PhD Student: Anum Khurshid, RISE Cybersecurity Lab, Stockholm <anum.khurshid@ri.se>

Main Supervisor: Shahid Raza, RISE Cybersecurity

Title: Trusted Execution Environments for Resource-constrained IoT

Abstract:

Securing IoT devices is vital today as the security risks associated with these devices grow rapidly. The increase in Trusted Execution Environments (TEEs) in resource-constrained embedded device (e.g., TrustZone-M) in the infrastructures like industries, health monitoring, energy grids, automotive, etc., is a step towards isolation and secure execution of critical software. TEEs provide efficient mechanisms to isolate system resources and hence play a significant role in security-critical operations such as secure boot, crypto operations, software/firmware update and remote attestation. We have worked on identifying and resolving challenges in TEEs like securing the inter-world communication, mitigating unauthorized activities within devices and utilizing the TEEs for remote attestation and certification of software-state integrity. This goal is to not only improve the security of the IoT infrastructure but also increase the level of trust on these devices.

This work is partly funded by SSF aSSIst, EU Horizon 2020 CONCORDIA, H2020 VEDLIoT and RISE internal Knowledge Platform.