

DEPARTMENT OF COMPUTER SCIENCE

SEMINAR

2026 SERIES

Toward Trustworthy Machine Learning: From Data to Deployment

DATE & TIME

25 MAR 2026 (WED) 9:00 - 10:00 AM

ONLINE VIA ZOOM



DR. ZITAO CHEN

Assistant Professor
Department of Electrical Engineering and Computer Science
University of Kansas

ABSTRACT

Machine Learning (ML) systems are increasingly deployed in high-stakes scenarios in our society. Despite their impressive performance, ML systems are also subject to catastrophic failures throughout their life cycle, from data misuse in development to safety violations in operation. This talk will present strategies for enabling responsible data governance and safe deployment of ML systems.

First, I will introduce my work on advancing data privacy and accountability. I will present novel algorithms to quantify and mitigate privacy leakage, demonstrating that ML models can leak significant information while evading state-of-the-art privacy protections and auditing frameworks. I will then describe how privacy attacks can be repurposed as mechanisms for accountability, allowing data owners to detect unauthorized data use in model training. Beyond training-time risks, deployed ML models also face safety challenges due to unreliable computing hardware. I will discuss methods for building dependable ML systems that maintain safe operations despite hardware unreliability. Finally, I will outline future directions for advancing the trustworthy development and deployment of ML systems.



SPEAKER'S
BIOGRAPHY



REGISTER NOW