Call For Papers

Special Session: Adversarial Machine Learning at the Edge: Challenges and Opportunities
Conference: The 2022 International Conference on Cyber-physical Social Intelligence (ICCSI)

Date: October 21-24, 2022
Location: Nanjing, China
Meeting mode: Hybrid
Web site: https://iccsi2022.agist.org

Edge computing presents a new frontier for the ubiquity of computers in real-world applications. The computer systems used in edge computing generally interface directly with the end-user or the environment, and operate under severe resource constraints. Machine learning techniques, particularly deep learning methods, enable high-precision decision-making capabilities across a wide range of possible applications. Most high-level machine learning models require significant hardware resources. There exist multiple challenges within the context of deploying machine learning models on edge computing devices. Researchers in the field often employ approximation and compression techniques to allow high-performance machine learning models on resource-constrained edge computing devices. While such approaches are sufficient to bring machine learning capabilities to the edge, they do not account for the susceptibility of machine learning models to adversarial attacks. Generally, detection and mitigation of adversarial attacks on machine learning models demands the execution of resource-hungry algorithms. Hence, machine learning faces a two-fold challenge at the edge - the exposure of inference models to potential adversarial attacks, and the lack of computing resources to defend against such attacks. The combination of the above problems greatly compromises the fidelity of edge computing frameworks. The special session seeks contributions which aim to address the nature, impact and defense mechanisms in regards to adversarial attacks on edge computing devices and frameworks. Authors should evaluate problems of relevance, and/or explore new solutions to existing problems in the area.

Interested topics include (but not limited to):

- Adversarial attacks and defense for approximate and compressed deep neural networks.
- Adversarial attacks and defense for resource-constrained neural network architectures.
- Classical machine learning algorithms suitable for edge computing devices, with adversarial
- attack/defense evaluation.
- Hardware security issues on edge computing devices, specific to machine learning applications.
- Hardware security issues on deep learning co-processors and inference engines.
- Characterization of malicious attacks on machine learning at the edge.
- Federated learning and adversarial machine learning.
- Defense mechanisms for federated learning algorithms.
- Analysis of federated learning models at the edge.
- Adversarial attacks on IoT networks with machine learning capabilities.
- Power-performance analysis of adversarial defense mechanisms deployed on edge computing
- devices

Important Dates:

May 15, 2022,	Full paper submission
July 1, 2022,	Acceptance/Rejection notification
August 31, 2022,	Final camera-ready papers due

Special Session Co-chairs:
Assistant Professor Dwaipayan Chakraborty(Rowan University) email chakraborty@rowan.edu

Contributions (tentative):

1. "Adversarial robustness of TinyML models" by Russell Trafford.
2. "Adversarial machine learning and Privacy in Edge computing" by Vikas Hassija.
3. "Susceptibility of Hazard detection at the edge" by Faraz Hussain.
4. "Secure Computer Vision at the Edge" by Steven L. Fernandes.
5. "Secure systems for artificial intelligence in distributed networks" by Maurantonio Caprolu.
6. "Statistical methods for Security in Intelligent Edge Computing Frameworks" by Suresh ChandraSatapathy.
7. "Adversarial Machine Learning in IoT for Big Data applications" by Fatima Hussain.