NeurIPS-20 Workshop on Scalability, Privacy, and Security in Federated Learning (SpicyFL 2020)

General Chairs
Dejing Dou, Baidu Research and University of Oregon
Xiaolin Andy Li, Cognization Lab and Tongdun Technology
Ameet Talwalkar, Carnegie Mellon University and Determined

Program Chairs
Hongyu Li, Tongdun Technology
Jianzong Wang, Ping An Technology
Yanzhi Wang, Northeastern University

Panel Chairs
Yurong Chen, Intel Research
Jie Liu, Harbin Institute of Technology (Shenzhen)
Lingfei Wu, IBM Research

Award Chairs
Dimitris Papailiopoulos, University of Wisconsin-Madison
Dapeng Wu, University of Florida

Publicity Chairs
Dan Meng, Tongdun Technology
Xiaoyong Yuan, Michigan Technological University

Web Chairs
Hong Wang, Tongdun Technology
Yanlin Zhou, University of Florida

Invited Speakers
- John C. Duchi, Assistant Professor, Stanford University
  - ONR YIP, NSF CAREER Award
- H. Brendan McMahan, Senior Staff Research Scientist
  - Google Research, Pioneer of Federated Learning
- Ruslan Salakhutdinov, UPMC Professor, CMU
  - Director of AI Research, Apple; Sloan Fellow
- Virginia Smith, Assistant Professor, CMU
  - Carnegie Bosch Institute and Google Faculty Award
- Dawn Song, Professor, UC Berkeley
  - MacArthur Fellow
- Tao Yang, Professor, UCSB
  - Former Chief Scientist and SVP for ASK
- Tong Zhang, Professor, HKUST
  - Former Director of AI Lab, Tencent

In the recent decade, we have witnessed rapid progress in machine learning in general and deep learning in particular, mostly driven by tremendous data. As these intelligent algorithms, systems, and applications are deployed in real-world scenarios, we are now facing new challenges, such as scalability, security, privacy, trust, cost, regulation, and environmental and societal impacts. Meanwhile, data privacy and ownership has become more and more critical in many domains, e.g., finance, health, government, and social networks. Federated learning (FL) has emerged to address data privacy issues. To make FL practically scalable, useful, efficient, and effective on security and privacy mechanisms and policies, it calls for joint efforts from the community. Challenges, interplays, and tradeoffs in scalability, privacy, and security need to be investigated in a more holistic manner by the community. We are expecting broader, deeper, and greater evolution of these concepts and technologies, and confluence towards holistic trustworthy AI ecosystems.

This workshop provides an open forum for researchers, practitioners, and system builders to exchange ideas and shape roadmaps towards scalable and privacy-preserving federated learning and scalable and trustworthy AI.

Topics of Interest
- System scalability, reliability, and robustness in FL
- Data, model, and knowledge scalability, compression, distillation in FL
- Data, model, and knowledge privacy in FL
- Data, network, knowledge, and system security in FL
- Trustworthy assessment, audit, and verification in FL
- Holistic design and resource management of FL algorithms and systems
- Secure multi-party computation, learning, and reasoning
- Scalability, privacy, and security in knowledge federation
- Use cases and practices in real-world applications
- Theoretical and economic analysis of FL systems
- Attacks and defenses mechanisms and policies
- Valuation, reward, and penalty algorithms, assessment, arbitration, and regulations
- Scalable and trustworthy AI ecosystems
- General federated learning and distributed ML/DL

Paper Submission Guidelines

Submissions can be up to 6 pages (excluding references). All accepted papers will be presented as posters; some may be selected for highlights or contributed talks, depending on schedule constraints. Accepted papers will be posted on the workshop website. Please note that submissions should be anonymous, and will undergo double-blind peer review. Please follow the guidelines in the NeurIPS 2020 LaTeX style file. The final submission must be in PDF. Please submit your papers via EasyChair:https://easychair.org/conferences/?conf=spicyfl2020. Please contact us at spicyfl2020@easychair.org.

Important Dates

Submission Due	Oct 12, 2020
Notification	Oct 30, 2020
Camera-ready	Nov 10, 2020