NJIT

Department of Computer Science

Novel Approaches to Preserving Utility in Privacy Enhancing Technologies

Meisam Mohammady
Research Scientist at CSIRO Data61 and
Postdoctoral Research Scientist in the Data Science Institute at Columbia University

Hosted by Vincent Oria

DATE: Thursday February 3, 2022
TIME: **4:00 PM - 5:00 PM**
LOCATION: https://njit.webex.com/njit/j.php?MTID=m5746aeb0d81ed5cad2b05518bf199e6e

http://cs.njit.edu/seminars

Abstract: Significant amount of individual information is being collected and analyzed through a wide variety of applications across different industries. While pursuing better utility by discovering knowledge from the data, individuals' privacy may be compromised during an analysis: corporate networks monitor their online behavior, advertising companies collect and share their private information, and cybercriminals cause financial damages through security breaches. To address this issue, the data typically goes under certain anonymization techniques, e.g., Property Preserving Encryption (PPE) or Differential Privacy (DP). Unfortunately, most such techniques either are vulnerable to adversaries with prior knowledge, e.g., adversaries who fingerprint the network of a data owner, or require heavy data sanitization or perturbation, both of which may result in a significant loss of data utility.

Therefore, the fundamental trade-off between privacy and utility (i.e., analysis accuracy) has attracted significant attention in various settings and scenarios. In line with this track of research, we aim to build utility-maximized and privacy-preserving tools for Internet communications. Such tools can be employed not only by dissidents and whistleblowers, but also by ordinary Internet users on a daily basis. To this end, we combine the development of practical systems with rigorous theoretical analysis, and incorporate techniques from various disciplines such as computer networking, cryptography, and statistical analysis.

This presentation covers three different frameworks in some well-known settings. First, I will present the Multi-view approach which preserves both privacy and utility of data in network trace anonymization. Second, I will present the R^2 DP (Randomizing the Randomization mechanisms of Differentia Privacy) approach which is a novel technique on differentially private mechanism design with maximized w.r.t. any utility metric. Finally, I will present the DPOAD (Differentially Private Outsourcing of Anomaly Detection) approach which is a novel framework enabling privacy preserving anomaly detection in the outsourcing setting.

Bio:

Meisam is jointly a Postdoctoral Research Scientist in the Data Science Institute at Columbia University and an active Research Scientist in CSIRO Data61 which is the Australia's leading digital research network, helping various partners across business, government and industry to solve a wide range of data-centric problems. Meisam's research focuses on ethical and secure machine learning (private, fair and certifiably robust to adversaries), differential privacy, privacy preserving cloud security auditing and security issues pertaining to Internet of Things (IoT). He earned his PhD from the Concordia Institute for Information Systems Engineering (CIISE) at Concordia University, his MSc from the Department of Electrical Engineering at Ecole Polytechnique Montreal, and his BS from the Department of Electrical Engineering at Sharif University of Technology. He also had several collaborations in terms of research and supervision with both academia and industry such as the Department of Computer Science at the Illinois Institute of Technology (IIT), the University of New South Wales (UNSW), the University of Sydney, and Ericsson Research Canada, the governments of Western and Southern Australia and NAB bank. Meisam has co-authored several papers in top-tier security journals and conferences, and his PhD dissertation has won the Distinguished PhD Dissertation Awards among all Engineering and Natural Science PhD dissertations and selected as Concordia University's nominee for both Canada-wide CAGS and ADESAQ competitions