Journal of Current Research in Engineering and Science
Bi-Annual Online Journal ( ISSN: 2581 - 611X )
VOLUME:8, ISSUE:1, FEBRUARY 2025, PAPER NUMBER:24

# Leveraging Graph Neural Networks for Enhanced Money Laundering Detection in Financial Networks

Mohammad Farhan Ahmad
Department of Computer Science & *Engineering*
Hindustan Institute of Technology and *Science,Chennai,India.*
ahmedmuhamad625@gmail.com

Rakesh N
Department of Computer Science & *Engineering*
Hindustan Institute of Technology and *Science,Chennai,India.*
rakeshnagasamy@gmail.com

Praisy Evangelin A
Department of Computer Science & *Engineering*
Hindustan Institute of Technology and *Science,Chennai,India.*
*praisye@hindustanuniv.ac.in*

***Abstract*— Preventing money laundering is a major task in the complex world of finance since criminals are always coming up with new and creative ways to hide their illegal activities. Conventional machine learning methods work well for tabular data analysis, but they are not always able to handle the complex interconnectivity of graphical financial data. Our research uses Graph Neural Networks (GNN) and Graph Attention Networks (GAT) to improve detection accuracy in order to close this gap. Using 2 million transaction records from the IBM AML dataset as a starting point, our methodology applies GNNs to convert tabular data into a graphical representation that captures subtle correlations and features. By using attention mechanisms to dynamically weigh the significance of nearby nodes, the incorporation of GATs enhances our methodology even further, improving the precision of detection. This flexible approach overcomes the limitations of conventional algorithms and provides a thorough resolution to the problem of money laundering detection. Our approach strengthens the integrity of the global financial system by combining GNNs and GATs to spot suspicious transaction patterns with previously unheard-of accuracy. In addition to improving detection skills, this novel strategy gives institutions critical insights into the intricate network dynamics that underpin illegal financial activity, enabling them to fight money laundering more successfully. By combining cutting-edge graph-based learning methods, our research aims to establish a new benchmark in the continuous battle against financial crime.**

***Keywords*— *Money Laundering, IBM/AML Dataset, machine learning, Graph Neural Networks (GNN), Graph Attention Networks (GAT)***

## I. INTRODUCTION

Money laundering poses a serious threat to society and the global economy. Billions of individuals go unnoticed as this situation is addressed by conventional means. Because of their quick transaction speeds, modern financial systems offer greater avenues for money laundering [1].Money laundering poses a serious problem since, despite current efforts, existing detection methods cannot keep up with the financial systems' rapid changes. We suggest integrating machine learning into an anti-money laundering (AML) monitoring system to close this gap. Three primary concerns are addressed by this system: generating precise and non-redundant alerts; guaranteeing timely detection; and offering succinct explanations and risk evaluations for every alarm. With the help of professional input and empirical data, this innovative approach seeks to give financial institutions an improved tool to prevent money laundering [2].

Based on the aforementioned inadequacies of standard detection approaches, this study provides a comprehensive ML-based AML solution that covers self- and group comparison analysis to identify suspicious transactions. It enhances self-comparisons by incorporating transactional, product-specific, transactional, and geographic characteristics into KYC data beyond transactions. Group comparisons employ a new variance-based anomaly index to enhance grouping. This approach has better accuracy and lower false positive rates than rule-based systems, which can save financial organizations a lot of money when looking into questionable activities. Data from the real world has been used to evaluate it. [3]

However, traditional detection methods are frequently challenged by the intricate relationships and hidden patterns present in financial transactions. The suggested models that stand out in this regard are graphical attention networks (GAT) and graphical neural networks (GNN). They can depict the intricacies of financial networks using graph-based representations, allowing for a more in-depth comprehension of transaction flows and the identification of minute anomalies that might point to money laundering. This leads to a decrease in false negatives, which implies that fewer occurrences of money laundering go unreported and undiscovered. Furthermore, there are fewer false positives, which spares financial institutions the expense and burden of looking into seemingly innocent transactions.

Graph Attention Networks (GAT) employ a self-attention mechanism to adaptively priorities pertinent information within the transaction network, in addition to dynamically evaluating the significance of neighboring nodes. This makes it easier to identify subtle anomalies that may be signs of potential money laundering activities.

Additionally, the masked self-attention layer in graphic attention networks (GATs) is essential in keeping the model from concentrating on distracting or irrelevant data, which improves the model's resistance to adversarial attacks and guarantees more accurate detection of questionable activity. Furthermore, the embedding's that GNNs learn encompass both direct and indirect transaction linkages, offering a more

thorough comprehension of the transaction network's dynamics. Financial institutions can detect new patterns and trends that suggest possible money laundering schemes thanks to this thorough representation, which makes proactive action to stop financial crimes before they get out of hand possible. Organizations can continuously modify their detection techniques to changing threats by utilizing the combined strengths of GNNs and GATs, keeping one step ahead of criminal actors and maintaining the financial ecosystem's stability and integrity.

## II. Related Works

W. Hilal et al. [4] emphasizes a significant movement in machine learning towards the application of unsupervised and semi-supervised models. The main cause of this change is the difficulty in locating disaggregated data, which is frequently hard to come by and costly. As a feasible alternative, unsupervised and semi-supervised learning approaches allow models to learn from partially or not at all labelled data. Notably, generative models like variational autoencoders (VAEs) and generative adversarial networks (GANs) are receiving a lot of attention. Data scarcity can be efficiently addressed by these generative models, which demonstrate the ability to generate synthetic data that closely reflects real data distributions. Researchers and practitioners can investigate novel methods in machine learning applications across domains by utilizing these advancements.

Martin Gollum et al. [5] They contribute significantly to the by creating and evaluating a machine learning model especially made to rank financial transactions in order to identify possible money laundering activity, the field of financial crime detection will be advanced. Three significant categories of past transaction data are included in the model's training set, which was acquired from the biggest bank in Norway (DNB): reported suspicious transactions, regular transactions, and reported money laundering incidents. The programme can identify intricate patterns and connections that point to illegal financial activity thanks to this extensive data set. Financial institutions can improve their capacity to recognize and reduce money laundering concerns by incorporating machine learning into the manual investigative process. This will help to preserve the integrity of the financial system.

Johrha Alotibi et al.[6] focuses on addressing the growing issue of money laundering, especially as it relates to bitcoin transactions. In order to identify suspicious activity in cryptocurrency money laundering, the study investigates the application of machine learning (ML) and deep learning (DL) techniques, such as Deep Neural Network (DNN), Random Forest (RF), K-Nearest Neighbors (KNN), and Naive Bayes (NB).

M.E. Lokanan and K. Sharma et al. [7] focuses on addressing the problem of fraud in the Canadian securities market by putting out machine learning detection algorithms in an effort to strengthen regulators' capacity to stop fraudulent activity. The proposal of a hybrid anomaly detection method for Anti-Money Laundering (AML) systems is the main emphasis of Asma S. Larik et al. [8]. In order to create regular behaviors for clients, an effective AML system should automatically recognize odd financial activities. This study introduces a method that does just that by using clustering, specifically the Euclidean Adaptive Resonance Theory (TEART). The unsupervised nature of clustering is one of the paper's noted limitations. Since clustering is an unsupervised learning method, measuring its accuracy becomes difficult. Raza Saleha et al. [9] In the paper, a method called SARDBN (Suspicious Activity Reporting using Dynamic Bayesian Network) is presented. It mixes clustering Using dynamic Bayesian networks (DBN) to identify irregularities in transaction sequences. The goal of this paper [10] is to comprehend why businesses with strong MLG are less likely to have income-shifting agreements.

H. Ogbeide et al. [11] examines the overconfidence bias, distributional assessments, and the abilities of AML risk assessors with and without expertise. Using Bahrain as a case study, M. Turki et al. [12] investigate how Regulatory Technology (RegTech) improvements used by banks affect the efficacy of money laundering prevention. The study does acknowledge certain drawbacks, though, such as the possibility of non-response bias, the dependence on expert knowledge, and the difficulty of determining respondents' understanding of RegTech.

In light of growing international communication and technology improvements, the study [14] focuses on applying data science and cooperative efforts with Financial Crime Dynamics to provide an efficient method for preventing financial fraud and money laundering.

Xiaoqian Zhu et al. [15] Focuses on using part-of-speech (POS) features derived from textual risk disclosures in financial reports to detect financial fraud among US energy companies. The study collected and analyzed 10-K filings from 2006 to 2019, extracting risk disclosures and constructing financial variables as benchmarks. POS features were measured by measuring the percentage of different POS keywords using the natural language processing tool spaCy. Four machine learning models (logistic regression, support vector machines, artificial neural network, random forest, and XGBoost) were used for fraud detection, and four high-performance metrics were used for evaluation.

Finally, [18] proposes an ADASYN-TL balance technique and hyperparameter tuning with Random Search, Grid Search, and Bayesian Optimization are used in an ensemble learning approach. Decision Tree, Naive Bayes, K-Nearest Neighbors, and Random Forest classifiers are all combined in the created stacking model.

## III. Proposed System

The proposed system focuses on enhancing money laundering detection using advanced techniques such as graph neural networks (GNN) and specifically graph neural networks (GAT), a subclass of GNN. These structures are designed to process and understand data represented in graph structures. Traditional machine learning algorithms such as XGBoost, CatBoost, AdaBoost, Decision Trees, LightGBM, Random Forest, and Logistic Regression have outperformed in dealing with tabular data. However, to leverage the benefits of graph-based representations of transactional data, we aim to transform tabular data into a graphical form using GNN. This transformation enables GNN and GAT models to more effectively capture complex relationships and patterns in transaction flows. By leveraging graph-based algorithms, we expect to achieve higher accuracy in detecting money laundering activities. This approach not only addresses the limitations of traditional tabular data analysis, but also harnesses the power of graph-based representations for more precise and accurate detection of suspicious financial transactions.

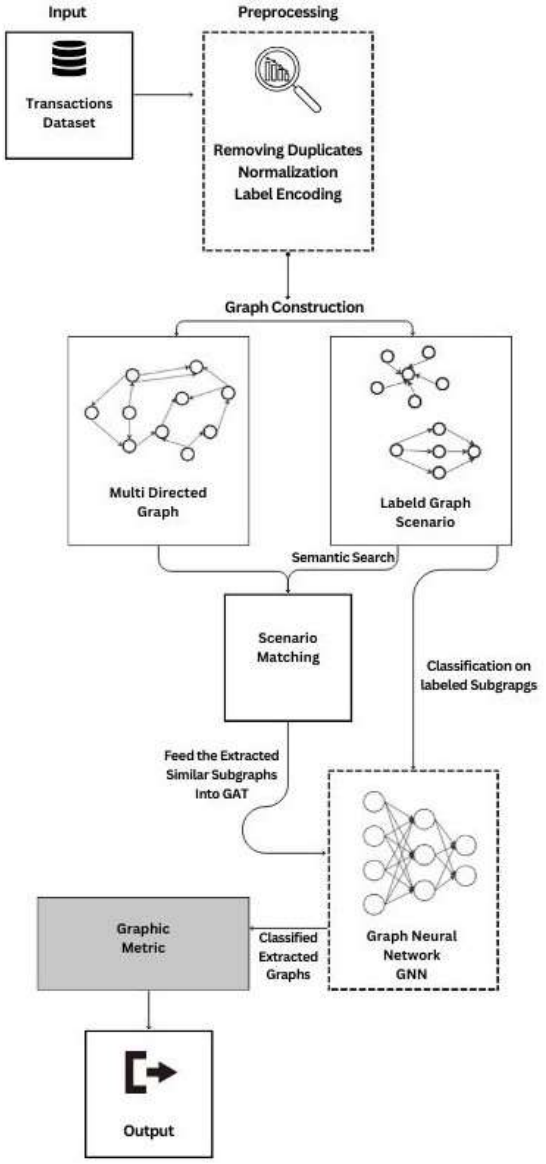


Fig. 1. Architecture diagram

*i. Data Collection:*

To enhance our analysis, we used the IBM Anti-Money Laundering (AML) dataset, a comprehensive set of 2 million multi-class instances extracted from an online environment. All the complex relationships between people, companies and banks are captured in this virtual world. They include consumer purchases, business orders, and loan repayments, all made possible through a variety of account types, such as checks, credit cards, and bitcoin. It is noteworthy that part of the entities is involved in illegal activities such as gambling and smuggling. The next step in the money laundering process is for criminals to attempt to hide the source of the funds using complex financial schemes. Since the dataset is labeled, it can be used to train and test anti-money laundering (AML) algorithms. Its broader application includes risk management and financial cybersecurity analytics, giving analysts a comprehensive understanding of various financial actions and potential risks in this online environment.

*ii. Transaction Data Preprocessing:*

In order to ensure the accuracy and dependability of transaction data, the IBM AML dataset underwent rigorous cleaning throughout the data preprocessing stage to address missing values, duplicates, and outliers. Then, useful information including transaction amounts, timestamps, and types—which are essential for identifying money laundering activity—were extracted using feature engineering. While categorical variables were encoded using either label encoding or one-hot encoding, numerical data was standardized through the use of normalization and scaling procedures. It was crucial to handle class imbalance by dividing the data into training, validation, and testing sets and oversampling or under sampling. In particular, the construction of the graph using transaction data, the extraction of node and edge properties, and the normalization of the graph were essential for Graph Neural Networks (GNNs) to learn and represent intricate interactions and dependencies inside the network of financial transactions. These thorough data pretreatment procedures guaranteed the data's quality, dependability, and applicability for further machine learning analysis—especially when it came to GNN-based AML detection.

*iii. Graph Construction:*

The transaction dataset is transformed into all of the nodes and edges that make up a graph. In the big network with 515,088 nodes and 5,078,345 edges, each transaction is represented as a link between nodes. At the same time, smaller graphs representing various money laundering scenarios are created from the IBM Anti-Money Laundering (AML) dataset. This graph-based representation provides a more connected and comprehensible view of the data. The graph structure of the IBM AML dataset captures the intricate web of relationships inside it, offering a comprehensive understanding of the financial world. The link between nodes, which represents the flow of money and interactions between entities, presents a complete picture of the financial activities. The partitioning of the IBM AML dataset into smaller graphs facilitates the analysis of certain money laundering scenarios and aids in the identification and understanding of potential criminal activities. Using graph-based approaches results in a unified and user-friendly data visualization in addition to improved interpretability. This makes it easier to look at transactional patterns in greater detail inside the virtual financial ecosystem, which is crucial for creating risk management evaluations and anti-money laundering (AML) models.

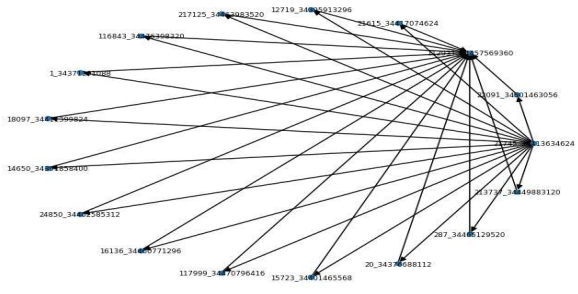

Fig. 2. Graph Formation

crimes.

*iv. Subgraph Extraction:*

Suppose a vast financial network where accounts are connected by transactions. With subgraph extraction, we can narrow down on dubious groups. We already know that recurring little payments between seemingly unconnected accounts are an example of a money laundering tactic. Subsequently, algorithms can explore the entire network for smaller groups that mimic similar suspicious tendencies. Discovering potential rings used for money laundering is like identifying the same fingerprints among many people. By identifying these subgraphs, we can identify unusual transaction patterns, hidden linkages, or specialized paths that criminals pursue. This makes it easier to spot potential money-laundering schemes and gives us a better understanding of the inner workings of the financial system.

*v. Training Graph Neural Network on Label Graphs:*

When a graph neural network (GNN) is trained on labelled subgraphs, it starts to truly learn. Every subgraph is supplied in one at a time. The GNN considers the properties of a node's linked neighbors in the subgraph in addition to its own unique qualities (e.g., transaction amount, node type). "Message-passing" allows the GNN to understand a node's role in its local network. The GNN creates complex representations for each node that include not only its own qualities but also the dynamics and relationships in its immediate neighborhood by simply moving information around the subgraph. After node processing, the GNN uses these learned representations to predict labels based on the specific task. To calculate how successful it was, the GNN compares these predicted labels with the actual labels in the training data using a loss function. The network then uses an optimizer to adjust its internal settings, which lowers this loss and increases accuracy on incoming unseen subgraphs. Subgraphs are fed iteratively, along with message delivery, prediction, loss calculation, and parameter adjustment, until the GNN achieves the desired level of performance on the training set.

*vi. Classifying Extracted Subgraphs and Calculating Similarity:*

Graph Neural Network (GNN) uses its acquired complex node representations to identify recovered subgraphs after training. The GNN uses these representations to forecast labels for certain tasks, which aids in the system's comprehension of the intricate functions that nodes in local networks play. Simultaneously, similarity measures are calculated to assess how much the classified subgraphs resemble the labelled graphs in the dataset. Topological and structural similarities are measured using graph-based criteria, which improves the accuracy of this similarity assessment. This twofold process ensures a comprehensive approach to identifying and categorizing potential money laundering activities by considering both the particular characteristics of nodes and the more general dynamics within their surrounding neighborhoods. The robust categorization system that the GNN's capacity to capture intricate interactions within subgraphs supports allows for the identification of suspicious patterns that bear resemblance to actual money laundering scenarios. Taken together, these combined techniques enhance the GNN's ability to analyze and categorize subgraphs, providing a powerful tool for detecting and preventing financial

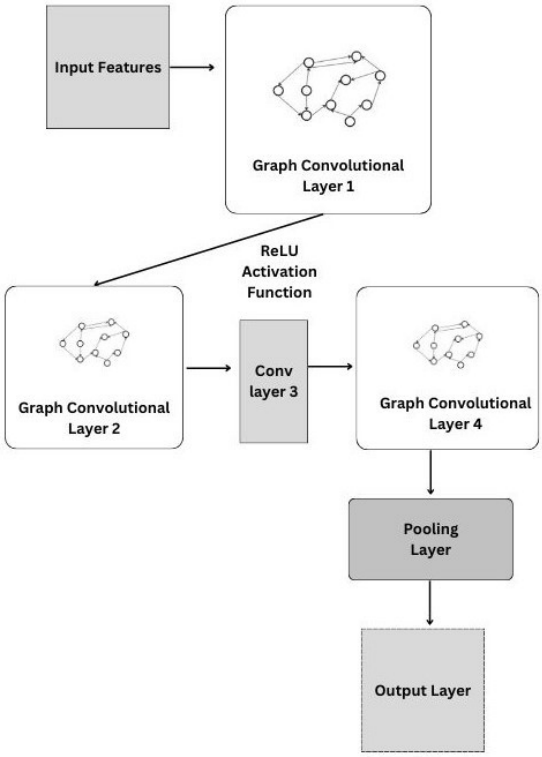


Fig. 3.Work Flow Diagram of GNN

A. Graph Neural Network Architecture:

We have created and put into use a Graph Neural Network (GNN) architecture that is specially designed to classify money laundering scenarios with accuracy. This GNN model has a linear layer for classification tasks after numerous graph convolutional layers (GCNConv). The model is able to efficiently capture complex relationships between nodes because of the architecture, which is painstakingly built to extract meaningful representations from the graphical financial data. Our GNN architecture enhances the capabilities of financial risk assessment and regulatory compliance measures by effectively utilizing graph convolutional techniques to identify potential instances of money laundering and discern complex patterns.

*i. Input Layer:*

In the input layer of a Graph Neural Network (GNN) architecture, node features are initialized, node connections and weights are used to encode the graph structure, information from nearby nodes is aggregated, feature transformations like scaling and normalization are carried out, and the overall graph representation may be initialized. Together, these procedures provide the initial embedding's, capture global and local patterns, and arrange features for the upcoming layers, so preparing the graph data. The input layer plays a crucial role in laying the groundwork for intricate computations, feature learning, and information propagation inside the GNN, enabling efficient graph-based data representation and analysis for a range of applications.

*ii. ReLU Activation Function:*

An essential part of Graph Neural Networks (GNNs) is the Rectified Linear Unit (ReLU) activation function, which introduces non-linearities in node-wise calculations. ReLU activation essentially introduces sparsity and improves the model's ability to capture intricate patterns and features by setting negative values to zero and leaving positive values unaltered. ReLU activation functions are commonly used in GNNs following linear transformations in each layer. This allows the network to learn complex representations and produce precise predictions by promoting the transmission of essential information while suppressing signals and noise that aren't relevant.

$$\mathrm{ReLU}(x)=\max(0,x)$$

*iii. Graph Convolutional Layer:*

When GNN architectures include more than one Graph Convolutional Network (GCN) layer, each GCN layer aggregates data from nearby nodes in the graph to successively improve node representations. Each node's feature vector is updated based on the features of its neighbors in the first feature propagation stage of this process. After that, activation functions like ReLU are applied to the revised node representations in order to improve feature expressiveness and add non-linearity. Each GCN layer is subjected to this procedure once more, enabling the model to recognize progressively intricate patterns and connections within the graph data. Ultimately, the improved node representations are applied to tasks such as graph-level analysis, connection prediction, and node categorization.

*iv. Model Evaluation of GNN:*

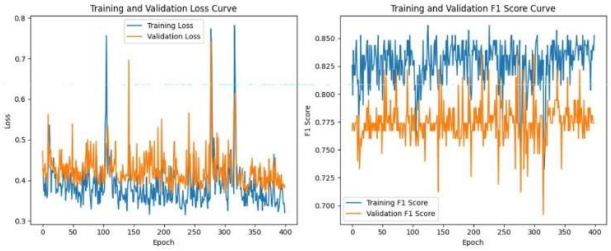


Fig. 4. Loss curve and F1 score curve of the Graph Neural Network (GNN)

The analysis of the Graph Neural Network (GNN) model, as shown in (Fig. 4), delivers important insights into the model's performance and training dynamics. When the model is first trained, it is unstable as evidenced by variations in performance metrics like test accuracy and loss. Using strategies like learning rate schedulers or more complex regularization could help stabilize training as a solution to this. The graph's trends indicate that overfitting can be controlled with early halting or by adjusting dropout rates and regularization strength. Around epochs 10-15, an increase in training loss and a fall in test performance indicate overfitting. Despite these difficulties, the model exhibits hints of convergence with appreciable gains in test accuracy and F1 score as training moves towards later epochs.

This suggests the possibility efficiency of the model architecture for the given task but also raises the possibility that extra epochs or a more dynamic learning rate strategy could be useful in order to improve the model's performance even further. The model demonstrates effective learning over time by reaching its best F1 score and test accuracy by the final epoch. Nevertheless, the significant discrepancy between test and training performance highlights the necessity of additional tuning to improve generalization abilities and reach optimal model performance.

B. Graph Attention Network:

A specific type of GNN called the Graph Attention Network (GAT) is intended to handle graph-structured data, including social networks or citation networks. In order to focus on pertinent nodes and capture complex interactions inside the graph, it uses attention techniques to allocate significance to neighboring nodes during information aggregation. Graph Annotation Technology (GAT) transforms tabular data into a graph representation, where nodes are data items and edges are links or dependencies. Effective feature extraction and representation learning from tabular data with intricate interdependencies is made possible by the attention method in GAT, which computes attention coefficients for every pair of neighboring nodes.

*i. Model Architecture:*

Utilizing a self-attention method to calculate attention scores for each node's neighbors, the Graph Attention Network (GAT) architecture allows nodes to dynamically determine the significance of information based on feature similarities. Afterwards, by aggregating characteristics from nearby nodes using a number of attention heads, these attention scores are used to capture various relationship patterns. After applying dropout regularization to the combined features, a graph convolution operation is used to improve node representations and extract structural information of a higher order. Due to its adaptive attention mechanisms, GAT performs better on a variety of graph-based tasks, including node classification, link prediction, and graph clustering, once these revised representations are processed by the final output layer.

*ii. Model Training:*

By minimizing binary cross-entropy loss for AML detection, the Graph Attention Network (GAT) is trained by stochastic gradient descent (SGD) optimization. Using Neighbor Loader, the training data is loaded in batches for processing after being divided into train and validation sets. The model optimizes the accuracy of AML behavior classification by updating its parameters at each epoch using gradients obtained through backpropagation. The training loop compares predictions with ground truth labels to calculate accuracy, assessing the model's performance on the validation set every 10 epochs. The GAT's attention mechanisms are improved through this iterative process, which also increases the tool's usefulness for financial network analysis.

*iii. Model Evaluation of GAT:*

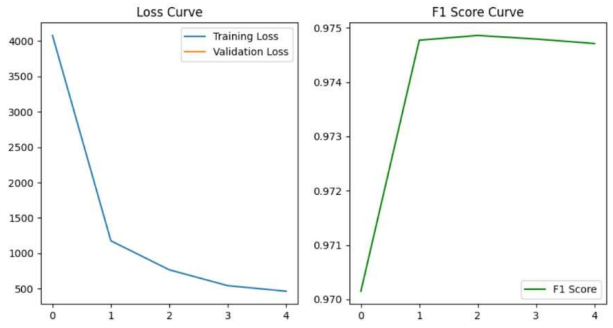


Fig. 5. Loss curve and F1 score curve of the Graph Attention Network (GAT)

The training process of the Graph Attention Network (GAT) over 40 epochs produced a progressive decline in the loss curve, beginning at 4000 and ending at 500, indicating successful learning and model refinement, according to the data from the above diagram (Fig. 5). Concurrently, the GAT's F1 score increased gradually before stabilizing at a high 0.974, demonstrating the model's strong ability to identify money laundering activity in financial networks.

## IV. Result Analysis

In our study of advanced graph-based methods for identifying money laundering in financial networks, we focused on implementing and comparing Graph Neural Networks (GNNs) and Graph Attention Networks (GATs). These technologies have demonstrated potential in navigating the intricate structures of financial transaction networks to detect suspicious patterns associated with money laundering activities.

### *i. Performance Assessment:*

To evaluate the effectiveness of these models, we conducted a thorough analysis using loss and validation curves. These curves are essential for understanding a model's learning progress, as the decrease in loss over epochs indicates its ability to learn efficiently from training data. On the other hand, the validation curve assesses the model's ability to generalize by measuring its performance on unseen data at different training stages.

Our comprehensive analysis yielded significant results. The GNN exhibited proficiency in learning from complex network data, achieving a test accuracy of 0.8136 after being trained for 400 epochs. However, it displayed a relatively higher frequency of lower confidence scores in its correct classifications, with 1874 instances scoring under 0.9 and the minimum confidence score noted at approximately 0.392.

In contrast, the GAT model, with its attention mechanism that assigns varying levels of importance to nodes in a network, demonstrated superior performance. Remarkably, it achieved a testing accuracy of 0.9718 within a shorter training period of just 40 epochs. The F1 scores recorded during training further validate this superior performance, consistently remaining above 0.97. This underscores the model's exceptional precision in classification and robustness in scenario analysis.

### *ii. Implications:*

The notable disparity in performance between the two models underscores the effectiveness of GATs in discerning the nuanced relationships within financial networks associated with money laundering activities. By effectively prioritizing crucial transactional connections and patterns, the GAT model substantially reduces the occurrence of false alerts, a common challenge in anti-money laundering (AML) systems. This fosters a highly efficient and accurate classification and predictive model, crucial for real-world AML applications where the cost of false negatives is exceedingly high.

In conclusion, our study confirms that Graph Attention Networks (GATs) can greatly improve the detection of money laundering in financial systems. The GAT model is a notable improvement in using graph-based deep learning to improve AML efforts because it not only shows improved accuracy but also speeds up the learning process. Moreover, the attention mechanism built into GATs provides a strong use case for its adoption in identifying and forecasting intricate cycles of money laundering crime within financial networks, thereby addressing the crucial difficulty of lowering false alerts.

## V. Future Works

There are several key areas that can be explored in future work to enhance the potential of Graph Attention Networks (GATs) in detecting financial fraud. One area is the integration of temporal dynamics, which can provide deeper insights into evolving transaction patterns. Additionally, the integration of multi-modal data can improve predictive accuracy. It will also be crucial to scale GATs for complex, large-scale financial networks in order to conduct comprehensive fraud analysis.

To facilitate widespread adoption, it is important to enhance the interoperability of GAT models with existing financial infrastructures. This will enable seamless integration and utilization of GATs in real-world systems. Furthermore, continuous learning approaches should be employed to ensure that GATs remain effective in recognizing new laundering tactics as they emerge.

Collaborative initiatives with financial entities and regulatory bodies are essential for obtaining rich datasets and validation. By working together, these entities can contribute to the robustness and reliability of GATs in preventing financial fraud. Ultimately, these advancements have the potential to significantly contribute to safeguarding global financial systems against illicit activities.

In the context of our project, future work could focus on exploring these areas to further enhance the effectiveness of GATs in detecting and preventing financial fraud.

## VII. Conclusion

In conclusion, our study has shown a major advancement in the identification of money laundering inside financial networks by utilizing Graph Neural Networks (GNNs) and Graph Attention Networks (GATs). For practical anti-money laundering (AML) applications, the GATs in particular have demonstrated greater capabilities in spotting complex fraudulent patterns with high accuracy and fewer false warnings.

The encouraging findings of this study provide the groundwork for further research projects in addition to demonstrating the potential of GATs as an effective tool for financial institutions.

It is clear from looking ahead that the way forward involves investigating dynamic graph models that have the ability to record temporal transaction patterns, which will give a more comprehensive context for anomaly detection. The use of multi-modal data sources is expected to enhance the model's comprehension of transactions even further. Moreover, meeting the requirements of large-scale financial systems will depend on scaling the models to effectively manage dense and complicated networks.

To optimize the models' impact and ease their adoption, it is imperative to ensure their compatibility with current financial systems and regulatory frameworks. Maintaining the relevance of detection algorithms in the face of adaptive laundering tactics will require ongoing learning processes. In addition to improving the models using a variety of datasets, cooperation with industry partners and regulatory agencies will guarantee that the study is in line with practical issues.

Through the advancement of study in these crucial areas, we will be able to provide even more reliable, accurate, and effective money laundering prevention technologies. This will protect economies, strengthen the integrity of financial institutions throughout the world, and make the global financial system easier to access.

## REFERENCES


[1] Dattatray Vishnu Kutte, Biswajeet Pradhan, Nagesh Shukla and Abdullah Alamri, " Deep Learning and Explainable Artificial Intelligence Techniques Applied for Detecting Money Laundering–A Critical Review," 2021.

[2] Pavlo Tertychnyi, Mariia Godgildieva, Marlon Dumas and Madis Ollikainen, " Time-aware and interpretable predictive monitoring system for Anti-Money Laundering," 2022.

[3] Jos´e-de-Jesús Rocha-Salazar, María-Jesús Segovia-Vargas and María-del-Mar Camacho-Minano, "Money laundering and terrorism financing detection using neural and an abnormality indicattor," 2021.

[4] Waleed Hilal, S.Andrew Gadsden and john Yawney "Financial Fraud: A Review of anomaly Detection Techniques and Recent Advances ," 2022.

[5] Martin Jullum, Anders Loland and Ragnar Bang Huseby, "Detecting Money laundering transactions with machine learning," 2020

[6] Johrha Alotibi, Badriah Almutanni, Tahani Alsubait, Hosam Alhakami, Abdullah Baz, " Money Laundering Detection using MachineLearning and Deep Learning," 2022.

[7] Mark Eshwar Lokanan, and Kush Sharma, "Fraud prediction using machine learning: The case of investment advisors in canada," 2022

[8] Asma S.Larik and Sajjad Haider, "Clustering based Anomalous Transaction Reporting," 2010.

[9] Saleha Raza and Sajjad Haider, " Suspicious activity reporting using dynamic bayesian networks," 2010.

[10] Baban Eulaiwi, Nihad Shareef Khalaf, Ahmed Al-Hadi, Lien Duong and Grantley Taylor " Money laundering governance and income shifting: Evidence from Australian financial institutions," 2024.

[11] Henry Ogbeide, Mary Elixabeth Thomson, Mustafa Sinan Gonul, Andrew Castairs Pallock, Sanjay Bhowmick and Abdullahi Usman Bello, "The anti-money laundering risk assessment: Aprobablistic approch," 2023

[12] Meaad Turki, Allam Hamdan, Richard Thomas Cummings, Adel Sarea, Magdalena Karolak and Mohammad Anasweh "The regulatory technology “RegTech” and money laundering prevention in Islamic and conventional banking industry, "2020.

[13] Daniel Otero Gomez, Santiago Cartagena Agudelo and Andres Ospina patino, " Anomaly Detection applied to Money Laundering Detection using Ensemble Learning,"2021

[14] Gleidson Sobreira Leite, Adriano Bessa Albuquerque and Plácido Rogerio Pinheiro, "Application of Technological Solutions in the Fight Against Money Laundering—A Systematic Literature Review," 2019.

[15] Xiaoqian Zhu, Jianping Li, and Hao Sun, ‘‘Financial fraud detection based on the part-of-speech features of textual risk disclosures in financial reports,’’ 2023

[16] Leonid Garin, and Vladimir Gisin‘‘Machine learning in classifying bitcoin addresses,’’ 2023.

[17] Kamal Omari, `` Phishing Detection using Gradient Boosting Classifier," 2023.

**[18]** Noor Nayyer, Nadeem Javid, Mariam Akbar,Abdulaziz Aldegheishem,Nabil Alrajeh, and Moshin Jamil, “A New Framework for Fraud Detection in Bitcoin Transactions Through Ensemble Stacking Model in Smart Cities,”2023.