UNIVERSITY of GUELPH

COLLEGE of ENGINEERING AND PHYSICAL SCIENCES

SCHOOL OF COMPUTER SCIENCE

PhD Seminar 1

Monday August 28, 2023 at 2pm via Zoom [Remote]

Nan Li

Blockchain-based Federated learning for untrusted participants in Healthcare system

Advisor: Dr. Xiaodong Lin
Advisory: Dr. Ahmed Refaey Hussein [SoE]
Advisory: Dr. Lei Lei [SoE]

Abstract:

Federated Learning (FL) is a collaborative machine learning approach allowing participants to jointly train a model without having to share their private, potentially sensitive local datasets with others, which are really suitable for protecting healthcare records. However, a typical FL still faces new security and privacy problems. First, the aggregation task from a single server faces the risk of single-point failure, and through the collected gradients, an adversary may implement inference or reconstruction attacks.

Second, the aggregator (i.e., server) losses direct control to local training processes. For a malicious participant, for example, it may only perform a small portion of the correct training process or directly use the old results and proof as the final training result.

Based on these, this paper will distribute the aggregation task from the single server to a set of blockchain nodes. At the same time, leveraging blockchain and Trusted Execution Environments (TEEs) guarantees the confidentiality, integrity and verification of the correctness of gradient collecting and model aggregation as well.