HP3C 2025

2025 9th International Conference on High Performance Compilation, Computing and Communications

2025年第九届高性能编译、计算和通信国际会议

June 18-20, 2025
Jinan, China

2025年6月18-20日
山东济南

SPECIAL SESSION 3: Cybersecurity and Forensics: Advancing Secure and Resilient Digital Systems

As communication networks grow increasingly complex, the demand for advanced theories, methodologies, and tools to ensure robust security—particularly in forensics and AI-driven cybersecurity—has become both critical and challenging. Conventional security technologies often fail to meet the stringent requirements of users operating in open, heterogeneous, dynamic, mobile, distributed, and wireless environments. This rising complexity highlights the necessity for comprehensive frameworks that support collaboration across diverse applications while maintaining high security standards and effectively addressing forensic and cybercrime challenges. This session aims to bring together researchers and practitioners in security, cybersecurity, cyber defense, forensics, and cybercrime prevention to explore and discuss innovative approaches for designing secure systems and networks. A particular emphasis is placed on forensic analysis, AI-driven cybersecurity solutions, and counter-cybercrime strategies. We invite submissions that incorporate formal methods as well as AI, machine learning (ML), deep learning (DL), explainable AI (XAI), and natural language processing (NLP) to advance forensic and cybersecurity capabilities.

TOPICS

- Cryptographic protocols and cryptanalysis
- Quantum cryptography
- Formal methods for security and forensic validation
- AI applications in cybersecurity and forensic science
- Machine learning for threat detection and forensic investigation
- Security in networks, hardware, and software
- Biometric authentication and identity verification
- Intrusion and anomaly detection systems
- Web security and digital crime forensics
- Privacy, trust, and anonymity frameworks
- Authentication, identity management, and access control
- Security architecture and design principles
- Wireless and mobile security
- Detection and moderation of harmful content on social networks
- Security challenges in 5G/6G networks
- Security in components, microelectronics, and antennas
- LiFi security mechanisms
- Security in robotic aerial systems and drones
- Autonomous vehicle security and forensic investigations
- AI-driven tools for cyber incident response
- Deep learning for cybersecurity analytics and malware forensics
- Explainable AI (XAI) for enhanced cybersecurity and forensic applications
- Data privacy in information retrieval

SPECIAL SESSION ORGANIZIERS

Associate Prof. Jaouhar Fattahi, Laval University, Québec, Canada
Prof. Mohamed Mejri, Laval University, Québec, Canada
Associate Prof. Ridha Ghayoula, Moncton University, New Brunswick, Canada

SUBMISSION INSTRUCTION

★ ★Please submit your manuscript to hp3c_conf@outlook.com by email and mark which special session. ★ ★

Template Paper: Word: http://hp3c.net/acm_template.docx
Template Paper: LaTex: http://hp3c.net/LaTeX-Templates.zip
Submission Instruction: http://hp3c.net/sub.html

Paper Submission Deadline:
March 5, 2025

Notification of Acceptance:
March 30, 2025

MAIN CONTACT PERSON

Name: Jaouhar Fattahi
Email Address: jaouhar.fattahi.1@ulaval.ca
Phone Number: 1-581-888-3258