Title

Security for AI and AI for Security

Abstract

As artificial intelligence (AI) continues to transform industries, the intersection of AI and security becomes increasingly critical. This talk explores the dual roles of AI in enhancing security measures and the importance of securing AI systems themselves. We will delve into how AI technologies are being leveraged to detect and respond to cyber threats in real-time, and how they contribute to strengthening overall cybersecurity frameworks. Additionally, the talk will address the unique security challenges that AI systems face, such as malicious attacks, data leakage, and model theft, while discussing strategies and secure environments, such as Trusted Execution Environments (TEEs), for safeguarding AI models and data, especially working with AI accelerators. By examining both "Security for AI" and "AI for Security," this talk aims to explore the collaborative relationship between these two domains and offer insights into building more resilient and secure AI-powered systems.

Bio

Deming Chen is the Abel Bliss Professor in the Grainger College of Engineering at the University of Illinois at Urbana-Champaign. His current research interests include hybrid cloud, reconfigurable and heterogeneous computing, system-level design methodologies, machine learning and AI, and security and confidential computing. He has published more than 280 research papers, received 10 Best Paper Awards and one ACM/SIGDA TCFPGA Hall-of-Fame Paper Award, and has given more than 150 invited talks. His research has had significant impact, with open-source solutions adopted by industry (e.g., FCUDA, DNNBuilder, CSRNet, SkyNet, ScaleHLS, Medusa). For example, Medusa has been incorporated into Nvidia's TensorRT-LLM for parallel token generation, improving the speed of LLM (large language model) execution by 2.3-3.6x. He is an IEEE Fellow, an ACM Distinguished Speaker, and the Editor-in-Chief of ACM Transactions on Reconfigurable Technology and Systems (TRETS). Under his leadership, the impact factor of ACM TRETS has increased by 3.8x. He is the Director of the AMD-Xilinx Center of Excellence and the Hybrid-Cloud Thrust Co-Lead of the IBM-Illinois Discovery Accelerator Institute. He has also been involved in several startup companies, including AutoESL and Inspirit IoT. He received his Ph.D. from the Computer Science Department at UCLA in 2005.