THE CENTER FOR ADVANCED COMPUTER STUDIES

at

*the University of Louisiana at Lafayette*

Lafayette, Louisiana

Proudly announces a presentation

**Dr. Neil Gong**

*Assistant Professor*
*Department of Electrical and Computer Engineering and*
*Department of Computer Science*
*Duke University*

will give a presentation entitled

# Secure Federated Learning

* * * *

## Abstract

Federated learning is an emerging machine learning paradigm to enable many clients (e.g., smartphones, IoT devices, and edge devices) to collaboratively learn a model, with help of a server, without sharing their raw local data. Due to its communication efficiency and potential promise of protecting private or proprietary user data, and in light of emerging privacy regulations such as GDPR, federated learning has become a central playground for innovation. However, due to its distributed nature, federated learning is vulnerable to malicious clients. In this talk, we will discuss local model poisoning attacks to federated learning, in which malicious clients send carefully crafted local models or their updates to the server to corrupt the global model. Moreover, we will discuss our work on building federated learning methods that are secure against a bounded number of malicious clients.

**DATE: FRIDAY, FEBRUARY 12, 2021**
**TIME: 11:00 A.M. - 12:00 NOON**
**LOCATION: Via ZOOM**

## Biography

Neil Gong is an Assistant Professor in the Department of Electrical and Computer Engineering and Department of Computer Science (secondary appointment) at Duke University. He is broadly interested in cybersecurity with a recent focus on the intersections between security, privacy, and machine learning. He received a Ph.D. in Computer Science from the University of California at Berkeley in 2015. He has received an NSF CAREER Award, Rising Star Award from the Association of Chinese Scholars in Computing, an IBM Faculty Award, and multiple paper awards.

Join Zoom Meeting:

https://ullafayette.zoom.us/j/95570241062?pwd=QTlRV3FYVjdWSCtnVTFRN2c2QmErUT09

Passcode: Fri11Semi