Call For Papers

Invited Session
Adversarial Learning

We invite you to submit paper to Invited Session on Adversarial Learning in International Conference on Machine Learning and Cybernetics (ICMLC) 2022. High quality papers after extension will be published in a special issue of International Journal on Machine Learning ad Cybernetics.

Description

In security-related applications, an adversary is able to fool a model by using carefully crafted samples. A traditional machine learning method may be compromised through an adversarial attack that violates the implicit assumption of the same distributions on training and test samples. This security problem may become more serious in deep learning since public dataset and pre-trained models are used more frequently in recent years, and those datasets and models can be easily compromised by a nefarious third-party supplier.

Topics of Interest

- Adversarial Attack Method
- Defence Method
- Data Sanitization
- Attack Detection
- Vulnerability Analysis
- Robust Learning
- Generative Adversarial Network (GAN)
- Adversarial Sample

Import/ant Dates

Submission Due:	**15 Jun 2022**
Notification of Acceptance:	**1 Aug 2022**
Registration Due:	**15 Aug 2022**
Camera-Ready:	**15 Aug 2022**

Paper Submission

Authors must submit an electronic copy (in word or pdf) of their complete manuscript directly to the Session Organizer (patrickchan@ieee.org) before June 15, 2022

Organizer

Prof. Daniel Yeung
Past President, IEEE SMC Society, USA
(danyeung@ieee.org)

Prof. Xizhao Wang
Shenzhen University, China
(xizhaowang@ieee.org)

Dr. Patrick Chan
South China University of Technology, China
(patrickchan@ieee.org)

Dr. Eric Tsang
Macau University of Science and Technology, Macau
(cctsang@must.edu.mo)