# THE CENTER FOR ADVANCED COMPUTER STUDIES

*at*

*the University of Louisiana at Lafayette*

Lafayette, Louisiana

Proudly announces a presentation

***Dr. Yuan Tian***

*Assistant Professor of Computer Science*
*University of Virginia*

will give a presentation entitled

## When Machine Learning Meets Security and Privacy: Challenges and Opportunities

****

**Abstract:** Modern computing platforms are pervasive, interconnected, scalable, and data-intensive. From smartphones to IoT devices, and to cloud servers, these computing platforms bring more functionality and convenience for people; however, these new platforms also expose users to security and privacy risks. The massive amount of data in these computing platforms provides great opportunities for data-driven security solutions, however, there are still many challenges to make such solutions robust, scalable, and privacy-friendly. For example, how to build a reliable anomaly detection model when only a handful of labeled data is available? How to protect user privacy while running machine learning models?

In this talk, I'll present my example projects in the thrusts of (1) AI for information security and privacy, as well as (2) design and implement secure and privacy-preserving machine learning systems. In the first thrust, I will introduce our work on transfer-learning-based privacy violation detection across different platforms with a limited amount of labeled data, and explain our scalable anomaly detection frameworks that are deployed in Facebook and Microsoft Azure. In the second thrust, I will introduce our efforts in designing secure and privacy-preserving machine learning algorithms by system and security co-design.

**DATE: FRIDAY, MARCH 19, 2021**

**TIME: 11:00 A.M – 12:00 NOON**

**LOCATION: Via Zoom**

**Biography:** Yuan Tian is an Assistant Professor of Computer Science at the University of Virginia. Before joining UVA, she obtained her Ph.D. from Carnegie Mellon University in 2017, and interned at Microsoft Research, Facebook, and Samsung Research. Her research focuses on designing principled and practical secure and privacy-preserving systems, drawing from program analysis, machine learning, and human-computer interaction. Her work has generated real-world impact as countermeasures and design changes have been integrated into platforms (such as Android, Chrome, SmartThings, Azure, and iOS), and also impacted the security recommendations of standard organizations such as Internet Engineering Task Force (IETF) and World Wide Web Consortium (W3C). She is a recipient of Google Research Scholar Award 2021, NSF CAREER award 2020, NSF CRII award 2019, Amazon AI Faculty Fellowship 2019, CSAW Best Security Paper Award 2019, Rising Stars in EECS 2016, and Black Hat Future Female Leaders in Cyber Security 2015. Her research has appeared in top-tier venues in Security, Machine Learning, and Systems. Her projects have been covered by media outlets such as IEEE Spectrum, Forbes, Fortune, Wired, and Telegraph.

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

**Passcode**: Fri11Semi