

I have been working towards holistically addressing real-world bottlenecks in large-scale distributed computing, including federated learning. My [projects](#) are broadly classified into the following three exciting paradigms:

- **Privacy-Preserving and Robust Machine Learning at the Edge:** In many machine learning applications, private training data is distributed across multiple users, such as patient records at multiple hospitals, giving rise to the following multi-dimensional problem: How can individual users jointly train an ML model while (1) keeping their individual datasets private; (2) exploiting the heterogeneity of data across users; and (3) being resilient against straggling and malicious users. For example, a key difficulty in mitigating malicious users when data is non-IID across users is that even the updates from non-malicious users are quite diverse, hence prior outlier based strategies perform poorly. My focus has been to resolve this conundrum both in the federated learning setting (where a central server orchestrates the training), as well as in the serverless decentralized training setting.
- **Efficient Large-Scale Distributed Learning in the Cloud:** In large-scale training tasks, such as pre-training of NLP models with billions of parameters (e.g., GPT-3), straggling nodes adversely impact the performance by increasing the tail latency. A simple way herein is to ignore the computations carried out at the straggling nodes. However, in many industry settings, ignoring straggling tasks is not favored as it reduces the model quality. This is very critical since the model will be used by millions of people and even a slight improvement is quite remarkable in practice. My focus in this domain has been to leverage novel computation redundancy for making distributed training straggler-resilient, leading to a significant improvement in the overall training time while simultaneously preserving the optimal convergence performance.
- **Foundations of Coded Computing:** Coded computing is a nascent transformative framework for injecting computation redundancy in unorthodox encoded forms in order to efficiently deal with communication bottleneck and system disturbances including stragglers, system and statistical heterogeneity, and adversarial computations in distributed systems. Two of the key research problems where I have leveraged as well as advanced the coded computing domain are (1) communication efficient large-scale graph processing, and (2) low-latency federated learning in wireless edge networks.