



IFIP IoT 2021 Special Session

AI-Enabled Security for IoT

Scope

Artificial Intelligence (AI) encompasses a broad range of learning algorithms with important implications for diverse domains and computing applications. In particular, the security aspects of AI, from software and networks, to hardware platforms, have intrigued researchers in recent years, both from the perspective of potential attacks, as well as countermeasures. IoT systems, from the cloud to the edge, present unique, multiscale challenges for security and privacy. This special session will broadly solicit contributions that deal with how AI threatens traditional approaches to network, software, and hardware security, the research challenges this presents, and what opportunities exist for AI-enabled security for multiscale IoT systems. Topics of interest include, but are not limited to:

- AI-guided security verification for IoT software and hardware,
- AI-based security monitoring and intrusion detection,
- Big data analysis for IoT security using AI,
- Tools for scalable AI integration for IoT security,
- AI-based security protocols for IoT technologies
- Risk and challenges in AI for IoT security,
- AI-guided hardware attacks,
- Current trends and future directions in AI for IoT security

This special session will serve as a venue for prospective authors whose cross-domain contributions may not fit well within the existing conference sessions on either security and privacy in IoT, or AI in IoT.

Session Organizers

Dr. Robert Karam, University of South Florida, rkaram@usf.edu

Dr. Tamzidul Hoque, University of Kansas, hoque@ku.edu

Topics / Keywords

Artificial Intelligence, Machine Learning, Hardware Security, Software Security, Network Security

All papers must be written in English. Full papers should be at most 18 pages long in total including references and appendices. The paper should be intelligible without having to read the appendices. Poster presentations should be at most 4 pages. Submissions should not be anonymized. Authors must follow the Springer formatting instructions. For paper submissions go to

<https://easychair.org/conferences/?conf=ifipiot2021>

Deadlines:

Abstract Due - 15 May 2021

Full Paper Due - 15 June 2021

Notification of Acceptance - 31 August 2021

Deadline for final version - 15 December 2021