



# CALL FOR PAPERS

August 17-20, 2023  
Xi'an, Shaanxi, China



## 2023 IEEE 11th International Conference on Information, Communication and Networks

# Track 8

The 2023 IEEE 11th International Conference on Information, Communication and Networks (ICICN) is set to take place in Xi'an, Shaanxi, China during August 17-20, 2023.



All submissions will be peer reviewed. Accepted, registered and presented papers will be published in the **ICICN 2023 IEEE conference Proceedings**, included in IEEE Xplore and indexed by **El Compendex, SCOPUS**, etc.

### Machine Learning and Security

Submission Deadline: June 10, 2023

#### Brief introduction

Artificial Intelligence (AI) techniques, e.g., deep neural networks (DNNs), have been significantly refreshing the state-of-the-art performance of various tasks, e.g., face recognition, robotic grasping, obstacle avoidance of autonomous-driving cars. However, recent works report that DNNs are vulnerable to adversarial attacks, and could be easily fooled by adversarial examples that have imperceptible differences with the inputs, mostly in the image field. Therefore, applying these applications to real-world scenarios has hidden security risks.

**Topics** Interested topics include (but not limited to):

- Adversarial attack methods on images
- Adversarial defense methods on images
- Adversarial attack methods on 3D point clouds
- Adversarial defense methods on 3D point clouds
- Adversarial attack methods on meshes
- Adversarial defense methods on meshes
- Adversarial attack methods on videos
- Adversarial defense methods on videos
- Robust artificial intelligence design
- Adversarial machine learning
- Explainable AI
- Hardware implementation of AI techniques

#### Track Chairs and Co-chairs:

- Zhan Qin, Zhejiang University, China
- Chenhao Lin, Xi'an Jiaotong University, China
- Qian Wang, Wuhan University, China
- Zhe Liu, Nanjing University of Aeronautics and Astronautics, China
- Peican Zhu, Northwestern Polytechnical University, China

#### Track TPC Members

- Manman Yuan, Inner Mongolia University, China
- Jianfu Chen, ESIEE Paris, France
- Haifeng Zhang, Anhui University, China

Co-sponsored by



Hosted by



Organizer



Patrons



会议官网

