ICDAM-2026
7th International Conference on Data Analysis and Management

Organized by *London Metropolitan University, London, UK (Venue Partner)*
in association with
WSG University, Bydgoszcz, Poland, Europe
&
Portalegre Polytechnic University, Portugal, Europe
&
SGGW Management Institute, Poland, Portugal
Date: 12th – 14th June 2026

********** CALL FOR PAPERS **********

SPECIAL SESSION ON

Federated Learning for Cybersecurity: Towards Decentralized, Privacy-Preserving Threat Intelligence

SESSION ORGANIZERS:

Dr. Himanshi Babbar, Assistant Professor, Chitkara University, Punjab, India
Dr. Muhammad Azeem Akbar, Associate Professor and Adjunct Professor (Docent) of Software Process Improvement and Management in the Software Engineering Department at LUT University, Finland.

EDITORIAL BOARD: (Optional):

SESSION DESCRIPTION:

The increasing reliance on distributed computing environments such as IoT, edge computing, and 5G networks has introduced unprecedented cybersecurity challenges. Traditional centralized machine learning approaches to threat detection and mitigation face limitations in scalability, privacy, and latency. Federated Learning (FL) has emerged as a transformative approach that enables decentralized model training across multiple clients without exposing raw data, thereby enhancing privacy and security.

This special issue invites original research, reviews, and case studies that explore the intersection of federated learning and cybersecurity. The aim is to advance the state-of-the-art in privacy-preserving, distributed intelligence for threat detection, anomaly analysis, malware detection, intrusion prevention, and more. The issue will highlight practical implementations, framework developments, adversarial robustness, and ethical considerations in federated cybersecurity systems.

RECOMMENDED TOPICS:

Topics to be discussed in this special session include (but are not limited to) the following:

- Federated learning for intrusion detection and prevention systems (IDPS)

- Privacy-preserving threat intelligence sharing using FL
- Adversarial attacks and defenses in federated settings
- FL for malware and ransomware detection
- Trust management and incentive mechanisms in FL
- Lightweight FL models for edge and IoT cybersecurity
- Differential privacy and homomorphic encryption in FL-based security
- Federated reinforcement learning for autonomous cyber defense
- Benchmarking and simulation frameworks for FL in cybersecurity
- Blockchain-enhanced federated cybersecurity architectures
- FL in smart grids, healthcare, autonomous vehicles, and critical infrastructure security
- Explainable federated learning models in cyber threat analysis

SUBMISSION PROCEDURE:

Researchers and practitioners are invited to submit papers for this special theme session on **[Federated Learning for Cybersecurity: Towards Decentralized, Privacy-Preserving Threat Intelligence].** All submissions must be original and may not be under review by another publication. INTERESTED AUTHORS SHOULD CONSULT THE CONFERENCE'S GUIDELINES FOR MANUSCRIPT SUBMISSIONS at https://icdam-conf.com/downloads . All submitted papers will be reviewed on a double-blind, peer-review basis.

NOTE: While submitting a paper in this special session, please specify **[Federated Learning for Cybersecurity: Towards Decentralized, Privacy-Preserving Threat Intelligence]** at the top (above paper title) of the first page of your paper.

* * * * * *