Asrin Abdollahi
Industrial PhD Student at RISE/Mälardalen University
asrin.abdollahi@ri.se/mdu.se
Isafjordsgatan 22, SE-164 40 Kista, Stockholm, Sweden

May 26, 2026

Title: A Minimalistic TEE for Low-Power RISC-V-Based IoT
Authors: Asrin Abdollahi, Simon Bouget, Giuseppe Nebbione, Shahid Raza
Poster/Presentation: Poster

Abstract:
Securing IoT devices can be challenging due to their limited battery power and resource constraints. Protection at the hardware level is necessary to mitigate the attack surface. RISC-V offers an open-source, license-free, and customizable architecture, making it ideal for small IoT devices and custom designs. Trusted Execution Environment (TEE) is a hardware-based security mechanism that provides the private execution environment for sensitive tasks, which prevents unauthorized access and exploitation. A Security Monitor (SM) with privileged access can ensure that only trusted applications with approved tasks are executed in the enclave (the secure world). This can be achieved using RISC-V features, including a well-defined isolation through Physical Memory Protection (PMP). The key contribution is a custom RISC-V design that features a lightweight TEE controlled by SM with extended PMP policies, ensuring isolated execution for trusted applications. The evaluation results demonstrate strong security assurance with minimal execution overhead during context switching.