**Project title:** Graph modeling of log files for attack detections in IoT networks

**Lead faculty:** Mohamed-Lamine Messai, Université Lumière Lyon 2,

<mailto:mohamed-lamine.messai@univ-lyon2.fr>

**General area:** Computer science: IoT networks security, IA-based anomaly detection

**Description:**

The main objective of this small project is to model log files in a graph database in order to analyze this data to detect cyber-attacks. Achieving this goal requires accomplishing the following points :

\_ Modeling log files of a dataset using a graph-oriented database (under Neo4j

for example).

\_ Identify and study the various cyber threats that can be detected by analyzing

log files.

\_ The use of Machine learning for the early detection of a targeted attack (eg. DDoS).