CALL FOR PAPERS - SPECIAL SESSION

"Emerging theories, tools and methodologies for cybersecurity and digital forensics"

for CODIT 2025

July 15-18, 2025 ■ Split, Croatia

Session Co-Chairs:

1- Associate Prof. Jaouhar Fattahi, Laval University, Québec, Canada (E-mail: jaouhar.fattahi.1@ulaval.ca).
2- Prof. Mohamed Mejri, Laval University, Québec, Canada (E-mail: mohamed.mejri@ift.ulaval.ca).
3- Associate Prof. Ridha Ghayoula, Moncton University, New Brunswick, Canada (E-mail: ridha.ghayoula@umoncton.ca).
4- Maître Assistante, Hager Kammoun, University of Sfax, Tunisia (E-mail: hager.kammoun@fss.usf.tn).

Session description:

As communication networks expand in complexity, the need for advanced theories, techniques, and tools to ensure robust security, particularly in forensics and AI-driven cybersecurity, has become both essential and challenging. Traditional security technologies often fall short in meeting the rigorous demands of users operating in open, heterogeneous, dynamic, mobile, distributed, and wireless environments. This growing complexity emphasizes the need for comprehensive frameworks that facilitate collaboration across diverse applications while maintaining stringent security standards and effectively addressing forensic and cybercrime concerns. The goal of this session is to bring together researchers and practitioners in the fields of security, cybersecurity, cyber defense, forensics, and cybercriminality prevention. The emphasis is on exploring and discussing new methods and techniques for designing secure systems and networks, with a special focus on forensic analysis, AI applied to cybersecurity, and counter-cybercrime measures. We encourage submissions that incorporate formal methods, as well as approaches that leverage AI, ML, DL, XAI, and NLP to advance the state of the art in forensic and cybersecurity solutions. Topics of interest include, but are not limited to:

- Cryptographic protocols
- Cryptography and cryptanalysis
- Quantum cryptography

- Formal methods for security and forensic verification
- AI applications in cybersecurity and forensic science
- Machine learning for threat detection and forensic analysis
- Network, hardware, and software security
- Biometric technologies and identity verification
- Intrusion and anomaly detection systems
- Security in web applications and forensics in digital crimes
- Privacy, trust, and anonymity frameworks
- Authentication, identity management, and access control
- Security architecture and design principles
- Wireless and mobile security
- Detection and moderation of toxic content on social networks
- Security concerns in 5G/6G networks
- Security for components, microelectronics, and antennas
- LiFi security mechanisms
- Security in robotic aerial systems and drones
- Autonomous vehicle security and forensic
- investigation tools for AI-driven cyber incidents
- Deep learning for cybersecurity analytics and malware forensics
- Explainable AI (XAI) for enhanced cybersecurity and forensic analysis
- Privacy in Data Retrieval
- Model Security in Knowledge Discovery
- Intellectual property protection in Data Mining
- Bias management in classification and learning

This session aims to serve as a platform for sharing insights and advancing security practices. By addressing the evolving challenges of forensic investigation, AI-driven threat detection, and cybercrime prevention, the session seeks to make a meaningful contribution to developing secure, intelligent, and resilient digital environments.

SUBMISSION

Papers must be submitted electronically for peer review through PaperCept by **February 07, 2025:** **http://controls.papercept.net/conferences/scripts/start.pl**. In PaperCept, click on the **CoDIT 2025 link "Submit a Contribution to CoDIT 2025" and follow the steps.**

IMPORTANT: All papers must be written in English and should describe original work. The length of the paper is limited to a maximum of 6 pages (in the standard IEEE conference double column format).

DEADLINES

February 07, 2025: deadline for paper submission
April 27, 2025: notification of acceptance/reject
May 17, 2025: deadline for final paper and registration