ResilientFL: Workshop on Systems Challenges in Reliable and Secure Federated Learning

Co-located with ACM SOSP 2021

Saurabh Bagchi
Purdue University

PURDUE
UNIVERSITY

October 25, 2021

What It Is?

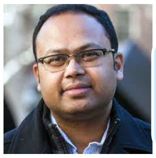
- A rich and fast growing body of work in federated learning, some of which is focused on reliability and security
- This workshop attempts to:
  - Look at budding work at the intersection of systems, FL, and resilience
  - Provide a unifying perspective on resilience in FL
  - Bring together parts of the ML, security, and systems communities

Who We Are

Saurabh Bagchi (Purdue)

Tom Jacobs (Adobe Research)

Kevin Chan (Army Research Lab)



Suman Jana (Columbia University)

Christof Fetzer (TU Dresden)

Prateek Mittal (Princeton University)

What Happened?

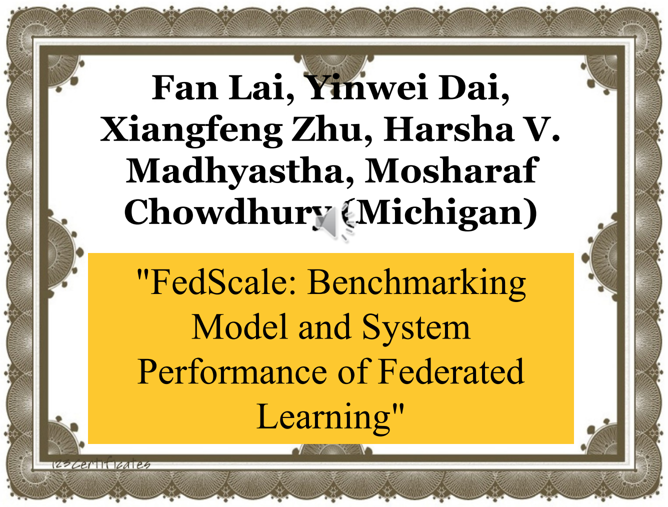
- Mix of invited papers/talks and peer-reviewed papers
- 9 peer-reviewed submissions
- We accepted 6 papers
  - Based on 2-3 reviews per submission
  - Represents 10 institutions
  - One paper has 4 affiliations from 3 countries
  - Aghiles Ait Messaoud (ESI, Algeria), Vlad Nitu (INSA Lyon), Valerio Schiavoni (University of Neuchatel, Switzerland), Sonia Ben Mokhtar (LIRIS-CNRS, France), "GradSec: a TEE-based Scheme Against Federated Learning Inference Attacks"

What's Happening

- A day-long program with

1. 6 peer-reviewed papers
2. 5 invited talks: 3 from industry, 2 from academia
   – Dinesh Verma (IBM Watson), Reza Shokri (NUS), Do Le Quoc (Huawei Research), Andrea Olgiati (AWS), Neil Gong (Duke)
3. A heated panel: "FL security: Old wine in new bottle, or NWNB?"
   – Panelists: Salman Avestimehr (USC), Ameet Talwalkar (CMU), Shiva Kasiviswanathan (Amazon), Gerome Bovet (Armasuisse)

The Award Winner



Fan Lai, Yinwei Dai, Xiangfeng Zhu, Harsha V. Madhyastha, Mosharaf Chowdhury (Michigan)

"FedScale: Benchmarking Model and System Performance of Federated Learning"

123certificates

It Takes a Village

- Manos Kapritsos, U of Michigan, as Workshop Chair of SOSP
- ***Theory/Applied ML***
  Yin Li, University of Wisconsin at Madison
  Rachid Guerraoui, EPFL
  Shiqiang Wang, IBM
  Salman Avestimehr, University of Southern California
  Saeed Mahloujifar, Princeton University
- ***Systems***
  Baishakhi Ray, Columbia University
  Brendan McMahan, Google Research
  Ivan Beschastnikh, University of British Columbia
  Michael Reiter, Duke University
  Neil Gong, Duke University
  Reza Shokri, National University of Singapore
- ***Applications***
  Somali Chaterji, Purdue University
  Gerome Bovet, Armasuisse
  Erin Hestir, University of California at Merced
  Shiv Saini, Adobe