NJIT

Department of Computer Science

Balancing Privacy with System Guarantees: Key to Practical Private Databases

Chenghong Wang
Duke University

Hosted by Shantanu Sharma

Date: Friday, March 31, 2023
Coffee: **1:**45 PM – 2:00 PM
Time: 2:00 PM – 3:00 PM
Location: GITC 4402 (4th floor Seminar Lecture Hall)
WebEx Link: https://njit.webex.com/njit/j.php?MTID=me4d1485e806ec804ffd5e4852f3eb0c8

http://cs.njit.edu/seminars

Abstract: Private databases allow untrusted platforms to manage and process encrypted data, thereby enabling collaborative computations over confidential data. However, the efforts to combat side-channel leakages and maintain strong privacy promises often lead to substantial compromises of essential system guarantees such as accuracy and performance, thereby rendering their implementation in real-world industries a highly improbable scenario. In this talk, I will show how to build practical private databases that balance privacy and system guarantees. To achieve this, my key insight is to have the privacy of private databases quantifiable and adjustable. This allows for fine-tuning of privacy levels to balance between privacy and system guarantees, enabling individuals to navigate system tradeoffs according to their actual needs.

First, I will introduce a new privacy model for private growing databases, where we leverage differential privacy constraints to rigorously quantify update leakages. Rather than defining a fixed privacy guarantee, our model allows for adjustable privacy, which offers flexibility for systems built on top of it to navigate tradeoffs. Next, I will showcase novel system designs that are based on the new model and demonstrate how we can construct actual private databases that strike a balance between privacy and other system guarantees. Finally, I will share my long-term research vision for building future private databases and my ambition to make real-world impacts.

Bio: Chenghong Wang is a Ph.D. candidate in the department of computer science at Duke University, advised by Prof. Ashwin Machanavajjhala and Prof. Kartik Nayak. His research interests are differential privacy, applied cryptography, distributes systems (Blockchains), and databases. Other than his primary research area, he has collaborated extensively with domain experts in various fields and has made extensive interdisciplinary contributions in the areas of AI, ML, hardware, healthcare, and biomedicine.