Title:

Artificial Intelligence Security

Abstract:

If AI is the crown of the Internet and even the entire information technology category, security is undoubtedly the base of the crown. Just like any new skill, the safety of artificial intelligence has a great influence on its future development and application. Today, the security and risk managers need to determine whether the use of artificial intelligence or machine learning in R & D, operations, and application security tests is of practical value. They must be aware that application of artificial intelligence and machine learning means the need for a large amount of data and talent, and that it is necessary to predict the speed, accuracy and other potential practical problems of the implementation of artificial intelligence. The purpose of this topic is to introduce the safety problems of artificial intelligence, especially the vulnerability in deep learning software implementation and possible hidden dangers.

Scope and Topics:

Potential topics include but are not limited to:

- ✧ Reliability of artificial intelligence system
- ✧ Accuracy of artificial intelligence system
- ✧ Network security prevention based on AI

Program Committee Chairs:

Zhenguang Gao, Professor of Computer Science, Chair, Department of Computer Science, Framingham State University, Framingham, MA 01772
zgao@framingham.edu)
Zhenguang Gao (received his Ph.D. in Applied Mathematics from the University of South Carolina. His interests include information science, signal processing, pattern recognition, and discrete mathematics. He currently teaches computer science at Framingham State University.

Shaozhang Niu, Beijing University of Posts and Telecommunications, China

Program Committee:

Shaozhang Niu, Beijing University of Posts and Telecommunications, China
Rongrong Ni, Beijing Jiaotong University, China
Jiancheng Zou, North China University of Technology, China