香港城市大學
City University of Hong Kong

電腦科學系
Department of
Computer Science

COMPUTER SCIENCE COLLOQUIUM

Keeping Big Data Private

SPEAKER **Prof Sen-ching Samson CHEUNG**

Visiting Professor
Department of Electrical & Computer Engineering
University of California, Davis
USA

DATE 30 May 2019 (Thursday)
TIME 2:30 pm - 3:30 pm
VENUE CS Seminar Room, Y6405
6th Floor, Yellow Zone
Yeung Kin Man Academic Building
City University of Hong Kong
83 Tat Chee Avenue
Kowloon Tong

ABSTRACT

From smart grid to healthcare, the Big Data paradigm is bringing dramatic changes to our lives. Machine Learning (ML) is at the heart of this transformational process from raw data to knowledge. A dream of all ML practitioners is to be able to collect data from diverse sources regardless of governmental, enterprise, or even personal boundaries. The main obstacle to massive data collection is on protecting the privacy of sensitive information in medical data, financial records and personal data archives, etc. This is particularly challenging for big signal data like images and videos, characterized by their large volume and velocity. Cryptographic approaches like homomorphic encryption and garbled circuits are too computationally intensive for such applications, while efficient differentially private schemes may not be able to protect semantic contents embedded within these unstructured data.

In this talk, I will discuss, from both algorithmic and infrastructure vintage points, how to provide efficient secure computation that enables distributed ML on private data. From the algorithmic standpoints, I will present two different approaches: first, we use Generative Adversarial Models (GAN) to learn a model from private local data and generate synthetic data for public centralized learning. The effectiveness of this approach is demonstrated by using synthetic face images for different face learning tasks. Second, I present light-weight privacy-preserving transformations (PPT) for privacy protection on IoT platforms. Specifically, I will focus on a novel class of random neural networks that can obfuscate semantic image contents while producing good learning performance. Finally, I will present a peer-to-peer computational framework that provides distributed privacy-preserving computation in a massive scale. The framework is based on secret sharing, which is far more efficient than garbled circuit and homomorphic encryption but prone to collusion attacks. Using novel game-theoretic mechanisms, we demonstrate how collusion can be thwarted using data cleansing, proper rewards and deterrence.

BIOGRAPHY

Prof Sen-ching "Samson" Cheung is a visiting professor at UC Davis Department of Electrical & Computer Engineering. He is also a Professor of Electrical and Computer Engineering and the director of Multimedia Information Laboratory (Mialab) at University of Kentucky (UKY), Lexington, KY, USA. Before joining UKY in 2004, he was a postdoctoral researcher with the Sapphire Scientific Data Mining Group at Lawrence Livermore National Laboratory. He received his Ph.D. degree from University of California, Berkeley in 2002. He is a senior member of both IEEE and ACM. He has the fortune of working with a team of talented students and collaborators in many different areas in multimedia including video surveillance, privacy protection, encrypted domain signal processing, 3D data processing, virtual and augmented reality as well as computational multimedia for autism therapy. More details about his current and past research projects can be found at http://www.mialab.net.

All are welcome!

In case of questions, please contact Prof KWONG Tak Wu Sam at Tel: 3442 7704, E-mail: cssamk@cityu.edu.hk, or visit the CS Departmental Seminar Web at http://www.cs.cityu.edu.hk/.