ISTeC
The Information Science and Technology Center

COLORADO STATE UNIVERSITY

Distinguished Lectures

Spring 2024

Dr. Ling Liu

Professor
School of Computer Science
Georgia Institute of Technology

From Centralized Learning to Federated Learning: Opportunities and Challenges

Monday, April 29, 2024
Reception with Refreshments: 10:30 AM
Lecture: 11:00 AM - 12:00 noon.
CSB 130

Security and Privacy in Federated Learning

Monday, April 29, 2024
Lecture: 2:00-3:00 PM
Lory Student Center 324

Sponsored by
Colorado State University's Information Science and Technology Center (ISTeC)

In conjunction with the Department of Computer Science, and Department of Electrical and Computer Engineering Seminar Series

Abstracts

From Centralized Learning to Federated Learning: Opportunities and Challenges

Machine learning has blossomed through (centralized) learning over massive data, evidenced by recent advances in self-supervised multi-modal learning and generative AI powered large language models (LLMs). Most of the benchmark datasets are publicly available data sources and can be freely collected to a centralized Cloud repository to train large models, such as ChatGPT, LLaMA. However, for the missions-critical applications in the real world, massive proprietary data are generated 24x7 at the edge of the Internet. Centralized collection of such geographically distributed and proprietary datasets is neither feasible nor realistic w.r.t. resource / latency demand and data privacy / confidentiality requirement. In this distinguished lecture, I will illustrate the potential of self-supervised learning and generative AI, and discuss two important technological advancements in Generative AI, which aim to scale the training and the deployment of large models on the edge. First, we will describe and compare a suite of large model reduction techniques for large foundation models and their fine-tuning of downstream learning tasks. Second, we will introduce Federated learning (FL), an emerging distributed learning paradigm, enabling joint training of a large global model by a distributed population of edge clients, while keeping their sensitive data local and only share their local model updates with the FL server(s). I will conclude with an outlook of generative AI and LLMs.

Security and Privacy in Federated Learning

We have witnessed two existing trends of computing: one is the rapid advances in AI technology fueled by recent generative AI and Large Language Models (LLMs), and the other is the new world of device-edge-cloud computing continuum. These two emerging trends are urging the synergistic alliances of AI and cyber-security in both research and development of next generation of AI-powered device-edge-cloud computing systems. In this talk, I will first discuss privacy and security vulnerabilities in federated learning. Then I will describe the state of the art (SOTA) trustworthy AI methods and techniques against data and model trojan attacks and privacy leakage risks, including lessons learned from our trustworthy AI research projects. I will conclude with an outlook of security and privacy challenges in the rapid growth of generative AI and LLMs.

Speaker Biography

Ling Liu is a full Professor in the School of Computer Science at Georgia Institute of Technology. She directs the research programs in the Distributed Data Intensive Systems Lab (DiSL), examining various aspects of big data-powered artificial intelligence (AI) systems, and machine learning (ML) algorithms and analytics, including performance, availability, privacy, security, and trust. Prof. Liu is an elected IEEE Fellow, a recipient of IEEE Computer Society Technical Achievement Award (2012), and a recipient of the best paper award from numerous top venues, including IEEE ICDCS, WWW, ACM / IEEE CCGrid, IEEE Cloud, IEEE ICWS. Prof. Liu served on editorial board of over a dozen international journals, including the editor in chief of IEEE Transactions on Service Computing (2013-2016). Currently, Prof. Liu is the editor in chief of ACM Transactions on Internet Computing (since 2019) and the chair of IEEE CS Fellow Evaluation Committee (FY2024). Prof. Liu is a frequent keynote speaker in top-tier venues in Big Data systems, AI / ML systems and applications, Cloud Computing, Services Computing, Privacy, Security and Trust. Her current research is primarily supported by USA National Science Foundation under CISE programs, CISCO and IBM

ISTeC (Information Science and Technology Center) is a university-wide organization for promoting, facilitating, and enhancing CSU's research, education, and outreach activities pertaining to the design and innovative application of computer, communication, and information systems. For more information please see ISTeC.ColoState.edu.

To arrange a meeting with the speaker, please contact Prof. Indrakshi Ray <Indrakshi.Ray@colostate.edu>.