Faculty Name:

Junfeng Yang

Faculty Email:

junfeng.yang@columbia.edu

Lab:

Software Systems Lab

Project Title:

Trustworthy AI for Trustworthy Software

Description:

Our lab is interested in making software systems secure, reliable, and fast. We are looking for 1 or 2 strong students this summer (dates flexible) to help investigate how to secure software using large language models. Tools like GitHub Copilot have shown promise at simplifying software development, yet researchers found that 40% of the Copilot-generated code is vulnerable because the underlying large language models treat code simply as text and completely ignores the rigorous programming language semantics. In this summer project, students will investigate techniques to make the large models aware of programming language semantics and generate secure code. Participants should have (1) significant prior experience training neural networks and (2) solid systems programming skills (e.g., did well in COMS W3157).

Location of Research:

On-Site

# of hrs/week:

40

Department/Program:

Computer Science

Eligibility:

(1) significant experience training neural networks and (2) good systems programming skills (e.g., did well in COMS W3157). BS, Third Year, BS, Fourth Year, MS

To apply, please contact:

Junfeng Yang, junfeng@cs.columbia.edu