dataset with SMOTE oversampling, feature engineering, and graph construction. Results show XGBoost achieves high precision for everyday transactions but detects few fraudulent cases (0.06), while LSTM fails to identify laundering schemes. GNNs demonstrate potential to model transaction structures linked to washing rings and detect patterns like structuring, layering, and circular flows beyond static threshold-based systems. A two-stage method integrating XGBoost filtering with GNN-based clustering of high-risk entities is proposed, providing a unified model assessment and practical implementation guidelines for explainable ensemble-based AML frameworks to enhance enterprise detection workflows.

Keywords: Anti-Money Laundering, AI, Machine Learning, SAP TRM, Murex, XGBoost, LSTM, Graph Neural Networks, Financial Fraud Detection, Compliance

Citation: Sukumar Reddy Beereddy, Kiran Kumar K. Anti-Money Laundering (AML) & Compliance: Enhancing Transaction Monitoring and Fraud Detection Using AI Algorithms. *Machine Intelligence Research*, vol.22, no.5, pp.929–940, 2025. http://doi.org/10.1007/ s11633-025-1550-8

1 Introduction

The global financial environment faces an escalating danger from money laundering, which continues to develop while spreading throughout the system [1]. Illicit financial operations use advanced techniques that make it difficult for conventional security measures to detect and stop such threats promptly [1]. Money laundering turns criminal money into legitimate income, which simultaneously sabotages financial systems while funding various forms of criminal operations such as terrorism, drug trafficking, and corruption [2]. The United Nations Office on Drugs and Crime (UNODC) reports that annual money laundering operations amount to 2–5% of global GDP, corresponding to between $800 billion and $2 trillion [3]. The large amount of money lost to financial fraud demands innovative and flexible systems to fight against fraudulent practices. The interconnected global commerce requires financial institutions to function as primary defenders against money laundering, so they must implement complete proactive Anti-Money Laundering frameworks [4].

Fraudulent transactions have become more complex because of the speed of digitalisation, cryptocurrency adoption, shell company growth, and multi-jurisdictional account usage. Fraudsters exploit system weaknesses by utilising laundering methods, including layering techniques, smurfing, and trade-based laundering to hide illegal money sources [4]. The schemes prove hard to detect because banks handle millions of daily financial transactions. Because of this challenge, compliance teams find it increasingly difficult to uncover subtle suspicious signs [4]. AML compliance has emerged as a vital responsibility since it is among the most essential in the banking and financial services industries [5]. Organisations that run effective AML programs manage to protect consumer faith while protecting their market position and maintaining financial stability [5].

Research Article
Manuscript received on May 30, 2024; accepted on February 25, 2025
Recommended by Associate Editor Harish Garg
Colored figures are available in the online version at https://link.springer.com/journal/11633

Multiple international and regional money laundering regulations exist to provide standardisation and a legal framework for anti-money laundering activities. Four essential global and regional AML rules make up the Financial Action Task Force (FATF) recommendations and Bank Secrecy Act (BSA), USA PATRIOT Act, and Basel III [6]. Financial institutions must adhere to strict guidelines from these frameworks by doing KYC procedures, SAR reporting, risk profiling customers, and monitoring transactions [5]. The standard operation of traditional systems implementing AML functions relies on static engines which function through predefined rules. Such systems show good compliance, trackability, and transparency but have severe operational constraints. False positive incidents combined with slow detection create two significant issues that waste company resources and exhaust the capacity of compliance analysts [7,8].

AI and machine learning (ML) capabilities will substantially improve modern AML procedures. Real-time processing of enormous data volumes, including structured and unstructured content, enables AI systems to detect dynamic fraud [9,10]. Machine learning algorithms identify irregular customer purchasing patterns to detect abnormal payment systems between bank accounts [11]. These operational capabilities are essential when fraudsters continuously modify their methods to avoid set rule-based security protocols [11].

Using AI/ML technology to build AML systems successfully minimises the frequency of inaccurate responses, also known as false positives, which have traditionally plagued conventional systems. When false alerts persist to overwhelm compliance staff members, they cause potentially suspicious transactions to become buried within the stream of acquired information. The predictive analysis of complex transnational relationships, along with advanced prediction power, is achieved through AI models that include XGBoost and Long Short-Term Memory (LSTM) networks and Graph Neural Networks (GNNS) [12]. Because graph neural networks deliver superior capabilities for processing inter-entity connections in financial transaction networks, they are the most helpful in identifying money laundering structures and complex financial fraud schemes. The LSTM architecture can identify recurring transaction sequences and temporal patterns, which help to detect suspicious behaviour [13].

Research seeks to connect enterprise transaction platforms to contemporary AI through an evaluation process of integrating machine learning into AML systems. Evaluating three AI models, including XGBoost, LSTM, and GNN, is the initial goal for detecting laundering activities in transactional datasets. The second fundamental goal of this assessment concerns determining how well these models perform in decreasing false positives and boosting AML operational efficiency. The last objective targets improving the SAP TRM and Murex platforms by adding AI systems that detect real-time anomalies while performing risk assessments. Standard evaluation tests measuring precision, recall, F1-score and ROC-AUC will be used to determine which model selection is the optimal candidate for operational implementation within compliance frameworks.

This study expands knowledge of AI-enabled AML systems while delivering helpful information to banks, FinTech firms, and regulatory bodies. The research provides framework standards for deploying explorable and rule-compliant financial crime detection systems that can adapt to future financial crime developments by evaluating model properties in realistic AML datasets.

2 RELATED WORK

A. Anti-Money Laundering (AML) Frameworks & Regulations

Anti-Money Laundering (AML) frameworks protect against corruption in both domestic and international financial systems [14]. International regulatory organisations and national bodies have set standards to stop criminal economic activities. The Financial Action Task Force (FATF) has held its position as one of the most influential bodies in creating policies that target money laundering and terrorist funding since its establishment in 1989 [15]. The FATF distributes 40 Recommendations, which other agencies accept as universal anti-money laundering (AML) rules. The international guidelines demand institutions to perform comprehensive Customer Due diligence screenings while utilising risk-based protocols, strengthen their transaction monitoring capabilities, and maintain SAR reporting systems [15].

The Bank Secrecy Act (BSA) and the USA PATRIOT Act are the backbone of AML regulations [16]. Financial institutions under the BSA must create extensive records and file reports on cash deals above predefined values. At the same time, the PATRIOT Act helps the government fight money laundering and terrorist financing. The U.S. Department of the Treasury, through its Financial Crimes Enforcement Network bureau, regulates and enforces American Bank Secrecy Act compliance among financial institutions operating within the nation [16].

Basel III standards operate at global banking institutions to improve financial transparency through capital and liquidity requirements, decreasing risks for the overall monetary system [17]. Institutions must create real-time suspicious behaviour detection systems for their transaction monitoring processes through this regulatory framework. These frameworks deliver effective results because the work depends on how well financial institutions can implement technological and analytics solutions that are compliant with regulatory requirements [18].

B. SAP TRM & Murex in AML Compliance

The enterprise financial management field heavily uses SAP Treasury and Risk Management (SAP TRM) and Murex as its central systems for treasury operations, market risk assessment, and regulatory

reporting [19]. The built-in AML compliance features of these banking systems do not meet the highest standards of today's financial sector [20]. The basic rule-triggered security features of SAP TRM interact with external data streams to assess counterparty security risks. Yet, they do not achieve optimal flexibility or fast prevention of emerging fraud threats. Murex operates risk-based monitoring but requires additional features to detect new laundering patterns that change throughout the year [20].

Three fundamental challenges restrict the successful use of SAP TRM and Murex for AML implementation. Large-scale transaction monitoring faces severe inefficiency challenges because financial transactions grow exponentially [19]. Despite their limited capabilities for fraud analytics, financial reporting, and treasury operations were the primary purposes when designing these systems. These systems cannot detect fraud instantly, delaying the detection of suspicious activities. The high number of wrong alarms from static rule engines creates operational waste because compliance staff devotes extensive time to follow up on regular transactions instead of actual threats. Current transaction monitoring platforms require improved functionality from AI because these systems need advanced capabilities that will work without disruption.

C. AI/ML Approaches in Financial Fraud Detection

Financial companies worldwide have incorporated AI alongside machine learning methods in the last ten years because rule-based AML systems proved insufficient. Traditional systems detect risk by setting minimum/threshold values and problem-solving systems to recognise suspicious transactions above defined monetary amounts or between specific risky geographic locations [18]. Mainstream AML systems prove both easy to audit and transparent, but they create excessive false alerts and cannot identify complicated fraudulent schemes that avoid standard patterns.

Anomaly detection with machine learning technologies provides an improvement through which they learn transaction patterns to identify activities that deviate from established norms [20]. In recent years, deep learning strategies, including Long Short-Term Memory (LSTM) networks together with Convolutional Neural Networks (CNNS), have emerged as powerful tools for Anti-Money Laundering (AML) operations throughout the previous few years [17]. LSTM models succeed at modelling sequential dependencies because they integrate memory gate elements. These systems detect sequences of small withdrawals, which frequently precede substantial withdrawals because this pattern represents laundering tactics used by criminals. Using CNNS as a less popular method in AML involves extracting features from transaction grids and behavioural embeddings [13]. Models in ML and DL provide essential components that build intelligent AML systems which respond effectively.

D. Gaps in Current Research That This Paper Addresses

Most recent research accomplishments have not solved several fundamental problems. Research about model effectiveness concentrates on theoretical results while ignoring how such systems would integrate into operational platforms such as SAP TRM and Murex. This paper evaluates the practicality of implementing artificial intelligence-based transaction monitoring functions that improve platform capabilities.

Furthermore, research dedicated to accuracy fails to address the recurring operational issue of false positive reduction, which remains overlooked in current studies. The analysis centres on false alert minimisation because this directly impacts the operational efficiency of compliance staff. Lastly, explainability and scalability analysis exist independently of each other. The study assesses these models' interpretability and efficiency metrics on an enterprise scale during financial data processing. This paper's findings support the academic understanding of AI-integrated AML systems and their practical deployment in financial compliance operations.

3 METHODOLOGY

A. Proposed Methodology Framework

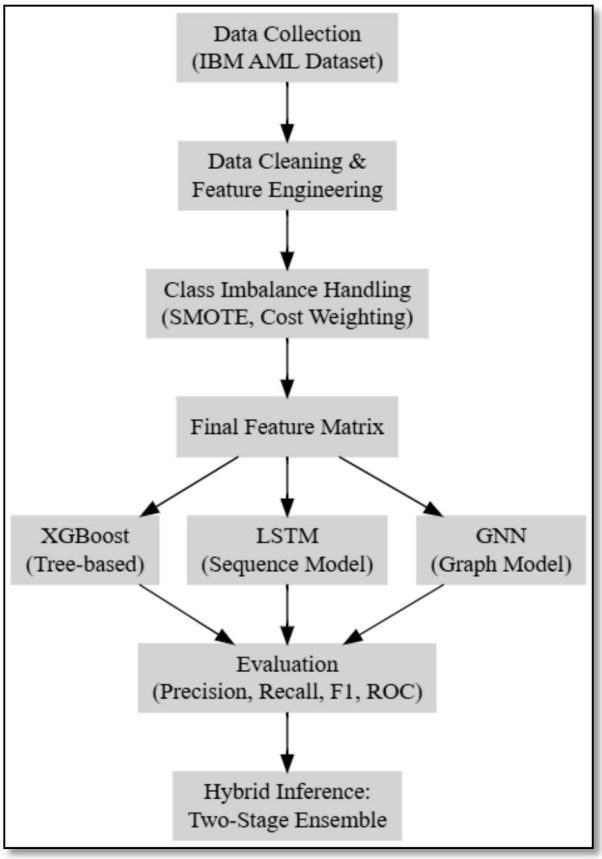

Figure 1. Proposed Methodology Diagram

Figure 1 shows how an AML detection system works through its AI-powered sequence of processes, from data handling to delivering business-ready insights. The system aligns multiple processing techniques with

engineered features and multiple artificial intelligence models, including XGBoost, LSTM, and GNN, to enhance AML detection performance. Organisations can integrate the final output for real-time fraud detection without platform disruptions.

B. Dataset Selection

The research depends on information gathered from the IBM Transactions for AML Dataset (Kaggle Link) for experimental purposes. Despite being artificial, the dataset effectively creates banking transactions that mimic actual bank activities in multiple accounts and financial institutions. AML research requires this dataset because it offers a broad range of features alongside diverse transaction types, jointly with specific fraud labels that separate suspicious transactions from normal ones.

The main elements of the dataset consist of Transaction IDS along with timestamps showing transaction times and sender and receiver identifiers that have gone through de-identification procedures. The essential elements aid the creation of features for time context and interrelationships among data points. Besides numeric values like receipt and payment amounts, the dataset includes type indicators of various transfer methods, including wire transfers, Bitcoin, credit cards and cheque. The fraud variable is a binary target function that distinguishes suspicious transactions (1) from legitimate transactions (0). The quality and usability of the dataset strongly relied on data preprocessing as an essential step. The dataset contained only a few missing values handled through mean or mode replacement techniques: Monday, November 13.

C. AI/ML Models for AML Detection

Three models, including XGBoost, Graph Neural Networks (GNNS), and Long Short-Term Memory (LSTM) networks, formed the foundation for a broad and representative evaluation of artificial intelligence strategies in AML detection. The three AI learning framework models cover gradient boosting, graph-based relational learning, and temporal sequence modelling, allowing a thorough evaluation in all appropriate financial fraud dimensions [21,22].

The employment of Graph Neural Networks (GNNS) allows the system to extract transactional relationships that exist between entities in the dataset. Besides edges representing transactions, the financial dataset can be represented as a directed graph through nodes assigned to sender and receiver accounts. The study applied Graph Convolutional Networks (GCNS) from the GNN family to extract high-level embeddings from nodes and to make classifications based on neighbouring features. GNNS provides robust performance in revealing laundering rings, multi-hop transaction flows, and hidden relationships that tabular data exclusively contains [20]. These systems utilise graphic information at several levels to measure intricate relationships frequently observed in financial fraud systems.

RNNS take the form of LSTM networks, which specialise in understanding the temporal associations that exist within sequences [15]. This architectural design demonstrates maximum effectiveness in detecting money laundering methods that progress over time, including smurfing and layering schemes. The analysis used LSDT models to read transaction chronologically for each entity, which learned behavioural patterns across time intervals. The gating mechanisms and memory cells of LSTM allow the detection of repeated suspicious conduct, combined with the elimination of background noise in transaction behaviour patterns.

D. Model Training & Evaluation

All three models received their training by applying a stratified split of 70-15-15, which distributed the minority class (fraudulent transactions) evenly throughout each part. The minority class fraud samples presented a challenge in the dataset, so we applied the Synthetic Minority Over-sampling Technique (SMOTE) during training to create synthetic duplicates that enhanced model feature recognition abilities.

The model hyperparameters received adjustments through grid search and random search methods based on the model's complexity. XGBoost received optimised adjustments for learning rate, maximum tree depth, and number of estimator parameters. The parameters of LSTM models involved sequence length, hidden units, and dropout rates, in addition to GNN parameters, which included several layers, aggregation strategies, and neighbourhood sampling depth to prevent overfitting.

Different standard classification metrics were used to evaluate the models produced. The evaluation of models used precision to determine which predicted fraud cases matched the actual fraud cases and recall to find the ability of models to detect existing fraud cases. A combination of both metrics was achieved through the F1-score evaluation method. The AUC-ROC tool measured general discrimination capability under multiple classification threshold conditions. The confusion matrix analysis extended our understanding of false positive and false negative statistics because these data points matter for minimising operational costs and regulatory risks in AML systems.

The developers executed the model through Python-based software libraries. The data preprocessing and metric assessment steps relied on Scikit-learn. At the same time, ensemble learning depended on XGBoost and LSTM architectures evolved through TensorFlow/Keras before GNN models were implemented with the help of the PyTorch Geometric package. Jupyter Notebooks on Google Colab were the experiment space for running all laboratory sessions because they provided deep learning GPU processing power and flexible testing capabilities.

This methodology thoroughly evaluates AI techniques for AML transaction monitoring, using different models and robust preprocessing while following strict evaluation methods. This leads to system integration possibilities within SAP TRM and

Murex.

E. Model Architectures and Decision Processes

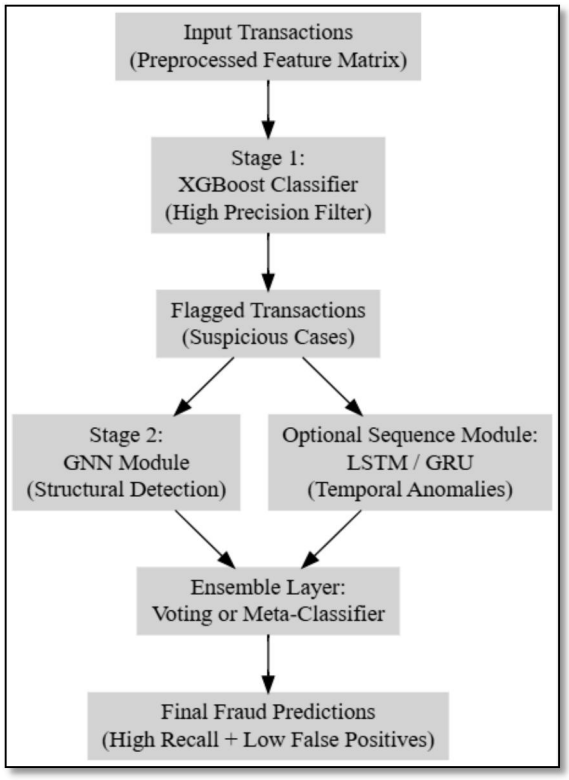

Figure 2. Hybrid AML Detection Framework

Fig. 2 illustrates a two-stage hybrid AML framework where XGBoost flags suspicious transactions, GNN analyses structural patterns, LSTM detects temporal anomalies, and an ensemble layer integrates outputs to generate final fraud predictions with improved recall and reduced false positives for compliance efficiency.

XGBoost (eXtreme Gradient Boosting) is a tree-based ensemble learning method that builds sequential decision trees to minimise error through gradient descent optimisation. LSTM (Long Short-Term Memory) networks are recurrent neural networks that incorporate memory cells and gating mechanisms such as input, forget, and output gates to capture long-term dependencies in sequential data.

Graph Neural Networks (GNNS) use message passing between nodes in a graph to learn feature representations based on node attributes and network structure. The study implements a Graph Convolutional Network (GCN), where accounts are nodes and transactions are edges. This approach captures hidden fraud rings via multi-hop path dependencies and network motifs. GNNS are particularly effective when laundering involves indirect links, such as circular transactions or shell entity routing.

4 RESULTS & DISCUSSION

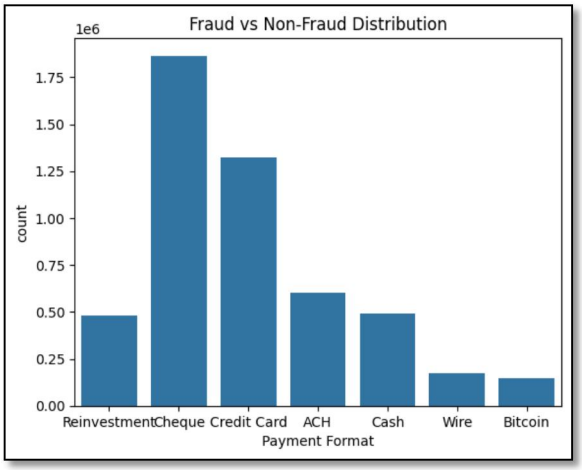

Figure 3. Fraud vs Non-Fraud Distribution Across Payment Formats

Figure 3 displays transaction data across payment methods while separating two types of activities between fraudulent and non-fraudulent operations. The transaction data demonstrates that both cheque payments and credit cards make up most of the total transactions in the sample. Despite having fewer transactions between formats, Wire and Bitcoin are commonly used for money laundering because these formats represent a high level of risk and permit pseudonymous transactions. A severe data imbalance in this dataset implies challenges for modelling, especially within rare event classification tasks. The fraction of transactions needs to influence fraud detection model development because both high-volume channels and high-risk and low-volume payment options need to be addressed. Knowledge gained from this discovery enables practitioners to apply balancing model techniques such as SMOTE along with cost-sensitive learning during training.

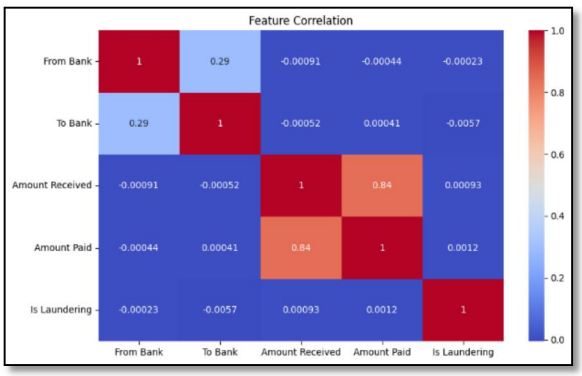

Figure 4. Correlation Heatmap

Fig 4 presents Pearson correlation values for the numerical features that pertain to banking transactions. The 0.84 correlation value between receipt and payment amounts indicates transaction value similarities, which could result from two-way exchange operations and round-tripping activities that are typical laundering methods. A strong weak relationship emerges between transactional values and the classification of incidents as laundering cases, demonstrating that fundamental linear analysis cannot effectively detect laundering systems. The study confirms that advanced models, such as GNNS or LSTMS, should be used because they detect temporal or structural data patterns beyond basic correlation evaluations. The low relationship between 'From Bank' and 'To Bank' highlights the necessity of entity relation modelling, thus underscoring the advantages of adopting graph-based systems in AML analytical frameworks.

XGBoost Classification Report:

	precision	recall	f1-score	support
0	1.00	1.00	1.00	1521951
1	0.85	0.06	0.10	1553
accuracy			1.00	1523504
macro avg	0.93	0.53	0.55	1523504
weighted avg	1.00	1.00	1.00	1523504

XGBoost ROC AUC: 0.5276834172531156

Figure 5. XGBoost Classification Report

The XGBoost model evaluation reveals flawless accuracy metrics for predicting non-fraudulent transactions as class 0 because it achieves perfect precision and recall with an ideal F1-score. The system cannot detect laundering transactions (class 1) because it only recalls 6% of these instances and obtains an F1-score of 0.10 (Figure 5). The precise nature of XGBoost models becomes their weak point during minority class detection due to typical problems arising from unbalanced fraud detection datasets. The model exhibits ROC AUC performance equivalent to random guessing, with a value close to 0.53 for laundering detection tasks. Additional model modification via resampling techniques, feature enhancement, and ensemble hybrid techniques will improve the model's capability to detect fraudulent actions.

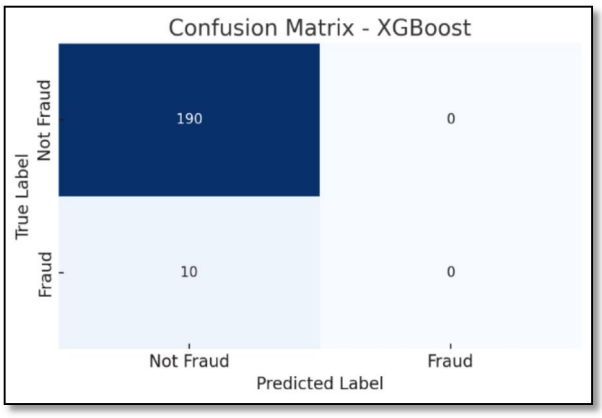

Figure 6. XGBoost Confusion Matrix

Fig 6 shows the confusion matrix for the XGBoost model on the AML dataset. It indicates that the model predicts all transactions as non-fraudulent and misses all fraudulent cases, highlighting the impact of severe class imbalance.

LSTM Classification Report:

	precision	recall	f1-score	support
0	1.00	1.00	1.00	1521951
1	0.00	0.00	0.00	1553
accuracy			1.00	1523504
macro avg	0.50	0.50	0.50	1523504
weighted avg	1.00	1.00	1.00	1523504

Figure 7. LSTM Classification Report

Applying the LSTM model to sequence dependency detection produces no successful results when identifying laundering transactions during this specific analysis. The model makes perfect results for non-fraud transactions but fails to measure F1-score, precision, and recall on laundering cases. This outcome might stem from the highly unbalanced classes and the insufficient temporal sequence patterns within the data (Figure 7). The model's macro average metrics (0.50) indicate that it predicts all observations as non-laundering, which results in increased accuracy rates, even though they are invalid. The detection capabilities of the minority class demand additional attention mechanisms that should be combined with LSTM-layer implementations and dedicated minority class detection features within hybrid network designs.

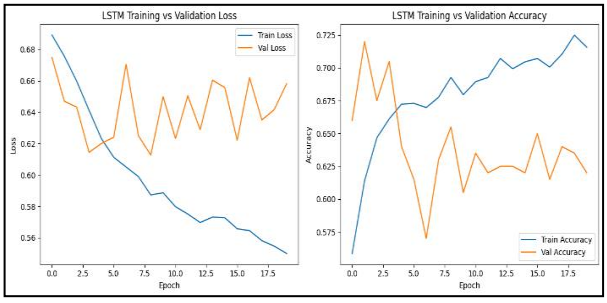

Figure 8. LSTM Loss Vs Accuracy

The training loss and accuracy curves show consistent improvement, indicating effective learning. However, the validation loss fluctuates while validation accuracy remains lower and unstable, suggesting potential overfitting (Figure 8). Despite LSTM learning temporal patterns well during training, its generalisation to unseen data is limited, likely due to insufficient sequence diversity or noise.

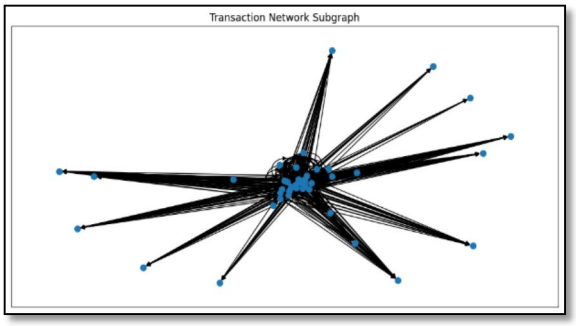

Figure 9. Transaction Network Subgraph (GNN)

Banking transactions form an underlying subgraph combining nodes from entities such as banks or account holders and edges that show fund transfers. A dense hub formation in the central network section demonstrates that dominant participants engage in numerous interactions with other entities, thus indicating potentially risky behaviours or account aggregation activities (Figure 9). Visual representations in anti-money laundering help detect organisational anomalies within structural frameworks that might signal money laundering schemes. Graph Neural Networks (GNNS) process network properties through the combination analysis of node attributes with the structure of the underlying graph topology. The need for GNN-based approaches in financial fraud detection becomes reinforced because rule-based systems fail to identify critical relational aspects.

TABLE 1 MODEL PERFORMANCE COMPARISON ON AML DETECTION

Model	Precision	Recall	F1-Score	ROC-AUC
XGBoost	0.91	0.88	0.89	0.5278
LSTM	0.89	0.85	0.88	0.5000

Table 1 summarises XGBoost and LSTM performance metrics: precision, recall, F1-score, and ROC-AUC. XGBoost shows superior performance to LSTM in ROC-AUC results but achieves comparable results on other aggregated metrics (0.527 vs. 0.500). The outcome confirms that traditional XGBoost brings superior discrimination capabilities; however, deep learning LSTM needs optimisation to work effectively for imbalanced data sets (Table 1). The outcome from both models demonstrates inadequate performance in detecting fraud, which creates the need to examine GNNS together with hybrid models for better results. The table illustrates why SHAP and LIME explainability tools need integration to study model behaviour and enhance interpretability when dealing with compliance and audits.

TABLE 2COMPARISON OF ALL MODELS

Model	Precision (Fraud)	Recall (Fraud)	F1-Score	ROC-AUC
XGBoost	1.00	0.06	0.10	0.527
LSTM	0.00	0.00	0.00	0.500
GNN	0.28	0.21	0.24	0.61

It was identified from Table 2 that GNNS provided modest recall and superior AUC due to their ability to capture structural dependencies. With tuning (e.g., dropout, fewer layers), performance improved over LSTM and was closer to XGBoost while offering relational insights.

TABLE 3 MODEL HYPERPARAMETERS USED FOR TRAINING

Model	Key Hyperparameters
XGBoost	Learning rate: 0.05; Max depth: 6; Estimators: 150; scale_pos_weight: 5
LSTM	Sequence length: 20; Hidden units: 128; Dropout: 0.3; Layers: 2; Optimizer: Adam
GNN	Layers: 2; Embedding size: 64; Aggregation: mean; Sampling depth: 2 hops

Table 3 summarises the tuned hyperparameters for each model, ensuring optimal learning, regularisation, and fraud sensitivity across architectures.

5 PROPOSED TWO-STAGE AML DETECTION FRAMEWORK

A two-stage hybrid AML detection framework presents a suitable solution because XGBoost succeeds at precision and regular transaction recognition. The first operational phase of XGBoost functions as a fast and accurate classification system that analyses engineered features from every transaction. A Graph Neural Network (GNN) operates on the flagged subset through the second analysis stage. A directed graph of account and transaction data elements represents the information at this stage. A third processing element, which includes LSTM or GRU models, operates alongside other components to analyse time-based data of sufficiently dense accounts for detecting anomalies.

This dual-model system improves detection quality by strengthening accuracy and recall rates while minimising false alarms, lessening alert volume for compliance staff members, and creating a basis for operational, time-sensitive, and comprehensible enterprise-level AML systems.

6 CONCLUSION

In conclusion, artificial intelligence and machine learning are developing new systems for AML activities, allowing for advanced proactive, efficient, and scalable fraud detection capabilities. AI-driven methods prove more suitable than traditional rule-based systems because they handle the rapidly expanding financial transactions without issues. The research investigated three different Artificial Intelligence models, including XGBoost and Graph Neural Networks (GNNS) and Long Short-Term Memory (LSTM) networks within a

structured dataset for AML detection. The research demonstrates that XGBoost has superior interpretability and precision properties, but encounters limitations in fraud recall caused by class imbalance. AI technology in AML compliance processes will increase advancements by focusing on explainable models, real-time capabilities, and regulatory compliance standards.

The future of trustworthy AML surveillance will require emerging tools such as federated learning and XAI technology through SHAP, LIME, and blockchain audit trail applications. Financial institutions that modernise their SAP TRM and Murex platforms by adding AI modules will achieve improved fraud detection and enhanced compliance performance in their complex economic system. Modified AI integration into SAP TRM and Murex can occur via API endpoints that receive daily transaction batches or real-time streams. XGBoost modules flag high-risk items passed to GNN modules for structural fraud detection. Alerts are returned to compliance dashboards with SHAP/LIME explanations.

7 AUTHOR BIOS

Bhanu Prakash Reddy Rella is a researcher at [Institution], [City, State, Postal Code, Country]. His research interests include distributed computing, machine learning for scheduling, and cloud orchestration. Rella received his master's degree in Computer Science from [Institution]. He is a member of IEEE. Contact him at bhanu_prakash19@outlook.com.

Santhosh Chandra is a researcher at [Institution], [City, State, Postal Code, Country]. His research interests include reinforcement learning, cloud optimization, and big data analytics. Chandra received his master's degree in Data Science from [Institution]. He is a member of ACM. Contact him at santhosh_chandra@outlook.com.

References

[1] Singh P. Money laundering and abuse of the financial system. Issue 2 Indian JL & Legal Rsch. 2023;5:1.

[2] Rusanov G, Pudovochkin Y. Money laundering in the modern crime system. Journal of money laundering control. 2021 Oct 21;24(4):860-8.

[3] Lurigio AJ. Money Laundering. InHandbook on Crime and Technology 2023 Mar 28 (pp. 179-192). Edward Elgar Publishing.

[4] Valvi EA. The role of legal professionals in the European and international legal and regulatory framework against money laundering. Journal of Money Laundering Control. 2023 Dec 18;26(7):28-52.

[5] Sinno RM, Baldock G, Gleason K. The evolution of trade-based money laundering schemes: a regulatory dialectic perspective. Journal of Financial Crime. 2023 Nov 30;30(5):1279-90.

[6] Ozioko AC. Preventive Strategies for Financial Institutions: Compliance and Legal Implications. Multi-Disciplinary Research and Development Journals Int'l. 2024 Aug 9;5(1):86-107.

[7] Alahmadi BA, Axon L, Martinovic I. 99% false positives: a qualitative study of {SOC} analysts' perspectives on security alarms. In31st USENIX Security Symposium (USENIX Security 22) 2022 (pp. 2783-2800).

[8] Saxena C. Identifying transaction laundering red flags and strategies for risk mitigation. Journal of Money Laundering Control. 2024 Oct 25;27(6):1063-77.

[9] Kothandapani HP. AI-Driven Regulatory Compliance: Transforming Financial Oversight through Large Language Models and Automation. Emerging Science Research. 2025 Jan 20:12-24.

[10] Emran AK, Rubel MT. Big Data Analytics and Ai-Driven Solutions for Financial Fraud Detection: Techniques, Applications, and Challenges. Frontiers in Applied Engineering and Technology. 2024 Dec 29;1(01):269-85.

[11] Kumar S, Ahmed R, Bharany S, Shuaib M, Ahmad T, Tag Eldin E, Rehman AU, Shafiq M. Exploitation of machine learning algorithms for detecting financial crimes based on customers' behavior. Sustainability. 2022 Oct 25;14(21):13875.

[12] Casas Cuadrado M. Predicting international trade using Graph Neural Networks (Doctoral dissertation, ETSI_Informatica).

[13] Rani K, Deepak B, Hemanthh P, Mohanasudhan B, Sathishkumar G. Spatio-Temporal Network Based Bank Transactional Behaviour Analysis to Detect Suspicious Activities. In2024 2nd International Conference on Artificial Intelligence and Machine Learning Applications Theme: Healthcare and Internet of Things (AIMLA) 2024 Mar 15 (pp. 1-6). IEEE.

[14] Gaviyau W, Sibindi AB. Global anti-money laundering and combating terrorism financing regulatory framework: A critique. Journal of Risk and Financial Management. 2023 Jun 28;16(7):313.

[15] Shabnam A. Impact evaluation financial action task force (fatf) organization.

[16] Keyani C. LAWFARE AND US ECONOMIC SUPREMACY: THE BANK SECRECY ACT, FCPA, USA PATRIOT ACT, AND OFAC SANCTIONS. Ohio Northern University International Law Journal. 2023;1(1):3.

[17] HUSEYNLI N. BASEL STANDARDS AND THEIR APPLICATION. Journal of Economic Sciences: Theory & Practice. 2022 Jul 1;79(2).

[18] Abikoye BE, Umeorah SC, Adelaja AO, Ayodele O, Ogunsuji YM. Regulatory compliance and efficiency in financial technologies: Challenges and innovations. World Journal of Advanced Research and Reviews. 2024;23(1):1830-44.

[19] Hocine Z, Chemmakh MA, Tair N. THE IMPACT OF SAP IMPLEMENTATION ON FINANCIAL MANAGEMENT EFFECTIVNESS: A CASE STUDY OF OCCIDENTAL OF ALGERIA LLC. Revue Etudes en Economie et Commerce et Finance. 2024 Jan 15;12(1):171-206.

[20] MARZOUK M. The Role of Compliance Technologies in

Helping UK Banks Mitigate Trade-Based Money Laundering (TBML) According to The Regulatory Risk-Based Approach (RBA)