UNIVERSITY of GUELPH

COLLEGE of ENGINEERING AND PHYSICAL SCIENCES

SCHOOL OF COMPUTER SCIENCE

PhD Seminar 1

Monday November 6, 2023 at 9AM online via Zoom (remote)

Le Wang

Protecting Bilateral Privacy in Machine Learning-as-a-Service:
A Differential Privacy-Based Defense

Advisor: Dr. Xiaodong Lin
Advisory: Dr. Rongxing Lu (University of New Brunswick)
Advisory: Dr. Rozita Dara

Abstract:

With the continuous promotion and deepened application of Machine Learning-as-a-Service (MLaaS) across various societal domains, its privacy problems occur frequently and receive more and more attention from researchers. However, existing research focuses only on the client-side query privacy problem or only focuses on the server-side model privacy problem and lacks a simultaneous focus on bilateral privacy defense schemes.

In this paper, we design privacy-preserving mechanisms based on differential privacy for the client and server side respectively for the first time. By injecting noise into query requests and model responses, both the client and server sides in MLaaS are privacy-protected. Experimental results also demonstrate the effectiveness of the proposed solution in ensuring accuracy and providing privacy protection for both the clients and servers in MLaaS.