COMPUTER SCIENCE & ENGINEERING
UNIVERSITY OF MICHIGAN

DISSERTATION DEFENSE

Deepika Natarajan

Enabling Practical Deployments of Privacy-Preserving Technologies

Monday, December 19, 2022
2:00 – 4:00pm
Virtual – Zoom
Passcode: defense

ABSTRACT: The past decade has seen huge growth in several application domains, including big data analytics, the Internet of Things (IoT), and machine learning (ML). Alongside the rise in cloud computing, these technologies have been able to reach all aspects of human lives at increasingly large scales. Though capable of providing users with unprecedented insights into their data, applications in these domains have one troubling characteristic in common: they require users to sacrifice privacy of their personal data in order to obtain application results.
To address this problem, this dissertation presents several strides towards practical solutions for privacy-preserving computation. First, I look at the problem of providing privacy and security to both users and model providers during ML inference in an untrusted cloud setting. I propose a solution to this problem based on a combination of homomorphic encryption (HE) and trusted execution environments (TEEs), where HE is used to provide clients with data privacy, and TEEs are used to provide model providers with model privacy and protect the integrity of computation from malicious cloud adversaries.
Next, I address the fact that both the performance and memory requirements of homomorphic encryption prevent it from being used in a variety of deployment settings. Though much research focuses on optimizing the server evaluation portion of HE, few works have addressed the problem of providing efficient client-side HE encryption and encoding. I discuss how we tackled this problem through an efficient memory re-use scheme as part of the SEAL-Embedded HE library for IoT devices.
Finally, I describe approaches for multi-party computation between two parties (2PC), including garbled circuits, secret sharing, and a lesser-known scheme called Gate Evaluation Secret Sharing (GESS). I first present our implementation of GESS in GESSlib, a library that accurately calculates the communication cost of GESS for any 2-input Boolean circuit. I then discuss how we integrate GESSlib into a framework for more comprehensively analyzing the cost of 2PC schemes, and show how this framework enables us to better understand the performance of 2PC schemes across a range of deployment settings for a privacy-preserving machine learning workload.

CHAIR: Prof. Ronald Dreslinski