Faculty Name:

Junfeng Yang

Faculty Email:

junfeng@cs.columbia.edu

Lab:

Reliable Computer Systems

Project Title:

LLMs Meet Cybersecurity

Description:

In the rapidly evolving landscape of cybersecurity, LLMs have emerged as transformative tools. These advanced AI systems, capable of understanding and generating human-like text, are revolutionizing how we approach complex problems, including those in cybersecurity. We are excited to offer two groundbreaking projects on the intersection of LLMs and cybersecurity.

Project 1: Securing the Future of LLMs

This project delves into the security of LLMs themselves. As these models become more integral to various applications, ensuring their robustness and resistance to adversarial attacks is paramount. Students will investigate potential vulnerabilities in LLMs and develop strategies to fortify them against emerging threats.

Project 2: Harnessing LLMs for Cybersecurity Solutions

The second project explores the application of LLMs in solving complex cybersecurity challenges. Students will leverage the advanced capabilities of LLMs to identify, analyze, and mitigate cybersecurity threats, contributing to the development of smarter, more efficient security systems.

Students will work under the guidance of Professor Yang and his PhD students and Postdocs. Past summer projects have led to e.g. publications in top-tier conferences and the discovery of over 100 zero-day vulnerabilities in deployed smart contracts.

Join us in shaping the future of cybersecurity with the power of LLMs.**Location of Research:**

Hybrid (both Remote and On Site)

# of hrs/week:

40

Department/Program:

Computer Science

Eligibility:

BS, First Year, BS, Second Year, BS, Third Year, BS, Fourth Year, MS

To apply, please contact:

Junfeng Yang

junfeng@cs.columbia.edu