M2 Internship – Explainable Anomaly Detection and Augmented Reality Visualization for Cybersecurity

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: Cybersecurity, Computer Networks, Network Monitoring, Statistical Anomaly Detection, Graph Analysis, Augmented Reality, WebXR, Immersive Analytics.

1 Context and Summary

Modern computer networks generate continuous streams of heterogeneous data: communications between hosts, user connections, service dependencies, authentication events, network flows, and security alerts.

Graphs provide a natural abstraction for representing such systems. Nodes may represent hosts, users, services, processes, applications, or network devices, while edges represent communications, accesses, dependencies, or information flows.

Network activity can therefore be represented as a dynamic graph

$$G_t = (V_t, E_t),$$

whose structure evolves continuously over time.

A major challenge in cybersecurity monitoring is to identify abnormal behaviors while preserving enough contextual information to understand why an event is suspicious and how it relates to the surrounding network.

Many anomaly-detection approaches rely on complex machine-learning models. Although powerful, their decisions can be difficult to interpret. In the context of this internship, we deliberately focus on **simple and explainable statistical anomaly-detection methods**.

The objective is to detect anomalies for which the reason for the detection can be directly expressed through measurable network or graph properties, such as:

- an unusually large number of communications;
- a sudden increase in traffic volume;
- communication with an unusually large number of destinations;
- abnormal values with respect to historical behavior;
- unusual local graph structure;
- abrupt changes in the neighborhood of a host;
- rare or unexpected communication patterns.

Such methods are particularly suitable for Augmented Reality (AR), since the statistical properties responsible for an anomaly can be directly translated into visual information presented to the analyst.

The project already benefits from an existing **WebXR prototype** capable of visualizing streaming graphs in an immersive environment.

The objective of the internship is to transform this prototype into an experimental platform for **network monitoring and explainable anomaly investigation in Augmented Reality**.

The internship will investigate two complementary questions:

> *Which network-security monitoring and anomaly-investigation tasks can benefit from an Augmented-Reality representation?*

and

> *How can simple statistical anomaly-detection and graph-processing methods be adapted so that detected anomalies and their causes are directly visible and understandable in an immersive monitoring environment?*

2 Objectives

2.1 O1 – Define Relevant Cybersecurity Monitoring Use Cases

The first objective will be to identify realistic cybersecurity scenarios for which AR-based monitoring may provide added value to a 2D monitring. For each scenario, the student will identify:

- the relevant network information;

- the graph representation;
- the statistical indicator associated with the anomaly;
- the information required by the analyst;
- the potential benefit of the AR representation.

2.2 O2 – Adapt/Design Explainable Statistical Anomaly Detection for AR-based monitoring context

This research component will investigate how anomaly detection and graph processing should be adapted when the results are intended for continuous monitoring in an AR environment.

The AR interface should make both the anomaly and its cause immediately accessible to the analyst.

3 Candidate Profile

The internship is intended for a Master 2 student in Computer Science, Computer Networks, Cybersecurity, or a related field.

The candidate should have:

- good programming skills;
- fundamental knowledge of computer networks: IP networking, TCP/UDP, network flows, ports and common protocols;
- fundamental knowledge of cybersecurity: network attacks, intrusion detection, security monitoring and logs;
- basic knowledge of statistics and data analysis;
- basic knowledge of algorithms and data structures.

[] Knowledge of graph algorithms, network monitoring tools, JavaScript/TypeScript, Three.js, or WebXR would be appreciated. [2], [6]

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] Ricardo Cabello and Three.js Authors. Three.js: A javascript 3d library. https://github.com, 2010. Accessed: 2026-09-14.

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

[4] Chao Li, Runshuo Liu, Zhongying Zhao, Hui Zhou, and Qingtian Zeng. Freqtad: multi-scale frequency encoding and time-frequency attention for anomaly detection in dynamic graphs. In *Proceedings of the Fortieth AAAI Conference on Artificial Intelligence and Thirty-Eighth Conference on Innovative Applications of Artificial Intelligence and Sixteenth Symposium on Educational Advances in Artificial Intelligence*, AAAI'26/IAAI'26/EAAI'26. AAAI Press, 2026.

[5] Yingxuan Li, Yuanyuan Xu, Xuemin Lin, and Ying Zhang. Mitigating anomaly hallucination: A model-agnostic framework for unsupervised anomaly detection on dynamic graphs. In *Proceedings of the 32nd ACM SIGKDD Conference on Knowledge Discovery and Data Mining V.2*, KDD '26, page 2838–2849, New York, NY, USA, 2026. Association for Computing Machinery.

[6] W3C Immersive Web Working Group. Webxr device api. W3c working draft, World Wide Web Consortium (W3C), 2026. Accessed: 2026-09-14.

[7] 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.