**Secure Object Detection on Edge Devices**

Ling Liu

School of Computer Science

Georgia Institute of Technology

Deep neural networks (DNNs) have fueled the wide deployment of object detection models in a number of mission-critical domains, such as traffic sign detection on autonomous vehicles, and intrusion detection on surveillance systems. Recent studies have revealed that deep object detectors can also be compromised under adversarial attacks, causing a victim detector to detect no object, fake objects, or wrong objects. However, very few studies how to guarantee the robustness of object detection against adversarial manipulations. This keynote presents an in-depth understanding of vulnerabilities of deep object detection systems by analyzing the adversarial robustness under different DNN detector training algorithms, different attack strategies, different adverse effects and costs. Then I will describe a set of mitigation strategies and techniques for robust object detection by guaranteeing high adversarial robustness while maintaining high benign detection accuracy.



Ling Liu is a Professor in the School of Computer Science at Georgia Institute of Technology. She directs the research programs in the Distributed Data Intensive Systems Lab (DiSL), examining various aspects of large scale big data-powered artificial intelligence (AI) systems, and machine learning (ML) algorithms and analytics, including performance, availability, privacy, security and trust. Prof. Liu is an elected IEEE Fellow, a recipient of IEEE Computer Society Technical Achievement Award (2012), and a recipient of the best paper award from numerous top venues, including IEEE ICDCS, WWW, ACM/IEEE CCGrid, IEEE Cloud, IEEE ICWS. Prof. Liu served on editorial board of over a dozen international journals, including the editor in chief of IEEE Transactions on Service Computing (2013-2016) and currently, the editor in chief of ACM Transactions on Internet Computing (TOIT). Prof. Liu is a frequent keynote speaker in top-tier venues in Big Data, AI and ML systems and applications, Cloud Computing, Services Computing, Privacy, Security and Trust. Her current research is primarily supported by USA National Science Foundation under CISE programs and IBM.