New Frontiers in Adversarial Machine Learning

ICML 2022 Workshop

July 22 (In-person)

Baltimore, MD, USA

Website: https://advml-frontier.github.io

Topics of interest:

- **Adversarial ML Theories:** foundations; Metrics and their interconnections; Neurobiology-inspired foundations.
- **Adversarial ML Algorithms:** New optimization methods; Data foundations; Scalability on the edge & distributed systems.
- **Adversarial ML Applications:** New use cases; Adversarial ML for good.

Call for papers:

- **Full paper submission track: 6 pages** with unlimited references or supplementary materials.
- **Blue Sky Ideas submission track: 2 pages** targeting the high-risk, high-reward research ideas on adversarial ML.

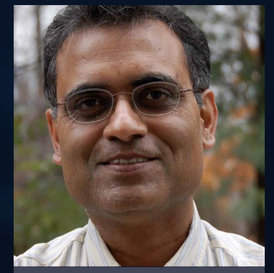
Important Dates:

- Submission deadline: May 23rd, 2022
- Notification to authors: June 13th, 2022
- Camera ready deadline: July 8th, 2022
- Conference: July 22nd, 2022
- Submission: **AdvML Frontiers 2022 @ ICML 2022**

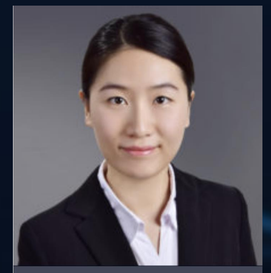
Keynote Speakers

Somesh Jha
University of Wisconsin, Madison, USA

Aleksander Madry
Massachusetts Institute of Technology, USA



Atul Prakash
University of Michigan, USA



Changliu Liu
Carnegie Mellon University, USA

Celia Cintas
IBM Research Africa, Kenya

Ajmal Mian
The University of Western Australia, Australia

Battista Biggio
University of Cagliari, Italy

Joel Dapello
Harvard University, USA

Nitesh Chawla
University of Notre Dame, USA