Dr.

Najwa Aaraj

Chief Researcher
Technology Innovation Institute

"Cryptography, Cyber Security and Machine Learning: Interdisciplinary benefits"

19 OCTOBER, 2022

10:00 - 10:50 AM

C209 OR ZOOM

Join by Zoom
Meeting ID: 926 2132 6004
Passcode: 974188

Cyber Security and machine learning have typically been separate disciplines. Moreover, Cryptography and machine learning have typically been separate disciplines. New cross-discipline research is needed to improve the three domains

In this talk, we discuss how machine learning can be used as an enabler to advanced cryptography, privacy preserving protocols and cryptanalysis. We also discuss how efficient machine learning models can enable local inference and advanced vulnerability management on edge devices. The talk also covers how Neural Network algorithms and cryptographic cores will co-exist in future Neural Processor Units.

We cover the role of cryptography in securing Machine Learning models by (1) ensuring confidentiality of both data & model during training and classification; (2) protection of models from being tampered-with or introducing bias for profit or control; (3) protection against model poisoning; and (4) introducing cryptographic randomness in training Deep Neural Networks. This could help drive the adoption of AI in privacy-sensitive industries, including medicine and finance.

Contact: AHR@oist.jp / 098-966-1546