Journal of Information System and Technology Management
JISTM
EISSN: 0128-1666
Volume 11 Issue 43 (June 2026) PP 132-145

JOURNAL OF INFORMATION SYSTEM AND TECHNOLOGY MANAGEMENT (JISTM)
www.gaexcellence.com/jistm

FROM RULES TO GRAPH LEARNING: A REVIEW OF COMPUTATIONAL APPROACHES TO DETECT SUSPICIOUS BANK TRANSACTIONS

Nordaliela Mohd Rusli[1,2]*, Anazida Zainal[3]

[1]Cybersecurity Research Group, Universiti Malaysia Sabah (UMS), Malaysia
daliela@ums.edu.my https://orcid.org/0000-0002-5793-546X
[2] Faculty of Computing Universiti Teknologi Malaysia (UTM), Malaysia
daliela@ums.edu.my https://orcid.org/0000-0002-5793-546X
[3] Faculty of Computing Universiti Teknologi Malaysia (UTM), Malaysia
anazida@utm.edu.my https://orcid.org/0000-0003-0022-3039
*Corresponding Author

Article Info:

Article history:
Received date: 12.02.2026
Revised date: 26.02.2026
Accepted date: 12.06.2026
Published date: 25.06.2026

To cite this document:

Rusli, N. M., & Zainal, A. (2026). From Rules to Graph Learning: A Review of Computational Approaches to Detect Suspicious Bank Transactions. *Journal of Information System and Technology Management, 11* (43), 132-145.

Abstract:

Automated systems for detecting suspicious transaction were introduced in the early 2000s to manage the growing volume and complexity of financial transactions. Subsequent technological advancements have driven the convergence of Artificial Intelligence (AI) and Big Data Analytics for transaction data analysis. However, these advancements come at considerable implementation cost and despite significant investment, critical limitations persist that require attention to mitigate financial losses. This review maps the evolution of approaches used to detect suspicious bank transactions between 2012 and 2025, and analyses the datasets employed in the reviewed studies. Articles were sourced from Scopus-indexed journals using the search term "money laundering detection", and the collection was restricted to computer science publications focusing on suspicious bank transaction detection. The screening process excluded studies on conceptual profiling, risk assessment, Hawala networks, and fraud. The remaining articles were then analysed to extract identified problems and limitations, proposed solutions, algorithms, and dataset characteristics. Datasets were classified into three categories: forensic criminal investigation datasets, operational bank AML/SAR-level datasets, and synthetic or simulator-based datasets. The findings indicate a clear methodological progression from rule-based and clustering approaches to supervised machine learning, and subsequently to graph-based and deep learning models. However, more than 20% of the reviewed studies relied on synthetic datasets which are unvalidated using actual money laundering activity. Given the absence of detailed forensic insights in

Journal of Information System and Technology Management
JISTM
EISSN: 0128-1666
Volume 11 Issue 43 (June 2026) PP 132-145

such datasets, findings derived from synthetic data must be interpreted with caution. Beyond detection methods and algorithms, dataset realism is equally critical, particularly in the context of public policy and banking practice.

DOI: 10.35631/JISTM.1143008 **Keyword:**

Anti-Money Laundering, Bank Transactions, Dataset Tier, Machine Learning, Suspicious Transaction Detection

Introduction

Suspicious transactions involve unusual activity, such as amounts inconsistent with a customer's profile or complex transfers across multiple accounts. These are key indicators of money laundering. When identified, financial institutions are required to file a formal Suspicious Activity Report (SAR) under Anti-Money Laundering (AML) regulations. Institutions that fail to report such transactions risk facing penalties from their respective central banks and regulators.

Banks rely on rule-based systems and threshold conditions to detect suspicious transactions. For example, any transaction exceeding the defined threshold of RM50,000 will be flagged for further investigation (Bank Negara Malaysia, n.d.).

While these rule-based thresholds are straightforward for regulators to interpret, they have a significant limitation — they cannot adapt to evolving or complex transactions. Criminals often exploit this weakness by deliberately structuring their activities to stay below detection limits, concealing the true origins and ownership of illicit funds. As a result, these static systems generate many false alarms while allowing perpetrators to evade detection.

However, existing literature has given limited attention to the types of datasets used to train and evaluate detection models. This raises an important question: What datasets were these models trained and evaluated on?

Datasets used in this domain vary significantly in type and setting. They can be broadly categorized into three types: real bank transactions with actual SAR filings, forensic datasets derived from investigations, and synthetic datasets generated by simulators. Given these differences, results across dataset types cannot be treated as equivalent. A model that performs

Journal of Information System and Technology Management
JISTM
EISSN: 0128-1666
Volume 11 Issue 43 (June 2026) PP 132-145
well on synthetic data may not deliver the same performance when deployed in a real financial institution.

To address this gap, this review has two objectives:

1. To analyse the progression of suspicious transaction detection methods from 2012 to 2025.
2. To classify findings based on dataset fidelity, distinguishing between forensic datasets, alert-level datasets, and synthetic datasets.

Ultimately, this study aims to differentiate findings derived from operationally validated datasets from those based on synthetic datasets, while acknowledging the latter as promising prototypes.

Historical Background

Early AML systems in the banking sector relied on rule-based settings with pre-defined thresholds. Domain experts were also involved in identifying AML red flags. Key indicators considered by these systems included transaction-level attributes such as amount, frequency, and destination.

To improve detection, Dreżewski et al. (2012) and Jayasree and Balan (2016) incorporated data mining techniques. Their approaches demonstrated that unsupervised methods could identify unusual transactions beyond the limitations of fixed rules. However, these systems produced high false-positive rates. Their static nature and reliance on expert-defined features made them unable to detect coordinated or evolving transaction patterns.

These shortcomings prompted a broader shift in AML research and practice. The researchers turned to machine learning, graph-based analysis and deep learning technique to address the weakness of rule-based and traditional data mining approaches.

Technological Evolution

Research on anti-money laundering (AML) detection using bank transaction data has evolved considerably over the past decade. This evolution reflects advancements in analytical techniques, a growing understanding of data availability, demonstrated feasibility, and operational constraints.

Supervised Machine Learning for AML Detection

As an alternative to rule-based systems, researchers began adopting supervised machine learning models to improve the detection of suspicious transactions. These models were trained on data from SAR reports using techniques such as logistic regression, decision trees, and support vector machines. Compared to traditional approaches, supervised machine learning methods achieved higher accuracy with fewer false positives (Zhang & Trubey, 2019; Jullum et al., 2020; Ketenci et al., 2021).

Journal of Information System and Technology Management
JISTM
EISSN: 0128-1666
Volume 11 Issue 43 (June 2026) PP 132-145

Despite these improvements, supervised approaches face several challenges. Labelled money laundering data is scarce, and available datasets are often highly imbalanced and noisy. Furthermore, models trained on institution-specific data have limited generalizability across different banking systems.

Graph-Based and Network-Oriented AML Detection

Researchers later recognized that money laundering is inherently organized and collaborative in nature. This led to the adoption of graph-based models, where financial transactions are represented as networks. In this representation, nodes correspond to accounts and edges represent transactions between them. Unlike transaction-level models, this approach enables the analysis of transaction flows, detection of social clusters, and identification of interaction trends.

Early graph-based studies relied on Social Network Analysis (SNA), employing techniques such as centrality measures, community detection, and subgraph analysis. Mahootiha et al. (2021) demonstrated that network features enhance analysts' ability to identify money laundering schemes. Similarly, Sousa Lima et al. (2022) highlighted the significance of network-oriented analysis in detecting suspicious transactions.

However, early graph-based approaches were constrained by manual feature engineering and static graph snapshots. These limitations hindered their ability to capture evolving suspicious patterns and maintain performance on large-scale transactional graphs.

Graph Neural Networks and Temporal Models

Recent AML research has increasingly adopted Graph Neural Network (GNN)-based models to learn relational patterns within transaction graphs. Models such as Graph Convolutional Networks (GCN), GraphSAGE, and Graph Attention Networks (GAT) facilitate message propagation across transaction graphs, enabling the discovery of complex relationships and sophisticated money laundering schemes.

Recognizing that historical transactions influence current ones, researchers introduced hybrid models incorporating advanced techniques such as Long Short-Term Memory (LSTM) and attention mechanisms. These models are designed to capture intricate spatiotemporal dependencies. Xia et al. (2022) demonstrated that combining spatial and temporal dependencies enhances detection performance. Similarly, the Temporal-Aware Graph Attention (TAPA) model improves the ability to recognize indirect relationships over time (Zhang et al., 2025).

Despite their potential, deep learning models face several notable limitations. They struggle to learn complex patterns within large-scale financial graphs (Sharma & Gupta, 2024) and exhibit bias when trained on imbalanced datasets (Cui et al., 2025). Additionally, their lack of interpretability poses a significant challenge (Sharma & Gupta, 2024). Explainability and transparency are critical in the banking sector, as they are essential for maintaining client confidence and ensuring regulatory compliance.

Journal of Information System and Technology Management
JISTM
EISSN: 0128-1666
Volume 11 Issue 43 (June 2026) PP 132-145

Literature Search Methodology

This review intends to examine the evolution of AML detection methods applied to the bank transaction data. The process of conducting the study consists of six major steps (Xiao & Watson, 2019). The search was conducted using Scopus database with the search term "money laundering detection". Once the search is completed, all titles from the results were reviewed to ensure the articles are journal articles published between the year 2012 and 2025. Then, the abstracts from each publication were reviewed to narrow down the selection of the studies to bank transactions. Abstracts are known to provide a summary that highlights the important details from the sections of the publication. Abstracts do not provide the authors with enough details to assess the quality of the publication, including the risk of being biased and the reliability of the result. Therefore, the next step is to review the full text of every publication and identify the methodological trends, dataset origin, and validation gaps. Studies were excluded if they focus on cryptocurrency, hawala (transferring money outside geographical border based on trust), and non-bank transactions. Consequently, the selected publications are analysed to classify the dataset used in the studies, inspired by Jones & Steel (2018). Figure 1 shows the process flow of this study according to the steps as suggested by Xiao and Watson (2019).

The evidence-tier framework used in this study is based on the principles for evaluating real-world medical evidence, that focus on context-dependent quality (Jones & Steel, 2018). Medical evidence is assessed through hierarchies rather than applying a one-size-fits-all standards. These hierarchies are based on where the data originally from, validation context and its potential to be bias. This similar perspective is applied to AML detection research as bank transactions dataset involved in the studies varies from synthetic simulation to verified investigation evidence, and the precision of their data tags (Fraud/Normal).

Thus, the datasets are classified based on their specific context, where datasets used for initial experiments do not have similar weights as datasets from real investigations. The datasets in the reviewed studies were categorized into four evidence tiers, as shown in Table 1.

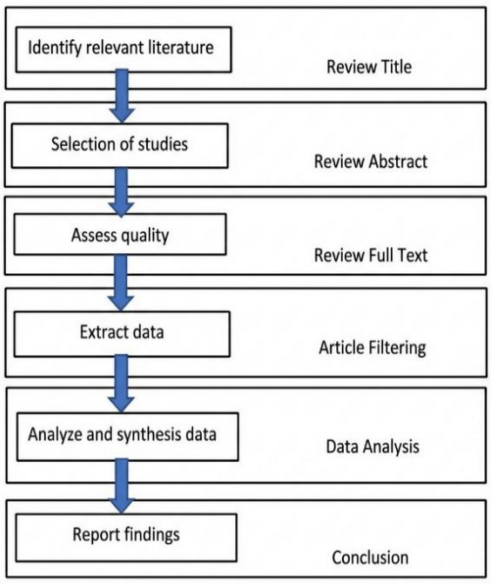

Figure 1: Study Methodology

Source: (Xiao & Watson, 2019)

Journal of Information System and Technology Management
JISTM
EISSN: 0128-1666
Volume 11 Issue 43 (June 2026) PP 132-145

Table 1: Evidence Tier Description

Evidence Tier	Description
A+	These datasets consist of confirmed money laundering case that have been verified by human experts. They provide the highest standard of evidence for assessing model's detection capabilities.
A	These datasets are from live banking environments. They are primarily used to train systems to reduce the false alarms, but they do not have verified labels confirming actual money laundering.
B	These datasets consist of real transactions records and synthetically generated examples. The merge between real banking data and the synthetic examples was conducted to address the scarcity of actual fraud cases.
C	These datasets are fully synthetic and were generated through simulation. They offer the lowest evidence and usually used for benchmarking or methodological prototyping.

Source: Source: Authors' interpretation

This classification system is used to examine the gap between algorithmic progress and data quality. It is to evaluate whether high quality data is used to test the sophisticated algorithms as shown in the evidence standards from medical research (Jones & Steel, 2018).

Dataset Classification

A total of 28 studies published between 2012 and 2025 met the inclusion criteria. The studies were categorized into four evidence tiers based on dataset origin and evidential strength:

- **Tier A+**: Forensic or investigative datasets (n = 3)
- **Tier A**: Operational datasets (n = 17)
- **Tier B**: Hybrid datasets (n = 3)
- **Tier C**: Synthetic datasets (n = 5)

Tier A+ carries the highest evidential value, as it comprises real transaction data sourced from federal investigations, Financial Intelligence Unit (FIU) inquiries, or seized financial records. Tier A consists of real datasets obtained from financial institutions, labelled based on SAR filings. This tier is referred to as AML operational datasets, as it includes transactions that have triggered alerts from monitoring systems as well as client risk profiles. Tier B encompasses hybrid studies that combine real and synthetic datasets. Datasets generated from real data using simulation techniques are also classified under this tier. Tier C represents fully synthetic datasets generated by simulators such as AMLSim, PaySim, and Node2Vec-based simulators. Only a small number of studies utilized forensic datasets (Tier A+), reflecting the highly restricted access to investigative data. Most studies relied on AML operational datasets (Tier A), while hybrid (Tier B) and fully synthetic (Tier C) datasets represented a minority of the reviewed studies.

Journal of Information System and Technology Management
JISTM
EISSN: 0128-1666
Volume 11 Issue 43 (June 2026) PP 132-145

Methodological Evolution and Evidential Grounding

This section presents the findings of evaluating the reviewed studies according to dataset origin and the evidential value of the data in reflecting real-world money laundering behaviour. It also explores the progression of AML detection methods from rule-based systems to advanced deep learning approaches while examining whether these methodological advances are supported by datasets with sufficient evidential value.

Phase 1: Rule-based Systems and Data Mining (2012-2016)

Between 2012 and 2016, detection approaches that rely on predefined threshold and static rules were the predominant AML detection methods. These approaches were supplemented by clustering, and data mining techniques too. These methods are rigid and unable to capture complex or evolving transaction behaviour, resulting in high false-positive rates. From an evidential standpoint, the dataset underpinning this phase were rarely sourced from confirmed laundering investigations. The investigation during this phase depends on both Tier B or Tier C data, which shows there are absence of verified ground truths that limit meaningful evaluation of real-world detection capability.

Phase 2: Supervised Machine Learning (2017-2020)

Research shifted towards supervised models; logistic regression, random forest and support vector machine to improve detection performance and address the shortcomings of rule-based systems. Key challenges during this period until now include managing class imbalance and maintaining model interpretability. Critically, performance was also constrained by the scarcity of labelled data. Studies that utilized operational dataset (Tier A) during this phase focused on alert prioritization and false-positive reduction, but the model outputs could not be benchmarked against confirmed criminal behaviour. This is because of the absence of the verified laundering labels. The majorities of studies continue to operate within the Tier B and Tier C evidence tier.

Phase 3: Graph-based Approaches and Network Analysis (2020 onwards)

Recognizing that transaction data possesses inherent relational and structural properties, researchers began exploring graph-based approaches and Social Network Analysis (SNA). These approaches proved particularly suited to identify complex layering and structuring patterns characteristic of money laundering schemes. Studies utilizing confirmed laundering structures (Tier A+) predominantly used network analysis, as the relational properties of verified case align directly with graph representations. Early graph-based studies focused on community detection and anomaly scoring however, they failed to account for temporal evolution and became computationally inefficient as dataset sizes grew.

Phase 4: Deep Learning and Hybrid Architectures (2022-2025)

Literature increasingly emphasized more sophisticated models, including Graph Convolutional Networks (GCN), Generative Adversarial Networks (GAN), Graph Attention Networks (GAT), and hybrid models combining GNNs with LSTM in the recent phase. These models enable the modelling of fund movements across multiple accounts, capture changing transaction patterns, and account for the sequential influence of historical transactions on future events.

Journal of Information System and Technology Management
JISTM
EISSN: 0128-1666
Volume 11 Issue 43 (June 2026) PP 132-145

Nevertheless, these models demand higher data quality and greater computational resources, leading many studies to rely on synthetic or partially synthetic datasets (Tier B and Tier C). Studies using Tier B hybrid datasets typically employed semi-supervised models, autoencoders, and GANs to address class imbalance. 20% of the sample articles are Tier C studies, which relied entirely on synthetic datasets and were primarily oriented toward method benchmarking and scalability testing. While these studies reported high-precision results, their findings remain unvalidated against actual money laundering operations, which means they could fail when dealing with real transaction streams. Model interpretability has also emerged as a significant challenge, as regulatory bodies require transparent and explainable decision-making logic. Tier A studies in this phase focused on GNN and hybrid supervised models to refine alert prioritization and minimizing false positives, but without confirmed laundering labels to ground evaluation. Table 2 summarizes the mapping between evidence tiers and method types.

Table 2: Mapping of Evidence Tier and Method Types

Evidence Tier	Dataset Characteristics	Method types	Authors
A^+	Forensic or investigative datasets	Graph-based analysis, SNA, Temporal network analysis	Luo, et al. (2024), Oliveira, et al. (2025), Sousa Lima et al. (2022)
A	Operational dataset	Supervised machine learning, GNNs, hybrid risk model	Bakry et al. (2024), Capozzi et al. (2025), Irshad et al. (2024), Jullum et al. (2020), Ketenci et al. (2021), Khan et al. (2013), Khanuja & Adane (2020), Koo et al. (2024), Lebid & Veits (2020), Li et al. (2020), Magomedov et al. (2018), Martínez-Sánchez et al. (2020), Qiu et al. (2023), Reite et al. (2025), Rocha-Salazar et al. (2021), Vilella et al. (2025), Zhang & Trubey (2019)
B	Hybrid dataset	Semi-supervised models, autoencoder, GAN enhanced machine learning	Chen et al. (2021), Dumitrescu et al. (2022), Xia et al. (2022)
C	Synthetic dataset	Deep learning, GNNs, simulation-based method	Çağlayan & Bahtiyar (2022), Dreżewski et al. (2012), Jayasree & Balan (2016), Karim et al. (2024), Usman et al. (2023)

Source: Authors' interpretation

Journal of Information System and Technology Management
JISTM
EISSN: 0128-1666
Volume 11 Issue 43 (June 2026) PP 132-145

Limitations, Gaps, and Implications for Future Research

Despite significant methodological progress over the past decade, research on suspicious bank transactions detection faces several persistent challenges. The field has advanced from rule-based system and data mining techniques through supervised machine learning and GNNs, to temporal graph hybrids and adversarial simulation frameworks. The availability of datasets with sufficient evidential value, however, has not matched these methodological advances.

The main challenge lies in the evidential quality of the datasets use to validate the detection models. Tier A+ datasets derived from law enforcement investigations remain inaccessible to the research community. As a result, many studies depend on partially synthetic and fully synthetic datasets for benchmarking and prototyping. As a result, findings derived from such datasets do not reliably show how well models would work in real world banking settings. Performance metric alone is therefore misleading when the evaluation datasets do not represent real banking environment. To address this, regulators should establish minimum validation protocols for synthetic datasets and provide incentives for the development of privacy-preserving datasets that can be shared for scientific verification.

Model explainability presents a further challenge. The more complex the models become, the harder it is to understand how they arrive at their decision. This is a concern in regulated financial settings, as regulators and financial institutions require transparent decision logic from the detection systems. This ensures that every flagged transaction is justifiable and auditable.

Finally, this review is limited to journal articles indexed in Scopus, which means relevant studies published in conference proceedings may not have been captured. This scope was intentional, as journal articles offer more comprehensive validation compared to conference proceedings, which typically present early-stage findings. Nevertheless, future reviews may consider broadening the scope to include conference proceedings to provide a more exhaustive coverage of the field.

Acknowledgements: The authors wish to thank all colleagues and peers who provided valuable insights and constructive feedback throughout the course of this research. Their contributions have greatly enhanced the quality of this work.

Funding Statement: No Funding

Conflict of Interest Statement: The authors declare that there is no conflict of interest regarding the publication of this paper. All authors have contributed to this work and approved the final version of the manuscript for submission to the Journal of Information System and Technology Management (JISTM)

Ethics Statement: This study did not involve any human participants, animals, or sensitive data requiring ethical approval. The authors confirm that the research was conducted in accordance with accepted academic integrity and ethical publishing standards.

Author Contribution Statement: All authors contributed significantly to the development of this manuscript. Nordaliela Mohd Rusli conducted the conceptualization, methodology, data collection, analysis, and drafting of this manuscript. Anazida Zainal contributed through supervisory oversight and critical review of the manuscript. All authors read and approved the final version prior to submission.

Journal of Information System and Technology Management
JISTM
EISSN: 0128-1666
Volume 11 Issue 43 (June 2026) PP 132-145

References

Bakry, A. N., Alsharkawy, A. S., Farag, M. S., & Raslan, K. R. (2024). Automatic suppression of false positive alerts in anti-money laundering systems using machine learning. The Journal of Supercomputing, 80(5), 6264-6284. https://doi.org/10.1007/s11227-023-05708-z

Bank Negara Malaysia. (n.d) https://www.bnm.gov.my/

Capozzi, A., Vilella, S., Moncalvo, D., Fornasiero, M., Ricci, V., Ronchiadin, S., & Ruffo,G. (2025). FlowSeries: flow analysis on financial networks. Applied Network Science, 10(1),28. https://doi.org/10.1007/s41109-025-00711-0

Çağlayan, M., & Bahtiyar, Ş. (2022). Money Laundering Detection with Node2Vec. *Gazi University Journal of Science*, *35*(3), 854-873. https://doi.org/10.35378/gujs.854725

Chen, Z., Soliman, W. M., Nazir, A., & Shorfuzzaman, M. (2021). Variational autoencoders and wasserstein generative adversarial networks for improving the anti-money laundering process. IEEE Access, 9, 83762-83785. https://doi.org/10.1109/ACCESS.2021.3086359

Cui, Y., Han, X., Chen, J., Zhang, X., Yang, J., & Zhang, X. (2025). FraudGNN-RL: a graph neural network with reinforcement learning for adaptive financial fraud detection. *IEEE Open Journal of the Computer Society*. https://doi.org/10.1109/OJCS.2025.3543450

Dreżewski, R., Sepielak, J., & Filipkowski, W. (2012). System supporting money laundering detection. Digital Investigation, 9(1), 8-21. https://doi.org/10.1016/j.diin.2012.04.003

Dumitrescu, B., Băltoiu, A., & Budulan, Ş. (2022). Anomaly detection in graphs of bank transactions for anti money laundering applications. IEEE Access, 10, 47699-47714. https://doi.org/10.1109/ACCESS.2022.3170467

Guo, X., Wu, Y., Xu, W., Liu, Z., Du, X., & Zhou, T. (2025, April). Graph-Based Representation Learning for Identifying Fraud in Transaction Networks. In *2025 IEEE 6th International Seminar on Artificial Intelligence, Networking and Information Technology (AINIT)* (pp. 1598-1602). IEEE. https://doi.org/10.1109/AINIT65432.2025.11035591

Imani, M., Beikmohammadi, A., & Arabnia, H. R. (2025). Comprehensive analysis of random forest and XGBoost performance with SMOTE, ADASYN, and GNUS under varying imbalance levels. *Technologies*, *13*(3), 88. https://doi.org/10.3390/technologies13030088

Irshad, F., Alkhalifah, T., Alturise, F., & Khan, Y. D. (2024). GCF-MLD: integrated approach for money laundering detection using machine learning and graph network analysis. IEEE Access. https://doi.org/10.1109/ACCESS.2024.3510115

Jayasree, V., & Balan, R. S. (2016). Anti money laundering in financial institutions using affiliation mapping calculation and sequential mining. Journal of Engineering and Applied Sciences, 11(1), 51-56. https://doi.org/10.1109/ACCESS.2021.3086230

Jensen, R. I. T., Iosifidis, A., & Bank, S. N. (2022). Fighting Money Laundering with Statistics and Machine Learning : An Introduction and Review. IEEE Access, 11, 8889-8903. https://doi.org/10.1109/ACCESS.2023.3239549

Jones, A., & Steel, D. (2018). Evaluating the quality of medical evidence in real-world contexts. *Journal of Evaluation in Clinical Practice*, *24*(5), 950-956. https://doi.org/10.1111/jep.12983

Jullum, M., Løland, A., Huseby, R. B., Ånonsen, G., & Lorentzen, J. (2020). Detecting money laundering transactions with machine learning. Journal of Money Laundering Control, 23(1), 173-186. https://doi.org/10.1108/JMLC-07-2019-0055

Karim, M. R., Hermsen, F., Chala, S. A., De Perthuis, P., & Mandal, A. (2024). Scalable semi-supervised graph learning techniques for anti-money laundering. IEEE Access, 12, 50012-50029. https://doi.org/10.1109/ACCESS.2024.3383784

Ketenci, U. G., Kurt, T., Önal, S., Erbil, C., Aktürkoğlu, S., & İlhan, H. Ş. (2021). A time-frequency based suspicious activity detection for anti-money laundering. IEEE Access, 9, 59957-59967. https://doi.org/10.1109/ACCESS.2021.3072114

Khan, N. S., Larik, A. S., Rajput, Q., & Haider, S. (2013). A Bayesian approach for suspicious financial activity reporting. International Journal of Computers and Applications, 35(4), 181-187. https://doi.org/10.2316/Journal.202.2013.4.202-3864

Khanuja, H.K., & Adane, D.S. (2020). Monitor and detect suspicious transactions with database forensics and Dempster-Shafer theory of evidence. Int. J. Electron. Secur. Digit. Forensics, 12, 154-173. https://doi.org/10.1504/IJESDF.2020.106302

Koo, K., Park, M., & Yoon, B. (2024). A suspicious financial transaction detection model using autoencoder and risk-based approach. IEEE Access, 12, 68926-68939. http://dx.doi.org/10.1109/ACCESS.2024.3399824

Lebid, O. V., & Veits, O. (2020). Search for statistically approved criteria for identifying money laundering risk. Banks and Bank Systems, 15(4),150–163. http://dx.doi.org/10.21511/bbs.15(4).2020.13

Leon, M., Shagñay, F., Rivas, C., & Echeverria, F. (2022, July). A Predictive Model for the Detection of Clients Suspicious Behavior. In *International Conference on Computational Science and Its Applications* (pp. 294-312). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-031-10548-7_22

Li, X., Liu, S., Li, Z., Han, X., Shi, C., Hooi, B., ... & Cheng, X. (2020, April). Flowscope: Spotting money laundering based on graphs. In Proceedings of the AAAI conference on artificial intelligence (Vol. 34, No. 04, pp. 4731-4738). https://doi.org/10.1609/aaai.v34i04.5906

Luo, X., Han, X., Zuo, W., Wu, X., & Liu, W. (2024). MLaD²: A Semi-Supervised Money Laundering Detection Framework Based on Decoupling Training. IEEE Transactions on Information Forensics and Security, 19, 4518-4533. http://dx.doi.org/10.1109/TIFS.2024.3380262

Magomedov, S.G., Pavelyev, S., Ivanova, I., Dobrotvorsky, A., Khrestina, M.P., & Yusubaliev, T. (2018). Anomaly Detection with Machine Learning and Graph Databases in Fraud Management. International Journal of Advanced Computer Science and Applications, 9(11). http://dx.doi.org/10.14569/IJACSA.2018.091104

Mahootiha, M., Golpayegani, A. H., & Sadeghian, B. (2021, March). Designing a new method for detecting money laundering based on social network analysis. In 2021 26th International Computer Conference, Computer Society of Iran (CSICC) (pp. 1-7). IEEE. https://doi.org/10.1109/CSICC52343.2021.9420621

Martínez-Sánchez, J. F., Cruz-García, S., & Venegas-Martínez, F. (2020). Money laundering control in Mexico: a risk management approach through regression trees (data mining). Journal of Money Laundering Control, 23(2), 427-439. https://doi.org/10.1108/JMLC-10-2019-0083

Oliveira, R. M. A., Sant'Anna, A. M. O., & Ferreira, P. H. (2025). Complex networks-based anomaly detection for financial transactions in anti-money laundering. Forensic Science International: Digital Investigation, 55, 302005. https://doi.org/10.1016/j.fsidi.2025.302005

Pambudi, B. N., Hidayah, I., & Fauziati, S. (2019, December). Improving money laundering detection using optimized support vector machine. In *2019 International Seminar on*

Research of Information Technology and Intelligent Systems (ISRITI) (pp. 273-278). IEEE. https://doi.org/10.1109/ISRITI48646.2019.9034655

Qiu, X., Xu, Y., Shi, Y., Deepa, S. K., & Balakumar, S. (2023). Maximum Entropy Principle Based on Bank Customer Account Validation Using the Spark Method. Journal of Computer Networks and Communications, 2023(1), 8840168. https://doi.org/10.1155/2023/8840168

Rajaprkash, S., Kumar, A., Reddy, G. S. K., Reddy, A. S., & Lokesh, B. (2025, June). Supervised and Unsupervised Learning for Fraud Detection in Banking Transactions. In *2025 International Conference on Emerging Technologies in Engineering Applications (ICETEA)* (pp. 1-4). IEEE. https://doi.org/10.1109/ICETEA64585.2025.11099764

Reite, E. J., Karlsen, J., & Westgaard, E. G. (2025). Improving client risk classification with machine learning to increase anti-money laundering detection efficiency. Journal of Money Laundering Control, 28(1), 93-107. https://doi.org/10.1108/JMLC-03-2024-0040

Rocha-Salazar, J., Segovia-Vargas, M.J., & Camacho-Miñano, M. (2021). Money laundering and terrorism financing detection using neural networks and an abnormality indicator. Expert Syst. Appl., 169, 114470. https://doi.org/10.1016/j.eswa.2020.114470.

Sharma, R., & Gupta, S. (2024, August). Strategic Deployment of Deep Learning Algorithms to Mitigate Fraud in Online Finance. In *2024 7th International Conference on Circuit Power and Computing Technologies (ICCPCT)* (Vol. 1, pp. 1007-1011). IEEE. 10.1109/ICCPCT61902.2024.10673115

Singh, D. R., & Gupta, N. (2025, July). Adaptive Hybrid Learning for Credit Card Fraud Detection: A Comparative Study of Supervised, Reinforcement, and Hybrid Models. In *2025 International Conference on Computing Technologies & Data Communication (ICCTDC)* (pp. 1-6). IEEE. https://doi.org/10.1109/ICCTDC64446.2025.11158136

Sousa Lima, R., Marques Serrano, A. L., Onome Imoniana, J., & Medeiros Cupertino, C. (2022). Identifying financial patterns of money laundering with social network analysis: a Brazilian case study. *Journal of Money Laundering Control*, *25*(1), 118-134. https://doi.org/10.1108/JMLC-12-2020-0139

Tan, X. S., Yang, Z., Benlimane, Y., & Liu, E. (2020, December). Using Classification with K-means Clustering to Investigate Transaction Anomaly. In *2020 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM)* (pp. 171-174). IEEE. https://doi.org/10.1109/IEEM45057.2020.9309909

Uma Maheswari, V and Priya, R (2023). Analysis of Offensive Data over Multi-Source Social Media Environment Using Modified Random Forest Algorithm. International Journal of Electronics and Communication Engineering, 10 (9). pp. 63-71. ISSN 23488549. https://doi.org/10.14445/23488549/IJECE-V10I9P107

Usman, A., Naveed, N., & Munawar, S. (2023). Intelligent anti-money laundering fraud control using graph-based machine learning model for the financial domain. Journal of Cases on Information Technology (JCIT), 25(1), 1-20. https://doi.org/10.4018/JCIT.316665

Vilella, S., Capozzi, A., Fornasiero, M. et al. (2025). Weirdnodes: centrality based anomaly detection on temporal networks for the anti-financial crime domain. Appl Netw Sci 10, 14. https://doi.org/10.1007/s41109-025-00702-1

Wang, Y., Zhan, H., & Jiang, W. (2024, January). Time Encoding Graph Attention Model for Financial Fraud Detection in Large-scale Financial Social Networks. In *Proceedings of the 2024 3rd International Conference on Cryptography, Network Security and Communication Technology* (pp. 70-74). https://doi.org/10.1145/3673277.3673290

Xia, P., Ni, Z., Xiao, H., Zhu, X., & Peng, P. (2022). A novel spatiotemporal prediction approach based on graph convolution neural networks and long short-term memory for money laundering fraud. Arabian Journal for Science and Engineering, 47(2), 1921-1937. https://doi.org/10.1007/s13369-021-06116-2

Xiao, Y., & Watson, M. (2019). Guidance on conducting a systematic literature review. Journal of planning education and research, 39,1, 93-112. https://doi.org/10.1177/0739456X17723971

Zhang, Y., & Trubey, P. (2019). Machine learning and sampling scheme: An empirical study of money laundering detection. Computational Economics, 54, 1043-1063. http://dx.doi.org/10.2139/ssrn.3161436

Zhang, Q., Zhu, Y., Zhang, R., Chen, R., & Lan, T. (2025, February). Research on anti-money laundering technology based on graph attention mechanism. In *Tenth Symposium on Novel Optoelectronic Detection Technology and Applications* (Vol. 13511, pp. 565-575). SPIE. https://doi.org/10.1117/12.3056070