Special Session on Cybersecurity Issues of IoT in Ambient Intelligence (Ami) Environment (2nd Edition)

IEEE 9th World Forum on Internet of Things
October 12-27 2023
Aveiro Congress Center, Portugal
IEEE WF-IoT 2023

Special Session on Cybersecurity Issues of IoT in Ambient Intelligence (Ami) Environment (2nd Edition)

Organizing Chairs:

Dr Abdellah Chehri
Royal Military College of Canada
Dr Gwanggil Jeon
Incheon National University
Dr Muhammad Zeeshan Shakir
University of the West of Scotland
Dr Imran Ahmed
Anglia Ruskin University

Programme Committee:

Luiz F. Bittencourt
Rafael Tolosana Calasanz
Marcelo Keese Albertini
Awais Ahmad
Marco Anisetti
Wahabou Abdou
Nordine Quadar
Xiaomin Yang
Nicola Bena
Filippo Berto
Qin Pu
Kashif Naseer Qureshi
Vu Khanh Quy
Rachid Saadane
Nguyen Minh Quy
Andand Paul
Aryan Kaushik
Tanzila Saba
Khalid Haseeb
Amjad Rehman
Xiangyu Guo
Mingliang Gao

Important dates:
Paper submission: Jul 30, 2023
Notification of acceptance: Aug 21, 2023
Camera-ready submission: Sep 29, 2023
Presentation submission: Oct 2, 2023

Description:
Over the years, the use of the Internet of Things (IoT) has come to dominate several areas, e.g., improving our lives, offering us convenience, and reshaping our daily work circumstances. Ambient intelligence (AmI) refers to the ability of devices to interact seamlessly with their surroundings. The increased use of IoT in ambient intelligence has led to a heightened concern for cybersecurity. Hackers could exploit vulnerabilities in the software or firmware of IoT devices to gain control of the devices or the networks they are connected to. They could also use ambient intelligence systems to collect sensitive data from IoT devices. In order to protect these devices, it's essential to understand the various types of attacks that are possible and deploy appropriate security measures.

Topics of Interest:
The proposed special session provides a forum for bringing together researchers from academia and industry to explore and present their findings in Artificial Intelligence, cybersecurity issues of IoT, and AmI. The participants are encouraged to discuss the theories, systems, technologies, and approaches for testing and validating them on challenging real-world, safety-critical applications.

The session aims to address but not limit to the following:

- Formal security and resilience analysis on AI.
- IoT security, trust, and trustworthy
- Secure and privacy-preserving IoT communications
- Cognitive models and bio-inspired AI.
- AI-assisted critical infrastructure security.
- Applied cryptography for IoT and AmI.
- Security and privacy of AmI.
- Applications of formal methods to IoT and AmI security.
- Blockchain for trustworthy AmI-based applications.
- IoT and embedded systems security.
- Cyber threat intelligence for IoT and AmI.
- Privacy-Preserving Machine Learning for IoT.
- Federated learning for IoT networks.

Paper Submission:
All papers must be submitted through eWorks. You must choose the session track (**Track ID: Spes-02**) when submitting your paper in order to be considered for this Special Session. The paper should be up to six (6) pages in length. The conference allows up to two additional pages for a maximum length of eight (8) pages upon payment of extra page fees once the paper has been accepted.

The paper can be prepared using the template available through the Authors / Proposers tab from the WF-IoT conference website main page at:
https://wfiot2023.iot.ieee.org

More information on the special session:
https://wfiot2023.iot.ieee.org/special-session-cybersecurity-issues-iot-ambient-intelligence-environment-2nd-edition