COLLEGE OF ENGINEERING AND COMPUTER SCIENCE

FACULTY RESEARCH TALKS

LISTEN. LEARN. COLLABORATE.

Zoom talk | Friday, Sept. 20, 2024 | Noon to 1 p.m.

PRESENTER 1:
AMRIT SINGH BEDI
Assistant Professor
Computer Science
Artificial Intelligence Initiative

Safe, Robust and Reliable Artificial Intelligence

The emergence of foundational models has pushed artificial intelligence (AI) to the forefront across various domains, from everyday tasks like writing to complex processes such as data analysis. Despite these advancements, are we fully prepared to harness AI's potential in fields such as robotics, education, finance and healthcare? The answer is no; there is still a considerable journey ahead. In this talk, Dr. Bedi explores the significant challenges we face regarding the safety, robustness and reliability of AI systems.

Before coming to UCF, Dr. Bedi was a research assistant professor at the University of Maryland, College Park. He received his doctorate in electrical engineering from Indian Institute of Technology, Kanpur. He worked as a research associate within the computational and information sciences directorate at the U.S. Army Research Laboratory from 2019 to 2022. His research interests lie in AI for autonomous systems, with specific emphasis on scalable and sample-efficient learning algorithms. Currently, he is working on the problem of AI alignment in language models. His paper was selected as a Best Paper Finalist at the 2017 IEEE Asilomar Conference on Signals, Systems and Computers. He received an honorable mention from IEEE Robotics and Automation Letters in 2020. He received the Amazon Research Award in 2022.

PRESENTER 2:
SER-NAM LIM
Associate Professor
Computer Science
Artificial Intelligence Initiatve

Towards Automatic Movie Creation by Learning to Generate Long Videos

AI has advanced rapidly towards a capability to generate videos automatically when given a textual description. This has opened doors to the potential for automatic movie production, ad creation and advanced educational tools, promising to bring about groundbreaking impacts in our society. Two major obstacles stand in the way of this aspiration: AI technologies still struggle with generating long videos with the required temporal cohesiveness and quality; and the computational resources needed are prohibitive for consumer level utility. Dr. Lim will discuss progress on generating long videos, as well as an approach that enables running large models on consumer hardware.

Dr. Lim's background is in computer vision and the field of AI. He earned his doctorate at the University of Maryland, College Park. He spent a decade at GE Research working on different areas of computer vision including video recognition, 3D reconstruction, representation and visual matching. At Meta, he led projects focused on AI for user content recommendations, as well as search engines that include the intersection of large language models and computer vision. His group at UCF conducts research in image and video generation, AI for augmented reality, visual-language representation and understanding, and other major topics in AI. Dr. Lim has published over 100 peer-refereed papers, with more than half in top AI venues.

PRESENTER 3:
MENGXIN ZHENG
Assistant Professor
Computer Science
Cyber Security and Privacy Cluster

Towards Trustworthy Machine Learning: Secure and Private Large Transformer Models

Deep learning's integration into critical sectors like autonomous vehicles and medical treatments underscores the necessity for creating learning methods that are safe, secure, privacy-conscious and reliable. However, the critical aspects of data privacy and security in deep learning, particularly in attention-based transformers, have not been well studied. In this presentation, Dr. Zheng will discuss her research on trustworthy machine learning, focusing on innovative Trojan attack designs, empirical attack mitigation and defense, certified robustness, and private transformer inference to establish trustworthy AI systems.

Dr. Zheng received her doctoral degree in intelligent systems engineering from Indiana University Bloomington. Her research focuses on the development of secure learning models, with particular emphasis on Trojan attack strategies, defense mechanisms and privacy protection in transformer models. She has been recognized as a 2023 DAC Young Fellow, received the Best Student Paper Award at the SPIE Conference and was the runner-up in the 2019 Cheng Wu Innovation Challenge. She has published in esteemed conferences such as NeurIPS, CVPR, ECCV, ACL and DAC.

JOIN THE ZOOM MEETING | VIEW PREVIOUS RESEARCH TALKS