The 2nd International Workshop on Cybersecurity Issues of IoT in Ambient Intelligence (AmI) Environment

In conjunction with

The 23rd IEEE International Conference on Pervasive Intelligence and Computing (PICom 2025)

October 21-24, 2025 - Hakodate City, Hokkaido, Japan

https://cyber-science.org/2025/picom/

Sponsored by IEEE, **IEEE Computer Society**

http://cyber-science.org/2025/picom/

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.

Workshop Objectives, Scope and Topics:

This workshop aims to provide a comprehensive understanding of IoT and Ambient Intelligence (AmI) technologies, highlighting their influence on modern life and work environments. This workshop is ideal for researchers, engineers, cybersecurity professionals, and technology enthusiasts interested in IoT, AmI, and AI-based solutions for cybersecurity. Participants will delve into common cybersecurity threats affecting IoT devices and AmI systems, gaining insights into potential attack vectors and their associated consequences. The workshop will also explore practical security measures and effective strategies to protect IoT systems against cyber threats, ensuring robust and reliable

operations in increasingly interconnected environments. 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:

- IoT and Ambient Intelligence systems.
- Common vulnerabilities in IoT device software and firmware.
- Cybersecurity challenges in AmI integration.
- Emerging solutions using Artificial Intelligence (AI) and deep learning techniques to mitigate risks.
- Formal security and resilience analysis on 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.

Learning Outcomes:

Participants will gain insights into the intersection of IoT, AmI, and cybersecurity. They will learn how AI-driven approaches, such as deep learning, can address previously unsolved challenges and protect devices from potential threats.

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:

Papers must be submitted though the EDAS conference submission link by choosing "**PICom / 2nd International Workshop on Cybersecurity Issues of IoT in Ambient Intelligence (AmI) Environment**". Submission link through EasyChair: https://edas.info/N33777

Accepted Papers

All the accepted papers must be presented in the workshop and will also be included in the IEEE PICom 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.

Important Dates:

- Workshop/Special Session Paper Due: June 20, 2025
- Authors Notification: July 30, 2025
- Camera-ready Submission: September 12, 2025

Organizing Committee:

- **Chair:** Pr. Abdellah Chehri, Royal Military College of Canada, Canada (chehri@rmc.ca)
- **Co-Organizer:** Pr. Gwanggil Jeon, Incheon National University, Korea (gjeon@inu.ac.kr)
- **Co-Organizer:** Pr. Imran Ahmed, Anglia Ruskin University, UK (imran.ahmed@aru.ac.uk)
- **Co-Organizer:** Rachid Saadane, Pr. Hassania School of Public Works, Morocco (saadane@ehtp.ac.ma)
- **Co-Organizer:** Pr. Marco Anisetti, University of Milan, Italy (marco.anisetti@unimi.it)

Technical Program Committee

- Abdellah Chehri, Royal Military College of Canada, Canada
- Marcelo Keese Albertini Federal University of Uberlandia, Brazil.
- Awais Ahmad, University of Milan, Italy.
- Hasna Chaibi, Moulay Ismail University, Morocco.
- Huaiyu Chen, University of Ottawa, Canada.
- Martin Bouchard, University of Ottawa, Canada.
- Gwanggil Jeon, Incheon National University, Korea.
- Tadashi Matsumo, Japan Advance Institute of Science and Technology.
- Wahabou Abdou, University of Burgundy, France.
- Cem Kaptan, University of Ottawa, Canada.
- Abdeslam Jakimi, Faculty of Science and Technology Errachidia, Morocco.
- Liu Jinxin, University of Ottawa, Canada.
- Saleh Bouarafa. LRIT, Morocco.
- Nadir Hakem, University of Quebec, UQAT, Canada.
- Nordine Quadar, Royal Military College of Canada, Canada
- Ali Abedi, University of Maine, USA.
- Jun Cai, Concordia University, Canada.

Sponsored By

TCSC IEEE | IEEE SMC TC on CyberMatics | IEEE CIS Smart World TC | IEEE HI-TC Hyper Intelligence Technical Committee

Sponsored by

IEEE | IEEE computer society

Hosted by

公立はこだて未来大学 FUTURE UNIVERSITY HAKODATE