8th Dependable and Secure Machine Learning (DSML) Workshop

Co-located with the 55th IEEE/IFIP DSN 2025

June 23, 2025 | Naples, Italy

Website: https://dependablesecureml.github.io

Important Dates (AOE)

Website Open:	2/5/2025
Paper Submission:	3/31/2025
Notification of Acceptance:	4/30/2025
Camera Ready:	5/10/2025

The DSN Workshop on Dependable and Secure Machine Learning (DSML) is an open forum for researchers, practitioners, and regulatory experts, to present and discuss innovative ideas and practical techniques and tools for producing dependable and secure machine learning (ML) systems. A major goal of the workshop is to draw the attention of the research community to the problem of establishing guarantees of reliability, security, safety, and robustness for systems that incorporate increasingly complex ML models, and to the challenge of determining whether such systems can comply with the requirements for safety-critical systems. A further goal is to build a research community at the intersection of machine learning and dependable and secure computing.

Topics of Interest:

- Testing, certification, and verification of systems that incorporate ML models (including both software and hardware)
- Metrics for benchmarking the dependability and security of ML systems
- Adversarial machine learning (an emphasis will be put on defenses)
- Resilient and repairable ML models and algorithms, including mechanisms for failsafe defaults and smooth degradation of performance
- Safety, robustness, and alignment of ML systems
- Interpretability, explainability, and transparency of ML systems
- Reliability/ security of ML architectures, comp. platforms, and distributed system
- Faults in the implementation of ML algorithms and their consequences
- Dependability of ML accelerators and hardware platforms

Submissions:

DSML welcomes both research papers reporting results from mature work, and more speculative papers describing new ideas with preliminary exploratory work. Papers reporting industry experiences, case studies, and datasets will also be encouraged. This year, we are also soliciting proposals for research talks based on work previously published elsewhere (reference to previous work is required). We strongly encourage these research talks to also include new ideas and provocative opinions and not just summarize previous work that is already published. Specifically, we accept submissions in the following formats:

- Regular research papers (up to 6 pages + 3 pages for references and appendix)
- Proposals for research talks (1 page + 3 pages for references and appendix)

All submissions should be in PDF format and must adhere to the IEEE Computer Society 8.5x11 two-column camera-ready format (using a 10-point font on 12-point single-spaced leading).

We will use a **double-blind** review process **only for the regular research papers**, so the authors must anonymize their submissions. The first page must include the title of the paper, but no information on authors names and affiliations. Research talks need not be anonymous.

Submission site: https://dsml25.hotcrp.com/

General and PC Chairs

Xugui Zhou, Louisiana State Univ.
Yangsibo Huang, Google NYC

Steering Committee

Homa Alemzadeh, Univ. of Virginia
Rakesh Bobba, Oregon State Univ.
Varun Chandrasekaran, Microsoft Research & UIUC
David Evans, Univ. of Virginia
Nicolas Papernot, Univ. of Toronto & Vector Institute
Karthik Pattabiraman, UBC
Lishan Yang, George Mason Univ.

Program Committee

Elias Bou-Harb, Louisiana State Univ.
Sai Sree Laya Chukkapalli, IBM
Aolin Ding, Accenture Labs
Bo Fang, Pacific NW National Lab
Hanqing Guo, Univ. of Hawai‘i at Mānoa
Junfeng Guo, Univ. of Maryland at College Park
Sihong He, UT Arlington
Fanxin Kong, Univ. of Notre Dame
Igibek Koishybayev, Qualcomm
Linyi Li, Simon Fraser Univ.
Yan Long, Univ. of Virginia
Fumio Machida, Univ. of Tsukuba
Jing Ma, CWRU
Uttam Thakore, Meta
Ning Wang, Univ. of South Florida
Wenpeng Wang, Apple
Honghui Xu, Kennesaw State Univ.
Hui Xu, Fudan Univ.
Zongxing Xie, Kennesaw State Univ.
Shaohu Zhang, UNC Pembroke
Yanfu Zhang, College of W&M

Join us in Naples, Italy, for DSML 2025!