callforpaper.org

France September 8-11, 2025

CONFERENCE WEBSITE: https://spritz.math.unipd.it/events/2025/CPS-Sec2025/CFP.html

About the Conference

With the rapid advancement of emerging technologies such as the Industrial Internet of Things (IIoT), artificial intelligence (AI), and large language models (LLMs), Cyber-Physical System (CPS) ecosystems are becoming increasingly dynamic and adaptive. CPS encompasses a wide array of intelligent devices, ranging from smartphones and tablets to industrial machinery, transportation infrastructure, medical devices, emergency response systems, power grids, and more. These systems are complexly interconnected, enabling automation, real-time monitoring, and control of both cyber and physical components. The integration of LLMs into CPS has significantly enhanced the capability of these systems by providing advanced data processing, natural language understanding, and autonomous decision-making.

The interconnected nature of CPS introduces significant challenges related to data security and privacy, system resilience, and protection against evolving cyber threats. Although, the integration of LLMs improves the efficiency of CPS, it also

Important Dates

SEP 08

CONFERENCE DATE

September 8-11, 2025

introduces new challenges related to data security, privacy, and system robustness. These challenges have profound implications for society and the economy. Ensuring the security of CPS is crucial to safeguarding these systems from cyber threats that could manipulate physical processes, disrupt operations, or pose safety hazards.

Building on the success of previous years, the 10th IEEE International Workshop on Cyber-Physical Systems Security (CPS-Sec 2025) aims to provide a premier platform for researchers and practitioners from industry and academia to discuss and address CPS security challenges. We invite innovative submissions that present practical and theoretical solutions to cybersecurity issues within CPS. Example topics of interest are given below, but are not limited to:

● Secure CPS architectures and protocols
● Authentication mechanisms for CPS
● Access control and anonymization for CPS
● Blockchain applications for CPS
● Data security and privacy for CPS
● Forensics for CPS
● Intrusion detection for CPS
● Energy-efficient and secure CPS
● Availability, recovery, and auditing for CPS
● Distributed secure solutions for CPS
● Threat modelling for CPS
● Security of CPS in automotive systems
● Security of CPS in medical devices/systems ● AI-driven security solutions for CPS
● Generative AI for CPS security
● Adversarial AI for CPS
● Defense mechanisms against adversarial AI for

CPS

- Usage of LLMs for security and threat detection/analysis in CPS
- Human-machine interaction and natural language interfaces in CPS
- Privacy-preserving techniques for CPS data
- Cyber-physical threat intelligence and information sharing
- Security testing and validation for CPS

TOPICS OF INTEREST

2 topics

Research papers are invited in, but not limited to, the following areas:

- Uncategorized
- Cybersecurity & Privacy