CYBERSECURITY IN DIGITAL SERVICE SYSTEMS

Special Issue Proposal

CALL FOR PAPERS

Applied Cybersecurity & Internet Governance (ACIG)

SCOPE AND OBJECTIVES

This special issue encompasses theoretical work and practical approaches that advance research in all aspects of securing interconnected digital services in IT systems and infrastructures. Successful contributions may range from advanced technologies, applications, and innovative solutions for modelling, simulation, and predicting cyber threats in complex systems, to modern cryptographic methods, as well as the development of methods, conceptual and theoretical models, and simulations related to the secure operation of digital supply chains and services in IT systems.

The publication topics include (but are not limited to) the following:

- Modelling and simulation of cyber-threats in complex systems
- Prediction and detection of attack kill chains
- Advanced ML and AI techniques for detecting cyberattacks
- Models and protocols for security-related data collection, processing, and delivery
- Automated response and mitigation of cyberattacks
- Modern cryptographic methods
- Modern physical/cyber Digital Twins for simulation and prediction
- Secure and privacy-aware visibility over multi-ownership systems
- Secure and effective creation, sharing, and consumption of Threat Intelligence
- Federated Learning and Transfer Learning over multi-ownership and complex systems
- Coordinated and federated cybersecurity operations in complex systems
- Scalable identity and authentication protocols for sharing data and controls in federated environments
- Cyber-threat challenges for large digital service chains, including Smart City, Smart Grid, critical infrastructures, and supply chains
- Secure communication in Smart Grid installations using Mobile Ad Hoc Network protocols
- Privacy architectures and models for interconnected systems
- Secure attestation of digital resources across providers in complex systems
- Trust management and risk assessment across digital service chains

This Special Issue is open for high-quality papers from all experts in the domain.

PAPER SUBMISSIONS

The submission should include a cover page with the authors' names, affiliations, addresses, phone numbers, and email addresses. Please, indicate the corresponding author and include up to 6 keywords from the above list of topics and an abstract of no more than 400 words. Only PDF files will be accepted. Each paper will receive a minimum of two reviews. Papers will be selected based on their originality, relevance, technical clarity and presentation.

Papers must be submitted to https://www.editorialsystem.com/acig/article/add/ Choose Special Issue – Cybersecurity in digital service systems- 2/2025 vol. 4.

Submissions should be prepared for publication according to the journal's author guidelines: https://www.acigjournal.com/For-Authors,4555.html

IMPORTANT DATES

~~**Abstract Submission:** -- **August 31, 2025**~~
Paper submission: -- **November 5, 2025**
Authors Notification: --- December 5, 2025
Final Manuscripts Due:: -------------------------------------- December 22, 2025
Publication Date: --- **March 2026**

SPECIAL ISSUE GUEST EDITORS

Joanna Kolodziej
NASK
Warsaw, Poland
Cracow University of Technology
joanna.kolodziej68[a]gmail.com

Matteo Repetto
Consiglio Nazionale delle Ricerche
Genoa, Italy
matteo.repetto[a]cnr.it