STEVENS
INSTITUTE OF TECHNOLOGY
1870

Ph.D. DISSERTATION DEFENSE

Candidate:	Zhuosheng Zhang
Degree:	Doctor of Philosophy
School/Department:	Department of Electrical and Computer Engineering
Date:	Tuesday, December 12, 2023
Time/Location:	11:00 am / https://stevens.zoom.us/j/96005852449
Title:	Enhancing Security And Efficiency In Distributed Learning
Chairperson:	Dr, Shucheng Yu, Department of Electrical and Computer Engineering, Charles V. Schaefer, Jr. School of Engineering and Science
Committee Members:	Min Song, Department of Electrical and Computer Engineering, Charles V. Schaefer, Jr. School of Engineering and Science Koduvayur Subbalakshmi, Department of Electrical and Computer Engineering, Charles V. Schaefer, Jr. School of Engineering and Science Jie Shen, Department of Electrical and Computer Engineering, Charles V. Schaefer, Jr. School of Engineering and Science

ABSTRACT

The emergence of next-generation communications and computing paradigms such as edge computing has made distributed learning, a multinode machine learning system designed to improve performance, increase accuracy, and scale to larger input data sizes, increasingly popular in emerging applications. Depending on the level of user privacy protection, distributed learning can be categorized into centralized learning, where users upload all data to a central server, distributed learning with the exchange of model parameters, where users reveal model parameters to other users or the server, and distributed learning with the exchange of soft-decisions, where users only need to exchange distilled knowledge with each other. While different learning systems offer distinct advantages and encounter specific challenges, security and efficiency are crucial and common challenges in designing distributed learning systems. This thesis begins by exploring security threats in distributed learning and subsequently focuses on two representative frameworks, federated learning and distributed distillation, each providing different levels of privacy guarantees. New designs are proposed to enhance the efficiency and security of these learning frameworks.