Inference with Trained Model: Use the trained GCN model to perform inference on the new transaction data represented in the heterogeneous graph.

Anomaly Detection: After inference, the model will assign anomaly scores to each transaction node in the graph. These scores represent the likelihood of each transaction being fraudulent.

Threshold Setting: Set a threshold on the anomaly scores to classify transactions as normal or fraudulent. Transactions with anomaly scores above the threshold are considered potential fraudulent transactions.

Flagging Fraudulent Transactions: Identify and flag transactions with anomaly scores above the threshold as potentially fraudulent.

Validation and Refinement: Validate the performance of the model in detecting fraudulent transactions using appropriate evaluation metrics. Refine the threshold and the model if necessary to improve accuracy and reduce false positives/negatives.

Deployment and Monitoring: Deploy the model into your system for real-time monitoring of transactions. Continuously monitor the performance of the model and update it as needed to adapt to changing patterns of fraudulent activities.

By following these steps, you can effectively leverage the trained GCN model to detect fraudulent transactions in your dataset. Remember to fine-tune the model parameters and threshold based on the specific characteristics of your data and the desired level of sensitivity to fraud detection.

Inference with Trained Model: Use the trained GCN model to perform inference on the new transaction data represented in the heterogeneous graph. how do i do this

To perform inference with the trained GCN model on new transaction data represented in a heterogeneous graph, you need to follow these steps:

Prepare the New Transaction Data: Convert the new transaction data into a format that can be used by the GCN model. This typically involves creating a PyTorch Geometric Data object with node features and edge information.

Load the Trained Model: Load the trained GCN model that you previously trained on the heterogeneous graph.

Perform Inference: Pass the new transaction data through the trained GCN model to obtain predictions or anomaly scores for each transaction node in the graph.

Analyze Results: Analyze the output of the inference to identify potentially fraudulent transactions based on the anomaly scores or predictions generated by the model.

Here's a more detailed explanation of each step: