Description of Master's Research Internship Proposal

Title: Knowledge Graph-based Modeling of Dynamic Vulnerability Data and Organizational Knowledge for Cybersecurity Enhancement

Reference: ROMANCE (to be quoted in all correspondence)
Location: ERIC Laboratory, Porte des Alpes Campus, Bron. Tel: 04 78 77 31 54
Internship supervisors (Emails):
- Mohamed-Lamine Messai (mohamed-lamine.messai@univ-lyon2.fr)
- Hamida Seba (hamida.seba@univ-lyon1.fr)

Internship for a Master 2 student (or equivalent)
Duration: 5-6 months. The gratification will be around 550 €/month.
Desired period: from February 2024

Description

In the era of increasing cyber threats, it is crucial for organizations to have a comprehensive understanding of their vulnerabilities and the interconnectedness of their digital assets. This research internship aims to explore the potential of knowledge graphs [1] in the field of cybersecurity by developing a dynamic vulnerability data model (e.g., CVE) integrated with an organizational knowledge graph representing network architecture, host operating systems, software versions (e.g., web server version, libraries, database server version), and more. The ultimate goal is to empower organizations to gain insights into threat dependencies and enhance their cybersecurity measures [2]. Additionally, we aim to investigate the construction of digital twins using knowledge graphs to provide a visual and conceptual representation of an organization's cyber environment [3].

Objectives of this internship :

- Knowledge Graph Modeling: Design and develop a knowledge graph schema that incorporates dynamic vulnerability data (e.g., CVEs) and organizational information (network architecture, software versions, etc.).
- Data Integration: Establish mechanisms to extract, transform, and load vulnerability data and organizational information into the knowledge graph.

- Dependency Analysis: Analyze the knowledge graph to identify and visualize the dependencies and relationships between vulnerabilities and organizational assets, enabling a better understanding of threat landscapes.
- Digital Twin Construction: Investigate the utilization of knowledge graphs to construct digital twins that mimic the behavior and interactions within an organization's cyber ecosystem, providing a simulated environment for testing security strategies and evaluating risk scenarios.
- Machine Learning: propose knowledge graph embedding to detect vulnerabilities and attacks [4, 5, 6].
- Implementation and tests

To apply: The candidate must have advanced skills (M2 level) in computer science (data science, machine learning and notions of graph theory and computer security are highly desirable). Please send, before 31/12/2023, your application with a CV, a cover letter, as well as your grades for the current academic year and last year to mohamed-lamine.messai@univ-lyon2.fr

References

[1] Ji, S., Pan, S., Cambria, E., Marttinen, P., & Philip, S. Y. A survey on knowledge graphs: Representation, acquisition, and applications. *IEEE transactions on neural networks and learning systems* 33.2 : 494-514. 2021.

[2] Liu, K., Wang, F., Ding, Z., Liang, S., Yu, Z., & Zhou, Y. A review of knowledge graph application scenarios in cyber security. arXiv preprint arXiv:2204.04769. 2022.

[3] Alcaraz, Cristina, and Javier Lopez. Digital twin: A comprehensive survey of security threats. *IEEE Communications Surveys & Tutorials*. 2022.

[4] Ikenna Oluigbo, Mohammed Haddad & Hamida Seba. Evaluating Network Embedding Models for Machine Learning Tasks. 8th International Conference on Complex Networks and their Applications, 10 décembre, Lisbon (Portugal). 2019.

[5] Mohamed-Lamine Messai, Hamida Seba: IoT Network Attack Detection: Leveraging Graph Learning for Enhanced Security. Proceedings of the 18th International Conference on Availability, Reliability and Security, ARES 2023, Benevento, Italy, 29 August 2023- 1 September 2023. ACM 2023: 84:1-84:7

[6] William L. Hamilton. Graph Representation Learning. Synthesis Lectures on Artificial Intelligence and Machine Learning, 14(3), pages: 1-159, Morgan and Claypool, 2020.