NGI EXPLORERS

CHALLENGE #23
WMICH-SMART-01

Robust Learning based Anomaly Detection in Smart Living IoT Systems

Meet the expectations of this US Node through the technology challenge described below

GOALS

Numerous machine learning and AI approaches exist for anomaly based attack detection in IoT systems, with the assumption that training data is accurate and attack free and training and test sets follow the same distribution However, these assumptions are not true especially for large scale IoT applications for smart living where the device heterogeneity and differences human behaviour makes anomaly based detection and challenging problem. Furthermore, it has been shown that attacks or noise hidden in the training data leads to learning the wrong model, which fails to detect the anomalies in the testing/ deployment. There we need to develop novel machine learning approaches for anomaly detection specifically for smart living IoT applications, which BY-DESIGN are robust to training data attacks and noise.

DETAILS

Smart work on the theoretical foundation for the robust anomaly detection in Smart Living IoT.

Applying the theory using datasets from one out of the following: real smart living IoT domains, such as Smart Metering, Smart Transportation, Smart Homes, Dynamic Spectrum Sensing and Access.

SKILLS REQUIRED

A good understanding of convex optimization, Machine Learning, Python/Matlab/R scripting language. Knowledge of AI and Computer Networking is a plus.

FUNDED BY NGI

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 825183