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

Title: Machine Learning for IoT Security

Abstract:
Along with the growing of IoT network, immense volume of data is generated which is valuable to be analyzed. Especially, IoT security now has raised high attention, and Machine Learning (ML) is getting attention to secure IoT by learning the behavior of the attacks and detecting outlier. Current state of the art ML solutions for IoT collect IoT data in a cloud environment and perform ML there. Due to privacy reasons such as those enforced by GDPR, and the fact that energy is one of the most constrained resources in IoT devices and most energy is consumes by radio (for transmitting and receiving), it is major trend to bring ML closer to (IoT) devices where data collection and actuation is performed. We are working on employing ML method in an "edge" device or in actual IoT devices to address IoT security problems such as malware detection with focus on malicious Microservice within IoT, detection of malicious/curious IoT vendors, detection of compromised IoT devices connected to telecom networks.
The PhD student who works on this has started a couple of months ago and currently writing an investigative paper on comparison of state-of-the-art ML approaches and their suitability in IoT devices or in an edge.
This work is done in collaboration with Ericsson 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.