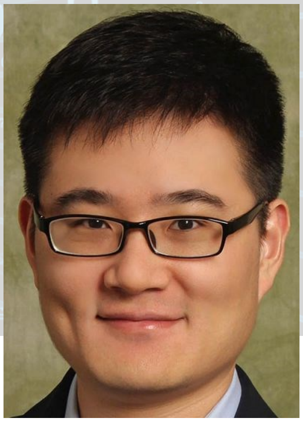
Data Science Transdisciplinary Area of Excellence

Data Salon 2024 — 2025

From Text to Impact: Large Language Models as Responsible Cross-Disciplinary Copilots



Zhaohan Xi, School of Computing

Friday, March 28, 2025, 12:00-1:00 PM
AD-148, with lunch served
Zoom Option: https://binghamton.zoom.us/j/98837835995

Abstract

Large Language Models (LLMs) have evolved from simple conversational agents to powerful copilots capable of navigating complex, cross-disciplinary challenges. Their ability to synthesize vast amounts of information, adapt to domain-specific needs, and enhance decision-making has positioned them as indispensable tools across critical sectors.

In the realm of healthcare, clinical LLM copilots offer unprecedented opportunities for enhancing diagnostic accuracy, decision support, and patient care. By seamlessly integrating professional knowledge with real-time patient-centric diagnostics, these models provide expertise-driven recommendations, guiding clinicians with precision while alleviating cognitive overload. Their potential to improve medical workflows, personalize treatment plans, and expand access to high-quality care underscores their transformative role in modern healthcare systems.

In cybersecurity, LLMs serve as both proactive defenders and intelligent risk assessors, identifying vulnerabilities, analyzing threat patterns, and fortifying digital infrastructures. They assist security professionals in monitoring cyber threats, automating incident response, and mitigating risks in real time.

However, the expanding role of LLMs also surfaces critical challenges related to trust, security, and ethical governance. Ensuring their robustness against external vulnerabilities—particularly when interfacing with third-party APIs and dynamic data sources—is crucial to their responsible deployment. This talk delves into strategies for mitigating these risks, specifically focusing on secure data curation to safeguard against misuse and misinformation.

This presentation underscores the dual nature of LLMs as transformative agents of progress and potential vectors for risk. By emphasizing a balanced, responsible approach to LLM integration, we can harness their full potential while ensuring their safe, ethical, and effective deployment across diverse, high-stakes domains.

About the speakers: Dr. Zhaohan Xi earned his Ph.D. at Pennsylvania State University – College of Information Sciences and Technology. He was also a visiting scholar at Stony Brook University (SUNY) – Computer Science Department. Prior to that, he received his master's degree from Lehigh University. Dr. Xi's research focuses on AI Security & Privacy and Clinical AI in the context of Large Language Models (LLMs), aiming to develop responsible, robust, and resilient strategies to improve AI's expertise and reliability. Beyond LLMs, his research also involves advanced AI techniques, including Graph Learning, Knowledge Graph Reasoning, Prompt Engineering, and AutoML.