



# USC+Amazon Center Kick-off Meeting

# **Opening Remarks**

## Salman Avestimehr



**USC+Amazon Center on Trusted AI** 







## **Center Administrations**

**Director:** Salman Avestimehr

Liaison for Amazon: Prem Natarajan

### **Advisory Board Members**

- Shrikanth Narayanan, Cyrus Shahabi and Kristina Lerman (USC)
- Shankar Anathakrishnan, Arindam Mandal and Shiv Vitaladevuni (Amazon)

Advisor from Dean's VSOE office: Assad Oberai and Mahta Moghaddam

Administrative Program Managers: Ariana Perez (USC), Rajiv Dhawan (Amazon, Avni Fein (Amazon)

Website, USC + Amazon Center on Secure & Trusted ML





## **Project Selection Process**

**Call for proposals:** Each year, through a competition process, the Center will provide support for several research projects focused on the development of new methodologies for secure and privacy-preserving machine learning solutions. The Center will also provide annual fellowships to doctoral students working in this research area, enabling them to advance research frontiers. Fellowship recipients will be named as Amazon ML Fellows in recognition of their promise and achievements. In addition to funded research projects and annual fellowships for doctoral students, the collaborators will host an annual joint public research symposium to share their knowledge with the machine learning and AI communities.

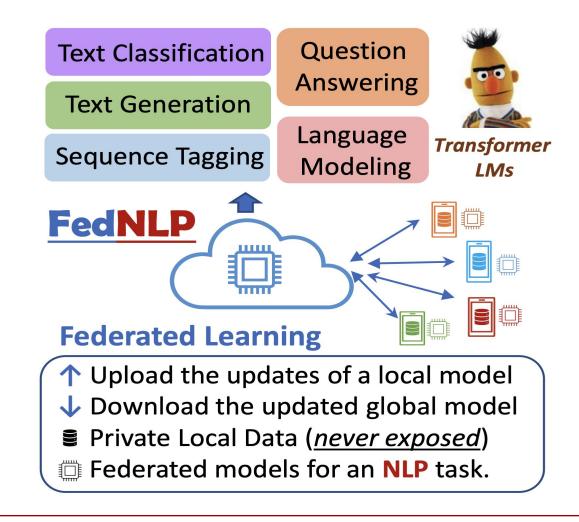
Proposals received: due date: March 22, 2021
New projects start date: July 2021-July 2023
Review process: All proposals were evaluated by an advisory committee composed of 2 USC faculty and 2 researchers from Amazon.
Results: Five research projects were selected for 2021-2022.





## Federated Learning for Natural Language Processing

Xiang Ren and Mahdi Soltanolkotabi

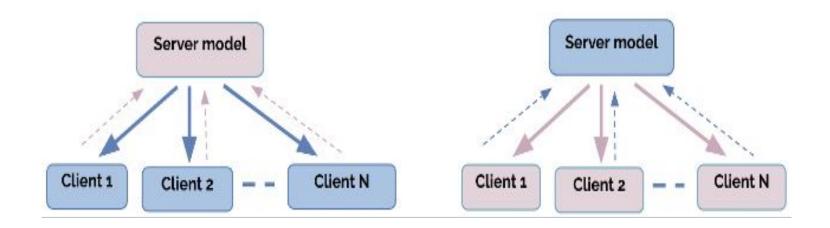






## Federated Learning for Human-centered Experience and Perception Modeling with Biobehavioral Data

Shrikanth Narayanan

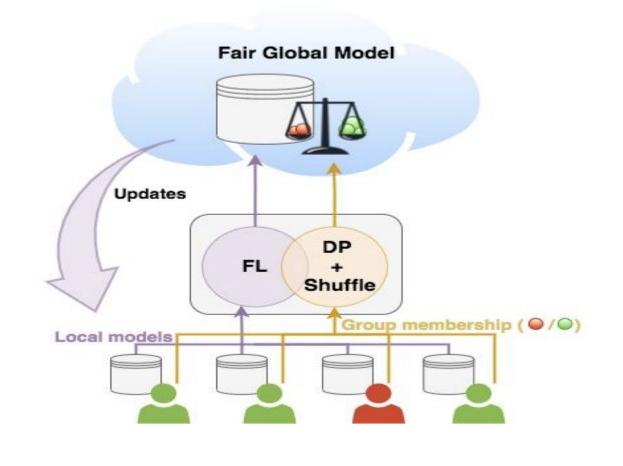


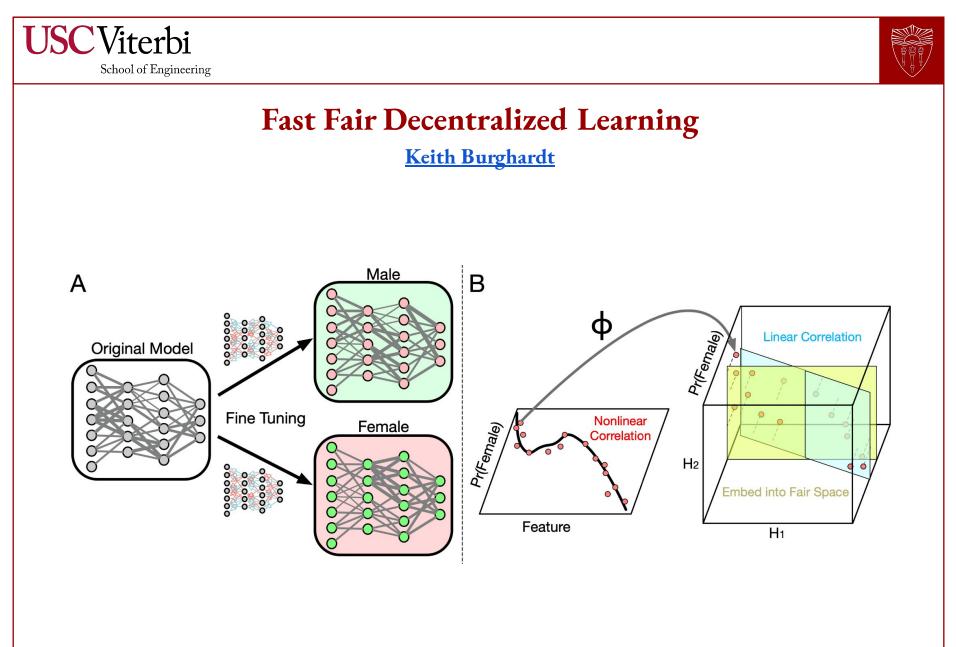




### **Reconciling Privacy and Fairness in Federated Learning**

<u>Aleksandra Korolova & Marc Juarez</u>









#### Efficient Federated Learning in Heterogeneous and **Corrupted Environments by Secure Performance Weighting** Jose Luis Ambite, Muhammad Naveed, and Paul Thompson MWca MW. **Caching Tier** MW Encrypted Federation Controller Computation $W_{c} = \frac{1}{N_{c}} \sum h_{c} W_{b}$ **Community Tier** R7: VScore. R6: VScore, $R1: W_{1}^{t_{1}}$ R5: VScore, Model Exchange Tier Encrypted R2: W! Transmission R4: W R3: W9 R8: W Trainer Trainer Trainer aluator Evaluator valuator Learners Tier 3 181 10 .... **Training Set Training Set Training Set** didation Set Encrypted Encrypted Encrypted Computation. Computation Computation Data Tier





## **Collaborators from the Amazon side**

Funded Programs	USC Lead(s)	Amazon POC
Efficient Federated Learning in Heterogeneous & Corrupted Environments by Secure Performance Weighting	Jose Luis Ambite, Muhammad Naveed & Paul Thompson	Tanya Roosta (troosta@)
Fast Fair Decentralized Learning	Keith Burghardt	Peng Liu (liupng@), Tao Zhang (taozhng@)
Federated Learning for Human-centered Experience and Perception Modeling with Biobehavioral Data	Shrikanth Narayanan	Rahul Gupta (gupra@) & Anil Ramakrishna (aniramak@)
Federated Learning for Natural Language Processing	Xiang Ren & Mahdi Soltanolkotabi	Christophe Dupuy (dupuychr@)
Reconciling Privacy and Fairness in Federated Learning	Aleksandra Korolova & Marc Juarez	Shuang Wu (wushuan@), Tao Zhang (taozhng@)





## **PhD Fellowship Selection**

**Call for proposals:** Each year, through a competition process, the Center will provide support for several research projects focused on the development of new methodologies for secure and privacy-preserving machine learning solutions. The Center will also provide annual fellowships to *three* doctoral students working in this research area, enabling them to advance research frontiers. Fellowship recipients will be named as *Amazon ML Fellows* in recognition of their promise and achievements. In addition to funded research projects and annual fellowships for doctoral students, the collaborators will host an annual joint public research symposium to share their knowledge with the machine learning and AI communities. We hereby invite USC faculty to nominate qualifying PhD students for 2021-2022 Amazon ML Fellowships.

Nominations received: due date April 12, 2021

**Selection process:** All nominations were evaluated by the advisory committee composed of USC faculty and researchers from Amazon.

Results: Two Ph.D. Fellows were selected for 2021-2022.





## Distributed/Federated Learning Chaoyang He







## **Towards Trustworthy AI**

<u>Ninareh Mehrabi</u>







### **Plans for Future Events**

## Fall 2021

• Kick-off Virtual Meeting: Friday, September 24 from 9:00-1:00pm PT

## Spring 2022

- **Symposium:** March/April
- Workshop: Jan/Feb, early 2022

### USC+Amazon Center Kick-off Meeting

Friday, September 24 9:00 a.m. - 1:00 p.m. Pacific time

Zoom: https://usc.zoom.us/j/92435252005 Password: 155014

9:00 a.m. - Opening Remarks: Salman Avestimehr (Director of USC-Amazon Center) and Prem Natarajan (USC-Amazon Center Liaison)

**9:15 a.m.** -Federated Learning for Human-centered Experience & Perception Modeling with Biobehavioral Data, Shrikanth Narayanan. (Professor of Electrical & Computer Engineering, Computer Science)

9:45 a.m. - Reconciling Privacy and Fairness in Federated Learning, Aleksandra Korolova (Assistant Professor of Computer Science) and Marc Juarez (Postdoctoral Scholar)

10:15 a.m. - Distributed/Federated Learning for NLP, Chaoyang He. (Ph.D. student, Amazon ML Fellow)

10:45 a.m. - Fast Fair Decentralized Learning, Keith Burghardt (Computer Scientist, ISI)

11:15 a.m. - 15 Minute Break

11:30 a.m. - Federated Learning for Natural Language Processing, Xiang Ren (Assistant Professor of Computer Science) and Mahdi Soltanolkotabi (Associate Professor of Electrical and Computer Engineering, Computer Science)

12:00 p.m. - Efficient Federated Learning in Heterogeneous & Corrupted Environments by Secure Performance Weighting, Jose Luis Ambite, (Associate Research Professor, Computer Science) Muhammad Naveed, (Assistant Professor of Computer Science) and Paul Thompson (Professor of Engineering)

12:30 p.m. - Towards Trustworthy AI, Ninareh Mehrabi (Ph.D. student, Amazon ML Fellow)