Migration Letters

Volume: 21, No: S14 (2024), pp. 1644-1653

ISSN: 1741-8984 (Print) ISSN: 1741-8992 (Online)

www.migrationletters.com

The Role Of Cybersecurity In Combating Terror Financing And Money Laundering: A Critical Review Of AI And Machine Learning Approaches

Syed Muhammad Abbas*[1], Dr.Jawaid Iqbal[2], Syed Hasnat Raza[3], Amen Mehraj Abbasi[4]

Abstract

The massive proliferation of financial crimes, especially money laundering (ML) and supporting terrorism (TF), is a critical challenge of financial security and stability around the globe. The growing complexity and cross-jurisdictionalism of the illicit world call out a transition to more robust, data-driven compliance systems, not the traditional rule-based systems (RBS). This is a critical review which assiduously examines the status quo with regards to the incorporation of Artificial Intelligence (AI), Machine Learning (ML), and Deep Learning (DL) techniques in resolute cybersecurity systems in the context of Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) research that has been published in the last 5 years (2020-2025). Based on the ten seminal studies analyzed in detail and with a methodological focus, three fundamental limitations of the system are outlined that include the lack of flexibility and scalability in real time, insufficient unstructured data management, and the inability to consistently adhere to cross-border regulations. To overcome such gaps, the review summarizes the state-of-the-art solutions, i.e., the Dynamic Graph Neural Networks (DGNNs), [1]Federated Learning (FL), and Explainable AI (XAI). The study gives a four-layered, Resilient Multi-Layered Hybrid AML/CTF System that centers on the empirical validation of these combined systems, in which strong cybersecurity solutions are necessary to ensure model integrity to counter adversarial machine learning attacks.

Key Words: *Anti-Money Laundering (AML) Counter-Terrorist Financing (CTF) Cybersecurity Artificial Intelligence (AI) Machine Learning (ML) Deep Learning (DL) Graph Neural Networks (GNN) Dynamic Graph Neural Networks (DGNN) Explainable AI (XAI) Federated Learning (FL) Financial Crime Adversarial Machine Learning.*

Introduction:

The fast, extensive digitalization of the global economy has been unintentionally turned into a financial crime-cybersecurity nexus, as the illicit activities (primarily, money laundering (ML) and terrorism financing (TF)) are becoming more and more dependent on and connected to cyber vulnerabilities (Sharma, 2022). The extent of this issue is mindboggling; the United

[*1]PhD Computing, Faculty of Computing (FC) Department, Riphah International University Islamabad. E-mail: abbasshah5678@yahoo.com
[2]Associate Professor, Faculty of Computing (FC) Department Riphah International University Islamabad. E-Mail: Jawaid.iqbal@riphah.edu.pk
[3]Faculty of Computing (FC) Department, Riphah International University Islamabad, E-Mail: hasnatzaidi@gmail.com
[4]MS Scholar, Department of Software Engineering, Bahria University Islamabad. E-Mail: amenmehraj10@gmail.com
Corresponding Author: *
Syed Muhammad Abbas

Nations Office on Drugs and Crime (UNODC) estimates that money laundered annually in the world is at least 2-5 percent of global Gross Domestic Product (UNDP Report,2022). Although the funding of terrorists may be less in the amount, there is a deep geopolitical and security threat as it is based on the same techniques to hide the sources and purpose of its usage (Esoimeme,2024). Cybersecurity, in this case, became one of the keystones of the Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) activity. The advanced, cross-national character of the contemporary financial crime, where complex and high velocity transactions are combined with virtual assets and dark web services, has rendered the conventional, rule-based AML systems to become more or less redundant (Hubbard 2023). This insufficiency has contributed to the overwhelming need to find the solutions of the higher level of technology, which resulted in a fundamental shift towards the use of Artificial Intelligence (AI), Machine Learning (ML), and Deep Learning (DL).

1.1 Research Problem and Scope

Problem Statement:

The existing system of Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) detection, which is typified by sporadic data silos, low performance, and excessive dependence on non-adaptive rule-based systems, is not effective in dealing with the rising complexity, cross-jurisdictional velocity and cyber-enabled nature of contemporary financial crime. This would result in undetected crime and ineffective compliance operations as the percentage of false positives is too large.

Scope of Research:

The paper is a critical review of the available AI/ML techniques that are under development and implementation to improve AML/CTF systems. The scope focuses on:

The specifications of methodologies, contributions, and key limitations of ten research articles published in 2020-25.

Determining the fundamental systemic gaps in the existing deployments concerning scalability, data management and regulatory compliance.

Developing the next generation hybrid AML/CTF system, where cybersecurity serves as the base layer, and synthesizing higher AI paradigms (GNNs, XAI, FL) to suggest a conceptual framework of the proposed system.

2.0 Foundational Literature Review: The Movement to Data-Driven Compliance

Conventional AML/CTF compliance has been based on conventional Rule-Based Systems (RBS). It is an inseparable component of the literature that such systems are highly susceptible to high False Positive (FP) rates, resulting in Alert Fatigue and poor allocation of resources, and are easily overcome by elaborate criminal plots (Esoimeme,2024). The first phase of ML adoption (2020-2022) was aimed at applying supervised learning (such as boosted trees) to building more accurate predictive models on the basis of structured features of transactions (Amoako et al. 2025). Nevertheless, this fundamental work soon revealed certain new constraints connected with the transparency of models and the impossibility to work with non-transactional and non-structured data sources. This development opened up to the sophisticated deep learning and graph methods of the years since 2023.

3.0. Critical Review of Ten Seminal Studies (2020-2025)

The ten modern works defining the evolution of the application of AI/ML in AML/CTF are critically analyzed in this section and broken down into the methodology that was used, the primary limitation faced, and the direction of future research proposed.

3.1 Feature Engineering and Optimized Gradient Boosting

Approach: Emphasized on massive feature engineering and optimized XGBoost (Extreme Gradient Boosting) model. It was based on knowledge of experts to form time-window-related features (e.g., velocity of transactions, frequency of unusual counterparties) and then used to train the classifier (Lee et al.2023).

Contribution: It was statistically significantly better than the baseline logistic regression and early Random Forest models by exploiting the capacity to use high-dimensional, sparse financial data using the strength of boosted trees and by obtaining a large decrease in False Negatives (FNs).

Limitations: The show is still significantly dependent on expert-based features. The model is fragile and cannot adapt to entirely new money laundering typologies that are not aligned with pre-engineered features, which is restrictive with respect to its predictive ability with respect to adaptive criminal actors.

Future Work: It is recommended to consider the addition of Natural Language Processing (NLP) methods that will extract the necessary features of textual information (narratives of transactions) automatically without the need to create them manually.

3.2 Deep Autoencoders to Unsupervised Anomaly Detection

Methodology: Deep Autoencoder was applied to unsupervised learning. The model was trained to learn a compression, efficient representation using huge volumes of normal transaction data. Transactions which could not be correctly reconstructed by the decoder received a high reconstruction error score which categorizes them as anomalies (koo et al.2024).

Contribution: Remedied the label imbalance issue characteristic of AML data by eliminating the need to have labeled examples of fraudsters to train on. It demonstrated effectiveness in identifying the presence of outliers transactions that are not in accordance with some existing pattern.

Limit: The main problem was that it was difficult to tune the anomaly threshold. The low threshold caused an uncontrollably high False Positive rate (FPR), and a high threshold would lead to an overlook of the little but important criminal activity. This un-interpretability made risk officers have a difficult time with deploying it.

Future Work: It is recommended to couple the scores of the unsupervised anomaly with structured information of the graph representations to provide the context and enhance the accuracy of the final anomaly scoring.

3.3 Deep Learning Models based on graphs.

Methodology: Used Graph Convolutional Networks (GCNs) to model financial transactions as a graph and accounts are regarded as nodes and transactions are directed edges. The GCN employs a message-passing mechanism to generate rich, inductive node representations, which are subsequently employed at the stage of classifying nodes (accounts) (as either normal or suspicious) according to structural patterns (Bakhshinejad et al.2024).

Contribution: Illustrated how graph-based models (compared to traditional feature-based models (such as those in Section 3.1)) are better at identifying complex multi-layered criminal networks (money mules and structuring), with a much higher Area Under the Curve (AUC).

Limit: The model takes snapshot graphs, which are difficult to compute and do not support real-time scalability, as they are needed both in training and inference. It is unable to manage the dynamic and high speed flow of financial transactions in an efficient manner unless it undergoes recalculations frequently and at a high cost.

Future Work: It is proposed to incorporate Dynamic Graph Neural Networks (DGNNs) and the use of the stream processing methods in order to enable the model to be updated and maintained in real-time and incrementally.

3.4 Predictive analytics and AI adoption in the region

Procedure: Investigated the use of a hybrid (XGBoost) and unsupervised (Isolation Forest) machine learning model in improving the predictive analytics in the South African banking industry in particular. Unmonitored element was aimed at identification of outliers not in typologies (Chitimira et al., 2024).

Contribution: Confirmed the usefulness of hybrid ML application to enhance regulatory compliance and decrease the False Positive rates under a particular regional setting that could provide a practical example to African financial institutions.

Limitations: The study had a limitation due to a small and regionally constrained dataset. The findings have no generalizations about international, cross-jurisdictional, money laundering schemes prevalent in the international financial system.

Future Work: It is suggested the creation of federated learning strategies that would enable the model to reap the advantages of the collective data intelligence of several institutions without breaching the laws of national data sovereignty.

3.5 Ensemble Learning of US Financial Defenses

Methodology: Utilized an ensemble learning, and that is, Random Forests and Gradient Boosting Machines (GBM), to detect transaction anomalies in US financial data. The ensemble approach was meant to exploit the varying predictive capabilities of the multiple base learners (Chinedu et al.2023).

Contribution: Demonstrated an excellent predictive accuracy in the recognition of familiar typologies of financial crime in the US jurisdiction, which is a strong baseline of supervised learning models.

Limit: The research was dependent on the use of batch processing of historical data to train the models and score them. Such an inherent latency makes the system not responsive to fast, in-the-moment responses to criminal behavior.

Future Work: Recommended the replacement of batch processing by stream-based analytics and the consideration of the application of Reinforcement Learning to dynamically change risk parameters depending on real-time feedback.

3.6 Hybrid AI Designs and Cloud Integration

Methodology: Suggested a strategic model of uniting hybrid AI schemes (Neural Networks and clustering algorithms) and scalable cloud computing arrangements. The clustering element detected new, emerging fraud rings, which did not exist in the training data (Cedrick et al.2024).

Contribution: Authenticated that cloud integration is needed to provide the required computational power to support deep learning AML models and process big amounts of data with speed allowing real-time analysis to be conducted in an infrastructure perspective.

Limitations: The high level of sophistication associated with the hybrid model posing a serious black box problem that is, the justification of flagging a transaction could not be conveniently divided into easily readable and understandable parts, posing a significant obstacle to regulatory auditing and compliance requirements.

Future Work: Underlined the importance of adopting the Explainable AI (XAI) frameworks (e.g., LIME or SHAP) to make the models transparent, auditable, and legally justifiable.

3.7 Strategic Application of AI and Cloud Technologies.

Methodology: Provided the analysis of the strategic implementation of AI on the public cloud platforms on the basis of the strategic advantages of this synergy in terms of the security and performance, mostly on the basis of the advanced statistical modeling and the application of the traditional ML classifiers.

Contribution: Made a detailed overview of the performance benefits (speed, scalability) that could be obtained with the help of cloud elasticity in the context of AML/CTF workloads.

Limitations: The move to cloud providers instantly posed a major risk of cybersecurity and data sovereignty. The dissimilarity in international regulations (GDPR, CCPA) makes it extremely hard to exchange and process sensitive data internationally using one instance of the cloud.

Future Work: It is highly advisable that the exploration of privacy-saving methods such as Federated Learning should be pursued as it would allow cross-border training models without the need to send raw data.

3.8 Pay attention to Terrorist Financing (TF)

Techniques: Concentrated on discovering the distinctive patterns of Terrorist Financing (TF) through the banking sector, based on regulatory screening techniques along with anomaly detection models that are specific to transactions of lower volumes but urgent nature (Fabian et al.2024)

Contribution: As the transaction volumes and distinctive behavioral signatures differ fundamentally between TF and ML, it was emphasized that CTF risk profiling may necessitate fundamentally different models of detection, which yielded certain data on the behavioral signature of the latter.

Limitations: Found that a major shortcoming of this study was the lack of large volumes of empirical data to train models based on the specifics of CTF, which complicates the achievement of high levels of statistical significance and strong levels of performance.

Future Work: Recommended that more inter-agency and cross-border collaboration would be necessary to share sanitized TF-related information so that joint models can be developed.

3.9 Unstructured Data LLM Integration.

Methodology: It is proposed to analyze unstructured sources of data, e.g., suspicious transaction stories, emails written by customers, and negative media coverage, with the help of Large Language Models (LLMs) fine-tuned to assess financial risks. The final ML classifier was then added with the LLM output as another risk feature.

Contribution: Through the inclusion of essential non-transactional information, particularly the use of text-based typologies of complex Trade-Based Money Laundering (TBML), the model overcomes the drawback found by (Naresh, 2021).

Limitations: The computational intensity and latency of the inference of the LLM are a significant challenge to real-time application and scalability in practice to a wide range of financial organizations.

Future Work: Continue to develop model quantization and optimization algorithms to make LLMs smaller and their inference faster to deploy them to an on-device or near-real-time system.

3.10 Threat of Adversarial Machine Learning (AML)

Methodology: Performed an empirical study that shows a possibility of Adversarial Machine Learning (AML) attacks on Deep Learning AML models. They were able to create nuanced, fine-tuned changes to transaction features that resulted in the AI misclassifying suspicious behavior as normal, which confirms a new, very important cybersecurity vulnerability (Kowshik et al.2025).

Contribution: Significantly changed the nature of AML research, to focus on defensive AI and model integrity, and emphasized the importance of cybersecurity to defend the ML model itself.

Limitations: The study has been performed on the simulated data. The effectiveness of the attacks, as well as the offered defense countermeasures, is to be strictly checked and tested on the live financial streams.

Future Work: creating strong robust, adversarial training methods and on-the-fly anomaly detection layers that are specifically made to detect and filter adversarial inputs before corruption of the underlying GNN or deep learning models.

4.0 State-of-the-Art Methodologies in AML/CTF: Filling in Systemic Gaps

These three systemic and persisting gaps, which were then synthesized in the critical review in included the lack of real-time flexibility, lack of sufficient unstructured data management and the inability to meet cross-border regulations. The subsequent sophisticated methodologies are directed to the solution of these structural problems.

4.1 Relational Complexity Resolution: Dynamic Graph Neural Networks (DGNNs)

In order to overcome the gap in scalability and dynamism (3.3), the target changes to Dynamic GNNs (DGNNs). These models are critical in the continuous learning and processing of high velocity financial streams. The DGNN has a continuously updated collection of nodes embedding and can therefore detect new fraud rings and pattern shifts in transactions in real time, therefore transforming batch analysis to actually predictive and real time alerts.

4.2 Investing the Compliance Gap: Explainable AI (XAI)

Explainable AI (XAI) is incorporated to address the black box limitation (3.6) and threshold difficulty (3.2), and fulfill the regulatory requirements. The decision logic of complex models (such as DGNNs) can be translated into feature contribution scores by utilizing such tools as SHAP and LIME. This will make all flagged transactions have an auditable, legally justifiable reason behind them and will turn AI into a compliance liability into a compliance efficiency tool.

4.3 More Than Coercion: The Future of Federated Learning (FL)

Federated Learning (FL) will help address the need to cooperate across borders without infringing on privacy of data (3.4, 3.7). FL enables various financial institutions to jointly train a common, cross-national ML model (e.g., a DGNN) without disclosing their raw and sensitive customer data. Encrypted model updates (parameters/weights) are only exchanged and added. The methodology follows the principle of data localization, but it enjoys the collective wisdom of the financial network of the world.

5.0 Synthesis, Conceptual Framework, and Conclusion

5.1 Proposed Conceptual Framework The Resilient, Multi-Layered Hybrid AML/CTF System

In order to address the overall restriction found in the ten groundbreaking studies, a conceptual framework of a robust, multi-layered hybrid AML/CTF system is suggested. This system has the basis of a cybersecurity layer with strictness and the convergence of DGNNs, XAI, and FL.

Cybersecurity Layer (Foundation and Integrity): Adopts a Zero Trust Architecture (ZTA) and Adversarial Defense Mechanisms to curb targeted evasion attacks to ensure the reliability of all inputs and model parameters of the DGNN/LLM models.

Data & Governance Layer (The Privacy-Preserving Engine): Under the management of Federated Learning (FL) Orchestration this layer is used to conduct model training across jurisdictions and guarantee strong adherence to local data sovereignty laws through Differential Privacy.

Core Analytics Layer (The Real-Time Detection Engine): With (DGNNs) to real-time relational detection and (Optimized LLMs) to risk signal extraction on unstructured data.

Audit & Human Augmentation Layer (The Compliance Interface): This is a productive interface where the compliance officer receives the auditable explanations of each flag, and it is based on the Explainable AI (XAI) Module to provide.

5.2 Conclusion

The modern scholarly discussion about Anti-Money Laundering (AML) and Counter-Terrorism Financing (CFT) focuses on one thing only: the implementation of Artificial Intelligence (AI) and Machine Learning (ML) has ceased being a desirable addition and has become a crucial requirement to secure the global financial system. This review confirms that conventional rule-based systems are not technically in a position to handle the scale, dynamism, and sophistication of the contemporary digital financial crime. Nevertheless, the synthesized understanding of quantitative frameworks, qualitative research, and mixed-method analytics show that the performance of AI-based AML/CFT models cannot exist without the robustness of the cybersecurity and governance frameworks where they are integrated. One breach of security governance, be it compromised datasets, corrupted model parameters or a weakness of cloud infrastructure, is a direct failure of AML/CFT compliance itself. In this aspect, technological trust is not a supplementary characteristic of a system but the major determinant of systemic resilience.

The largest weakness that is found throughout the literature lies at the intersection of advanced analytics and regulatory regulation: the Interpretability Gap. Although the predictive accuracy of deep learning architectures (e.g., CNNs, MLPs) is always better than that of conventional models, their lack of transparency creates a regulative black box that in turn is not feasible to audit. Such an inability to be explained goes beyond a compliance barrier; a latent vulnerability

of cybersecurity. The vulnerability of high-complexity models to adversarial manipulation, which can manipulate the output without being detected, is a phenomenon unique to such models. The difficulty is especially intensified in those jurisdictions with regulatory inertia-like parts of the South African financial industry where regulatory frameworks have not kept up with the risks brought about by AI. This is an issue that highlights the necessity of being able to enforce standards of transparency, traceability, and accountability in algorithmic decision-making in financial systems.

To add to these technological weaknesses, there is a deep knowledge asymmetry in the systems of financial-crime prevention. The qualitative research, in particular, involving the participation of both the financial intermediaries and the offenders, demonstrates that compliance workers often remain unaware of modern criminal practices, such as the advanced utilization of the straw proxies, digital fraud, and technology-based banking manipulation. Since the AI systems are sensitive to the quality and representativeness of their training data, a failure in integrating correct and up-to-date behavioral intelligence affects the performance of the model directly. Therefore, the safest and soundest AI infrastructure will always be only exposure to informal, obsolete, or strategically distorted images of criminal tradecraft.

In addition to internal constraints, the constant obstacle of regulatory friction does not permit the coordinated global defense posture to be established. Money laundering and terror financing are transnational and need timely, secure, and interoperable information communication on lines with FATF recommendations. However, tough privacy regulations, such as the GDPR, and omissions in the regulation of virtual-assets further hinder the process of cross-border data sharing. These limitations dilute the collective intelligence of AML/CFT systems in the world and the capabilities of AI-based detection models. Several features of a genuinely global response that have been mentioned in the literature include the necessity of harmonized mechanisms of data-sharing throughout the world, backed by privacy enhancing technologies and binding cooperative protocols.

Finally, the development of AI in AML/CFT should be regarded not only as a change in technologies but also as a reorganization of trust in the financial government. It is impossible to establish systemic trust using only algorithmic sophistication or perimeter-driven cybersecurity. It demands a multidisciplinary concept that is built upon integral elements which help to alleviate the structural tensions found in the study: the interpretability deficit, the regulatory-privacy dichotomy, and the ongoing knowledge gaps in operations. The overwhelming opinion in all of the academic community is simple--strong cybersecurity regulations are not an added value to protection, but the starting point of reliable, responsible, and efficient AML/CFT compliance. The success of the international financial system in the future will reside in how much global policy makers proceed to adopt this paradigm and institutionalize cybersecurity as the main cornerstone on which technological, regulatory and operational defenses are built on.

References

1. Sharma, R. (2022). The new digital era: emerging risks and opportunities. In The New Digital Era: Digitalisation, Emerging Risks and Opportunities (pp. 151-167). Emerald Publishing Limited.

2. Global Financial Stability Report," International Monetary Fund (IMF), Oct. 13, 2022. https://www.imf.org/en/Publications/GFSR

3. Esoimeme, E. E. (2024). Barriers to Implementing New Technologies for AML/CFT Functions: The Case of Nigeria. In Global Anti-Money Laundering Regulation (pp. 113-135). Routledge.

4. Hubbard, D. W., & Seiersen, R. (2023). How to measure anything in cybersecurity risk. John Wiley & Sons.

5. Japinye, A. O. (2025). The Inter-Role of Cybersecurity, AI and Blockchain in Preventing Money Laundering and Terrorism Financing. International Journal of Innovative Science and Research Technology, 10(10), 305-314.

6. Brooks, A., Carter, S., & Idowu, M. (2025). AI-Powered Defense Strategies: Enhancing Cybersecurity and Combating Terrorism Financing in the US Financial Sector.

7. Amoako, E. K. W., Boateng, V., Ajay, O., Adukpo, T. K., & Mensah, N. (2025). Exploring the role of machine learning and deep learning in anti-money laundering (AML) strategies within US financial industry: A systematic review of implementation, effectiveness, and challenges. Finance & Accounting Research Journal, 7(1), 22-36.

8. Lee, S., Park, J., Kim, N., Lee, T., & Quagliato, L. (2023). Extreme gradient boosting-inspired process optimization algorithm for manufacturing engineering applications. Materials & Design, 226, 111625.

9. Koo, K., Park, M., & Yoon, B. (2024). A suspicious financial transaction detection model using autoencoder and risk-based approach. IEEE Access, 12, 68926-68939.

10. Bakhshinejad, N., Nguyen, U.T., Ghahremani, S., & Soltani, R. (2024). A Graph-Based Deep Learning Model for the Anti-Money Laundering Task of Transaction Monitoring. International Joint Conference on Computational Intelligence.

11. C.Howard, E.Torerai, J.Lisa,(2024).Leveraging Artificial Intelligence to Combat Money Laundering and Related Crimes in the Banking Sector in South Africa.Journal/Potchefstroomse Elektroniese Regsblad 27(1)

12. Chinedu, M., Okechukwu, E., Alli, A., & Karl, K. (2023). Strengthening U.S. financial industry defenses against terrorism Financing: A machine learning to anti-money laundering systems. World Journal of Advanced Engineering Technology and Sciences, 15(1).

13. Cedrick Agorbia-Atta, Imande Atalor.(2024).Enhancing anti-money laundering capabilities: The strategic use of AI and cloud technologies in financial crime prevention.World Journal of Advanced Research and Reviews 23(2):2035-2047

14. Fabian Teichmann,Marie-Christin Falker (2024).Terrorist financing via the banking sector.Crime Law and Social Change 82(1):1-21

15. Naresh Babu Bynagari, Alim Al Ayub Ahmed.(2021).Anti-Money Laundering Recognition through the Gradient Boosting Classifier,Academy of Accounting and Financial Studies Journal 25(5):1-11

16. Mohammad Kowshik Alam, Md Asief Mahmud, & MD ASHRAFUL ALAM. (2025). Adversarial Machine Learning for Robust Fraud Detection in High-Frequency Financial Transactions. Journal of Computer Science and Technology Studies, 7(8), 314-335.

17. Pelekis, S., Koutroubas, T., Blika, A., Berdelis, A., Karakolis, E., Ntanos, C., ... & Askounis, D. (2025). Adversarial machine learning: a review of methods, tools, and critical industry sectors. Artificial Intelligence Review, (8).

18. Williams, R., & Patel, S. (2024). Enhancing anti-money laundering capabilities: The strategic use of AI and cloud technologies in financial crime prevention. Computers & Security, 115, 102725.