M2 Internship – From Deep learning based Graph Anomaly Detection to Immersive Explanations in Augmented Reality

Duration: 6 months
Supervision: Jean-Philippe Farrugia (LIRIS, Lyon 1), Mohammed Lamine Messai (ERIC, Lyon 2) and Hamida SEBA (LIRIS, Lyon 1)
Location: LIRIS, campus de la Doua Villeurbanne or IUT Lyon 1, campus de Bourg en Bresse
Application should be sent to: Hamida.seba@univ-lyon1.fr (CV+Transcripts)
Keywords: Graph Anomaly Detection, Graph Neural Networks, Explainable AI, Graph-XAI, Augmented Reality, WebXR, Cybersecurity, Immersive Analytics.

1 Context

Cybersecurity systems generate large volumes of interconnected data: communications between machines, authentication events, processes, users, resources, and cyber-physical dependencies can naturally be represented as graphs.

Graph Anomaly Detection (GAD) aims to identify unusual nodes, edges, subgraphs, or graphs. Deep learning approaches, and Graph Neural Networks (GNNs) in particular, have recently become an important paradigm for Graph Anomaly Detection because of their ability to jointly exploit graph structure and node or edge attributes.

A deep anomaly detector can typically associate an entity v with an anomaly score

$$f_\theta(G, v) \to s(v).$$

However, knowing that $s(v)$ is high is generally insufficient for a cybersecurity analyst. The analyst also needs to understand **why** the entity was classified as anomalous and which surrounding entities, attributes, interactions, or structural patterns contributed to the decision.

This raises an explainability problem:

$$f_\theta(G, v) \to \underbrace{s(v)}_{What is anomalous?} + \underbrace{E(v)}_{Why is it anomalous?}.$$

Recent research has started to investigate interpretable and explainable Graph Anomaly Detection. However, producing an algorithmic explanation does not guarantee that this explanation can be easily understood by a human analyst.

At the same time, Augmented Reality offers new opportunities for presenting complex graph structures spatially and interactively.

This internship therefore investigates the connection between **Deep Graph Anomaly Detection, Explainable AI, and Augmented Reality**.

The central research question is:

> *How can an explanation produced by a deep graph anomaly detector be transformed into a perceptible, interactive, and useful spatial explanation for a cybersecurity analyst in Augmented Reality?*

The project will reuse and extend the existing WebXR graph prototype, allowing the student to focus primarily on the scientific relationship between explainability and immersive representation rather than on the development of an AR platform from scratch.

2 Objectives

2.1 O1 – Integrate a Deep Graph Anomaly Detection Model

The first objective will be to select and integrate one or two representative Deep Graph Anomaly Detection methods.

The objective is not to develop a new GNN architecture but to obtain a robust experimental pipeline producing anomaly scores for nodes, edges, or subgraphs:

The selected models will be evaluated on standard graph anomaly datasets and, when available, cybersecurity graph scenarios.

2.2 O2 – Extract and Compare Explanations

The second objective will investigate how the decisions of the selected detector can be explained.

The student will compare suitable Graph-XAI approaches according to criteria such as fidelity, sparsity, stability, and computational cost.

2.3 O3 – From Algorithmic Explanation to AR Explanation

This objective constitutes the central scientific contribution of the internship.

A Graph-XAI method may return tens or hundreds of relevant graph elements. Displaying all of them in AR may produce an explanation that is faithful to the model but unusable for a human analyst.

The student will therefore investigate a mapping

$$\Phi : E(v) \longrightarrow R_{AR}(v),$$

where $E(v)$ is the algorithmic explanation and $R_{AR}(v)$ is its Augmented-Reality representation.

The student will investigate how explanatory elements should be selected, prioritized, grouped, and spatially represented. []

References

[1] Wolfgang Büschel, Stefan Vogt, and Raimund Dachselt. Augmented reality graph visualizations: Investigation of visual styles in 3d node-link diagrams. *IEEE Computer Graphics and Applications*, 39(3):29–40, 2019.

[2] Adrien Fonnet and Yannick Prié. Survey of immersive analytics. *IEEE Transactions on Visualization and Computer Graphics*, 27(3):2101–2122, 2021.

[3] Yixin Liu, Shirui Pan, Yu Guang Wang, Fei Xiong, Liang Wang, Qingfeng Chen, and Vincent CS Lee. Anomaly detection in dynamic graphs via transformer. *IEEE Transactions on Knowledge and Data Engineering*, 35(12):12081–12094, 2023.

[4] Xiaoxiao Ma, Jia Wu, Shan Xue, Jian Yang, Chuan Zhou, Quan Z. Sheng, Hui Xiong, and Leman Akoglu. A comprehensive survey on graph anomaly detection with deep learning. *IEEE Transactions on Knowledge and Data Engineering*, 35(12):12012–12038, 2023.

[5] Simone Mungari, Albert Bifet, Giuseppe Manco, and Bernhard Pfahringer. Ares: Anomaly recognition model for edge streams. In *Proceedings of the 32nd ACM SIGKDD Conference on Knowledge Discovery and Data Mining V.1*, KDD '26, page 1078–1088, New York, NY, USA, 2026. Association for Computing Machinery.

[6] Zhen Yang, Xiaodong Liu, Tong Li, Di Wu, Jinjiang Wang, Yunwei Zhao, and Han Han. A systematic literature review of methods and datasets for anomaly-based network intrusion detection. *Computers Security*, 116:102675, 2022.