PhD Student: Han Wang, RISE Cybersecurity, Kista Stockholm <han.wang@ri.se>
Main Supervisor: Shahid Raza, RISE Cybersecurity

Title: Trustworthy Federated Learning for IoT security

Abstract:
With the introduction of new privacy laws, such as the General Data Protection Regulation (GDPR) in the EU, the amount of data shared should always be minimized. The most significant benefit of using AI at the edge of IoT networks is keeping data within personal/industrial spaces and at the same time allowing gaining ML advantages to help solving performance and IoT security problems such as anomaly detection. Federated Learning has emerged as a very promising paradigm for training distributed ML models. It enables IoT edge devices to collaboratively train models in a decentralized way and keep the private data staying on the devices at the same time. Despite the advantages, FL brings challenges as well. In a real-world setup, the collected data vary significantly among devices since the user's preferences and local environments are different. This is especially relevant for IoT anomaly detection, as the type of attacks or anomalies observed by each device can be different. Because of this heterogeneity in IoT network, the training data for ML models are usually non-IID and imbalanced which has been shown to degrade model's performance. This presentation will cover (i) background of federated learning, (ii) applications and challenges of federated learning.

These works are done in collaboration with Imperial College London and Northeastern University, and is partly funded by RISE internal funding and partly by the EU Horizon 2020 COCNCORDIA, a project that is building an EU cybersecurity center of excellence.