Join via Zoom and Youtube http://www.inmc.snu.ac.kr

ABSTRACT:

Federated learning (FL) is a promising framework for enabling privacy preserving machine learning across many decentralized users. Its key idea is to leverage local training at each user without the need for centralizing/moving any device's dataset in order to protect users' privacy.
In this talk, I will highlight several exciting research challenges for making such a decentralized system trustworthy and scalable to a large number of resource-constrained users.
In particular, I will discuss three directions:
(1) resilient and secure model aggregation, which is a key component and performance bottleneck in FL; (2) FL of large models, via knowledge transfer, over resource-constrained users; and (3) FedML, our open-source research library and benchmarking ecosystem for FL research (fedml.ai).

SEOUL NATIONAL UNIVERSITY
INSTITUTE OF NEW MEDIA AND COMMUNICATIONS

SHARING TUNNON COLLOQUIUM

May 14th (Fri) 1pm :

Trustworthy and Scalable Federated Learning

Prof. Salman Avestimehr

USC, Director of the USC-Amazon Center
on Secure and Trusted Machine Learning (Trusted AI)

Salman Avestimehr is a Dean's Professor, the inaugural director of the USC-Amazon Center on Secure and Trusted Machine Learning (https://trustedai.usc.edu), and the director of the Information Theory and Machine Learning (vITAL) research lab at the Electrical and Computer Engineering Department of University of Southern California. He is also an Amazon Scholar at Amazon/Alexa-AI. He received his Ph.D. in 2008 in Electrical Engineering and Computer Science from the University of California. His research interests include information theory, machine learning, distributed computing, and secure and private learning/computing.

Dr. Avestimehr has received a number of awards for his research and teaching, including the James L. Massey Research & Teaching Award from IEEE Information Theory Society, an Information Theory Society and Communication Society Joint Paper Award, a Presidential Early Career Award for Scientists and Engineers (PECASE) from the White House (President Obama), a USC Mentoring Award, a Young Investigator Program (YIP) award from the U. S. Air Force Office of Scientific Research, a National Science Foundation CAREER award, the David J. Sakrison Memorial Prize from UC Berkeley EECS Department, and several Best Paper Awards at Conferences. He has been an Associate Editor for IEEE Transactions on Information Theory and a general Co-Chair of the 2020 International Symposium on Information Theory (ISIT). He is a fellow of IEEE.