IEEE AMCAI 2025

2nd Afro-Mediterranean Conference on

Artificial Intelligence

October 14 -16, 2025

Valenciennes - France

AI-CyberDef 2025

Special Session on Artificial Intelligence based Cyber Defense

at the **2nd IEEE Afro-Mediterranean Conference on Artificial Intelligence** (**2025 IEEE AMCAI**)
Valenciennes, France, October 14-16, 2025
Conference website: https://amcai-atia.tn/

Special Session Organizers

Prof. Khaled JOUINI
MARS Research Lab., ISITCOM
University of Sousse, Tunisia
E-mail: Khaled.jouini@isitc.u-sousse.tn

Prof. Ouajdi KORBAA
MARS Research Lab., ISITCOM
University of Sousse, Tunisia
E-mail: ouajdi.korbaa@isitc.u-sousse.tn

Prof. Farah JEMILI
MARS Research Lab., ISITCOM
University of Sousse, Tunisia
E-mail: farah.jmili@isitc.u-sousse.tn

Objectives and topics

The special session AI-CyberDef 2025 explores the application of Artificial Intelligence (AI) and other advanced technologies in cyber defense. The objectives include utilizing AI algorithms and machine learning for real-time threat detection and prevention, enhancing incident response processes through AI-driven systems, conducting proactive vulnerability assessment and risk mitigation, improving user authentication and access control with AI and biometric technologies, promoting collaborative defense efforts through threat intelligence sharing, addressing the spread of fake news and misinformation using AI techniques, and ensuring privacy and ethical considerations in AI-based cyber defense systems. These objectives collectively aim to enhance cybersecurity measures and protect digital environments effectively.

The scope of the Special_Session_ AI-CyberDef 2025 includes, but is not limited to the following topics:

AI for Automated Cyber Defense

- Real-time threat detection and response.
- AI-powered intrusion detection and self-healing systems.
- Automated incident response and mitigation.

Generative AI: Security and Defense

- Detecting and mitigating AI-generated phishing, malware, and disinformation.
- Countering deepfakes and synthetic media manipulation.
- Secure and ethical development and deployment of generative AI models.

AI for Decentralized Security and Collaboration

- Blockchain for secure logging, auditing, and threat attribution.
- Privacy-preserving threat intelligence sharing and collaboration.
- Explainable AI (XAI) for trust and transparency in decentralized security.

AI-Powered Identity and Access Management

- Advanced biometrics with anti-spoofing and liveness detection.
- Context-aware and intelligent access control using AI.
- AI-driven fraud detection in identity and authentication systems.

AI for Critical Infrastructure Protection

- AI for anomaly detection and intrusion prevention in Industrial Control Systems.
- Anomaly detection and security monitoring in IoT environments.
- AI-driven resilience and self-healing in smart grids and energy infrastructure.

Future Directions in AI-Driven Cybersecurity

- AI for securing digital twins and the industrial metaverse.
- Securing edge computing and serverless environments with AI.
- Quantum-resistant cryptography with AI.

Important dates

Paper Submission deadline: April 15, 2025
Authors Notification: June 15, 2025
Camera Ready and Registration: July 05, 2025
Conference date: October 14-16, 2025

Program Committee

Clemens Dubslaff, Eindhoven University of Technology, The Netherlands

Imed Romdhani, Edinburgh Napier University, United Kingdom

Mohamed Ibn Khedher, Institut de Recherche Technologique SystemX, France

Sailesh Iyer, Rai School of Engineering, Rai University, India

Montassar Zaghdoud, Prince Sattam bin Abdulaziz University, Saudi Arabia

Dhilip Kumar, Institute of Science and Technology, Chennai India

Hanen Idoudi, ENSI-University of Manouba, Tunisia

Farah Barika Ktata, ISSAT-University of Sousse, Tunisia

Maha Khemaja, ISSAT-University of Sousse, Tunisia

Bayrem Triki, ISITCOM-University of Sousse, Tunisia

Submission

All contributions should be original and not published elsewhere or intended to be published during the review period. The contributions should address research questions that relate to one of the topics listed above.

Authors are invited to submit their papers electronically in pdf format, through EasyChair at https://easychair.org/conferences/?conf=amcai2025. All the special sessions are centralized as tracks in the same conference management system as the regular papers. Therefore, to submit a paper please activate the following link and select the track: ***AI-CyberDef 2025: Special Session on Artificial Intelligence based Cyber Defense.***

Manuscripts should be prepared in 10-point font using the IEEE 8.5" x 11" two-column conference format https://www.ieee.org/conferences/publishing/templates.html

Submitted papers are written in English, between 6 to 8 pages (including all figures, tables, and references).

Submissions not following these guidelines may be rejected without review. Also, submissions received after the due date, exceeding the length limit, or not appropriately structured may also not be considered.

To ensure high quality, all submissions are blind peer-reviewed by at least three reviewers from the ***AI-CyberDef 2025 Program Committee***.

All accepted papers must be presented by one of the authors who must register for the conference and pay the fee.

All accepted and presented regular papers will be submitted to IEEE Xplore for inclusion.