Deep Learning on Graphs (CSE-AIML) UE22AM342BA2

Course Project One Pager

Team Details

Name	Section	SRN
J Vignesh	B	PES1UG22AM074
Bharateesha Lvn	B	PES1UG22AM088
Jabez Lawrence G	B	PES1UG23AM802

Project Title : HGNN-Based Network Intrusion Detection System (HGNN-NIDS)

Possible Dataset and source : UNSW-NB15 Dataset

Link: https://www.unsw.adfa.edu.au/unsw-canberra-cyber/cybersecurity/ADFA-NB15-Datasets/

Uniqueness of the topic :

Novel Application of Heterogeneous Graph Neural Networks:
This project uniquely applies HGNNs to model network entities (IPs, ports, protocols) as diverse node types with their interconnections (network flows) as edges, thereby capturing complex multi-modal relationships for enhanced intrusion detection.

Edge Classification Approach:
Instead of classifying nodes, the model focuses on edge classification, which directly targets the suspicious connections between hosts. This focus improves detection precision since attacks often manifest through specific network flows rather than overall node behaviour.

Innovative Host Information Integration:
By inferring host-level details from IP-related features and grouping co-occurring flows, the approach overcomes the limitations of traditional datasets and adds novelty to the analysis.

Jan-July 2025 (6th Semester CSE-AIML 2025)

Deep Learning on Graphs (CSE-AIML) UE22AM342BA2

Course Project One Pager

Your Learning goal :

Understanding HGNNs and Graph Modelling:
Learn to represent real-world network traffic as heterogeneous graphs to capture rich relational data for intrusion detection.

Mastering Edge-Based Classification:
Discover why classifying edges (network connections) can yield more precise anomaly detection compared to node-based approaches.

Data Preprocessing & Feature Engineering:
Gain hands-on experience in extracting and preparing features from datasets like UNSW-NB15 for constructing effective graph-based models.

Applying Cybersecurity Concepts:
Apply theoretical graph methods to solve a critical real-world problem—detecting and isolating network intrusions—to improve overall network security.

Reference paper, if any (provide the URL)

No	Title	Link
1.	E-GraphSAGE: A Graph Neural Network based Intrusion Detection System for IoT	Link
2.	Network Intrusion Detection with Edge-Directed Graph Multi-Head Attention Networks	Link
3.	Anomal-E: A Self-Supervised Network Intrusion Detection System based on Graph Neural Networks	Link

Jan-July 2025 (6th Semester CSE-AIML 2025)