Proceedings of

The 1st International Workshop on Security and Privacy-Preserving AI/ML

SPAIML 2025

co-located with

The 28th European Conference on Artificial Intelligence
ECAI 2025

Bologna, Italy
October 26th, 2025

Workshop Organization

Organizers

Jens Leicht	University of Duisburg-Essen, Germany
Malte Josten	University of Duisburg-Essen, Germany

Technical Program Committee

Holger Schmidt	Dortmund University of Applied Sciences and Arts, Germany
Kimberly Cornell	University of Albany, USA
Lorenz Schwittmann	Independent Researcher, Germany
Maritta Heisel	University of Duisburg-Essen, Germany
Meiko Jensen	Karlstad University, Sweden
Nicolas Diaz-Ferreyra	Hamburg University of Technology, Germany
Oliver Hahm	Frankfurt University of Applied Sciences, Germany
Razvan Beuran	Japan Advanced Institute of Science and Technology, Japan
Simone Fischer-Hübner	Karlstad University, Sweden
Steffen Bondorf	Ruhr University Bochum, Germany
Stephan Sigg	Aalto University, Finland
Torben Weis	University of Duisburg-Essen, Germany
Vadim Safronov	University of Oxford, UK
Zoltán Mann	University of Halle, Germany

Editors

Jens Leicht	University of Duisburg-Essen, Germany
Julien Lukasewycz	University of Duisburg-Essen, Germany
Malte Josten	University of Duisburg-Essen, Germany
Torben Weis	University of Duisburg-Essen, Germany

https://spaiml.com/2025

Preface

The workshop focuses on the transformative potential of AI/ML technologies in addressing key challenges in security and privacy across diverse domains. In an era of increasing digitalization and interconnectedness, organizations face evolving threats, from sophisticated cyberattacks to complex data privacy concerns. Traditional methods often struggle to adapt to the dynamic nature of these challenges, particularly in scenarios requiring real-time analysis, anomaly detection, and large-scale data management. AI/ML presents a paradigm shift by enabling intelligent, scalable, and proactive approaches to security and privacy. For instance, machine learning models can detect patterns in network traffic indicative of cyberattacks, while AI-driven solutions can enable privacy-preserving data processing through federated learning or differential privacy techniques. By focusing on how AI/ML can be harnessed to safeguard sensitive data and systems across various domains, this workshop aims to advance the state of the art in security and privacy.

This year's workshop (`https://spaiml.com/2025`) took place on October 26th, 2025 in conjunction with the 28th European Conference on Artificial Intelligence (`https://www.ecai2025.org/`) in Bologna, Italy.

The double-blind review process involved 14 PC members whose affiliations came from 6 different countries: Finland (1), Germany (8), Japan (1), Sweden (2), United Kingdom (1), USA (1). We received a total of 10 submissions from authors based in 9 different countries: Austria (1), Finland (1), Germany (4), Italy (4), Japan (4), Netherlands (6), Sweden (2), United Kingdom (6), United States (4). Out of these 10 submissions, 7 were accepted for presentation at the workshop and inclusion in these proceedings as regular papers.

In addition to two paper sessions, this year's workshop hosted a keynote by Victor Morel, titled "Should I Trust It With My Data? Capabilities, Limits, and Perspectives of AI Technologies for Privacy."

We want to thank all authors for their submissions, the PC members for their efforts in reviewing the papers, and the keynote speaker for their inspiring talk.