The 1st International Workshop on Cybersecurity Issues of IoT in Ambient Intelligence (AmI) Environment

In conjunction with

The 7th IEEE Int'l Congress on Cyber Science and Technology (CyberSciTech 2022)

Calabria University, Italy, 12-15, September 2022

http://cyber-science.org/2022/cyberscitech/

Scope and Motivation:

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 in the process. 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. In recent years, Artificial Intelligence (AI) has got a lot of attention, especially for the success of deep learning to address problems that were considered hard before.

Scope and Topics:

The proposed special session (workshop) 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. Thus, suggested topics include, but are not limited to, the following points:

- Formal security and resilience analysis on AI.
- Cognitive models and bio-inspired AI.
- AI-Assisted Critical Infrastructure Security.
- Applied Cryptography for AI and AMI.
- Security and Privacy of AmI and/or IoT.
- Applications of Formal Methods to AmI Security.
- Blockchain for Trustworthy AmI-based applications.
- Embedded Systems Security.
- Cyber Threat Intelligence for AI and AmI.
- Privacy-Preserving Machine Learning.

Submission and Publication

Authors are required to submit fully formatted, original papers (PDF), with graphs, images, and other special areas arranged as intended for the final publication. Papers should be written in English conforming to the IEEE standard conference format (two-column, 10 pt font, etc., including figures, tables, and references). The review submissions are limited to six pages, (additional charges may apply for additional pages). Conference content will be submitted for inclusion into IEEE Xplore as well as other Abstracting and Indexing (A&I) databases. IEEE formatting information:

https://www.ieee.org/conferences/publishing/templates.html

Each accepted paper must be presented at the conference by one of the co-authors or a third party, otherwise it will not be indexed and archived through IEEE Xplore. Only timely submissions through EDAS will be accepted. For more details, please visit the CyberSciTech 2022 official website (http://cyber-science.org/2022/cyberscitech/

Accepted Papers

All the accepted papers must be presented in the workshop during and will also be included in the IEEE CyberSciTech proceedings, which will be published by IEEE CPS (EI indexed, in IEEE DL). All accepted papers will be published in the conference proceedings and presented for inclusion in IEEE Xplore Digital Library.

Best Paper Awards will be presented to high quality papers.

Important Dates:

Submission Due: **June 1, 2022**

Author Notification Due: July 1, 2022

Final Camera-ready Submission: July 15, 2022

Organizing Committee:

- Co-chair: Pr. Abdellah Chehri, University of Quebec, UQAC, Canada. Email: achehri@uqac.ca
- Co-chair: Pr. Gwanggil Jeon, Incheon National University, Korea. Email: gjeon@inu.ac.kr
- Co-chair: Pr. Imran Ahmed, Institute of Management Sciences, Pakistan. E-mail: imran.ahmed@imsciences.edu.pk
- Co-chair: Pr. Marco Anisetti, University of Milan, Italy. Email: marco.anisetti@unimi.it

Technical Program Committee

- Abdellah Chehri, University of Quebec- UQAC, Canada.
- Marcelo Keese Albertini Federal University of Uberlandia, Brazil.
- Salvatore Cuomo Univ. of Naples Federico, Italy.
- Awais Ahmad, University of Milan, Italy.
- Marco Anisetti, University of Milan, Italy
- Ernesto Damiani, Khalifa University, UAE
- Gwanggil Jeon, Incheon National University, Korea
- Tadashi Matsumo, Japan Advance Institute of Science and Technology,
- Muhammad Zeeshan Shakir, University of Western Ontario, Canada
- Wahabou Abdou, University of Burgundy, France
- Cem Kaptan, University of Ottawa, Canada
- Liu Jinxin, University of Ottawa, Canada
- Saleh Bouarafa. LRIT, Morocco.
- Nadir Hakem, University of Quebec, UQAT, Canada.

- Nordine Quadar, University of Ottawa, Canada
- Xiaomin Yang, Sichuan University, China
- Ali Abedi, University of Maine, USA.
- Jun Cai, Concordia University, Canada.

Sponsored By

Supported By

Italy Section SYSC Chapter

Italy Section VT/COM Joint Chapter

Italy Section CS Chapter

Italy Section SEN Chapter