aml/cft journal
journal of anti-money laundering / countering the financing of terrorism

Original paper

Money Laundering Typology Detection Using Graph Analytics and Neural Networks

Lalu Garin Alham[1]*, Nadia Tsabitah[2], Yusuf Muhammad Nur Zaman[2]

[1] Fraud Management & Authorization, PT Espay Debit Indonesia Koe (DANA), Indonesia
[2] Audit, PT Bank Rakyat Indonesia Tbk (BRI), Indonesia

Corresponding author: alhamgarin@gmail.com

Keywords:
Financial crime, Graph theory, Machine learning, Money laundering

Abstract

Money laundering accounts for an estimated 2–5% of global GDP annually with scale intensified by digital ecosystems. Conventional AML systems using primarily rule-based and transactional patterns struggle to detect relational behaviors of financial crimes. This study introduces an integrated graph-analytic framework to detect structural laundering patterns using graph-derived metrics to neural network pipeline. The paper evaluates eccentricity, degree, closeness measures, and directionality of flow to distinguish laundering activities, supported by Welch's t-test which confirms statistically significant differences across five of six metrics ($p < 0.001$). A Multi-Layer Perceptron (MLP) model is further applied to classify 17 typologies with ~80% accuracy. The key contribution of this research lies in demonstrating that financial crime typologies can be extracted from network topology itself instead of sole reliance on transactional features. By linking graph metrics with laundering behaviors including placement, layering, and integration patterns the study provides a scalable, network-aware approach to AML detection. Future work should focus on real-world validation and real-time classification pipelines using graph-neural inference.

Submitted: 15 July 2025
Accepted: 15 December 2025
Published: 31 December 2025

***To cite this article*:** Alham, L. G., Tsabitah, N., & Zaman, Y. M. N. 2025. *Money Laundering Typology Detection Using Graph Analytics and Neural Networks. AML/CFT Journal: The Journal of Anti Money Laundering and Countering the Financing of Terrorism* 4(1):49-67, https://doi.org/10.59593/amlcft.2025.v4i1.269

Introduction

Financial crime and money laundering continue to pose a significant threat to the integrity of the global financial system. Furthermore, the COVID pandemic increased criminal opportunities through rapid digitalization of communications and payment channels.[1] This is especially emphasized within the Asia-Pacific (APAC) region where the digitalization of the

[1] APG, "About Anti-Money Laundering and Counter Terrorism Financing | Asia / Pacific Group On Money Laundering," last modified 2021, https://www.apgml.org/about-us/about-anti-money-laundering-and-counter-terrorism-financing.

economy was manifested through e-commerce growth and innovation in financial technology.[2] The region is considered a hotspot for money laundering activities due to its rapid economic growth, diverse financial systems, and varying levels of regulatory enforcement. As such, Anti-Money Laundering (AML) efforts within APAC should take into consideration the collective social behavior and intricate financial strategies that transcend national borders.[3]

According to the United Nations Office on Drugs and Crime,[4] approximately 2-5% of global GDP is laundered annually, amounting to an estimated 1.7 trillion to 4.2 trillion in 2020. The East and Southeast Asia region contributes to this figure from primarily scam and financial ecosystem fraud with an estimated 18-37 billion USD.[5] Nonetheless, digital economies have exacerbated the risks. Another report[6] further mentioned that fraud (and the consequent illicit transaction flow) has spread into adjacent domains where oversight may be uneven. Despite those studies, the true scale of money laundering is likely underreported, especially in regions with a more lenient AML governance and limited enforcement capabilities. The money laundering risks relevant to the discussed issue in this paper are: (1) Cryptocurrencies and decentralized asset platforms enabling anonymous transactions amid unclear provisions;[7] (2) Online gambling and its exploitation for laundering via virtual assets;[8] (3) Permissive incorporation of company administrations facilitating establishment of shell companies;[9] (4) Forged and/or synthetic identities that bypass weak digital KYC measures;[10] (5) PEPs who abused regulatory gaps to launder illicit proceeds;[11] and (6) Trade-based schemes to masquerade movements of assets from criminal proceeds.[12]

---

[2] World Economic Forum, *Digital Transformation: Powering the Great Reset* (Switzerland: World Economic Forum, 2020).

[3] Jacopo Costa, "Research Case Study 3: Exposing the Networks behind Transnational Corruption and Money Laundering Schemes," Basel Institute on Governance, last modified May 31, 2023, https://baselgovernance.org/publications/research-case-3.

[4] APG, "About Anti-Money Laundering and Counter Terrorism Financing | Asia / Pacific Group On Money Laundering"; Ali Alkaabi et al., "A Comparative Analysis of the Extent of Money Laundering in Australia, UAE, UK and the USA," SSRN Scholarly Paper no. 1539843 (Rochester, NY: Social Science Research Network, 2010), https://doi.org/10.2139/ssrn.1539843.

[5] Sam Rogers, "Cyber-Fraud, Underground Banking, and Technological Innovation Fuels Crime in SE Asia," GASA, last modified December 17, 2024, https://www.gasa.org/post/unodc-cyber-fraud-underground-banking-and-technological-innovation-fuels-crime-in-se-asia; Dennis Miralis et al., *Anti-Money Laundering Laws and Regulations Anti-Money Laundering in the Asia-Pacific Region: An Overview 2025* (London: International Comparative Legal Guides (ICLG), 2025), United Kingdom.

[6] Katherine Cloud and Ilya Brovin, "How Identity Fraud Is Changing in the Age of AI," World Economic Forum, last modified December 11, 2025, https://www.weforum.org/stories/2025/12/how-identity-fraud-is-increasing-in-the-age-of-ai/.

[7] Jeffry Collins, "Cryptocurrencies and Financial Crimes: The Role of Decentralized Cryptocurrency in Facilitating Money Laundering and the Challenges Posed on Anti–Money Laundering Regulations," *University of Miami Business Law Review* 34, no. 1 (2025): 71; Chainalysis Team, "2023 Crypto Crime Trends: Illicit Cryptocurrency Volumes Reach All-Time Highs Amid Surge in Sanctions Designations and Hacking," Chainalysis, last modified January 12, 2023, https://www.chainalysis.com/blog/2025-crypto-crime-report-introduction/.

[8] UNODC, *The Nexus Between Cybercrime and Corruption* (Vienna: United Nations Office on Drugs and Crime, 2025).

[9] World Bank, "Corrupt Money Concealed in Shell Companies and Other Opaque Legal Entities, Finds New StAR Study," World Bank, last modified October 24, 2011, https://doi.org/10/24/corrupt-money-concealed-in-shell-companies-and-other-opaque-legal-entities-finds-new-star-study.

[10] Tom Vidovic, "The Rise of the Synthetic Identity: A Growing Threat in the Digital Age," Global Compliance Institute, last modified July 5, 2024, https://www.gci-ccm.org/.

[11] Costa, "Research Case Study 3."

[12] FATF - Egmont Group, *FATF/Egmont Trade-Based Money Laundering: Trends and Developments* (Paris: FATF - Egmont Group, 2020).

As financial crimes grow increasingly sophisticated within the inherently complex financial systems, traditional methods of detection and prevention may not be adequate in identifying these illicit activities. In recent years, graph theory and graph analytics have emerged as powerful tools for analyzing complex networks, including those in financial crimes. Graph databases and graph-based machine learning models provide a unique capability to map and examine relationships between entities, making them particularly effective for identifying patterns and anomalies in financial transactions. By leveraging graph metrics such as centrality measures (e.g., degree centrality, eigenvector centrality) and graph-based analytics, financial institutions can uncover hidden networks and detect suspicious activities indicative of money laundering.[13] Moreover, advancements in graph neural networks (GNNs) have enabled the creation of embeddings that capture the topology and properties of nodes within a graph to significantly enhance detection performances by aggregating networks of transactions into the observation.[14]

However, several gaps remain in implementation of graph theory and machine learning to fraud detection & AML. First, there is a need for more comprehensive datasets that capture the diversity and complexity of money laundering typologies. Second, the explainability of graph-based models, particularly GNNs, remains a challenge, as their decision-making processes are often opaque. Finally, there is a lack of predictive models capable of intercepting suspicious entities in real-time, which is critical for proactive AML efforts.

This paper responds to those gaps by examining money laundering typologies/schemes through graph-based representations and neural classification. The study identifies and analyses money laundering patterns using graph theory supported by AI/ML techniques, proposes an analytical framework for evaluating AML risks in transactional networks, and develops a predictive model that assesses whether a network segment is likely to reflect financial crime activity.

Literature Review

Financial crime and money laundering emerged as a critical challenge to global economic stability and integrity. However, implementation of Anti-Money Laundering (AML) regulatory frameworks placed significant operational demands on financial institutions, necessitating an adoption of advanced measures to detect and prevent illicit activities.[15] Money laundering often involves highly organized syndicates aided with corruptive acts from officials, employing sophisticated financial strategies to launder illicit funds, frequently operating across borders, and utilizing complex transactions to obscure the origins of the money. Despite increased awareness of these issues, the relationship between corruption and money laundering remains inadequately understood, particularly in terms of the structures, mechanisms, and the networks that facilitate these crimes.[16]

Efforts to improve detection accuracy have led to the adoption of machine learning techniques trained on transactional features such as value, frequency and timing. These models

[13] Milind Tiwari, Jamie Ferrill, and Vishal Mehrotra, "Using Graph Database Platforms to Fight Money Laundering: Advocating Large Scale Adoption," *Journal of Money Laundering Control* 26, no. 3 (2022): 474–87, https://doi.org/10.1108/JMLC-03-2022-0047.

[14] Dawei Cheng et al., "Anti-Money Laundering by Group-Aware Deep Graph Learning," *IEEE Transactions on Knowledge and Data Engineering* 35, no. 12 (2023): 12444–57, https://doi.org/10.1109/TKDE.2023.3272396.

[15] Costa, "Research Case Study 3."

[16] Costa, "Research Case Study 3."

are effective in identifying atypical behavior within transaction records,[17] but they generally assume that each transaction is independent. As a result, they provide limited insight into relational structures or multi-entity schemes, which are frequently exploited in placement, layering and integration processes described in AML typologies.[18]

Prior work on AML detection can be broadly grouped into three clusters: (i) rule-based transaction monitoring, (ii) adoption of machine-learning and deep-learning models trained on transactional features,[19] and (iii) network or graph-based approaches that explore relational properties between entities.[20] This group consists of several recent surveys and systematic reviews of AML systems and network analytics. Rising recognition of these limitations has led to increased interest in graph-based approaches, which model accounts or entities as nodes and transactions as edges. This representation enables the analysis of relationships, fund flow patterns and network structure that cannot be captured through transactional attributes alone. The foundations of graph theory originate from Euler's work on the geometry of connected systems,[21] and modern graph visualization algorithms have supported the interpretation of large-scale networks across many domains.[22] In AML research, graph analytics have been used to identify central actors, intermediaries and layered routing patterns within transaction networks.[23]

Hence, graph-based models have been increasingly adopted to leverage the relational structure of a Money Laundering scheme. Notable contributions include scalable graph learning frameworks applied to AML,[24] typology-aware deep graph learning approaches,[25] and graph-based fraud control models for financial institutions.[26] A systematic review by Deprez et al.[27] further emphasized this by highlighting the methodological expansion of network analytics for AML context and the increasing emphasis on relational modelling. Table 1 summarizes the comparative framework of AML approaches.

[17] Nazanin Bakhshinejad et al., "A Survey of Machine Learning Based Anti-Money Laundering Solutions," *Internet of Things—Applications and Future*, 2022, 73–87.
[18] Amel Muminovic and Festim Halili, "Money Laundering Prevention in the Digital Age: Leveraging Graph Databases for Effective Solutions," *Sciences (IJTNS)* 4, no. 1 (2024): 1–10.
[19] Bakhshinejad et al., "A Survey of Machine Learning Based Anti-Money Laundering Solutions."
[20] Ryan Weber et al., *A Spatial Analysis of City-Regions: Urban Form & Service Accessibility* (Stockholm: Nordregio, 2016); Bruno Deprez et al., "Network Analytics for Anti-Money Laundering—A Systematic Literature Review and Experimental Evaluation," *INFORMS Journal on Data Science* (2025), https://doi.org/10.1287/ijds.2024.0042.
[21] Leonhard Euler, "Solutio Problematis Ad Geometriam Situs Pertinentis," *Euler Archive - All Works* (1741): 128–40.
[22] Mathieu Jacomy et al., "ForceAtlas2, a Continuous Graph Layout Algorithm for Handy Network Visualization Designed for the Gephi Software," *PLoS One* 9, no. 6 (2014): e98679, https://doi.org/10.1371/journal.pone.0098679.
[23] Tiwari, Ferrill, and Mehrotra, "Using Graph Database Platforms to Fight Money Laundering."
[24] Weber et al., *A Spatial Analysis of City-Regions*.
[25] Cheng et al., "Anti-Money Laundering by Group-Aware Deep Graph Learning."
[26] Atif Usman, Nasir Naveed, and Saima Munawar, "Intelligent Anti-Money Laundering Fraud Control Using Graph-Based Machine Learning Model for the Financial Domain," *Journal of Cases on Information Technology (JCIT)* 25, no. 1 (2023): 1–20, https://doi.org/10.4018/JCIT.316665.
[27] Deprez et al., "Network Analytics for Anti-Money Laundering—A Systematic Literature Review and Experimental Evaluation."

Table 1. Comparative Matrix on AML Methodologies (various sources)

Approach	Strengths	Limitations	Representative Studies	Relation to Present Study
Rule-based / scenario monitoring	Transparent; straightforward to implement; aligned with regulatory models	High false positives; weak detection of structured or multi-entity laundering	FATF, APG guidance	Motivates the need for analytic methods beyond thresholds
ML using transactional features	Learning non-linear patterns; reduces manual review burden	Ignore relationships between entities; limited capacity to detect network structures	Bakhshinejad et al. (2022)[28]	Supports use of relational graph metrics as complementary features
Graph analytics (structural analysis)	Captures network topology; identifies intermediaries, hubs and laundering motifs	Often descriptive; predictive typology mapping limited	Tiwari et al. (2022);[29] Muminovic and Halili (2024);[30] Oztas et al. (2023)[31]	This study tests whether graph metrics statistically distinguish typologies
Graph-based ML / GNN	Learning relational patterns directly from graph structure	Higher computational cost; reduced interpretability	Weber et al. (2018);[32] Cheng et al. (2023);[33] Usman et al. (2023);[34] Deprez et al. (2025)[35]	MLP selected for interpretability and efficiency on synthetic graph metrics

[28] Bakhshinejad et al., "A Survey of Machine Learning Based Anti-Money Laundering Solutions."
[29] Tiwari, Ferrill, and Mehrotra, "Using Graph Database Platforms to Fight Money Laundering."
[30] Muminovic and Halili, "Money Laundering Prevention in the Digital Age."
[31] Berkan Oztas et al., "Enhancing Anti-Money Laundering: Development of a Synthetic Transaction Monitoring Dataset," *2023 IEEE International Conference on E-Business Engineering (ICEBE)*, November 2023, 47–54, https://doi.org/10.1109/ICEBE59045.2023.00028.
[32] Weber et al., *A Spatial Analysis of City-Regions*.
[33] Cheng et al., "Anti-Money Laundering by Group-Aware Deep Graph Learning."
[34] Usman, Naveed, and Munawar, "Intelligent Anti-Money Laundering Fraud Control Using Graph-Based Machine Learning Model for the Financial Domain."
[35] Deprez et al., "Network Analytics for Anti-Money Laundering—A Systematic Literature Review and Experimental Evaluation."

GNN offers capable network analysis power for relational data and has been used in multitudes of AML themed research,[36] but on the other hand this method requires hefty computational demands and reduced reasoning transparency due their black box characteristics. In this study, the authors opted for a Multilayer Perceptron (MLP)[37] for the analysis as they can also capture non-linear feature relationships, remain computationally efficient, and enable clearer attribution of each graph metric's influence. Thus, serving as an appropriate methodological alternative to the inherently complex graph-based models.

Data and Methodology

Graph Statistics

Metrics such as eccentricity, centrality, and degree can be utilized to measure and capture the behavior of a node in a graph and its significance of nodes in a network of financial transactions. This paper utilized centrality measurements[38] composed of *Betweenness*, *Eigenvector*, *Closeness*, and degree. In detail, the measured graph statistics are:

a. Eccentricity: The longest shortest path from a node to any other node. Identifies peripheral actors (high eccentricity) who might be "hidden" in the network and are unusually distant from others (e.g., shell companies with few connections).
b. Closeness Centrality: relative closeness of node to all other nodes (average shortest path). High closeness commonly acts as the central hub (e.g., payment facilitation). Low closeness is potentially isolated mules or layering accounts.
c. Harmonic Closeness Centrality: like closeness but gives more weight to nearby nodes (preferably for disconnected graphs composed of separated communities). Detect key intermediaries even if the network is fragmented (common in layered transactions).
d. Betweenness Centrality: measures how often a node lies on the shortest path between others. Flags critical nexus/choke points (e.g., money service businesses, casinos, or *gatekeepers* facilitating fund flows). High betweenness is potentially layering/structuring accounts.
e. Weighted Degree (*in-degree* and *out-degree*): measures the sum of all incoming and outgoing *edges*. Help identify anomalous high-activity nodes.

SAML-D Dataset

Synthetic datasets, such as the SAML-D framework[39] provided researchers to study money laundering typologies. These datasets incorporate a wide range of features, enabling the simulation of complex money laundering scenarios. Table 2 shows SAML-D dataset incorporates features based on existing/available information, academic literature, and interviews/primary accounts from AML specialists and is comprised of 9,504,852 transactions, 0.104% of which are labelled as 'suspicious' activities.

[36] Cheng et al., "Anti-Money Laundering by Group-Aware Deep Graph Learning"; Usman, Naveed, and Munawar, "Intelligent Anti-Money Laundering Fraud Control Using Graph-Based Machine Learning Model for the Financial Domain."
[37] Marius-Constantin Popescu et al., "Multilayer Perceptron and Neural Networks," *WSEAS Transactions on Circuits and Systems* 8, no. 7 (2009): 579–88.
[38] Mark E. J. Newman, *Networks—An Introduction* (Oxford: Oxford University Press, 2012).
[39] Oztas et al., "Enhancing Anti-Money Laundering."

Table 2. SAML-D Dataset Features

No.	Features	Description
1	a. Time b. Date	Essential for tracking transaction chronology.
2	a. Sender_Bank_Account b. Receiver_Bank_Account	Helps uncover behavioural patterns and complex banking connections. Acted as the nodes of a Graph function.
3	Transaction_Amount	Indicates transaction values to identify suspicious activities.
4	Payment_Type	Includes various methods such as credit card, debit card, cash, ACH transfers, cross-border, and cheque. Rendered as the *label* of *edges* for Graph function within this paper.
5	a. Sender_bank_location b. Receiver_bank_location	Pinpoints high-risk regions including Mexico, Turkey, Morocco, and the UAE.
6	a. Payment_Currency b. Received_Currency	Align with location features, adding complexity when mismatched.
7	Is_Suspicious	Boolean, [0, 1] (no' and 'yes' respectively) indicator differentiating normal from suspicious transactions.
8	Type	Classifies money laundering methods and typologies as in the following. a. *Smurfing*: Breaking large sums into smaller, less suspicious transactions (e.g., multiple deposits under reporting thresholds). b. *Cash_Withdrawal*: Withdrawing illicit cash to reintroduce it into the financial system via clean channels. c. *Single_large*: Direct placement of a single large transaction (risky but fast). d. *Structuring*: Similar to smurfing but with structured patterns (e.g., fixed amounts at regular intervals). e. *Layered_Fan_In*: Funds funneled into a central account from multiple sources (resembles a "wheel with spokes"). f. *Layered_Fan_Out*: Funds disbursed from a central account to many endpoints (reverse of Fan_In). g. *Scatter-Gather*: Funds split into smaller amounts, routed through intermediaries, then recombined. h. *Gather-Scatter*: The inverse: combined funds are split after initial gathering. i. *Cycle*: Circular transactions among accounts to obscure origins (e.g., A → B → C → A).

j. *Bipartite/Stacked Bipartite*: Funds move between two distinct groups of accounts (e.g., shell companies ↔ mules).

k. *Behavioural_Change*: Sudden shifts in transaction patterns (e.g., a dormant account becoming hyperactive).

l. *Over-Invoicing*: Inflating trade invoice values to legitimize illicit funds.

m. *Deposit-Send*: Depositing "clean" funds into an account, then sending them to a final beneficiary.

n. *Fan_In/Fan_Out*: Final aggregation (Fan_In) or distribution (Fan_Out) of laundered funds to appear legitimate.

Source : Oztas et al.[40]

Analytical framework & modelling

a. Data acquisition & preparation. Gathering of raw data from SAML-D repository. It encompasses data collection, cleaning, and preprocessing to transform the data into a suitable format for analysis.
b. Feature engineering. Selecting, modifying, or creating new features based on the acquired data to improve model accuracy and interpretability.
c. Graph analysis & layouting algorithm. Application of graph-based techniques to model relationships and interactions within the data. *Multigravity Force Atlas*[41] layouting algorithm in Gephi open-source graph processing software is utilized in this paper. The algorithm enhances network visualization by applying adjustable gravitational forces to separate clusters, minimizing overlapping nodes to enhance visibility, and the ability to handle large-scale networks.
d. Statistical Test (*Welch's Paired T-Test*). This paired t-test[42] is a statistical method to compare the means of two independent sample groups and does not assume equal variances, making it preferable for real-world data beyond controlled samples.
   The hypotheses tested are as follows:

   1. Null Hypothesis (H_0): $\mu_1 = \mu_2$ (the population means of both groups' graph statistics are equal).
   2. Alternative Hypothesis (H_1): $\mu_1 \neq \mu_2$ (two-tailed) or $\mu_1 > \mu_2$ / $\mu_1 < \mu_2$ (one-tailed). Where the graph statistics' properties are not statistically equal.
      Thus, the decision rule can be described as,

$$\text{Reject } H_0 \text{ if p-value} < \alpha \text{ (where } \alpha = 0.05).$$

   The developed model should first be able to differentiate between sample spaces. Takes s1 as fraudulent and/or money laundering actors and s2 as good actor/normal customers of a financial platform.

[40] Oztas et al., "Enhancing Anti-Money Laundering."
[41] Jacomy et al., "ForceAtlas2, a Continuous Graph Layout Algorithm for Handy Network Visualization Designed for the Gephi Software."
[42] B. L. Welch, "The Generalization of 'Student's' Problem When Several Different Population Varlances Are Involved," *Biometrika* 34, no. 1–2 (1947): 28–35, https://doi.org/10.1093/biomet/34.1-2.28.

e. Heuristic analysis. Augments graph-based statistical methods by incorporating domain-specific rules and behavioral red flags to identify suspicious activities.
f. Model Implementation: To classify transactions potentially associated with money laundering, we implemented a Multi-Layer Perceptron (MLP) model using the PyTorch framework. The model was trained on transactional data that had been enriched with graph-based features, including measures such as centrality and edge weight. The MLP architecture consists of multiple hidden layers with ReLU activation functions and an output layer with either a '*sigmoid*' or '*softmax*' activation function, depending on the classification scheme. The optimization process utilized the Adam optimizer in conjunction with a binary cross-entropy loss function.
g. Evaluation & Interpretation: The model was evaluated using standard classification metrics, including precision, recall, and F1-score. The classification results demonstrated the model's ability to identify typical patterns of money laundering typologies, such as *layering* and *smurfing*.

Result and Discussion

This section exhibits the analytical findings aligned with the three objectives of the study, namely, (1) to examine whether graph metrics differ between fraudulent and non-fraudulent networks, (2) to analyze how money laundering typologies represented through network topology & structure, and (3) to evaluate the classification performance of an MLP model trained on graph features.

Analysis of Graph Statistics Between Two Sample Spaces

These results presented that graph-derived indicators capture structural distinctions between illicit and normal network segments (Fraud [s_1] and Non-fraud [s_2] sample spaces), providing empirical support for the hypothesis that laundering activities exhibit measurable topological divergence.

Descriptive statistics comparison

Table 3a and 3b below are the measurement results of descriptive graph statistics from $s_1 = s_2$. Comparative analysis found that fraudulent and non-fraudulent graph exhibited different characteristics in terms of collective eccentricity, centrality, and degree.

Table 3a. Fraud Data Graph Statistics

Metric	Min.	1st qu.	Median	Mean	3rd qu.	Max
Eccentricity	0.00	0.00	1.00	1.19	1.00	14.00
Closeness centrality	0.00	0.00	0.57	0.53	1.00	1.00
Harmonic closeness centrality	0.00	0.00	0.63	0.55	1.00	1.00
Betweenness centrality	0.00	0.00	0.00	0.00	0.00	0.00
Weighted Indegree	0.00	0.00	0.00	0.41	0.00	37.00

Weighted Outdegree	0.00	0.00	0.00	0.41	0.00	37.00
Weighted Degree	0.00	0.00	0.00	0.82	0.00	37.00

Table 3b. Non-Fraud Data Graph Statistics

Metric	Min.	1st qu.	Median	Mean	3rd qu.	Max
Eccentricity	0.00	0.00	0.00	0.17	0.00	2.00
Closeness centrality	0.00	0.00	0.00	0.17	0.00	1.00
Harmonic closeness centrality	0.00	0.00	0.00	0.17	0.00	1.00
Betweenness centrality	0.00	0.00	0.00	0.01	0.00	15.00
Weighted Indegree	0.00	1.00	1.00	2.62	3.00	24.00
Weighted Outdegree	0.00	0.00	0.00	2.62	0.00	281.00
Weighted Degree	1.00	1.00	2.00	5.24	4.00	281.00

Welch's t-test result

Table 4 describe calculation of two sample tests between $s_{1:}$ *fraud* and $s_{2:}$ *non-fraud* sample spaces. Comparison between two populations using Welch's t-test on Table 4 confirmed significant differences (where p-value < 0.05) in five of six graph metrics between fraudulent and non-fraudulent transactions. Eccentricity (t = 41.14) and closeness centrality (t = 45.27) were particularly discriminative, highlighting their utility in identifying layered transactions and central hubs. Weighted degree metrics (indegree: t = -34.46; outdegree: t = -9.67) further distinguished placement and integration phases. Only betweenness centrality showed no significant difference (p = 0.094), suggesting its limited role in isolating ML-specific behaviors.

Table 4. Welch's t-statistic and Corresponding p-value

No.	Variable	*t-statistic*	*p-value*	Verdict
1	Eccentricity	41.1395	0.0000	Significant difference
2	Closeness centrality	45.2665	0.0000	Significant difference
3	Betweenness centrality	-1.6736	0.0943	No significant difference
4	Weighted indegree	-34.4598	0.0000	Significant difference

5	Weighted outdegree	-9.6737	0.0000	Significant difference
6	Weighted Degree	-19.2556	0.0000	Significant difference

Table 5. Summarized Graph Statistics Characteristics Grouped by Money Laundering Typologies

No.	ML typologies	Eccentricity		Closeness centrality		Harmonic closeness centrality		Weighted indegree		Weighted outdegree		Weighted Degree	
		mean	median	mean	median	mean	median	mean	median	mean	median	mean	median
1	*Behavioural Change*	1.00	1.00	1.00	1.00	1.00	1.00	0.00	0.00	0.02	0.00	0.02	0.00
2	*Bipartite*	1.00	1.00	1.00	1.00	1.00	1.00	0.00	0.00	0.55	0.00	0.55	0.00
3	*Cash Withdrawal*	1.00	1.00	1.00	1.00	1.00	1.00	0.00	0.00	15.16	15.00	15.16	15.00
4	*Cycle*	9.75	10.00	0.21	0.18	0.32	0.29	0.99	1.00	1.00	1.00	1.99	2.00
5	*Deposit Send*	1.84	2.00	0.62	0.55	0.65	0.58	0.00	0.00	0.00	0.00	0.00	0.00
6	*Fan In*	1.00	1.00	1.00	1.00	1.00	1.00	0.00	0.00	0.02	0.00	0.02	0.00
7	*Fan Out*	1.00	1.00	1.00	1.00	1.00	1.00	0.00	0.00	0.00	0.00	0.00	0.00
8	*Gather Scatter*	1.81	2.00	0.64	0.56	0.67	0.60	0.00	0.00	0.01	0.00	0.01	0.00
9	*Layered Fan In*	1.63	2.00	0.82	0.75	0.87	0.83	0.20	0.00	0.25	0.00	0.45	0.00
10	*Layered Fan Out*	1.19	1.00	0.92	1.00	0.94	1.00	0.06	0.00	0.96	1.00	1.02	1.00
11	*Over Invoicing*	1.50	1.50	0.83	0.83	0.88	0.88	0.50	0.50	1.00	1.00	1.50	1.50
12	*Scatter Gather*	1.18	1.00	0.97	1.00	0.98	1.00	0.13	0.00	0.27	0.00	0.40	0.00
13	*Single large*	1.00	1.00	1.00	1.00	1.00	1.00	0.00	0.00	0.33	0.00	0.33	0.00
14	*Smurfing*	1.00	1.00	1.00	1.00	1.00	1.00	0.00	0.00	14.79	15.00	14.79	15.00
15	*Stacked Bipartite*	1.36	1.00	0.92	1.00	0.94	1.00	0.11	0.00	0.40	0.00	0.50	0.00
16	*Structuring*	1.00	1.00	1.00	1.00	1.00	1.00	0.00	0.00	0.00	0.00	0.00	0.00

Analysis of Money Laundering Typologies Using Graph Metrics

Graph metric measurement of the money laundering typologies in Table 5 reveals distinct network patterns across different money laundering methods.

Key Observations

a. Transaction Patterns

Methods like *Cycle* and *Deposit-Send* show elongated transaction chains (high eccentricity) and lower centrality scores, suggesting multi-step layering behavior. In contrast, *Cash Withdrawal* and *Smurfing* demonstrate concentrated cash movement (low eccentricity) but high outbound transaction volumes.

b. Network Roles
Techniques such as *Layered_Fan_Out* and *Scatter-Gather* occupy intermediary positions in the network, with balanced centrality measures and moderate transaction weights. This aligns with their function as money redistribution mechanisms.

c. Distinctive Features
The *Over-Invoicing* method stands out with equal inbound and outbound transaction weights, indicating its use in circular value manipulation. Meanwhile, *Behavioural Change* and *Fan_Out* appear as endpoints in laundering chains, showing minimal inbound activity.

Interpretation

These measured graph metric characteristics correspond to money laundering typologies as follows:

a. Initial *placement* manifests as high outbound transaction volume from originating accounts/sources.

Placement (e.g., *Smurfing*, *Cash Withdrawal*) exhibited high outdegree (mean: 14.79–15.16) and low eccentricity (1.0), reflecting concentrated fund dispersal.

Figure 1. *Cash-withdrawal* scheme

b. *Layering* appears as complex transaction chains to disguise the underlying transactions.
Layering (e.g., *Layered Fan-out*, *Deposit-Send*) displayed elongated paths (eccentricity: 9.75) and low centrality, consistent with obfuscation strategies.

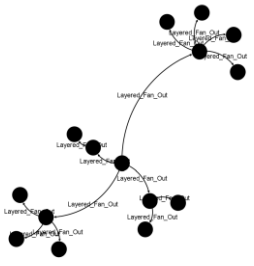

Figure 2. *Cycle* scheme

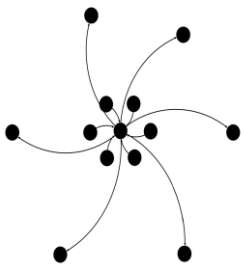

Figure 3. *Deposit-Send* scheme

c. Final *integration* shows as terminal/end-point nodes with imbalanced flows.
Integration (e.g., *Fan_Out*, *Behavioural_Change*) featured minimal indegree (0.0), marking endpoints in laundering chains.

Figure 4. *Fan-out* scheme

The consistent graph characteristics and patterns across above typologies suggest graph metrics can effectively flag suspicious financial behavior when calibrated appropriately. Thus, the analysis exhibits that graph metrics like centrality and degree of connectivity can be utilized for Money Laundering identification beyond a static rule-based/scenario monitoring system.

Model Implementation & Evaluation

In this study, the classification task was derived from a set of topological attributes (betweenness centrality, degree centrality, in-degree, and out-degree) as input features. This approach enables simplification of graph-based learning. To perform the classification, we implemented a feedforward neural network model, specifically a Multilayer Perceptron (MLP), using the PyTorch deep learning framework. The model architecture consists of an input layer corresponding to the number of extracted features, followed by a single hidden layer, and an output layer representing the class labels. This MLP-based approach enables the model to learn nonlinear relationships between graph-derived features and node classes in a supervised learning setting. The architecture is defined as follows:

```
class MLP(nn.Module):
  def __init__(self, input_dim, hidden_dim, output_dim):
      super(MLP, self).__init__()
      self.fc1 = nn.Linear(input_dim, hidden_dim)
      self.fc2 = nn.Linear(hidden_dim, output_dim)
   def forward(self, x):
      x = F.relu(self.fc1(x))
      return self.fc2(x)
```

The input layer receives features of dimensionality ‘input_dim’, corresponding to the number of features in the dataset. The hidden layer comprises ‘hidden_dim’ neurons and utilizes the ReLU as the activation function to introduce non-linearity. The output layer consists of ‘output_dim’ neurons, representing the number of target classes. The model parameters were optimized using the Adam optimizer with 0.01 learning rate. The Cross-Entropy Loss function was utilized as the objective function due to its suitability for multi-class classification tasks. The training setup is as follows.

```
model = MLP(
  input_dim=X.shape[1],
  hidden_dim=64,
  output_dim=len(encoder.classes_)
       )
optimizer = torch.optim.Adam(model.parameters(), lr=0.01)
criterion = nn.CrossEntropyLoss()
```

The MLP operates as a standard feedforward neural network where each layer is fully connected to the subsequent layer. The first linear transformation maps input features to a latent representation, followed by the ReLU activation to enable the model to learn complex, non-linear patterns. The second linear layer projects the representation to the output space corresponding to class probabilities. This architecture is suitable for classification problems where the relationship between input features and output classes is potentially non-linear and high-dimensional. The choice of Adam as the optimization algorithm enables adaptive learning rate adjustment, which improves convergence speed and stability during training. This paper used the multi-layer perceptron (MLP) neural network (NN) model to classify Laundering type. The MLP is applied in 17 classes.

Table 6. MLP predictive performance on money laundering typologies

Class	Precision	Recall	F1 - Score
Behavioural_Change_1	0.41	0.75	0.53
Behavioural_Change_2	0.57	0.67	0.62
Bipartite	0.54	0.86	0.67
Cash_withdrawal	0.40	1.00	0.57
Cycle	1.00	0.98	0.99
Deposit-Send	0.53	0.90	0.67
Fan_In	0.35	0.30	0.32
Fan_Out	0.00	0.00	0.00
Gather-Scatter	1.00	0.03	0.06
Layered_Fan_In	0.91	0.65	0.76
Layered_Fan_Out	0.88	0.88	0.88
Over-Invoicing	1.00	0.50	0.67
Scatter-Gather	0.90	0.87	0.88
Single_Large	0.00	0.00	0.00
Smurfing	0.00	0.00	0.00
Stacked Bipartite	0.98	0.82	0.88
Structuring	1.00	0.99	0.99

The Multi-Layer Perceptron (MLP) deep learning model showed robust performances in several cases of detecting money laundering activities and classifying suspicious transactions desirable high accuracy and F1-scores. The evaluation results demonstrate overall effectiveness of the MLP Classifier with 80% overall accuracy. *Fan_out*, *Gather-Scatter*, *Single_large*, *Smurfing*, and *Fan_In* exhibited poor classification performance that can be attributed to severe class imbalance in the dataset. The model struggled to learn distinctive patterns for these rare typologies. There are also typologies that fall into the medium-class category, where the model can recognize certain patterns despite inconsistent precision scores. Aside from imbalance in the dataset, the misclassification of certain typologies may also stem from hidden similarities in behavioral or structural patterns. Since MLP learns from input features, overlapping characteristics between typologies can reduce its ability to distinguish them. This suggests a need for more refined features or complementary models to capture nuanced differences more effectively. Typologies such as *Behavioural Change 1*, *Bipartite*, and *Deposit Send* indicated that while the model can partially identify their characteristics, further enhancement is needed to achieve more reliable precision. There are also classes with strong performance namely *Structuring*, *Layered_Fan_Out*, and *Scatter-Gather* with relatively large number of samples and exhibit patterns that are easier for the model to identify and learn contributing to their higher predictive performance.

Prior studies involving MLP typically focus on features derived directly from transactional data, with some incorporating hyperparameter tuning to enhance model effectiveness.[43] In contrast, this study incorporates graph-based variables such as node centrality and clustering coefficient to reflect the structural and relational aspects of transaction networks. By doing so, the model can capture behavioral patterns that go beyond isolated transactions, offering a network-wide perspective awareness that is still relatively underexplored in standard MLP applications.

Conclusions

Comparative analysis of descriptive statistics found that fraudulent and non-fraudulent graph exhibited different characteristics in terms of collective eccentricity, centrality, and degree. Welch's t-test provides empirical support for the hypothesis that laundering activity shows measurable topological differences. Analysis of Money Laundering Typologies Using Graph Metrics exhibits that graph metrics like centrality and degree of connectivity can be utilized for Money Laundering identification beyond a static rule-based/scenario monitoring system. The MLP relies solely on graph-derived features, typologies with non-distinct or ambiguous network characteristics are more difficult to label. The MLP findings shows that graph metrics can be implemented within a supervised model and can successfully classify laundering typologies with favorable performance on controlled baseline.

This study exhibits that graph-oriented analysis offers a structured means to identify money-laundering schemes within financial transaction networks. By utilizing the graph metrics, the findings indicate that eccentricity, closeness, weighted indegree, weighted outdegree and weighted degree can extrapolate the laundering typologies and demonstrating the value of structural features for AML detection. The results also provided insights into linking behaviors of network configurations. Patterns such as fund dispersion, consolidation, and multi-path layering correspond to measurable variations in graph topology, supporting the notion that illicit fund flows produce a distinctive graph signature.

[43] Hitarth Gandhi et al., "Navigating the Complexity of Money Laundering: Anti–Money Laundering Advancements with AI/ML Insights," *International Journal on Smart Sensing and Intelligent Systems* 17, no. 1 (2024): 1–29, https://doi.org/10.2478/ijssis-2024-0024.

It should be noted as well that the synthetic data for the modelling baseline may not fully capture the variability observed in real-world scenarios, which limits the applicability of the results. Future research should validate these findings using operational datasets, scrutinize multiple jurisdictions contexts, and explore hybrid approaches that combine graph metrics with other techniques such as GNN-based models or with real-time detection pipelines. Thus, further experimentation should be adjusted with real-life data to account for different permutations of conditions. One limitation of the current model lies in its reduced ability to distinguish between typologies that exhibit similar underlying patterns.

Given that MLP is a feedforward model that depends on the separability of input features, it may struggle when different typologies share hidden or overlapping behavioral characteristics. This limitation highlights the potential need for more expressive feature representations or alternative modeling approaches capable of capturing nuanced differences between closely related money laundering patterns.

All in all, this paper provides groundwork for elaboration of graph theory into AML industry practice and marks the potential of network structure as a leverage to detect Money Laundering activity in digitalized financial ecosystems.

References

Alkaabi, Ali, George Mohay, Adrian McCullagh, and Nicholas Chantler. "A Comparative Analysis of the Extent of Money Laundering in Australia, UAE, UK and the USA." SSRN Scholarly Paper No. 1539843. Rochester, NY: Social Science Research Network, 2010. https://doi.org/10.2139/ssrn.1539843.

APG. "About Anti-Money Laundering and Counter Terrorism Financing | Asia / Pacific Group On Money Laundering." Last modified 2021. https://www.apgml.org/about-us/about-anti-money-laundering-and-counter-terrorism-financing.

Bakhshinejad, Nazanin, Reza Soltani, U. Nguyen, and Paul Messina. "A Survey of Machine Learning Based Anti-Money Laundering Solutions." *Internet of Things—Applications and Future* (2022): 73–87.

Chainalysis Team. "2023 Crypto Crime Trends: Illicit Cryptocurrency Volumes Reach All-Time Highs Amid Surge in Sanctions Designations and Hacking." Chainalysis. Last modified January 12, 2023. https://www.chainalysis.com/blog/2025-crypto-crime-report-introduction/.

Cheng, Dawei, Yujia Ye, Sheng Xiang, Zhenwei Ma, Ying Zhang, and Changjun Jiang. "Anti-Money Laundering by Group-Aware Deep Graph Learning." *IEEE Transactions on Knowledge and Data Engineering* 35, no. 12 (2023): 12444–57. https://doi.org/10.1109/TKDE.2023.3272396.

Cloud, Katherine, and Ilya Brovin. "How Identity Fraud Is Changing in the Age of AI." World Economic Forum. Last modified December 11, 2025. https://www.weforum.org/stories/2025/12/how-identity-fraud-is-increasing-in-the-age-of-ai/.

Collins, Jeffry. "Cryptocurrencies and Financial Crimes: The Role of Decentralized Cryptocurrency in Facilitating Money Laundering and the Challenges Posed on Anti–Money Laundering Regulations." *University of Miami Business Law Review* 34, no. 1 (2025): 71.

Costa, Jacopo. "Research Case Study 3: Exposing the Networks behind Transnational Corruption and Money Laundering Schemes." Basel Institute on Governance. Last modified May 31, 2023. https://baselgovernance.org/publications/research-case-3.

Deprez, Bruno, Toon Vanderschueren, Bart Baesens, Tim Verdonck, and Wouter Verbeke. "Network Analytics for Anti-Money Laundering—A Systematic Literature Review and

Experimental Evaluation." *INFORMS Journal on Data Science* (2025), https://doi.org/10.1287/ijds.2024.0042.

Euler, Leonhard. "Solutio Problematis Ad Geometriam Situs Pertinentis." *Euler Archive - All Works* (1741): 128–40.

FATF - Egmont Group. *FATF/Egmont Trade-Based Money Laundering: Trends and Developments*. Paris: FATF - Egmont Group, 2020.

Gandhi, Hitarth, Kevin Tandon, Shilpa Gite, Biswajeet Pradhan, and Abdullah Alamri. "Navigating the Complexity of Money Laundering: Anti–Money Laundering Advancements with AI/ML Insights." *International Journal on Smart Sensing and Intelligent Systems* 17, no. 1 (2024): 1–29. https://doi.org/10.2478/ijssis-2024-0024.

Jacomy, Mathieu, Tommaso Venturini, Sebastien Heymann, and Mathieu Bastian. "ForceAtlas2, a Continuous Graph Layout Algorithm for Handy Network Visualization Designed for the Gephi Software." *PLoS One* 9, no. 6 (2014): e98679. https://doi.org/10.1371/journal.pone.0098679.

Miralis, Dennis, Harry Sultan, Henry Yu, and Zanthi Jordan. *Anti-Money Laundering Laws and Regulations Anti-Money Laundering in the Asia-Pacific Region: An Overview 2025*. London: International Comparative Legal Guides (ICLG), 2025.

Muminovic, Amel, and Festim Halili. "Money Laundering Prevention in the Digital Age: Leveraging Graph Databases for Effective Solutions." *Sciences (IJTNS)* 4, no. 1 (2024): 1–10.

Newman, Mark E. J. *Networks—An Introduction*. Oxford: Oxford University Press, 2012.

Oztas, Berkan, Deniz Cetinkaya, Festus Adedoyin, Marcin Budka, Huseyin Dogan, and Gokhan Aksu. "Enhancing Anti-Money Laundering: Development of a Synthetic Transaction Monitoring Dataset." *2023 IEEE International Conference on E-Business Engineering (ICEBE)*, November 2023, 47–54. https://doi.org/10.1109/ICEBE59045.2023.00028.

Popescu, Marius-Constantin, Valentina E. Balas, Liliana Perescu-Popescu, and Nikos Mastorakis. "Multilayer Perceptron and Neural Networks." *WSEAS Transactions on Circuits and Systems* 8, no. 7 (2009): 579–88.

Rogers, Sam. "Cyber-Fraud, Underground Banking, and Technological Innovation Fuels Crime in SE Asia." GASA. Last modified December 17, 2024. https://www.gasa.org/post/unodc-cyber-fraud-underground-banking-and-technological-innovation-fuels-crime-in-se-asia.

Tiwari, Milind, Jamie Ferrill, and Vishal Mehrotra. "Using Graph Database Platforms to Fight Money Laundering: Advocating Large Scale Adoption." *Journal of Money Laundering Control* 26, no. 3 (2022): 474–87. https://doi.org/10.1108/JMLC-03-2022-0047.

UNODC. *The Nexus Between Cybercrime and Corruption*. Vienna: United Nations Office on Drugs and Crime, 2025.

Usman, Atif, Nasir Naveed, and Saima Munawar. "Intelligent Anti-Money Laundering Fraud Control Using Graph-Based Machine Learning Model for the Financial Domain." *Journal of Cases on Information Technology (JCIT)* 25, no. 1 (2023): 1–20. https://doi.org/10.4018/JCIT.316665.

Vidovic, Tom. "The Rise of the Synthetic Identity: A Growing Threat in the Digital Age." Global Compliance Institute. Last modified July 5, 2024. https://www.gci-ccm.org/.

Weber, Ryan, Iilpo Tammi, Shinan Wang, and Timothy Anderson. *A Spatial Analysis of City-Regions: Urban Form & Service Accessibility*. Stockholm: Nordregio, 2016.

Welch, B. L. "The Generalization of 'Student's' Problem When Several Different Population Varlances Are Involved." *Biometrika* 34, no. 1–2 (1947): 28–35. https://doi.org/10.1093/biomet/34.1-2.28.

World Bank. "Corrupt Money Concealed in Shell Companies and Other Opaque Legal Entities, Finds New StAR Study." World Bank. Last modified October 24, 2011.

https://doi.org/10/24/corrupt-money-concealed-in-shell-companies-and-other-opaque-legal-entities-finds-new-star-study.

World Economic Forum. *Digital Transformation: Powering the Great Reset*. Switzerland: World Economic Forum, 2020.