**Special Session of ICACI2023**

**Poisoning attack in deep neural networks**

**Session Organizers:**

● Dr. Nankun Mu, Chongqing University, China; Email: [nankun.mu@cqu.edu.cn](mailto:nankun.mu@cqu.edu.cn.com)

**Session Description:**

Deep neural networks (DNNs) play a critical role in a wide range of applications, such as image classification, autonomous driving and facial recognition. As we all know, DNNs are data-driven, depending on the size and quality of the training data. Therefore, it seems that DNNs are vulnerable while attackers have access to the training data and they can make DNNs misclassify by modifying even a small proportion of the data. As a result, the poisoned model may not work as people originally expected. For example, the classification accuracy may drop dramatically and in a stealthier way, the classification accuracy will just decrease on some target poisoned samples and behave normally on other benign samples. To this end, we need to pay more attention to the poisoning attack in deep neural networks (DNNs). This special session is organized to focus on the various of poisoning attacks in deep neural networks and some corresponding defenses.

**Potential topics include but are not limited to the following:**

■ Adversarial examples in deep neural networks

■ Different backdoor attacks including poison-label attack and clean-label attack (i.e. without changing label of the poisoned samples)

■ Recent novel sample-targeted attacks towards DNNs

■ Some state-of-the-art defenses against the existing poisoning data attack