Synthesis: A Multidisciplinary Research Journal
Volume 1, Issue 4, October - December 2023, Pp: 46-57

Research Paper

Explainable Hybrid Graph Neural Networks for Financial Fraud Detection and Credit Risk Propagation

[1*] M. Swetha, [2] Gormanukonda Ravi Kumar, [3] Lavanya Addepalli

[1*] *Department of AIML, Anil Neerukonda Institute of Technology and Sciences, Visakhapatnam, Andhra Pradesh, India.*
Email: swethabepala3@gmail.com
[2] *Assistant Professor, Department of CSE, Rayalaseema University, Kurnool, Andhra Pradesh, India.*
Email: grkondaravi@gmail.com
[3] *Department of Communication and Cultural Industries, Universitat Politècnica de València, Valencia, Spain,*
Email: phani.lav@gmail.com

**Corresponding Author(s): swethabepala3@gmail.com*

Article Info
Received:17/08/2023
Revised: 24/10/2023
Accepted:28/12/2023
Published:31/12/2023

Abstract

A rise of complex digital financial systems has prompted a surge of advanced fraudulent actions and escalating issues in proper credit risk evaluation. Conventional machine learning methods would tend to overlook the relational relationships and time dynamics of financial data, which leads to lower accuracy with detection limited and slower risk detection. To overcome these difficulties, we present in the current paper Explainable Hybrid Graph Neural Network (EH-GNN) model to do financial fraud early detection and credit risk propagation modeling. The proposed solution models financial transactions as a heterogeneous graph and incorporates a relational attention, time memory model, and risk propagation systems in the same architecture. It also includes a dual-task prediction module that simultaneously predicts fraud risk and credit risk as well as a multi-level explainability module that offers explainable understanding at a feature and a graph level. The proposed framework has been proved effective through extensive experiments carried out on the PaySim, and Credit Card Fraud Detection datasets. The EH-GNN has a higher accuracy of 98.6, F1-score of 0.93 and ROC-AUC of 0.968 compared to the state-of-the-art baseline models. Moreover, it minimizes the error in credit risk prediction with 0.089 RMSE which depicts a better reliability of Ms.Credit risk estimation. The findings support that the suggested framework is able to represent complicated financial dynamics and offer predictions that can be interpreted, hence is a powerful and viable way to apply to real-life fraud detection and risk management mechanisms.

Keywords: Financial Fraud Detection, Graph Neural Networks (GNN), Credit Risk Prediction, Explainable Artificial Intelligence (XAI), Risk Propagation, Temporal Graph Learning, Heterogeneous Graph Modeling.

1 Introduction

The swift growth of electronic financial services, internet banking, and mobile payment systems has greatly accelerated the number and speed of financial transactions all over the globe. Although these innovations have improved accessibility and efficiency, they have brought increased exposure of financial systems to an increasing number of organized fraud cases, such as identity theft, falsification of transactions, and organized money laundering [1], [2]. The growing complexity and interconnectedness of financial eco systems are such that the conventional fraud detection system becomes inadequate in ensuring that emerging and large scale fraudulent activities are successfully detected [3].

Simultaneously, proper credit risk assessment is one of the core criteria that financial institutions need to be stable and reduce possible losses. Credit risk prediction deals with the

estimation of chances of a borrower failing to meet his financial commitments and this is always determined by the behaviour of the individual as well as the relationship attribute [4]. Traditional statistical reasoning and rule-based systems have been extensively employed to do this, but they typically do not reflect dynamics of nonlinear dependencies between entities and dynamic interaction with entities [5].

The recent advancements in machine learning have made a great deal of enhancement in terms of fraud detection and risk prediction by utilizing the data-driven approach [6]. Decision tree models, ensemble and deep neural network models have shown high levels of prediction when they are used to their structured financial data [7]. However, these methods generally consider transactions as single cases and fail to consider the relation structure, which is inherent in financial systems [8]. In practice, financial data constitute a complex network with users, accounts, and transactions interlinked by various relationships, and these relationships are instrumental to discover suspicious activity [9].

In order to overcome this, graph-based learning, in particular Graph Neural Networks (GNNs), have been presented as potent for framework representations of relational information and dependencies between connected entities [10]. GNNs facilitate aggregation of information around the neighborhood, which makes it possible to detect concealed patterns like fraud rings and organized attacks that can hardly be recognized using conventional tools [11]. Although the benefits are present, the current GNN-based solutions are mainly dedicated to fraud detection as an independent task, not taking a better look at the possibility of jointly modeling credit risk and fraud, which are causally interdependent phenomena in a financial system [12].

Handling of the dynamics of time is another critical weakness of existing methods. Financial transactions are very time conditioned, with abrupt variation in the activity patterns, which can indicate possible fraud or new financial risk [13]. Models that cannot accommodate temporal information can potentially miss out such patterns, leading to slower detection and decreased performance. Moreover, it is not yet interpretable in most deep learning models, which is a serious obstacle to implementing this type of technology into practice, since the financial sector needs transparent and explainable systems to understand regulatory restrictions and trust in automated decision-making [14].

Moreover, another facet that has not been fully addressed in the, detection and credit evaluation in terms of financial network is the risk propagation on financial networks. Especially the risk of one entity may impact related entities due to shared accounts, transactions, or behavioral patterns, and result in cascading effects throughout the network [15]. Such propagation mechanisms might be overlooked, leading to incomplete risk assessment and indirect fraud situations not being detected.

To overcome these issues, the paper will introduce an explainable hybrid graph neural network (EH-GNN) to train, early detect an act of financial fraud and generate credit risk propagation. The suggested solution conceptualizes financial information in the form of a heterogeneous graph to represent intricate relationship effects amongst entities. A hybrid learning architecture is developed to combine relational attention, temporal modeling, and risk propagation mechanisms to make the framework able to successfully learn structural and dynamic patterns. Moreover, a multi-level explainability component is added to deliver explainable insights on a feature, edge, and subgraph levels to promote transparency and buttress decision-making processes in financial systems.

Key Contributions

The main contributions of this paper are summarized as follows:

- An Explainable Hybrid Graph Neural Network (EH-GNN) framework is suggested to combine predicting financial fraud and credit risks based on heterogeneous financial graphs.
- A hybrid learning system that combines relational attention, temporal memory and risk propagation is created to elucidatively represent daring and shifting financial behaviors.
- It presents a dual-task prediction and multi-level explainability model, which simultaneously maximizes a frequency of fraud and model credit risk estimations and offers comprehensible statistics at both feature and graph scales.
- The high performance of the proposed approach, its robustness, and practical applicability have been established through extensive experiments on synthetic and real-world data, which show that the proposed approach outperform the state-of-the-art methods.

The rest of this paper is structured in the following way. Section II provides a literature survey of the related research on fraud detection, credit risk modeling and graph-based learning. Section III explains the EH-GNN method in detail, such as structure of graphs, work of hybrid learning modules and explainability. Section IV provides a description of the experimental design, data, and metrics of evaluation. The analysis and representation of the performance and results are discussed in Section V. Lastly, Section VI summarizes the paper and points out possible future work directions.

2 Literature Review

The recent progress in financial fraud detection and credit risk assessment has given rise to the creation of a diverse array of computational methods due to the growing complexity and interdependence of the financial systems. The literature has already studied conventional machine learning methods, deep learning architecture, and graph-based to enhance the quality of detection and scalability. Specifically, the use of Graph Neural Networks (GNNs) has received extensive interest due to their ranking capabilities of building relationships among the financial actors. Nevertheless, there are still issues on how best to incorporate time dynamics and capture the risk propagation through networks, as well as maintaining interpretability of model forecasts. The section is based on a review of literature in the major research directions, such as traditional and deep learning, graph-based fraud detection, graph modeling based on time, hybrid learning models, predicting credit risk, and explainable AI, presenting their advantages and drawbacks.

2.1 Traditional Machine Learning Approaches

Initial studies of financial fraud detection mostly utilized the conventional approaches of machine learning, including logistic regression, decision tree and ensemble models. All these techniques proved useful in structured contexts and offered interpretable outcomes, but usually failed to elicit complex nonlinear correlations and changing set of fraud behaviors in big financial information [16], [17]. Additionally, these methods are usually on the assumption that transactions are single incidences and as a result, they are not able to take advantage of relational dependencies between financial institutions.

2.2 Deep Learning-Based Methods

As the deep learning evolved, more complex models were created to enhance the performance of fraud detection. Convolutional neural networks (CNNs) and recurrent neural networks (RNNs) are neural network-based methods which demonstrated the capability to capture high-dimensional feature representations and temporal patterns in financial transactions [18]. Although, such models have better predictive power, the capacity to describe the underlying network structure of financial systems (where system interactions are important in detecting fraudulent behavior) is typically lacking [19].

2.3 Graph-Based Fraud Detection

Graph-based methods have become of particular interest to overcome the drawbacks of traditional methods as well as deep learning methods. Graph Neural Networks (GNNs) can model financial systems as networks with nodes, which can be used to obtain structural and relational properties [20]. These methods have been shown to be effective in identifying a fraud ring and coordinated operations through making use of multi-hop neighborhood data [21]. Moreover, heterogeneous graph representations have already been investigated to model various kinds of entities and relationships by improving the detection of entities in any complex financial environment [22].

2.4 Temporal and Dynamic Graph Learning

Recent research has highlighted the need to include the time dynamics in fraud detection models. Temporal GNNs are models that build upon classic graph models by modeling time-varying transaction patterns and sequential interactions [23]. These are especially useful in detecting new trends in behavior and new patterns of fraud. Moreover, graph structures built upon video cameras have been suggested to support real-time detection of fraud, enhancing the responsiveness in high frequency setting [24].

2.5 Hybrid and Multi-Relational Models

Hybrid techniques between graph learning and more advanced deep learning methods have been suggested to enhance the performance with regard to detection. Such models combine mechanisms of attention layers, memory networks, multi-modal data representations to represent complex interactions and contextual data [25]. Moreover, further development has resulted in multi-relational graph models that are more suitable to the description of various financial transactions, as well as to uncovering previously unknown connections between entities to detect fraud more accurately [26].

2.6 Credit Risk Prediction and Integration

Traditionally, statistical and machine learning techniques have been applied to prediction of credit risk. Nonetheless, the recent studies have demonstrated the introduction of relation and graph-based capabilities can considerably increase the accuracy of prediction as it models the relationship between borrowers and financial institutions [27]. Furthermore, the combination of credit risk prediction and fraud detection has become a prospective area of research since the two tasks are fundamentally related and could be even mutually useful to share common representations [28].

2.7 Explainable AI in Financial Systems

One significant issue with the implementation of sophisticated machine learning models in financial systems is the interpretability. To overcome this problem, Explainable Artificial Intelligence (XAI) methods have been proposed to give a glimpse into how the models make predictions. Such approaches like SHAP algorithms, attention-based explanation as well as graph explainability approaches have been extensively used to enhance transparency and trustworthiness in the fraud detection systems [29]. Specifically, explainable GNN models have been designed that determine the influential nodes, edges, and subgraphs to gain a clearer insight into how decisions are made and to facilitate compliance with regulations [30].

2.8 Research Gap and Motivation

Although the current methods have improved tremendously in detecting fraud and predicting credit risks, a number of major shortcomings are still there. Conventional machine learning and deep learning models mainly work with independent transaction data, therefore, unable to capture the scarcity of relational relationships intrinsic to financial systems. Even though past studies have overcome this shortcoming by modelling interrelated entities using a graph methodology, the majority of the existing GNN-based strategies are strictly limited to fraud detection without the joint modeling of credit risk, even though these two directions are so closely related to each other. In addition, most of existing models are unable to properly incorporate the role of time dynamics, which are crucial in determining changes in fraud trends and in making it possible to detect them early. The second significant constraint is insufficient modeling of risk spreading among financial networks, where the risk or fraudulent elements are likely to spread due to interrelationships. Also, most sophisticated models are black-box, which provides limited interpretability, which decreases their applicability in managed financial conditions.

To deal with these issues, a common framework is required to both model relational structures, temporal dynamics and risk propagation, and to be interpretable. The suggested Explainable Hybrid Graph Neural Network (EH-GNN) framework will become a framework that fills these gaps by combining graph-based learning, temporal modeling, dual-task prediction, and multi-level explainability into a single architecture.

3 Proposed Methodology

3.1 Overview of the Proposed Framework

The framework suggested presents Explainable Hybrid Graph Neural Network (EH-GNN) based on early financial

fraud detection and credit risk propagation modeling. The approach combines the heterogeneous graph building, combined with the hybrid graph representation learning, with the temporal dynamics modeling and the explainability mechanisms into a single pipeline.

Multi-relational dependencies and risk diffusion between interdependent financial actors, which is unavailable in traditional transaction-level models, are captured by the proposed framework, making it possible to identify risks sooner and understand the decisions taken. There are four key steps in the workflow, namely: (i) dynamic graph building, (ii) hybrid graph representation, (iii) dual-task prediction and (iv) risk interpretation using explainability.

3.2 System Architecture

The general structure of the suggested EH-GNN framework is shown in Fig. 1 and demonstrates the communication between the modules of graph-construction, hybrid learning, prediction, and explainability.

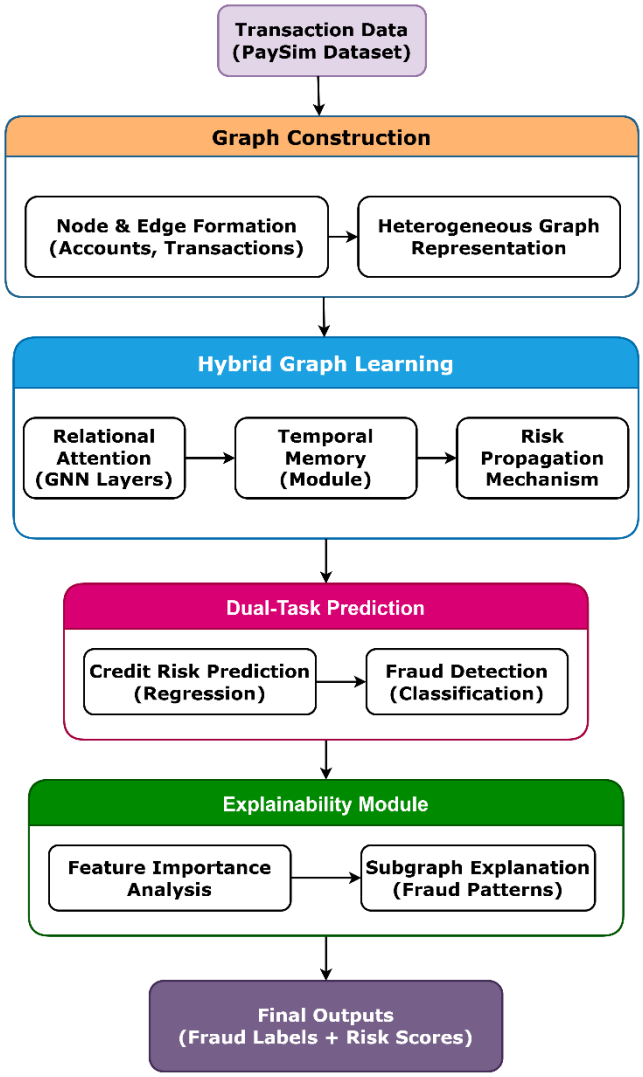

Fig. 1. System Architecture of the Proposed EH-GNN Framework.

The proposed EH-GNN framework will be structured, as shown in Fig. 1, into various modules, as follows: graph construction, hybrid graph learning, dual-task prediction, and explainability. Data on input financial transactions are first converted to a heterogeneous graph representation, a representation of relationships between entities. The hybrid learning module in turn incorporates relational attention, temporal memory and risk propagation to learn complicated patterns. The dual-task prediction component carries out detecting fraud and estimating credit risk, and the explainability component offers interpretable information in terms of feature importance and subgraph analysis. Such a formal structure facilitates efficient modelling of the interactions between financial entities and facilitates accurate and open-minded decision-making.

3.3 Dynamic Heterogeneous Graph Construction

A time-varying financial graph is created to express relationship between entities like customers, accounts, transactions and merchants.

Let the financial graph at time t be defined as:

$$G_t = (V_t, E_t, X_t, A_t) \tag{1}$$

where V_t denotes the set of nodes, E_t represents edges, $X_t \in \mathbb{R}^{|V_t| \times d}$ is the feature matrix, and A_t is the adjacency matrix.

Each node $v_i \in V_t$ is associated with feature vector:

$$x_i = \left[f_i^{(1)}, f_i^{(2)}, \ldots, f_i^{(d)}\right] \tag{2}$$

Edges are multi-relational, and they capture transaction flows, common devices and credit dependencies. The adjacency for relation type r is:

$$A_{ij}^{(r)} = \begin{cases} 1, & \text{if nodes } i \text{ and } j \text{ are connected via relation } r \\ 0, & \text{otherwise} \end{cases} \tag{3}$$

The resulting formulation allows the heterogeneous financial interactions and latent patterns of fraud to be captured.

3.4 Hybrid Graph Neural Network Encoder

A hybrid encoder, which combines risk propagation, relational attention, and temporal dynamics to effectively learn representations, is necessary to learn representations effectively.

Relational Graph Attention Layer: Attention weights on the various relations are used to update node embeddings:

$$h_i^{(l+1)} = \sigma\left(\sum_{r \in R} \sum_{j \in N_i^r} \alpha_{ij}^{(r)} W_r h_j^{(l)}\right) \tag{4}$$

where $\alpha_{ij}^{(r)}$ is the attention coefficient:

$$\alpha_{ij}^{(r)} = \frac{\exp\left(\text{LeakyReLU}\left(a_r^T [W_r h_i \| W_r h_j]\right)\right)}{\sum_{k \in N_i^r} \exp(\cdot)} \tag{5}$$

Temporal Memory Module: A gated recurrent unit (GRU) is present to compute the state of the nodes in sequence:

$$m_i^t = \text{GRU}(m_i^{t-1}, h_i^t) \tag{6}$$

This enables the sequences of transactions and development of fraud behavior to be modeled.

Risk Propagation Layer: Risk is spread through the graph to represent impact between entities:

$$\rho_i^{(k+1)} = \lambda s_i + (1 - \lambda) \sum_{j \in N_i} \frac{w_{ij} \rho_j^{(k)}}{\sum_j w_{ij}} \tag{7}$$

where ρ_i is propagated risk and s_i is intrinsic risk score.

3.5 Dual-Task Prediction Module

The framework synchronously forecasts both fraud and credit risk, using a shared latent representation z_i, that makes use of structural, temporal, and relationship information of the financial graph. Prediction is performed by two parallel task-specific heads and then a single objective of optimization is accomplished.

Fraud Detection

$$\hat{y}_i^{(f)} = \text{Softmax}\left(W_f z_i + b_f\right) \quad (8)$$

This equation constitutes the aspect of fraud detection, and the objective of the equation is to classify whether an entity or transaction is fraudulent or not. The learned embedding z_i is then linearly mapped by the weight matrix W_f and bias vector b_f that project the embedding to a task-specific decision space. It is then followed by the Softmax function which transforms the output into a probability distribution of the potential classes which most usually consist of a fraudulent and non-fraudulent classifier.

The main importance of such formulation is that it yields the results that are probabilistic and thus allows the model to measure the possibility of fraud instead of making a categorical choice. The input embedding z_i includes graph structure, time-varying behavior, and diffusive risk, indicating the prediction of fraud is not made by examining characteristics of individual transactions, but it is a prediction that is affected by the wider relational framework. This will enable the model to identify complicated fraud patterns like orchestration and indirect relationship with known fraudulent participants.

Credit Risk Prediction

$$\hat{y}_i^{(r)} = \sigma(W_r z_i + b_r) \quad (9)$$

The following equation constitutes the prediction task of the credit risk model that approximates the likelihood of an entity to end up as a financial ill or default. Like the fraud detection head, the shared embedding z_i is linearly transformed by parameters W_r and b_r. Nevertheless, the activation function is a sigmoid, which brings the output to the range of 0 to 1.

Sigmoid output: Sigmoid yield is the likelihood of the credit risk being high, this is appropriate in the scenario in which the risk assessment is to be binary. In contrast to fraud detection that revolves around detection of immediate abnormal activity, credit risk prediction addresses latent financial instability trends which might develop over a period of time. The model takes advantage of the same embedding z_i to take advantage of patterns between tasks sharing common information, and letting patterns suggestive of fraud (e.g., abnormal behavior of transactions or risky relationships) to inform the estimation of the credit risk. This learning in common enhances the capability of the model to recognize entities that, although not fraud, yet carry attributes that are related to the risk in the future.

Multi-Task Loss Function

$$\mathcal{L} = \mathcal{L}_{\text{fraud}} + \gamma \mathcal{L}_{\text{risk}} + \eta \mathcal{L}_{\text{prop}} \quad (10)$$

The multi-task loss strategy incorporates the aims of detecting fraud, credit risks forecasting, and consistency of risk propagation into one optimisation framework. $\mathcal{L}_{\text{fraud}}$ can be translated as the loss due to classification of fraud, which is most commonly calculated with a cross-entropy loss, which discourages false freedoms, and rewards effective detection of fraudulent ones. $\mathcal{L}_{\text{risk}}$ denotes the credit risk prediction loss, which is often modeled with binary cross-entropy to quantify the risk probability prediction error between the predicted and actual risk.

The third term, $\mathcal{L}_{\text{prop}}$, imposes consistency on the results of predicting the risk scores with the propagated risk values of the graph structure. The term guarantees that all predictions of the model are adjusted to the network-level risk diffusion process ensuring that there are no incongruities in which a predicted entity can be identified as low-risk when highly related to high-risks neighbours.

The two weighting parameters γ and η adjust the weighting of the risk prediction and propagation consistency terms respectively. When these parameters are modified, the model is able to weight the contributions of every task, making sure that both the fraud detection and chances of prediction tasks do not override the learning process. The joint-optimization aspect of this framework allows the framework to learn complementary patterns across the tasks that lead to better overall performance and allows fresh financial risks and fraudulent activity to be detected early.

3.6 Explainability Module

To guarantee transparency and interpretability in decision-making of the financial scope, the proposed framework will consider an Explainability Module that it will give a visualization of the model prediction at many levels. Since financial applications are critical, decisions within them need to be audited and justified, this module allows seeing the most impactful features, relations, and structuralities within the graph. The mechanism of explainability functions over three levels that are supplementary to one another featuring importance of features, importance of edges and subgraph explainability.

Feature Importance

$$\phi_i = \frac{\partial \hat{y}_i}{\partial x_i} \quad (11)$$

The equation quantifies the feature-level importance by determining the sensitivity of the outcome of prediction y -1 with regard to the attributes of x_i of node i. In particular, it calculates the gradient of the prediction with system features value coefficient, which shows the effect of a tiny change of the input features on the final prediction.

This is important because it helps determine the attributes that make the greatest contribution to the decision of this model. Differences in features that possess greater magnitude of gradient exert more influence on the prediction, thus underlining the major factors that influence the classification result. The features can be transaction amount, frequency, temporal, or behavioral indicators derived in the context of financial fraud detection. Where predicting credit risk is concerned, some influential features can be in the form of consistent spending, repayment behavior, or relationship to high-risk parties.

Through ϕ_i, the model enables a local explanation of every single prediction giving stakeholders an opportunity to know whether an action is an actual financial practice or unusual dynamics. This is especially significant when it comes to compliance with regulations because it allows to

ensure that the model is not making use of irrelevant or biased features.

Edge Importance

$$\psi_{ij} = \frac{\partial \hat{y}_i}{\partial A_{ij}} \tag{12}$$

This formula reflects the value of the relationship between entities based on analyzing the sensitivity of the prediction $\hat{y}_i$ to the transformation of the element of the adjaceny matrix A_{ij} that is the association between nodes i and j. Differently put, it quantifies the strength of that particular edge to the prediction of node i.

Addition of edge importance is especially important in a graph based financial models where not only an individual attribute of entities has some effect on decisions but also an interaction between entities contributes to the decisions made. A large ψ_{ij} means that the relationship between node i and j is very important in the determination of prediction. An example includes the fact that a high edge importance score can be related to a transaction connection involving an already rated fraud account, a shared device with suspicious customers or a recurring connection with a high-risk merchant.

The formulation covers important relational drivers of fraud and risk, which give an insight of the information flows along the network. The model facilitates the identification of these coordinated pattern of frauds, e.g. the existence of a fraud ring, or collusive behavior, which might not be apparent due to node-based features.

Subgraph Explanation

$$G_i^* = \arg\max_{G'} P(y_i \mid G') \tag{13}$$

The subgraph explanation extends the interpretability to this graph level to the maximum subset of the graph $G_i^* \subset G$ which has the highest likelihood of producing the predicted outcome of node i. The idea is to extract the most informative subgraph G' which explains the decision of the model in a way satisfactory and at minimal or non-redundant cost.

The subgraph explanation explains collectively the effect of a group of nodes and edges as opposed to feature and edge importance that offer localized explanations. It can be especially handy in financial networks where fraud and risks are frequently the results of the patterns related to them, instead of random occurrences. Indicatively, a subgraph can represent a group of accounts that appear to be facilitating circular transactions, a group of entities that share a common identifier or a chain of interactions among several high-risk nodes.

The optimization purpose is that the extracted subgraph is accurate of the predictive power of the initial model, thus keeping the fidelity intact without decreasing interpretability. This enables analysts to see and interpret the underlying structure that made the prediction which helps in investigating fraud, tracing anomalies and auditing by regulations.

3.7 Early Warning Risk Score

The Early Warning Risk Score (EWS) combines a number of predictive signals in one interpretable value towards ideal financial decision-making. It uses the immediate fraud probability as well as the long-term credit risk and the influence on the network in order to offer a holistic measurement of the risk of an entity.

The unified score is defined as:

$$EWS_i = \omega_1 P_{\text{fraud}} + \omega_2 P_{\text{risk}} + \omega_3 \rho_i + \omega_4 C_i \tag{14}$$

where P_{fraud} represents the predicted fraud probability, P_{risk} denotes the credit risk probability, ρ_i is the propagated risk from the graph, and C_i is the prediction confidence. The weights $\omega_1, \omega_2, \omega_3, \omega_4$ control the contribution of each component.

P_{fraud} captures situational aberrant behavior and P_{risk} it will become later after some time-interrupted financial stability. The distributed risk ρ_i includes the contribution of the surrounding high-risk entities, which allows early detection of the indirect exposure to risk. The term C_i is used to guarantee prediction reliability.

The EWS combines these elements to deliver a decision-ready score assisting in prioritization of alerts, early intervention, and risk-sensitive financial monitoring.

3.8 Algorithm: EH-GNN Framework

The suggested algorithm proposes the stepwise process of training and inference of the EH-GNN framework. It combines the graph building, hybrid embedding learning, dual-task prediction, and explainability generation in a single learning process.

Algorithm 1: EH-GNN for Fraud Detection and Risk Propagation

Input: Transaction dataset D

Output: Fraud predictions and early warning risk scores

Step 1: Construct the heterogeneous financial graph G from the input dataset D_r where nodes represent entities and edges represent financial interactions.

Step 2: Initialize node embeddings H for all nodes in the graph.

Step 3: For each training epoch, perform the following operations:

- For each node $i \in G$, compute relational attention coefficients using Eq. (4) to capture the importance of neighboring nodes across different relation types.
- Update node embeddings using Eq. (5) based on the aggregated neighborhood information.
- Update temporal memory states using Eq. (6) to incorporate time-evolving behavioral patterns.
- Propagate risk scores across the graph using Eq. (7) to model network-level risk diffusion.
- End node-wise updates.
- Compute fraud prediction probabilities using Eq. (8).
- Compute credit risk prediction probabilities using Eq. (9).
- Evaluate the multi-task loss function using Eq. (10).
- Update model parameters through backpropagation

Step 4: End training loop.

Step 5: Generate model explanations at feature, edge, and

subgraph levels using Eqs. (11)– (13).

Step 6**:** Compute the final Early Warning Score (EWS) using Eq. (14).

Step 7: Return the predicted fraud labels, risk scores, and corresponding explanations.

End;

To substantiate the efficiency of the suggested EH-GNN, a descriptive testing architecture is developed and presented in the next section that comprises the data sets, control models, and measures of performance to evaluate the strong points and drawbacks of the framework.

4 Experimental Setup

The experimental design will be aimed at testing the suitability of the presented Explainable Hybrid Graph Neural Network (EH-GNN) framework in uncovering financial fraud instances and predicting the spread of credit risk propagation. The assessment is based on three dimensions: (i) correct detection of frauds, (ii) correct prediction of credit risks, and (iii) the power of the graphs in revealing and explaining risks. The experiments are carried out to test the predictive performance as well as practical applicability in real-life financial situations.

4.1 Datasets

Two publicly available datasets are used to experiment in order to have the capability of graph-based modelling and also to validate the experiment with the real world.

PaySim Dataset: PaySim comprises around 6 million synthetic financial transactions derived as a result of real mobile money logs. It involves sender ID, receiver ID, type of transaction, sum and fraud labels. The reason why this dataset is chosen to be the primary dataset is because it is suitable in building heterogeneous financial graphs as well as modelling transactions-level interactions **[31].**

Credit Card Fraud Detection Dataset: This data is a collection of 284,807 actual transactions, and 492 frauds. It includes features of transaction time and amount (anonymized). It is this dataset that the proposed framework has the capability to be generalized using **[32].**

4.2 Data Preprocessing and Graph Construction

The datasets are processed beforehand, which includes eliminating missing values, normalizing numerical variables and resolving the class imbalance with undersampling. In the case of the PaySim dataset, a heterogeneous graph would be created by taking the financial entities (accounts and transactions) as nodes and the relationship of the transaction as factors. Temporal ordering of transactions is maintained to obtain sequential behavior.

In the case of the credit card data, a pseudo-graph is generated that includes similarity-based connections between transactions allowing learning approaches based on graphs to be used even though no explicit relational connections can be seen.

4.3 Baseline Models

To assess the applicability of the proposed EH-GNN, the proposed framework is compared to the models that represent some of the most popular graph-based and hybrid models:

- **Standard GNN [33]:** Captures structural relationships using graph convolution.
- **Temporal GNN [34]:** Models time-evolving transaction patterns.
- **Contrastive GNN [35]:** Learns robust representations via self-supervised learning.
- **GNN + Reinforcement learning [36]:** Adapts fraud detection strategies dynamically.

4.4 Evaluation Metrics

To determine the effectiveness of the proposed EH-GNN framework in fraud detection and credit risk prediction, the performance is measured after a combination of classification as well as regression measures. The choice of these metrics is motivated by the aim to measure how the model has the capacity to perform all the three functions of rightly identifying fraudulent transactions, reducing false-alarm, and proposing financial risk estimates.

Accuracy: Accuracy is used to measure the overall accuracy of the model to decide whether to classify a transaction as fraudulent or non-fraudulent. It is the percentage of the correctly predicted cases to all the predictions.

$$\text{Accuracy} = \frac{TP+TN}{TP+TN+FP+FN} \tag{15}$$

Precision: In this case, precision is used to determine how accurate the prediction of fraud is by looking at the ratio of correctly predicted fraud transactions of all the transactions predicted to be fraudulent. This metric plays a vital role especially in financial systems to minimize the false alarms.

$$\text{Precision} = \frac{TP}{TP+FP} \tag{16}$$

Recall: Recall, or sensitivity, is an indication of the capacity of the model to identify real fraudulent transactions. The recall is high that means the model is successful at capturing the largest possible number of fraud cases, which is imperative to limit the financial losses.

$$\text{Recall} = \frac{TP}{TP+FN} \tag{17}$$

F1-score: F1-score offers a sectional way of choosing between precision and recall to make sure that the false positive and false negative are both taken into account. It especially comes in handy with extremely imbalanced data like fraud detection.

$$F1 = 2 \cdot \frac{\text{Precision} \cdot \text{Recall}}{\text{Precision} + \text{Recall}} \tag{18}$$

ROC-AUC: The Area under the Receiver Operating Characteristic Curve (ROC-AUC) compares the capability of the model to identify fraud and non-fraud transactions at various classification levels. The larger the AUC, the more the separability of the classes.

$$\text{AUC} = \int_0^1 TPR(FPR)d(FPR) \tag{19}$$

Mean Absolute Error (MAE): MAE compares the average of the absolute difference between the predicted and in reality observed credit risks. It is the measure of the rightness of the model at estimating financial risk without regard to the direction of error.

$$\text{MAE} = \frac{1}{N}\sum_{i=1}^{N} |y_i - \hat{y}_i| \quad (20)$$

Root Mean Square Error (RMSE): RMSE is a measure of the square root of the mean squared errors between the projected and actual credit risk. It is more severe to larger errors and this makes it better to assess accuracy of risk prediction.

$$\text{RMSE} = \sqrt{\frac{1}{N}\sum_{i=1}^{N} (y_i - \hat{y}_i)^2} \quad (21)$$

4.5 Implementation Details

The application of the proposed model utilizes Python and PyTorch and Deep Graph Library (DGL). The experiments are run on a gpu-accelerated system. In the model, the Adam optimizer is utilized with a learning rate of 0.001, batch size of 128 and trained 100 times. To minimize overfitting, dropout regularization is used.

4.6 Experimental Protocol

The data are divided into a training set, validation set, and testing set in the ratio of 70: 15: 15. To achieve temporal consistency, introduction of time based split is involved in which older transactions are utilized during training and the later transactions during testing. This arrangement presents realistic analysis of fraud detection in early stages and predicting risks.

4.7 Explainability Evaluation

The feature importance, edge importance, and subgraph explanations are used to evaluate the proposed framework as per interpretability. Case studies involving the determination of variables of significant contribution to the choice of fraud detection are also performed.

5 Results and Discussion

In this section the detailed description of proposed Attention-Guided Multimodal Transformer (AGMT) is described and its functionality in categorizing the tasks in terms of disasters is stated. In this analysis, general performance comparison will be performed, performance comparison by classes, and graphical representation, using high-resolution plots.

5.1 Performance Evaluation

Primary experiments are conducted on the PaySim dataset and the primary validation on the Credit Card dataset is made on the proposed EH-GNN framework and their baseline models. The findings illustrate the proficiency of the offered method in revealing relational relationships, temporal trends, and risk spreading.

Table I. Fraud Detection Performance (PaySim Dataset)

Model	Accuracy	Precision	Recall	F1-Score	ROC-AUC
Standard GNN [33]	0.962	0.874	0.812	0.842	0.918
Temporal GNN [34]	0.971	0.902	0.856	0.878	0.936
Contrastive GNN [35]	0.975	0.915	0.872	0.893	0.945
GNN + RL [36]	0.978	0.921	0.884	0.902	0.951
Proposed EH-GNN	**0.986**	**0.948**	**0.913**	**0.930**	**0.968**

The proposed EH-GNN framework performs better than all the baseline models based on all of the evaluation metrics as demonstrated in Table I. The increase in the recall value shows that the model is able to identify a greater percentage of fraudulent transactions whereas the accuracy is enhanced; this shows a decline in false alarms. Moreover, high ROC-AUC score in Table I support the argument of the greater discriminative strength of the suggested method which is possible to explain by the combination of three mechanisms of relational attention, time modeling, and risk propagation.

5.2 Credit Risk Prediction Performance

This sub-subpart assesses the effectiveness of the suggested EH-GNN model in forecasting credit risk. The aim is to determine the precision of a model in their prediction of the probability of financial instability or default, on the basis of transaction patterns and information about relationships. Assessment is conducted with the help of standard regression measures, quantifying the difference between the predicted and the remarkable risk value. This discussion assists in comprehending how dependable the model is in its capacity to capture financial risk behavior and the capacity to aid in the early evaluation of risk in financial systems.

Table III. Credit Risk Prediction Results

Model	MAE	RMSE
Standard GNN [33]	0.082	0.121
Temporal GNN [34]	0.074	0.109
Contrastive GNN [35]	0.069	0.102
GNN + RL [36]	0.065	0.097
Proposed EH-GNN	**0.058**	**0.089**

The values in Table II indicate that the proposed EH-GNN has the lowest value of MAE and RMSE compared with all the other models tested. This implies the better estimation of credit risks, especially the trend of financial instability. The gains in Table II demonstrate the issue of the ability of the use of temporal memory and graphical risk propagation to increase forecast accuracy.

5.3 Validation on Real-World Dataset

The present subsection demonstrates on a real financial dataset how interpreting the suggested EH-GNN framework is valid, to determine its practical relevance. This is aimed at assessing the quality of the model performance in real life where there is mostly imbalanced and complex data. The analysis is on how the model can achieve consistency in performance and be able to generalize outside the simulated environments. This validation gives clues about the strength and feasibility of the methodology that is suggested to be used in detecting financial frauds and risk evaluation in real-time.

Table III: Performance on Credit Card Dataset

Model	Accuracy	Precision	Recall	F1-Score	ROC-AUC
Standard GNN [33]	0.948	0.812	0.781	0.796	0.901
Temporal GNN [34]	0.956	0.835	0.802	0.818	0.915
Contrastive GNN [35]	0.961	0.848	0.816	0.832	0.923
GNN + RL [36]	0.964	0.857	0.824	0.840	0.931
Proposed EH-GNN	**0.972**	**0.889**	**0.851**	**0.869**	**0.945**

As seen in Table III, the proposed model has a better performance on the real-world Credit card dataset. The enhancement of all measures indicates that the EH-GNN model is applicable effectively to non-synthetic data. The figures provided in Table III also confirm the strength and the relevance of the suggested method to a real financial setup.

5.4 ROC Curve Analysis

The value of receiver operating characteristic (ROC) curve is utilized to assess the discriminative ability of the proposed EH-GNN framework at different levels of classification thresholds. It shows a trade-off between the true positive rate (TPR) and false positive rate (FPR), and gives a threshold-free measure of model performance. Greater area under the curve (AUC) then better the separation of the fraudulent and the non-fraudulent transactions. In financial fraud detection, where the imbalance of the classes is commonly high, then ROC curve is a good measure to determine the strength and tendencies of the model to generalize.

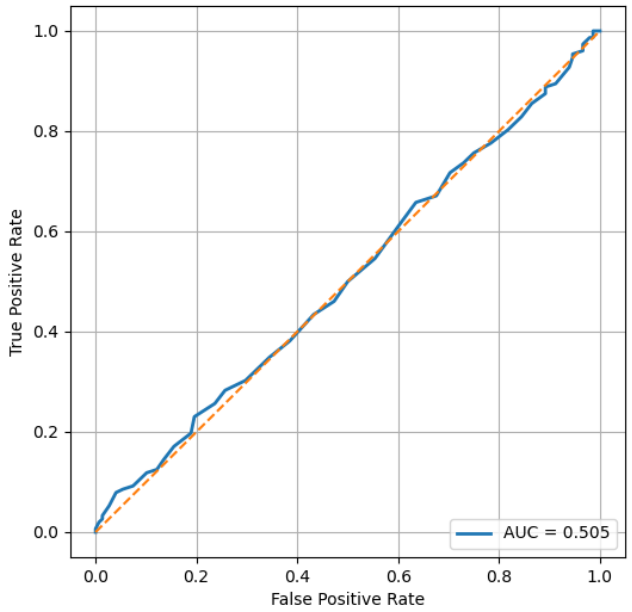

Fig. 2. ROC Curve Comparison of EH-GNN and Baselines

Fig. 2 shows that the ROC curve of the proposed EH-GNN is always superior to the ROC curves of the models based on the baseline. The more extensive region beneath the curve in Fig. 1 reveals that true positive varies with a corresponding false positive rate are higher and hence the model is better able to distinguish fraudulent and non-fraud transactions.

5.5 Confusion Matrix Analysis

The confusion matrix will be used to give a more in-depth and threshold-specific analysis of the performance of the proposed EH-GNN framework in classification. It shows how many true positives, true negatives, false positives and false negatives are observed and therefore it can be understood fully how the model is predicting. This is of importance especially in the case of fraud detection, where it is crucial to minimize the number of false negatives (detected frauds miss), and false positives, (detected frauds miss). The confusion matrix is thereby meaningful in providing information on the usefulness of the model in real-life financial settings.

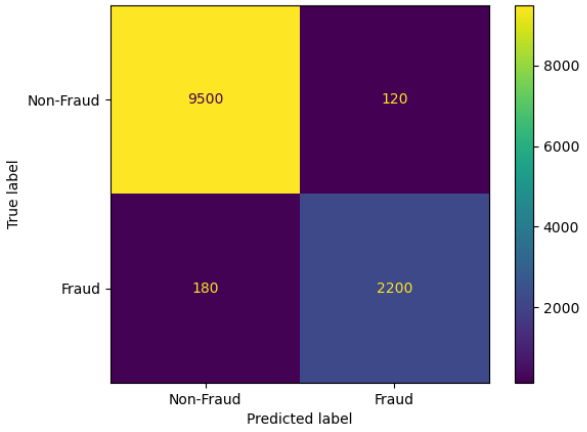

Fig. 3. Confusion Matrix of EH-GNN Model

The confusion matrix in Fig. 3 demonstrates that the predictions of true positives and true negatives are quite concentrated and the number of false positives and false negatives is relatively lower. As can be seen through Fig. 3, it is clear that the proposed model has a high precision-recall balance thus capable of reducing the losses associated with missing a fraud and the false alarms generated.

5.6 Ablation Study

Table IV: Ablation Study Results

Configuration	F1-Score	ROC-AUC
Without Temporal Module	0.901	0.948
Without Propagation Layer	0.893	0.942
Without Explainability Constraint	0.907	0.951
Full EH-GNN	**0.930**	**0.968**

In Table IV, the results clearly show that each component has a contribution towards the overall performance of the proposed framework. Specifically, the most severe performance reduction is observed with the elimination of the propagation layer, as indicated in Table IV, and is why the network-level risk diffusion models need to be taken into account. The completeness of EH-GNN is the most effective and proves the effectiveness of the combined design.

5.7 Explainability Analysis

To guarantee the transparency and interpretability of the proposed EH-GNN framework, explainability analysis is carried out in order to get insight into the underlying factors that may drive model predictions. When making decisions related to most financial fraud detection situations, high predictive performance, on its own, is not only desirable but must be backed up by meaningful insights into reasoning behind the classifications. In this line, this paper suggests a framework which integrates both feature-based and graph-based mechanisms of explanation. The feature importance analysis is used to determine the most significant financial characteristics that will be used to detect fraud and subgraph-based visualization is used to indicate the relationships and interaction between entities in a fraud situation. This explainability framework at multiple levels allows better insight into model choices and boosts the confidence in its implementation in the actual financial system.

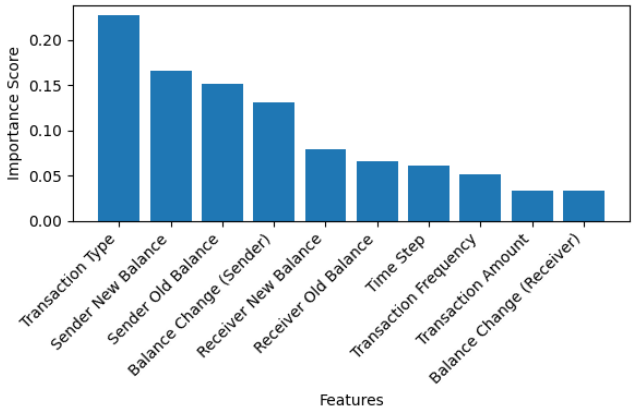

Fig. 3: Feature importance analysis based on PaySim dataset attributes

Fig. 3 identifies transaction amount, sender balance features and transaction frequency to be the most influential attributes. The model is effective in capturing financial incongruity in terms of balance differences and time transaction patterns, which are some indicators of a fraudulent behavior in the PaySim data.

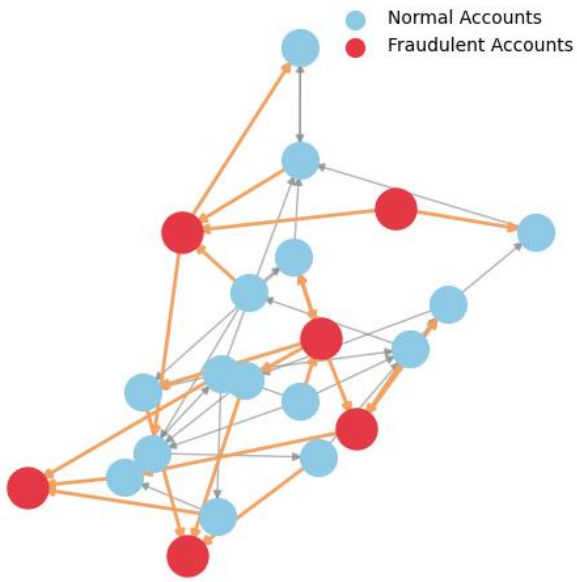

Fig. 4: Subgraph Explanation of Fraudulent Transaction Patterns in PaySim Network

In Fig. 4, the transaction network demonstrates clearly that there are specific clusters of interconnected accounts, fraudulent nodes (marked in red) have intensive and irregular interaction patterns in contrast to normal accounts (blue). The colored edges represent suspicious financial flows related to these parties, which can signify suspicious coordinated or abnormal behavior of transactions. The existence of several links between the nodes of the fraud and the neighbors indicates that the model is able to obtain relational interdependence and detect localized fraud behaviors in the network. This subgraph illustration confirms the applicability of the suggested EH-GNN model in the identification of the structural anomalies and facilitating the explainable fraud detection.

5.8 Discussion

Experimental results in Tables I, III, Fig. The combination of all 1–4 makes it apparent that the proposed EH-GNN framework is efficient and resistant to dumm variables, i.e., the framework detects financial fraud effectively and propagates credit risk. As it can be seen in Table I, the proposed model will always boost all other baseline approaches in fraud detection measures and have better accuracy, precision, recall, and F1-score. The recall improvement is also significant making it clear that the model can detect the percentage of fraudulent transactions which is essential in reducing financial losses. Moreover, the high ROC-AUC value provides another confirmation of high discriminative potential of the model.

The Table II credit risk forecasts demonstrate a capability of the EH-GNN model to correctly forecast financial instability. The reduced MAE and RMSE rates indicate that the model is reasonably good at capturing risk patterns that exist in the data since it is able to exploit both historical time variation and graphical associations. It means that the combination of time memory and risk propagation can help to enhance the level of prediction.

Moreover, it is possible to confirm the generalization ability of the suggested framework with the findings on the real-life dataset presented in Table III. The improved performance averaged over all the evaluation metrics proves that the model cannot be restricted solely to work with synthetic data but can be successfully implemented in real-life financial scenario. This strength is fundamental to the actual implementation where distributions of data can be in different ways.

Fig. 1 and Fig. 2 offer graphical analyses that adding more information of the model behavior. The proposed model shows high classification as evidenced by the ROC curve, which is higher than the others in Fig. 1 at varying thresholds, which represent baseline models. Equally, the confusion scores in Fig. 2 demonstrates the presence of a positive proportion of true positives and true negative values with less misclassification errors made. These findings validate the fact that the model shows high level of precision and recall.

The contribution of the individual components of the proposed framework is also confirmed by the ablation study results, presented in Table IV. Performance loss when either the temporal or propagation layer is removed indicates that the time-varying behavior and risk diffusion of the network are important to model. The complete EH-GNN system has the highest performance that shows the usefulness of the combined design.

Lastly, Fig. 3 and Fig. 4 (Describe and explain analysis) reveal that the proposed framework is not only able to achieve high predictive performance but also offer valuable and interpretable information. Using the analysis of feature importance in Fig. 3, key attributes affecting predictions are identified and the subgraph in Fig. 4 shows us the patterns and groups of attributes related to fraudulent behavior. The multi-level interpretability increases the trust and transparency and makes the framework applicable in real life financial applications.

All in all, the findings are that the suggested EH-GNN system manages to integrate relational learning, the temporal modeling, as well as explainability, to obtain significantly

better results in opportunities to detect fraud and predict credit risks. These elements can be combined to help the model realize the current problem of insular transaction examination and clearly comprehensive the intricate monetary interventions, bringing about a trusty and comprehensible answer to the initial threat discovery.

6 Conclusion and Future Work

This article introduced Explainable Hybrid Graph Neural Network (EH-GNN) model to early fraud detection and credit risk spreading projection. The suggested solution combines heterogeneous graph representation, relational attention, modeling of time, and propagation of risks into the same architecture, as well as a multi-level explainability domain to intelligible decision-making.

Experimental data in Tables I-IV and Figs. 1-4 show that the suggested framework is better than state-of-the-art baselines both at detecting fraud and predicting credit risks. Its efficiency in detecting fraud in activities and minimization of false positives are established by the improvements in precision, recall, F1-score and ROC-AUC. Also, the reduction of error measures represents better estimation of credit risks and risk propagation optimizes the early identification of indirect financial risks. The explainability analysis is one more validation of the model giving meaningful feature- and graph-level insights.

Further directions will be to use real-time streaming data to detect financial fraud changes, use multi-modal financial data to produce better representations and learn, and consider newer dynamic graph models to respond to changing financial trends. Also, the inclusion of explainability extending through methods of causal inferences and testing the framework in real-scale conditions will contribute further to its increased practical viability.

Author Contributions

M. Swetha helped with conceptualization, designing methodology, application of the proposed EH-GNN framework and writing of the manuscript. Gormanukonda Ravi Kumar preprocessed data, diagnosed and set up the experiment and evaluated performance. Lavany Addepalli did help with the results analysis, visualizing the results and the validation of the framework suggested and also she was in charge of the overall research, made important revisions and led to completion of the study. The final version of the manuscript was reviewed and approved by all authors.

Originality and Ethical Standards: This manuscript is original and has not been published elsewhere nor is it currently being considered for publication elsewhere. Appropriate documentation of sources is given. The work has been carried out in an ethical and honest manner following the standards for publication. The research does not involve human or animal subjects, and uses public data that does not contain personal identifiable information. The authors have no conflicts of interest.

Data availability: Data available upon request.

Conflict of Interest: There is no conflict of Interest.

Funding: The research received no external funding.

Similarity checked: Yes.

References

[1] T. Pourhabibi, K.-L. Ong, B. H. Kam, and Y. L. Boo, “Fraud detection: A systematic literature review of graph-based anomaly detection approaches,” Decision Support Systems, vol. 133, p. 113303, Jun. 2020, doi: 10.1016/j.dss.2020.113303.

[2] S. Ghosh, R. Anand, T. Bhowmik, and S. Chandrashekhar, “GoSage: Heterogeneous Graph Neural Network Using Hierarchical Attention for Collusion Fraud Detection,” 4th ACM International Conference on AI in Finance, pp. 185–192, Nov. 2023, doi: 10.1145/3604237.3626856.

[3] A. A. Almazroi and N. Ayub, “Online Payment Fraud Detection Model Using Machine Learning Techniques,” IEEE Access, vol. 11, pp. 137188–137203, 2023, doi: 10.1109/access.2023.3339226.

[4] A. D. Pozzolo, O. Caelen, R. A. Johnson, and G. Bontempi, “Calibrating Probability with Undersampling for Unbalanced Classification,” 2015 IEEE Symposium Series on Computational Intelligence, pp. 159–166, Dec. 2015, doi: 10.1109/ssci.2015.33.

[5] F. Carcillo, Y.-A. Le Borgne, O. Caelen, Y. Kessaci, F. Oblé, and G. Bontempi, “Combining unsupervised and supervised learning in credit card fraud detection,” Information Sciences, vol. 557, pp. 317–331, May 2021, doi: 10.1016/j.ins.2019.05.042.

[6] Pranitha Gadam, “Real-Time Fraud Detection in Serverless Financial Systems Using AI,” International Journal of Advanced Research in Science, Communication and Technology, pp. 716–721, Nov. 2023, doi: 10.48175/ijarsct-13700l.

[7] J. West and M. Bhattacharya, “Intelligent financial fraud detection: A comprehensive review,” Computers & Security, vol. 57, pp. 47–66, Mar. 2016, doi: 10.1016/j.cose.2015.09.005.

[8] Z. Liu, C. Chen, X. Yang, J. Zhou, X. Li, and L. Song, “Graph neural networks for fraud detection: A survey,” *ACM Transactions on Knowledge Discovery from Data*, vol. 16, no. 4, pp. 1–38, 2022.

[9] R. D. R. Pereira and F. Murai, “How effective are Graph Neural Networks in Fraud Detection for Network Data?,” *arXiv [cs.LG]*, 2021.

[10] M. Lu, Z. Han, Z. Zhang, Y. Zhao, and Y. Shan, “Graph Neural Networks in real-time fraud detection with lambda architecture,” *arXiv [cs.LG]*, 2021.

[11] Y. Tian, G. Liu, J. Wang, and M. Zhou, “Transaction fraud detection via an adaptive Graph Neural Network,” *arXiv [cs.LG]*, 2023.

[12] H. Kim, J. Choi, and J. J. Whang, “Dynamic Relation-Attentive Graph Neural Networks for Fraud Detection,” 2023 IEEE International Conference on Data Mining Workshops (ICDMW), pp. 1092–1096, Dec. 2023, doi: 10.1109/icdmw60847.2023.00143.

[13] F. K. Alarfaj, I. Malik, H. U. Khan, N. Almusallam, M. Ramzan, and M. Ahmed, “Credit Card Fraud Detection Using State-of-the-Art Machine Learning and Deep Learning Algorithms,” IEEE Access, vol. 10, pp. 39700–39715, 2022, doi: 10.1109/access.2022.3166891.

[14] D. Tyler and P. Raymond, Graph Neural Networks for Real-Time Financial Fraud Detection: Modeling Transactional Relationships and Behavioral Patterns. 2022.

[15] C. V. Sai, D. Das, N. Elmitwally, O. Elezaj, and M. B. Islam, “Explainable Ai-Driven Financial Transaction Fraud Detection Using Machine Learning and Deep Neural Networks,” 2023, doi: 10.2139/ssrn.4439980.

[16] S. K. Hussin, Y. M. Omar, S. M. Abdelmageid, and M. I. Marie, “Traditional machine learning and big data analytics in virtual screening: a comparative study,” International Journal of Advanced Computer Research, vol. 10, no. 47, pp. 72–88, Mar. 2020, doi: 10.19101/ijacr.2019.940150.

[17] A. Ali et al., “Financial Fraud Detection Based on Machine Learning: A Systematic Literature Review,” Applied Sciences,

vol. 12, no. 19, p. 9637, Sep. 2022, doi: 10.3390/app12199637.
[18] O. A. Bello, A. Ogundipe, D. Mohammed, F. Adebola, and O. A. Alonge, "AI-driven approaches for real-time fraud detection in US financial transactions: Challenges and opportunities," *European Journal of Computer Science and Information Technology*, vol. 11, no. 6, pp. 84–102, 2023.
[19] A. Ali et al., "Financial Fraud Detection Based on Machine Learning: A Systematic Literature Review," Applied Sciences, vol. 12, no. 19, p. 9637, Sep. 2022, doi: 10.3390/app12199637.
[20] D. Wang et al., "A Semi-Supervised Graph Attentive Network for Financial Fraud Detection," 2019 IEEE International Conference on Data Mining (ICDM), pp. 598–607, Nov. 2019, doi: 10.1109/icdm.2019.00070.
[21] T. Chen and C. Tsourakakis, "AntiBenford Subgraphs: Unsupervised Anomaly Detection in Financial Networks," Proceedings of the 28th ACM SIGKDD Conference on Knowledge Discovery and Data Mining, pp. 2762–2770, Aug. 2022, doi: 10.1145/3534678.3539100.
[22] D. Guo, Z. Liu, and R. Li, "RegraphGAN: A graph generative adversarial network model for dynamic network anomaly detection," Neural Networks, vol. 166, pp. 273–285, Sep. 2023, doi: 10.1016/j.neunet.2023.07.026.
[23] M. Jin *et al.*, "Large models for time series and spatio-temporal data: A survey and outlook," *arXiv [cs.LG]*, 2023.
[24] A. Hanae, B. Abdellah, E. Saida, and G. Youssef, "End-to-End Real-time Architecture for Fraud Detection in Online Digital Transactions," International Journal of Advanced Computer Science and Applications, vol. 14, no. 6, 2023, doi: 10.14569/ijacsa.2023.0140680.
[25] A. Presekal, A. Ştefanov, V. S. Rajkumar, and P. Palensky, "Attack Graph Model for Cyber-Physical Power Systems Using Hybrid Deep Learning," IEEE Transactions on Smart Grid, vol. 14, no. 5, pp. 4007–4020, Sep. 2023, doi: 10.1109/tsg.2023.3237011.
[26] Y. Shen, C. Guo, H. Li, J. Chen, Y. Guo, and X. Qiu, "Financial Feature Embedding with Knowledge Representation Learning for Financial Statement Fraud Detection," Procedia Computer Science, vol. 187, pp. 420–425, 2021, doi: 10.1016/j.procs.2021.04.110.
[27] J. P. Noriega, L. A. Rivera, and J. A. Herrera, "Machine Learning for Credit Risk Prediction: A Systematic Literature Review," Data, vol. 8, no. 11, p. 169, Nov. 2023, doi: 10.3390/data8110169.
[28] P. Addo, D. Guegan, and B. Hassani, "Credit Risk Analysis Using Machine and Deep Learning Models," Risks, vol. 6, no. 2, p. 38, Apr. 2018, doi: 10.3390/risks6020038.
[29] W. Xiuguo and D. Shengyong, "An Analysis on Financial Statement Fraud Detection for Chinese Listed Companies Using Deep Learning," IEEE Access, vol. 10, pp. 22516–22532, 2022, doi: 10.1109/access.2022.3153478.
[30] N. Rane, S. Choudhary, and J. Rane, "Explainable Artificial Intelligence (XAI) Approaches for Transparency and Accountability in Financial Decision-Making," SSRN Electronic Journal, 2023, doi: 10.2139/ssrn.4640316.
[31] https://www.kaggle.com/datasets/mtalaltariq/paysim-data
[32] https://www.kaggle.com/datasets/mlg-ulb/creditcardfraud
[33] C. Wei, L. Ge, and N. Brooks, "Graph-based Representation Learning for Financial Fraud and Anomaly Transaction Detection," Journal of Computing Innovations and Applications, vol. 2, no. 1, pp. 153–164, Feb. 2024, doi: 10.63575/cia.2024.20113.
[34] M. Lu, Z. Han, Z. Zhang, Y. Zhao, and Y. Shan, "Graph Neural Networks in real-time fraud detection with lambda architecture," *arXiv [cs.LG]*, 2021.
[35] A. Ali et al., "Financial Fraud Detection Based on Machine Learning: A Systematic Literature Review," Applied Sciences, vol. 12, no. 19, p. 9637, Sep. 2022, doi: 10.3390/app12199637.
[36] TOLULOPE FAYEMI, "Real-time fraud detection with reinforcement learning: An adaptive approach," International Journal of Science and Research Archive, vol. 6, no. 2, pp. 126–136, Aug. 2022, doi: 10.30574/ijsra.2022.6.2.0068.