Special track on Secure AI co-located in IEEE BDS 2026

July 27-30, 2026, Fukuoka, Japan

Artificial Intelligence (AI)-driven technologies have continued to proliferate across every sector, including healthcare, finance, transportation, education, and more, and are increasingly embedded in our daily lives. As a result, making decisions for such autonomous systems may have significant consequences, often without human intervention. While these advancements bring efficiency and innovation, they also raise critical concerns around security, privacy, and ethical accountability. As the human role in decision-making is progressively reduced, it becomes imperative to treat AI security and privacy not as afterthoughts, but as core design principles. AI systems are susceptible to a range of threats, including adversarial attacks, data poisoning, model extraction, and behavioral manipulation. Simultaneously, they can pose privacy risks through unintended information leakage, the misuse of personal data, or a lack of transparency in decision-making logic. These issues not only compromise system integrity but can also erode public trust in AI.

This track is part of IEEE CISOSE Congress. The SecAI conference aims to foster interdisciplinary discussion and explore novel approaches that address the pressing challenges at the intersection of AI security, privacy, and ethics. By bringing together researchers, practitioners, and policymakers, this symposium seeks to deepen understanding and stimulate collaboration toward the development of robust, trustworthy, and ethically aligned AI systems.

Topics of Interest

AI security and privacy

- Adversarial machine learning
- Distributed/federated learning
- Machine Unlearning
- AI approaches to trust and reputation
- AI misuse (e.g., misinformation, deepfakes)
- Machine learning and computer security

AI security and privacy

- Privacy-enhancing technologies, anonymity, and censorship (e.g., Differential privacy in AI)
- Security and privacy of Large Language Models (LLMs)
- Secure Large AI Systems and Models
- Large AI Systems and Models' Privacy and Security Vulnerabilities
- Copyright of AI
- AI, surveillance, and privacy

Important Dates

- **April 1, 2026** Paper submission deadline
- **May 20, 2026** Notification of acceptance
- **June 15, 2026** Final paper submission (camera-ready)
- **July 27 to July 30, 2026** Conference dates

Submission

Submit original manuscripts (not published or submitted elsewhere) with the following page limits: **regular papers (8 pages), short papers (4 pages), AI testing in practice (8 pages), and tool demo track (6 pages)**. We welcome submissions of both regular research papers that describe original and significant work or reports on case studies and empirical research and short papers that describe late-breaking research results or work in progress with timely and innovative ideas. All types of papers can have 2 extra pages subject to page charges. The AI Testing in Practice Track provides a forum for networking, exchanging ideas and innovative or experimental practices to address SE research that directly impacts the practice of software testing for AI. The tool track provides a forum to present and demonstrate innovative tools and/or new benchmarking datasets in the context of software testing for AI. All papers must be written in English. Papers must include a title, an abstract, and a list of 4-6 keywords. All papers must be prepared in the IEEE double-column proceedings format. Authors submit their papers via the link by **April 1, 2026, 23:59 AoE**. For more information, please visit the conference website. The use of content generated by AI in an article (including but not limited to text, figures, images, and code) shall be disclosed in the acknowledgments section of the submitted article.

Conference Proceedings & Special Section of SCI journals

All accepted papers will be published by IEEE Computer Society Press (EI-Index) and included in the IEEE Digital Library. The best papers will be invited to submit an extended version (with at least 30% novel content) to the selected special issues (TBA).

Committees

Track Chairs:

- Monowar Bhuyan, Umeå University, Sweden
- Michele Carminati, Politecnico di Milano, Italy

Web Chair:

- Adil Bin Bhutto, Umeå University, Sweden

General Inquiries

For more detailed and updated information, please refer to the conference website. For paper submission, review, or other questions, please send emails to michele.carminati@polimi.it