The role of artificial intelligence in anti-money laundering detecting repetitive and suspicious transaction patterns

Janpreet Singh[1], Puspal Mondal[2], Garvit Nayyar[3], Ashish Shrivastava[4], Shruti Abhijeet Ballal[5]

[1]Students, [2]Students, [3]Students, [4]Students, [5]Students

Institute of Management Development and Research (IMDR), DES Campus, Agarkar Road, Deccan Gymkhana, Pune, 411004, India

Abstract—Anti-Money Laundering has become a critical function for financial institutions due to the rapid expansion of digital transactions, increased globalization of financial systems, and the growing sophistication of financial crimes. The widespread use of online banking platforms, mobile payment systems, fintech services, and digital financial channels has significantly increased transaction volumes and complexity, making the detection of illicit financial activities more challenging.

Traditional rule-based AML systems rely on predefined rules, static thresholds, and manual intervention to monitor transactions. While these systems provide a foundational level of compliance, they often struggle to detect advanced money laundering techniques that continuously evolve over time. Consequently, such systems generate a high number of false-positive alerts, increasing operational costs and placing a heavy burden on compliance teams, while still failing to identify genuinely suspicious activities effectively.

Artificial Intelligence has emerged as a powerful and transformative tool for enhancing AML systems by enabling intelligent, data-driven analysis of large volumes of transaction data. AI-based models can learn from historical transaction behavior, identify repetitive transaction structures, detect abnormal patterns, and adapt to changing laundering techniques. This capability allows financial institutions to improve the accuracy and efficiency of suspicious transaction detection while minimizing unnecessary alerts.

This paper examines the role of AI in AML with a specific focus on detecting repetitive transactions and anomalous behavioral patterns commonly associated with money laundering activities. The study is based entirely on secondary data obtained from academic literature, industry reports, and regulatory publications, ensuring a comprehensive and reliable analysis. The paper highlights key AI techniques such as machine learning, anomaly detection, and network analysis, and discusses their benefits, limitations, and future potential in strengthening AML frameworks and enhancing financial crime prevention mechanisms.

Index Terms—Artificial Intelligence, Anti-Money Laundering, Machine Learning, Suspicious Transactions, Financial Crime Detection

I. INTRODUCTION

Anti-Money Laundering refers to a comprehensive set of laws, regulatory guidelines, and institutional procedures designed to prevent criminals from disguising illegally obtained funds as legitimate income[1]. With the rapid expansion of digital banking, mobile payments, fintech applications, and online financial platforms, the volume, velocity, and complexity of financial transactions have increased exponentially, creating new opportunities for criminals to exploit digital channels for illicit financial activities[3]. This digital transformation has significantly challenged the ability of traditional AML systems to effectively monitor, trace, and identify suspicious activities in real time[2].

Conventional AML frameworks rely heavily on rigid rule-based monitoring systems and predefined thresholds, such as transaction limits, frequency checks, unusual time-based patterns, or geographic risk indicators [4]. Although these systems offer a foundational level of surveillance, they are static in nature and lack the adaptability required to address evolving money laundering tactics. As laundering methods become more sophisticated—often involving complex layering, repetitive micro-transactions, multi-account structuring, and crypto-enabled transfers traditional systems struggle to detect subtle or well-disguised patterns[6]. This leads to large volumes of false-positive alerts, increased compliance costs, and significant inefficiencies for financial institutions [5].

Artificial Intelligence (AI) offers a dynamic, adaptive, and data-driven approach to resolving these limitations. AI systems can analyze massive datasets, learn from historical and behavioral transaction patterns, and identify unusual, repetitive, or hidden anomalies that may indicate money laundering activity [7]. Techniques such as machine learning, anomaly detection, and graph-based network analysis enable the discovery of complex laundering structures that rule-based systems typically overlook[8].

This paper explores how AI enhances AML effectiveness by improving the detection of repetitive transaction behavior, uncovering anomalous patterns, and strengthening overall financial crime prevention frameworks.

II. ROLE OF ARTIFICIAL INTELLIGENCE IN AML

Artificial Intelligence plays a central and transformative role in modern AML systems by improving the accuracy, efficiency, and adaptability of transaction monitoring processes. Unlike traditional rule-based systems that rely on static thresholds, AI-based frameworks can analyze both structured and unstructured data, detect subtle behavioral deviations, uncover hidden transactional relationships, and continuously improve through iterative learning mechanisms [1], AI technologies enable banks and financial institutions to identify complex laundering schemes that are often missed by conventional systems[2].

A. Machine Learning Algorithms

Machine learning algorithms are widely used in AML to classify transactions as legitimate or suspicious [3]. Supervised learning models are trained on historical datasets in which transactions have been labeled based on prior investigations[4]. Through this training, these models learn to recognize patterns such as:

- repeated low-value deposits or withdrawals,
- frequent transfers between the same accounts,
- unusual transaction timings,
- sudden deviations in account behavior.

Such behaviors often indicate structuring, layering, or account takeover attempts.

Unsupervised learning techniques are particularly effective for detecting previously unknown or emerging money laundering patterns [5]. These models analyze unlabeled data to identify deviations from normal customer behavior[6]. For example, if an account that typically processes low-frequency transactions suddenly initiates repetitive or unusually frequent transfers, the model will highlight the activity for further review. This capability allows AI systems to adapt to dynamic financial crime threats without relying on predefined rules.

B. Anomaly Detection

Anomaly detection is a critical AI application in AML systems, focusing on identifying transactions or behaviors that deviate significantly from established norms [7]. Money launderers often rely on repetitive or structured transaction patterns such as multiple transfers of similar amounts within a short time window to disguise illicit funds [8]. These techniques, including smurfing and micro-structuring, are difficult for traditional monitoring systems to detect.

AI-driven anomaly detection models examine various factors such as:

- transaction frequency,
- transaction amounts,
- geographic locations,
- customer behavior histories,
- counterparty relationships.

Based on these variables, AI models construct baseline behavioral profiles. Any significant deviation from these patterns, including unusual repetition or unexpected account activity, is automatically flagged for investigation. This improves response time and reduces the likelihood of undetected laundering.

C. Network and Graph Analysis

Money laundering operations frequently involve multiple accounts, intermediaries, shell companies, and layered transactions designed to obscure the true origin of illicit funds [9]. AI-powered network and graph analysis techniques visualize and model financial transactions as interconnected networks[10], enabling investigators to identify:

- circular or looped transaction flows,
- repeated fund movements among related entities,
- hidden relationships between accounts,
- coordinated activity involving multiple actors.

Graph Neural Networks (GNNs) can detect complex laundering structures by analyzing the topology of financial transaction networks and identifying abnormal clusters or flow patterns[12]. This approach is particularly effective in uncovering layered and sophisticated laundering schemes—especially those involving cryptocurrency or cross-border transactions—that traditional rule-based systems fail to detect [11].

III. BENEFITS OF AI IN DETECTING REPETITIVE AND SUSPICIOUS TRANSACTIONS

The adoption of AI in AML provides several significant advantages over traditional monitoring methods, offering superior adaptability, precision, and analytical depth compared to rule-based systems [14]. AI-driven systems leverage advanced computational techniques to observe transactional behavior over time, recognize evolving money laundering patterns, and adjust dynamically to new threats[15]. Unlike conventional approaches that rely on fixed thresholds and predefined rules, AI models continuously learn from real-world data, enabling more accurate identification of suspicious activity.

First, AI systems significantly reduce false positives by learning from actual transaction behavior rather than relying solely on static rules. Traditional monitoring generates large volumes of alerts, many of which involve legitimate transactions that merely exceed predetermined limits. AI-based algorithms, however, evaluate customer behavior holistically—considering factors such as frequency, transaction type, counterparties, and historical context—allowing them to distinguish between normal variations and genuinely suspicious anomalies. This enables compliance teams to focus on high-risk cases and improves operational efficiency within AML departments.

Second, AI improves detection accuracy by identifying subtle, repetitive patterns that traditional systems often fail to capture. Money launderers commonly use techniques such as structuring, smurfing, and repeated low-value transfers to evade regulatory scrutiny. AI models, especially those using machine learning and anomaly detection, can detect these patterns even when they are intentionally disguised. For instance, AI can identify multiple transactions structured just below regulatory reporting thresholds or repeated fund movements across interconnected accounts, both of which are common laundering strategies designed to avoid triggering alerts.

Third, AI enables real-time monitoring and scalability, which are essential in today's high-volume transaction environment. As financial institutions continue to process millions of transactions per day across digital channels, manual or rule-based systems become increasingly insufficient. AI-driven platforms can analyze large datasets at high speed, generate alerts instantly, and adapt to increased transaction volumes without requiring a proportional increase in compliance staff or infrastructure. This scalability ensures that AML detection capabilities remain robust even as financial ecosystems grow more complex.

IV. CHALLENGES AND LIMITATIONS

Despite its significant advantages, the implementation of AI in AML presents several important challenges that financial institutions must address to ensure effective and responsible deployment [16]. While AI-driven models offer superior detection capabilities, their performance depends heavily on the quality of data, the transparency of analytical processes, and the availability of technical expertise and supporting infrastructure.

A major challenge lies in data quality and availability[17]. AI systems require large, diverse, and accurately labeled datasets to perform effectively. Poor data quality—such as incomplete records, inconsistent formatting, or outdated information—can lead to inaccurate predictions, false alarms, or overlooked suspicious behaviors. Moreover, compliance data often exists in fragmented systems across multiple departments, making data integration difficult. If training data contains historical biases, AI systems may inadvertently replicate or amplify these biases, compromising AML effectiveness and fairness.

Another key limitation is model explainability. Many advanced AI approaches, especially deep learning models, function as "black boxes," providing outputs without clear reasoning behind their decisions. In the context of AML, regulators require detailed justification for why a transaction was flagged as suspicious. A lack of interpretability can therefore hinder regulatory compliance, slow down investigation processes, and reduce trust in AI-driven decisions. This challenge is particularly critical as financial institutions must demonstrate transparency and accountability in their AML workflows.

Additionally, high implementation costs and technological complexity pose barriers to widespread adoption. Building and maintaining AI systems requires significant investment in data infrastructure, cloud computing, cybersecurity frameworks, and model governance tools. Smaller financial institutions, in particular, may find these costs prohibitive. The shortage of skilled professionals—including data scientists, AML specialists, and AI engineers—further limits the ability of organizations to develop, deploy, and maintain advanced AI models effectively. Without proper expertise, institutions risk misconfiguring AI systems or failing to monitor them adequately.

In summary, while AI has strong potential to enhance AML monitoring, addressing these challenges is essential for achieving reliable, transparent, and sustainable AI-driven compliance frameworks.

V. FUTURE SCOPE OF AI IN AML

The future application of AI in AML is highly promising and is expected to drive transformative advancements across the financial crime detection landscape. As money laundering techniques continue to evolve, AML systems must become more adaptive, transparent, and capable of responding to complex transactional behaviors in real time. Emerging AI technologies are positioned to meet these demands and significantly enhance the effectiveness of AML frameworks.

One of the most important developments is the advancement of explainable AI (XAI). Traditional AI models, especially deep learning systems, often lack transparency, making it difficult for financial institutions to justify model outputs to regulators. XAI aims to address this concern by providing interpretable and transparent decision-making processes. This will not only improve regulatory acceptance but also enhance investigator trust and support more effective case management.

The integration of AI with blockchain analytics, biometric verification systems, and real-time payment infrastructures represents another major area of growth. Blockchain analytics will strengthen surveillance over cryptocurrency transactions, enabling better detection of cross-chain laundering and illicit fund flows. Biometric verification will enhance customer due diligence, while real-time payments data—combined with AI-driven anomaly detection—will support instant identification of suspicious activity.

In addition, collaborative AI platforms that enable secure and privacy-preserving information sharing across financial institutions may significantly enhance the detection of cross-border, multi-institution, and repetitive laundering schemes. Such collaborative models can help organizations identify patterns that may remain hidden when data is analyzed in isolation.

As regulatory standards evolve, AI will play a critical role in building adaptive, resilient, and intelligent AML systems. Future AML frameworks are expected to incorporate autonomous AI agents for continuous risk assessment, predictive analytics for emerging threats, and federated learning architectures that safeguard data privacy while improving model accuracy. Overall, the continued advancement and adoption of AI technologies will shape the next generation of global AML practices.

VI. CONCLUSION

Artificial Intelligence has significantly transformed Anti-Money Laundering practices by enabling more accurate, adaptive, and efficient detection of repetitive and suspicious transaction patterns [20]. Traditional rule-based AML systems are limited by static thresholds, high false-positive rates, and an inability to detect complex or evolving laundering typologies. AI overcomes many of these limitations by leveraging machine learning algorithms, anomaly detection techniques, and advanced network and graph analytics to analyze large-scale financial data and uncover hidden behavioral patterns.

Machine learning models enhance classification accuracy by learning from historical transactions, while anomaly detection systems identify deviations from expected customer behavior that may indicate laundering activities[21]. Network and graph analysis further strengthen AML frameworks by revealing complex fund flows, hidden account relationships, and circular transaction structures often associated with sophisticated financial crime schemes.

Despite these advancements, challenges related to data quality, model explainability, regulatory compliance, implementation costs, and the shortage of skilled AI professionals continue to pose obstacles to widespread adoption. Ensuring transparent and interpretable AI models remains crucial for meeting regulatory expectations, while high-quality, unbiased datasets are essential for achieving accurate and reliable outcomes.

Nonetheless, the overall contribution of AI to AML effectiveness is substantial. As technological innovation continues—particularly in areas such as explainable AI, federated learning, and blockchain analytics—AI-driven AML systems will become increasingly robust, transparent, and capable of addressing emerging financial crime risks. Continued regulatory support and industry collaboration will further strengthen AI's role in combating money laundering and ensuring the integrity of the global financial system.

ACKNOWLEDGMENT

The author expresses sincere gratitude to the faculty members and academic resources of the Institute of Management Development and Research (IMDR), Pune, for their continuous guidance, valuable insights, and support throughout the development and completion of this research work. Their encouragement and academic environment played a significant role in shaping the quality and direction of this study.

REFERENCES

[1] A. Ali, S. Abd Razak, S. H. Othman, T. A. E. Eisa, A. Al-Dhaqm, M. Nasser, T. Elhassan, H. Elshafie, and A. Saif, "Financial fraud detection based on machine learning: A systematic literature review," *Applied Sciences*, vol. 12, no. 19, p. 9637, 2022. Available: https://www.mdpi.com/2076-3417/12/19/9637

[2] M. N. U. Milon, "Gravitating towards artificial intelligence on anti-money laundering: A PRISMA based systematic review," *International Journal of Religion*, vol. 5, no. 7, pp. 303–315, 2024. Available: https://www.researchgate.net/publication/380440406_Gravitating_towards_Artificial_Intelligence_on_Anti-Money_Laundering_A_PRISMA_Based_Systematic_Review

[3] N. Husnaningtyas, G. F. Hanin, T. Dewayanto, and M. F. Malik, "A systematic review of anti-money laundering systems literature: Exploring the efficacy of machine learning and deep learning integration," *JEMA: Jurnal Ilmiah Bidang Akuntansi dan Manajemen*, vol. 20, no. 1, pp. 91–116, 2023. Available: https://www.researchgate.net/publication/376884056_A_systematic_review_of_anti-money_laundering_systems_literature_Exploring_the_efficacy_of_machine_learning_and_deep_learning_integration

[4] N. Bakhshinejad, R. Soltani, U. T. Nguyen, and P. Messina, "A survey of machine learning based anti-money laundering solutions," *ResearchGate*, 2022. Available: https://www.researchgate.net/publication/364326902_A_Survey_of_Machine_Learning_Based_Anti-Money_Laundering_Solutions

[5] W. Harrison, "AI for anti-money laundering (AML) and know your customer (KYC) compliance," *ResearchGate*, 2024. Available: https://www.researchgate.net/publication/389465811_AI_for_Anti-Money_Laundering_AML_and_Know_Your_Customer_KYC_Compliance

[6] O. Oyedokun, S. E. Ewim, and O. P. Oyeyemi, "A comprehensive review of machine learning applications in AML transaction monitoring," *International Journal of Engineering Research and Development*, vol. 20, no. 11, 2024. Available: https://www.researchgate.net/publication/388277251_A_Comprehensive_Review_of_Machine_Learning_Applications_in_AML_Transaction_Monitoring

[7] M. Weber, G. Domeniconi, J. Chen, D. K. I. Weidele, C. Bellei, T. Robinson, and C. E. Leiserson, "Anti-money laundering in Bitcoin: Experimenting with graph convolutional networks for financial forensics," *arXiv preprint*, 2019. Available: https://www.researchgate.net/publication/335028528_Anti-Money_Laundering_in_Bitcoin_Experimenting_with_Graph_Convolutional_Networks_for_Financial_Forensics

[8] O. Lawal, A. Okolie, and C. Obunadike, "An explainable graph neural network framework for anti-money laundering in cryptocurrency transactions using the Elliptic dataset," *International Journal of Network Security & Its Applications (IJNSA)*, vol. 17, no. 5/6, 2025. Available: https://www.researchgate.net/publication/398062882_AN_EXPLAINABLE_GRAPH_NEURAL_NETWORK_FRAMEWORK_FOR_ANTI-MONEY_LAUNDERING_IN_CRYPTOCURRENCY_TRANSACTIONS_USING_THE_ELLIPTIC_DATASET

[9] F. Johannessen and M. Jullum, "Finding money launderers using heterogeneous graph neural networks," *The Journal of Finance and Data Science*, vol. 11, p. 100175, 2025. Available: https://www.researchgate.net/publication/399010172_Finding_Money_Launderers_Using_Heterogeneous_Graph_Neural_Networks

[10] I. Alarab, S. Prakoonwit, and M. I. Nacer, "Comparative analysis using supervised learning methods for anti-money laundering in Bitcoin," in *ICMLT 2020: 5th International Conference on Machine Learning Technologies*, pp. 11–17, 2020. Available: https://www.researchgate.net/publication/343298733_Comparative_Analysis_Using_Supervised_Learning_Methods_for_Anti-Money_Laundering_in_Bitcoin

[11] O. R. Tiamiyu, "Unveiling hidden money laundering networks: The application of graph neural networks in financial transaction analysis," *Journal of Computational Analysis and Applications*, vol. 34, no. 9, pp. 50–74, 2025. Available: https://www.researchgate.net/publication/398103130_Unveiling_Hidden_Money_Laundering_Networks_The_Application_of_Graph_Neural_Networks_in_Financial_Transaction_Analysis

[12] Q. Yu, Z. Xu, and Z. Ke, "Deep learning for cross-border transaction anomaly detection in anti-money laundering systems," in *2024 6th International Conference on Machine Learning, Big Data and Business Intelligence (MLBDBI)*, 2024. Available: https://www.researchgate.net/publication/386947202_Deep_Learning_for_Cross-Border_Transaction_Anomaly_Detection_in_Anti-Money_Laundering_Systems

[13] S. Kaur and N. K. Sandhu, "Novel technique of anti-money laundering using deep learning," *Journal of Emerging Technologies and Innovative Research*, vol. 9, no. 5, pp. e532–e537, 2022. Available: https://www.researchgate.net/publication/361182351_Novel_Technique_of_Anti-Money_Laundering_Using_Deep_Learning

[14] D. Savage, Q. Wang, P. Chou, X. Zhang, and X. Yu, "Detection of money laundering groups using supervised learning in networks," *arXiv preprint*, 2016. Available: https://www.researchgate.net/publication/305779558_Detection_of_money_laundering_groups_using_supervised_learning_in_networks

[15] D. V. Kute, B. Pradhan, N. Shukla, and A. Alamri, "Explainable deep learning model for predicting money laundering transactions," *International Journal on Smart Sensing and Intelligent Systems*, vol. 17, no. 1, 2024. Available: https://www.researchgate.net/publication/382555029_Explainable_deep_learning_model_for_predicting_money_laundering_transactions

[16] A. Ray, "Applying AI in anti-money laundering operations," *Journal of AI Robotics & Workplace Automation*, vol. 1, no. 2, 2021. Available: https://www.researchgate.net/publication/382565301_Applying_AI_in_anti-money_laundering_operations

[17] R. El-Kady, "Regulating intelligence: Legal safeguards for AI in anti-money laundering," in *Financial Corruption and Money Laundering in the AI Era*, IGI Global, pp. 133–162, 2025. Available: https://www.researchgate.net/publication/396379970_Regulating_Intelligence_Legal_Safeguards_for_AI_in_Anti-Money_Laundering

[18] O. D. Iguodala and A. Oyiborhoro, "AI-powered anti-money laundering (AML) and fraud detection – enhancing financial security through intelligent fraud detection," *World Journal of Advanced Research and Reviews*, vol. 26, no. 2, pp. 3702–3714, 2025. Available: https://www.researchgate.net/publication/392235964_AI-Powered_Anti-Money_Laundering_AML_and_fraud_detection_-_enhancing_financial_security_through_intelligent_fraud_detection

[19] A. A. Paul and C. Ogburie, "The role of AI in preventing financial fraud and enhancing compliance," *GSC Advanced Research and Reviews*, vol. 22, no. 3, pp. 269–282, 2025. Available: https://doi.org/10.30574/gscarr.2025.22.3.0086

[20] T. A. Siddquee, "AI in banking risk management and fraud detection in preventing financial crimes and optimizing credit decisions," *International Journal of Social Science Research and Review*, vol. 8, no. 8, pp. 391–404, 2025. Available: https://ijssrr.com/journal/article/view/2889

[21] N. Husnaningtyas and T. Dewayanto, "Financial fraud detection and machine learning algorithm (unsupervised learning): Systematic literature review," *Jurnal Riset Akuntansi dan Bisnis Airlangga*, vol. 8, no. 2, pp. 1521–1542, 2023. Available: https://e-journal.unair.ac.id/jraba

[22] G. S. Sowmya and H. K. Sathisha, "Detecting financial fraud in the digital age: The AI and ML revolution," *International Journal for Multidisciplinary Research*, vol. 5, no. 5, 2023. Available: https://pdfs.semanticscholar.org/b19f/764069f155fbb60eed1c2977d1d33c665e34.pdf

[23] A. Mukhamadiyev, F. Nazarov, S. Yarmatov, and J. Cho, "Intelligent algorithms for the detection of suspicious transactions in payment data management systems based on LSTM neural networks," *Sensors*, vol. 25, no. 21, p. 6683, 2025. Available: https://pmc.ncbi.nlm.nih.gov/articles/PMC12610375/

[24] P. V. Naik, N. K. Dintakurthi, Z. Hu, Y. Wang, and R. Qiu, "Co-investigator AI: The rise of agentic AI for smarter, trustworthy AML compliance narratives," *arXiv preprint*, 2025. Available: https://arxiv.org/abs/2509.08380

[25] R. Craelius, "Enhancing fraud detection with graph-based machine learning," Master's thesis, KTH Royal Institute of Technology, 2025. Available: https://www.diva-portal.org/smash/get/diva2:1998930/FULLTEXT01.pdf

[26] D. Rube and I. Wirgén, "Supervised fraud detection of mobile money transactions on different distributions of imbalanced data," Bachelor's thesis, Uppsala University, 2021. Available: https://www.diva-portal.org/smash/get/diva2:1567972/FULLTEXT01.pdf

[27] A. I. Andreescu, S.-V. Oprea, A. G. Văduva, and A. Bâra, "Anti-money laundering compliance using feature engineering with SQL analytics, TF-IDF and oversampling: Conditional tabular generative adversarial networks," *Informatica*, vol. 36, no. 3, pp. 491–524, 2025. Available: https://doi.org/10.15388/25-INFOR598

[28] S. Mousavian and S. J. Miah, "Review of artificial intelligence-based applications for money laundering detection," *Intelligent Systems with Applications*, vol. 27, p. 200572, 2025. Available: https://doi.org/10.1016/j.iswa.2025.200572