UNIVERSITY of GUELPH

COLLEGE of ENGINEERING AND PHYSICAL SCIENCES

SCHOOL OF COMPUTER SCIENCE

PhD Seminar 2

Friday January 28, 2022 at 3:30pm via Zoom

Mohammad Amiri-Zarandi

A Privacy-Preserving Trust Management system for IoT

Advisor: Dr. Rozita Dara
Advisory: Dr. Xiaodong Lin
Advisory: Dr. Hassan Khan

Abstract:

In the Internet of Things (IoT), numerous devices are connected to perform tasks and services in different applications. Although providing a seamless and remote connection among devices is an excellent feature for IoT, it also raises some concerns regarding security and privacy. The IoT devices are numerous and have complex interactions. Being ubiquitous, these systems are also vulnerable to sensitive data leakage in different stages of the data lifecycle. Trust management systems are mechanisms to automatically evaluate the access requests in the system and handle the permissions based on the trust between IoT nodes. Trust management helps IoT devices to overcome perceptions of uncertainty and risk and prevent adversaries from accessing the services and applications in the network.

Trust management and privacy preservation mechanisms work together to reduce the risks related to data leakage and unapproved access in a system from two different perspectives. On the one hand, a trust management system can monitor communications and limit high-risk data access by different entities and, in turn, advance privacy protection. On the other hand, because trust management systems use sensitive data to operate, they need to be developed in a privacy-preserving manner. In this study, working on both aspects, Firstly, we aim to provide an enhanced trust management system that leverages AI and different available data sources in the trust evaluation mechanism. Moreover, the proposed system will be designed in a privacy-preserving manner that protects the sensitive data that is used in the developing phase of the system production. The proposed framework uses a decentralized AI-based mechanism that gathers data from diverse sources in the system and uses federated learning to extract knowledge and enhance trust management. The framework includes three different components for Social IoT analysis, network analysis, and user behavior analysis. The outputs of these components are aggregated in a decentralized Decision Support System (DSS) to be utilized for trust management and access control in IoT.