iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL
FOR RESEARCH
IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 Issue: VIII Month of publication: August 2025

DOI: https://doi.org/10.22214/ijraset.2025.73672

Anti-Money Laundering by Group-Aware Deep Graph Learning

Shwetha A B[1], Shreyas H G[2], Siddarameshwara J[3], Srinidhi M[4], Srujan T S[5]
[1]*Assistant Professor, Sapthagiri College of Engineering, Karnataka, India*
[2, 3, 4, 5]*Computer Science and Engineering, Sapthagiri College of Engineering, Karnataka, India*

Abstract: Money laundering (ML) is a serious challenge that supports organized and transnational crime, with far-reaching impacts on a country's economy, governance, and social welfare. Financial institutions, which manage the flow of money, Financial institutions have become essential partners in the global battle against money laundering. While traditional AML systems typically assess transactions one by one, they often fail to detects the large patterns that emerges when criminal groups operate in coordination. Today, money laundering is often orchestrated by organized networks rather than individuals acting alone. Recognizing this shift, a deep graph learning model now makes it possible to detect collaborative money laundering by zooming in on group dynamics and shared behaviors. Our approach models users and their transactions as interconnected nodes within a graph, using a community-based encoder to capture group dynamics and behavioral patterns. Additionally, we apply a local feature enhancement method to identify and group similar transactional behaviors, helping to uncover hidden laundering networks. This Experiments are using an actual data from a leading international bank card network revealed that this approach delivers notably higher accuracy in detecting suspicious activity. It delivers superior results compared to current anti-money laundering methods, consistently identifying suspicious activity more effectively in both live monitoring and scheduled data analysis. These findings underscore how using graph-based techniques to capture group-level patterns can make AML systems far more effective at spotting complex, coordinated financial crimes.

Keywords: Money laundering, financial crime detection, graph neural networks, deep learning, group behavior analysis.

I. INTRODUCTION

Money laundering is when someone tries to hide the origin of money they've earned through illegal means—like crime or fraud—by making it look like it came from a legal or honest source. It typically involves disguising the origins of funds earned through criminal activities such as drug trafficking, and it plays a major role in sustaining organized crime networks. According to global estimates, this underground financial activity may represent about 2.7% of the world's GDP. Tackling money laundering is essential—not just to maintain the integrity of financial systems, but also to protect broader economic and social structures. For many years, the financial sector has worked to confront this issue through a range of anti-money laundering (AML) methods and frameworks. Conventional methods for combating money laundering have typically depended on strict regulations and labor-intensive manual reviews—making the process both slow and resource-heavy. In recent years, however, machine learning has begun transforming these systems by streamlining and automating key parts of the AML workflow. However, many of these models struggle to detect sophisticated laundering tactics, especially when those tactics are coordinated by groups acting together.

A growing concern is that many money laundering operations today are carried out by tightly organized groups or criminal syndicates. Unfortunately, most existing models analyze accounts in isolation, ignoring the critical relationships and interactions among them. To address the limitations of traditional systems, the researchers present a fresh approach using deep graph learning that emphasizes group-based behavior analysis. Their method introduces a group-sensitive graph neural network, treating users as nodes and their transactions as connecting links within a broader network. A specialized encoder is designed to highlight community patterns and improve detection by pinpointing suspicious group activity. Tests conducted with data from a major global payment network showed that this technique significantly boosts the ability to identify both solo and coordinated money laundering efforts.

II. LITERATURE REVIEW

M. El Ammari, H. Rachidi, and Y. Benslimane (2021) [3] Another complementary approach focuses on detecting laundering behavior through the temporal dynamics of financial transactions. The study leverages techniques from signal processing, applying a Short-Time Fourier Transform (STFT) to transform transaction sequences into the time-frequency domain. This representation allows for a detailed analysis of how transaction patterns evolve over time.

The extracted time-frequency features are then fed into machine learning classifiers to distinguish between normal and suspicious activity. Unlike traditional time-series models, this approach captures both the timing and frequency of financial behaviors, which is particularly useful in identifying irregular or repetitive patterns often associated with laundering schemes.

Tests conducted on actual financial transaction data reveal that this approach delivers strong and reliable performance in identifying suspicious activity provides high accuracy in flagging suspicious activities. The integration of time-frequency features enables the system to detect subtle anomalies that might be missed by static or frequency-only analyses. This study makes a valuable contribution by introducing time-frequency signal processing to the AML domain, offering a novel perspective on how laundering behavior can be identified through dynamic temporal features.

A. Ghosh, M. V. R. K. R. R. Atrey, and A. B. Benerjee (2023) [4] Recent strides in deep learning have equipped financial institutions with powerful tools for identifying money laundering by recognizing intricate and hidden patterns in transactional data. This analysis explores how advanced models—like RNNs, LSTMs, CNNs, autoencoders, and Graph Neural Networks—are being used within anti-money laundering (AML) systems to improve predictive accuracy. Despite their effectiveness, these models often operate like black boxes, making it difficult for regulators to understand the rationale behind their decisions. To bridge this gap, explainable AI (XAI) techniques—such as LIME, SHAP, and attention mechanisms—are gaining traction as a means to enhance transparency and insight. The review underscores the importance of building trust in AI-driven financial tools by ensuring they are both reliable and accountable. It also advocates for blended approaches that offer a balance between predictive strength and interpretability. Crucially, it highlights the need for rigorous testing using standardized, real-world data to ensure these technologies can perform effectively in practical settings.All in all, the paper offers a thoughtful look at both the promise and the complexity of bringing deep learning and explainable AI into the fight against financial crime..

L. Butgereit (2021) [5] This study presents a rule-based approach for detecting funnel accounts—financial conduits commonly used in the layering stage of money laundering. By adapting the U.S. Immigration and Customs Enforcement's "12 Red Flags" to a South African, mobile-finance context, the authors designed an algorithm that effectively flags suspicious activity based on transaction patterns, frequency, and timing. The system was successfully applied in non-banking environments, proving its relevance in low-resource financial systems. While machine learning was not feasible due to limited labeled data, the rule-based framework provides a solid foundation for future AI integration. The work also emphasizes the ethical and legal tensions surrounding AML in privacy-sensitive regions. It contributes a practical, adaptable solution and encourages future transitions to data-driven models as labeled data becomes available. Overall, it reinforces the continued importance of interpretable, rules-based strategies in global AML efforts.

Wang, H., Wang, X., Yang, D., & Wu, Y. (2022). [6] This study introduces a visual analytics framework designed to support the detection of money laundering within cryptocurrency exchanges, where pseudonymity and decentralized control hinder traditional AML efforts. The system uses transaction flow visualizations, address clustering, and multi-hop path tracing to help investigators identify suspicious patterns such as mixers, peeling chains, and funneling. By leveraging visual tools like node-link diagrams and Sankey plots, the platform enhances interpretability for non-technical users. Case studies show that the tool enables more intuitive tracing of illicit flows compared to conventional data views. The research highlights the importance of human-centered design in blockchain AML investigations. It offers a flexible foundation for analyzing evolving laundering strategies in decentralized environments. This work demonstrates the growing role of visual analytics in supplementing algorithmic methods for AML in the cryptocurrency domain.

K. Koo, M. Park, and B. Yoon (2024) [7] This work introduces a blended approach of a hybrid framework for detecting suspicious financial transactions by integrating an autoencoder-based anomaly detection model with a risk-based scoring system. The autoencoder learns normal transaction patterns and flags deviations without relying on labeled data, making it well-suited for dynamic and evolving financial environments. Complementing this, the risk-based component evaluates transactions using domain-specific indicators such as frequency, value, and geographic risk. By merging statistical anomalies with expert-informed risk profiles, the model reduces false positives and improves interpretability. The results demonstrate high sensitivity and scalability, even in the absence of tagged suspicious data. This approach offers a practical and adaptable solution for real-world AML systems. It exemplifies how unsupervised deep learning can be effectively paired with risk assessment to enhance financial crime detection.

Yingtong Dou (IEEE,2020) [8] This paper introduces xGEMs, a model-agnostic framework that generates realistic counterfactual examples to interpret black-box machine learning models. By leveraging generative models such as VAEs or GANs, xGEMs identifies how small, semantically meaningful changes to an input can alters model's prediction. These exemplars help the users understand which features drive classification decisions, offering both visual clarity and quantitative insights. The approach is applicable across domains and reveals model biases and vulnerabilities effectively.

While not AML-specific, its ability to improve transparency is highly relevant for regulatory-focused domains like financial crime detection. xGEMs offers a practical path for integrating explainable AI into complex decision systems. Its emphasis on interpretable, human-aligned outputs makes it as a valuable contribution to trustworthy AI research.

Liu, A., Tong, Y., Li, Z., Deng, K., He, X., & Tong, H. (2020) [9] this study presents a flexible and efficient graph-based ML approach that helps uncover potential money laundering activities across vast networks of financial transactions, even with limited labeled data. By modeling accounts and their interactions as graph structures, the approach leverages limited labeled data while learning from vast amounts of unlabeled transactions. The system uses graph convolutional networks with sampling and embedding techniques to enhance efficiency and accuracy. It demonstrates strong performance in identifying suspicious entities even in sparse-label settings. The method also reduces computational overhead, making it suitable for real-time analysis of massive financial graphs. This contribution addresses key challenges of scalability and data scarcity in AML detection. It offers a practical, adaptive solution for enhancing fraud detection across complex financial systems.

III. METHODOLOGY

In this study, a deep learning approach is adopted to tackle the growing challenge of identifying organized money laundering activities. The proposed system is known as the Group-Aware Graph Neural Network (GAGNN), which is designed to uncover hidden relationships among suspicious financial transactions by leveraging both individual user behavior and collaborative patterns within user groups. Below is a simplified explanation of how this system works.

1) Creating the Transaction Network: To begin, a graph-based model is constructed where each user account is represented as a node, and each transaction between accounts forms an edge. These edges carry details such as transaction amount, frequency, and timestamps. By analyzing this structure, the system learns It’s not only about the actions of individual users, but also the patterns of interaction and relationships formed between accounts across the network..

2) Learning From Communities in the Network: A key part of the system is its ability to detect groups or communities of users who may be working together. To do this, it uses a combination of: *Graph Attention Networks (GAT)* – to determine which nearby users are most influential when analyzing a particular account. *Extended Markov Random Fields (eMRF)* – to encourage consistent labeling within groups by considering similarities in behavior and connections between users. Together, these layers help the system understand both the structure and the content of the transaction network.

3) Detecting Suspicious Accounts: The learned features from each user are passed through a simple neural network (MLP) to predict whether the account is likely to be involved in money laundering. This classification process is refined through continuous feedback using a standard loss function that compares predictions against actual known cases.

4) Evaluating Individual Transactions: Beyond user accounts, the model also assesses individual transactions. It does this by combining the features of the two participating accounts with transaction-specific details. This merged information is then evaluated using another neural network to determine the likelihood of the transaction being suspicious.

5) Identifying Suspicious Groups: Money laundering often involves groups of users working together. To detect such coordination, the model groups accounts that are connected through flagged transactions. These aggregated groups are treated as new, larger entities (called "super-nodes"), allowing the system to re-analyze their collective behavior. This grouping reveals patterns that would be difficult to detect by analyzing accounts separately.

6) Classifying Organized Activity: Once these user groups are formed, the model examines them using the same feature extraction and classification methods, now applied at the group level. This helps determine whether a group of users, as a whole, exhibits behavior typical of money laundering operations.

7) Training the Model Holistically

Rather than focusing on just one aspect, the system optimizes its learning across three levels:

- Individual users (to detect risky accounts),
- Transactions (to spot suspicious activity),
- User groups (to uncover coordinated schemes).

Each of these levels contributes to a combined loss function, allowing the model to learn in a more balanced and thorough way.

8) Scalability and Real-Time Use: The model is trained offline on large historical datasets and is capable of scaling to millions of transactions using sampling techniques. Once trained, it can be deployed in real-time settings, updating its predictions based on new transactions as they happen. The learning process is powered by the Adam optimizer, with finely tuned parameters for optimal performance. This multi-layered approach allows the system to detect not only isolated cases of fraud but also large, organized laundering schemes. Its combination of deep graph learning and community detection makes it particularly effective in identifying complex criminal behavior patterns within financial networks.

IV. DISCUSSION

The adoption of deep graph learning in anti-money laundering (AML) research marks a pivotal shift from traditional rule-based systems to more adaptive, relationship-driven models. By treating financial entities and transactions as interconnected graphs, these methods uncover hidden patterns and group behaviors often missed by conventional tools. Advanced techniques such as group-aware GNNs, semi-supervised learning, and risk-based aggregation enhance detection performance, even in data-scarce environments. Additional contributions like autoencoder-based anomaly detection and time-frequency modeling offer complementary perspectives. Yet, challenges persist—most notably, limited labeled data and the need for model interpretability in compliance-focused settings. Recent works addressing explainability through visual tools and counterfactual examples represent encouraging progress. Scalability also remains a concern, especially in real-world financial systems handling massive, dynamic graphs. Future directions should explore hybrid frameworks that combine deep learning with domain knowledge and privacy-aware learning. Together, these advancements point toward more robust and transparent AML solutions for modern financial ecosystems.

V. CONCLUSION

The growing complexity of financial crime demands more intelligent, adaptable, and interpretable solutions—deep graph learning offers a promising path forward in this effort. By modeling relationships between entities and capturing group behaviors within financial networks, graph-based approaches, This approach significantly surpasses the limitations of conventional anti-money laundering methods, offering deeper insights and more adaptive solutions. This survey has highlighted a range of innovative methods, from group-aware neural networks and semi-supervised frameworks to autoencoder-based anomaly detection and explainable AI tools. Each contributes uniquely to detecting both individual and collaborative money laundering patterns in real-world settings. Despite notable progress, challenges remain. Limited access to reliable data, concerns about how models make decisions, and challenges in scaling them up are still major roadblocks to broader adoption.. However, recent advancements in hybrid learning models, interpretability techniques, and scalable graph architectures suggest a promising future for research and practical deployment. Going forward, collaboration between financial institutions, regulatory bodies, and the research community will be essential to build AML systems that are not only accurate but also trustworthy and operationally viable. Ultimately, deep graph learning is not just a technical innovation—it's a foundational shift in how we understand and combat financial crime in the digital age.

REFERENCES

[1] Liu, H., Zuo, Y., Zhu, X., Yin, H., & Zhang, M. (2021). Anti-money laundering by group-aware deep graph learning. In Proceedings of the 27th ACM SIGKDD Conference on Knowledge Discovery & Data Mining (pp. 1113–1123). ACM.

[2] B. Unger, "Money laundering regulation: From al Capone to al qaeda," in Research Handbook on Money Laundering Anonymous 2013, .

[3] M. El Ammari, H. Rachidi, and Y. Benslimane, "A time-frequency based suspicious activity detection for anti-money laundering," in Proc. 2021 4th International Conference on Advanced Systems and Emergent Technologies (IC_ASET), Hammamet, Tunisia, 2021, pp. 177–182. doi: 10.1109/IC_ASET52486.2021.9691095.

[4] A. Ghosh, M. V. R. K. R. R. Atrey, and A. B. Benerjee, "Deep learning and explainable artificial intelligence techniques applied for detecting money laundering: A critical review," Computers & Security, vol. 130, 2023, Art. no. 103138, doi: 10.1016/j.cose.2023.103138.

[5] L. Butgereit, "Anti Money Laundering: Rule-Based Methods to Identify Funnel Accounts," in Proc. 2021 Conf. on Information Communications Technology and Society (ICTAS), Port Elizabeth, South Africa, 2021, pp. 20–26. doi: 10.1109/ICTAS50802.2021.9394990.

[6] Wang, H., Wang, X., Yang, D., & Wu, Y. (2022). "Visual analysis of money laundering in cryptocurrency exchange." IEEE Transactions on Visualization and Computer Graphics, 28(1), 98–108.

[7] K. Koo, M. Park, and B. Yoon, "A suspicious financial transaction detection model using autoencoder and risk-based approach," IEEE Access, vol. 12, pp. 68926–68939, May 2024, doi: 10.1109/ACCESS.2024.3399824.

[8] Yingtong Dou1, Zhiwei Liu1, Li Sun2, Yutong Deng2, Hao Peng3, Philip S. Yu1 ''Enhancing Graph Neural Network-based Fraud Detectors against Camouflaged Fraudsters,''. 1. IEEE, 2020.

[9] Liu, A., Tong, Y., Li, Z., Deng, K., He, X., & Tong, H. (2020). "Scalable semi-supervised graph learning techniques for anti-money laundering". arXiv preprint arXiv:2009.05344

[10] T. N. Kipf and M. Welling, ``Semi-supervised classification with graph convolutional networks," in Proc. Int. Conf. Learn. Represent. (ICLR), 2017, pp. 114.

[11] R. Liu, X.-L. Qian, S. Mao, and S.-Z. Zhu, ``Research on anti money laundering based on core decision tree algorithm," in Proc. IEEE Chin. Control Decis. Conf. (CCDC), May 2011, pp. 4322 4325.

[12] Z. Chen, L. Dinh Van Khoa, A. Nazir, E. N. Teoh, and E. K. Karupiah ``Exploration of the effectiveness of expectation maximization algorithm for suspicious transaction detection in anti money laundering," in Proc. IEEE Conf. Open Syst. (ICOS), Oct. 2014, pp. 145 149.

[13] K. Singh and P. Best, "Anti-money laundering: Using data visualization to identify suspicious activity," Int. J. Accounting Inf. Syst., vol. 34, no. 3, pp. 7–13, 2019.

[14] N. Heidarinia, A. Harounabadi, and M. Sadeghzadeh, "An intelligent anti-money laundering method for detecting risky users in the banking systems," Int. J. Comput. Appl., vol. 97, no. 22, pp. 35–39, Jul. 2014.

[15] M.-J. Segovia-Vargas et al., "Money laundering and terrorism financing detection using neural networks and an abnormality indicator," Expert Syst. Appl., vol. 169, 2021, Art. no. 11447