
Team Name : Neural Ninjas

Problem Statement : Bank Account Analysis

# Idea

Graph Neural Network (GNNs) can be used to detect money laundering by learning patterns in financial transaction data that are indicative of money laundering activity. Represented by each financial transaction as a node in a graph, with edges between nodes representing relationships between transactions. The GNN is trained on a labeled dataset of transactions, where some are labeled as being part of a money laundering scheme and others are not. During training, the GNN learns to classify transactions as being part of a money laundering scheme or not based on the patterns like degree of node, amount of transaction and type of transaction and various other features.

## We will be using following GNNs tasks for our solution :

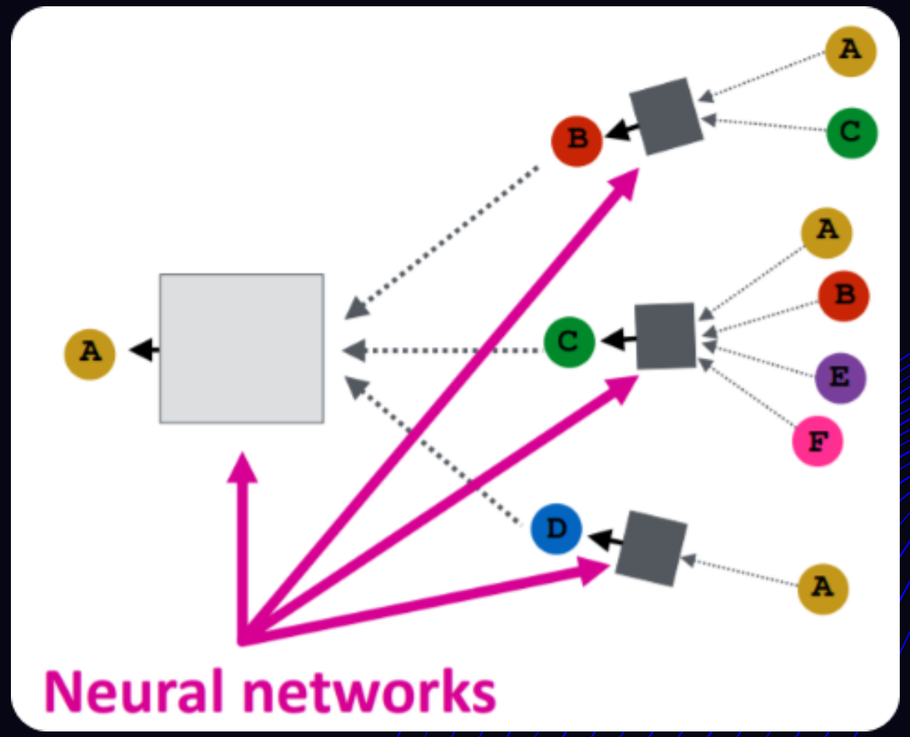
- **Node Classification :** this task uses neighboring node labels and previous node features to predict missing node labels in a graph.
- **Link Prediction :** predicts the link between a pair of nodes in a graph with an incomplete adjacency matrix. It is commonly used for social networks.
- **Community Detection :** divides nodes into various clusters based on edge structure. It learns from edge weights, and distance and graph objects similarly.
- **Graph Generation :** learns from sample graph distribution based on previous data to generate a new but similar graph structure.

# Opportunity

## How different is it from any other existing solutions & How will it be able to solve problems?

GNNs are able to learn patterns in financial transaction data represented as a graph. GNNs are particularly well-suited for this task because they are able to effectively incorporate information from the graph structure and the features of individual transactions. Other approaches, such as traditional machine learning algorithms, may not be as effective at identifying patterns that depend on the relationships between transactions. Once trained, the GNN can then be used to classify new, unseen transactions as being part of a money laundering scheme or not. This can be done by inputting the transaction data into the GNN.

The current solutions can just flag the fraudulent transaction but we can not only just flag fraudulent transaction but also we can predict fraudulent transaction, detect such communities which are doing such activities and we can find indirect link of these transactions and find real culprits and flag all the dummy accounts in between.



# GNN Architecture

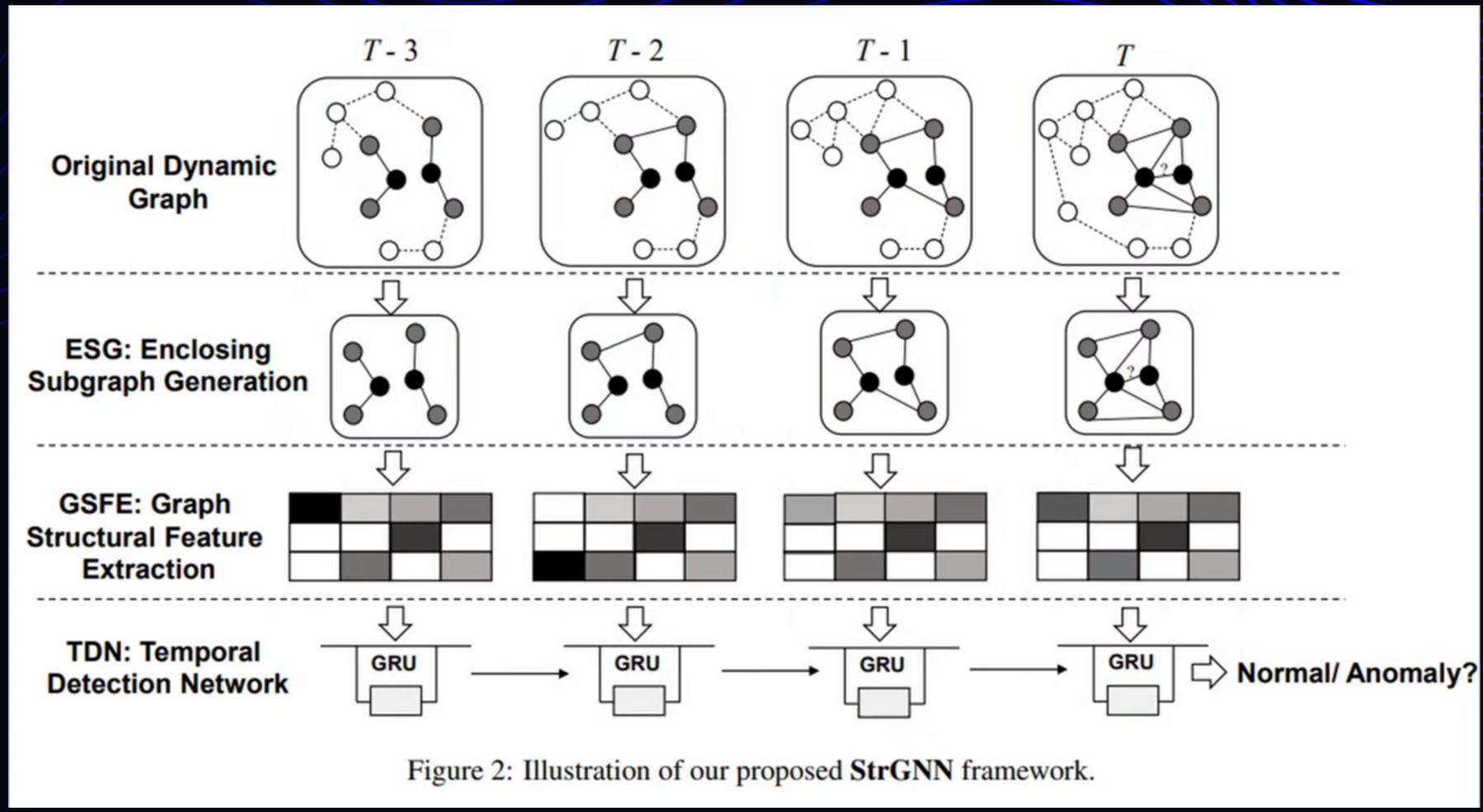


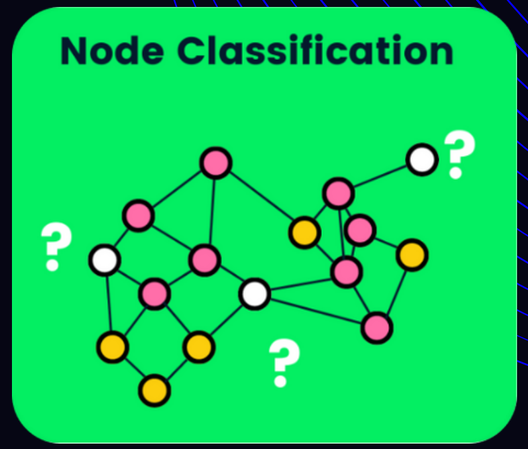

Figure 2: Illustration of our proposed **StrGNN** framework.

@ Taken from StrGNN

# Features Offered

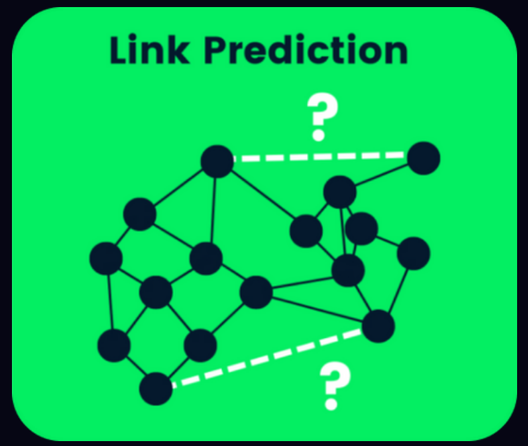
## 1 . FRAUDULENT ACCOUNT DETECTION.

This feature will detect the fraudulent account and it will be able to do it as we train our GNNs on transaction data so, it can learns the features and patterns of fraudulent account hence it can easily categorize accounts into 3 categories i.e. Fraudulent Accounts, Accounts Under Observation, Safe Accounts. This feature will mark such accounts Accordingly so that it can be identified easily and this will help police personnel in finding such account and taking action very easy and quick.




## 2 . INDIRECT LINK PREDICTION.

This feature will detect the indirect link between different account as in money laundering process money travels different accounts which makes hard to keep track of it. so this feature will keep track of such indirect transaction happening and can showcase the indirect link between accounts and flagging all the dummy accounts in between the main accounts which are just created for carrying out these fraudulent transactions. hence we can solve these problems from its root.

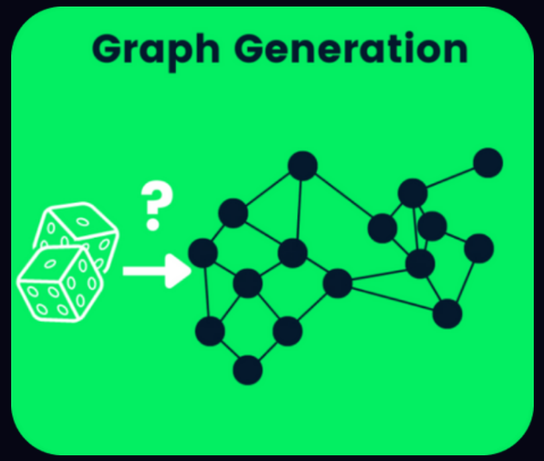


## 3 . COMMUNITY DETECTION.

This Feature can spot different community in transactions and help police to understand which types of account are doing such fraudulent activity and also banks can use this feature to see which types of customer they are serving and what future plans and scheme they need to make so that it can benefit their customer as well as them and also financial organization can make policies and laws which can prevent such activities.


## 4 . FUTURE PATTERN PRIDICTION

This Feature can predicts the subgroup fraudulent transactions, It will also use GNNs to do so our model can learn the patterns followed by previous fraudulent transaction and if similar patterns were found we can predict the behavior and path (accounts) followed by the money so if similar patterns were detected hence we can use this feature to find out what could be future fraudulent transactions. and we can inform the police, concerned banks and agencies before hand.

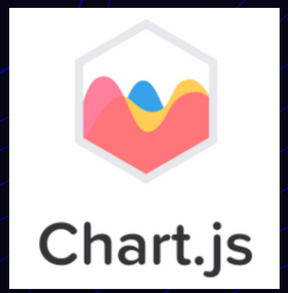


# Business Logic

- We can directly sell our software service  to other state police department and national agency.
- We can use the product to build similar products which can be used in other sectors.
- We can provide our software service to private banks, public banks, fintech company and financial institution as well.

# Technology Stack

## FrontEnd Tools


## BackEnd Dev Tools




## Model Building Tools




# Estimated Cost of the Solution

## SOFTWARE COST

- Tech employee.
- Services such as AWS, VPN, Database Management etc.
- Domain and hosting cost.

## MAINTENANCE COST

- Algo optimization as per requirements.
- Incorporating new features.

## HARDWARE COST

- Computers with good computational power.
- Cloud computing and online servers.
- Fast internet speed.

# Thank You!

We would love to join you guys offline during final rounds