Associate Professorship of Embedded Systems and Internet of Things
Department of Computer Engineering
Technical University of Munich

AI-based Attack Data Generation

Supervisor:	Dr.-Ing. Mohammad Hamad
Period:	24 weeks
Start Date:	ASAP
Type:	Master's Thesis

Context

In the rapidly advancing landscape of the Internet of Things (IoT) and IoT-Edge-Cloud technologies, physical environments are becoming increasingly sensor-equipped, developing intelligent space ecosystems. These ecosystems are fueled by the copious data generated by IoT devices, which are harnessed to exploit AI models and services. Consequently, this has given birth to the concept of Artificial Intelligence of Things (AIoT) systems. However, achieving security, robustness, efficiency, and continuous operation in AIoT systems demands access to realistic and reliable data at scale. Unfortunately, acquiring such data is often hindered by the cost of constructing smart spaces, the challenges of long-term device tracking, data gaps between sensors and knowledge in various intelligent space scenarios, and the constraints on sharing sensitive data. In this thesis, the aim is to proposes an AI-based framework for synthetic data generation, quantification of uncertainties, and data summarization to ensure the delivery of trustworthy datasets that reflect the different status of the system, including the off-nominal behaviors. Also, using this data to train/test the different AI models in the system, including the AI-based intrusion detection components.

Tasks

The detailed timeline, various tasks, and milestones will be deployed in agreement with the student.

Requirements

- **High motivation** for learning new things
- **Very good** programming skills: Python
- **(very) Good** experience AI and ML
- **Good** understanding of (IoT) security

Are you Interested?

please send your full application (CV, current transcript of records) to (mohammad.hamad@tum.de).