UNIVERSITY of GUELPH

COLLEGE of ENGINEERING AND PHYSICAL SCIENCES

SCHOOL OF COMPUTER SCIENCE

# PhD Defence

## Friday November 17, 2023 at 1PM, online via Zoom (Remote)


## Abbas Yazdinejad


*Secure and Private ML-based Cybersecurity Framework for Industrial Internet of Things (IIoT)*

**Chair:** Dr. Stacey Scott
**Advisor:** Dr. Ali Dehghantanha
**Advisory:** Dr. Gautam Srivastava [Brandon University]
**Non-Advisory:** Dr. Lei Lei [SoE]
**External Examiner: Dr. Arash Habibi Lashkari** [York University]

## Abstract:


The advent of the Industrial Internet of Things (IIoT) has revolutionized the operation and efficiency of various industries. However, it has also introduced un- precedented threats, posing significant security and privacy challenges threatening critical infrastructure systems' integrity, confidentiality, and availability. These challenges are exacerbated due to the unique characteristics of IIoT, including its network protocols, performance metrics, and asset characteristics, which render traditional cybersecurity solutions ineffective. The threats are further heightened when considering the integration of IIoT with other emerging technologies like blockchain, an area increasingly becoming an attractive target for cyber-attackers. On the one hand, the growing prevalence of IIoT devices and blockchain technologies increases the attack surface and, on the other hand, poses serious privacy concerns due to the inherent transparency of blockchain transactions and the sensitive nature of data handled by IIoT devices.

In response to these pressing concerns, this thesis introduces a secure and private machine learning-based framework for IIoT. This framework is designed to offer robust and comprehensive solutions to the security and privacy issues plaguing IIoT systems. The first component of the framework introduces an auditable privacy- preserving federated learning (PPFL) model. This model is developed to defend against poisoning attacks and non-identically independently distributed (Non-IID) data, providing robust protection against malicious intrusions while preserving data privacy and maintaining model accuracy. The second component proposes a novel approach to threat hunting in IIoT networks. It utilizes a combination of state-of- the-art machine learning classifiers and deep learning architectures like Long Short-Term Memory (LSTM) and Auto-Encoder (AE) to effectively detect and classify multi-class anomalies, thereby offering a proactive defense against potential cyber threats. The final component of the framework presents a unique approach to threat hunting in blockchain-based IIoT systems. It comprises a federated learning model for anomaly detection in blockchain-based IIoT networks and an intelligent fuzzy blockchain framework that manages uncertainty issues in IIoT networks, thereby enhancing the security and flexibility of the system. The proposed framework offers a comprehensive solution to the pressing security and privacy issues inherent in IIoT systems. This thesis contributes significantly to IIoT security and privacy by proactively addressing these challenges, offering promising future research and development directions.