Jiaqi Huang

(+1) 352-217-0452 jiaqih@illinois.edu HomePage 777lefty Jiaqi (Jerry) Huang

Research Interest

I am generally interested in topics related to *system reliability & security* and their intersection with *AI.* To be specific, building reliable & trustworthy software and systems for real-world problems and the problem of establishing security guarantee for systems and LLMs now draws my greatest interest and attention.

Education

Nanjing University Sept. 2022 - June 2026 (expected)
B.S. in Computer Science (National Elite Program Class) *Current GPA: 4.44/5.0*

North Carolina State University Jan. 2025 - Feb. 2025
Exchange Student (GEARS Program) *Courses Taken: Research Skills Workshop*

Publication

[DLSP2024] *Subtoxic Questions: Dive Into Attitude Change of LLM's Response in Jailbreak Attempts.* Tianyu Zhang, Zixuan Zhao, **Jiaqi Huang**, Jingyu Hua, Sheng Zhong [paper]

Research Experience

XLab, University of Illinois at Urbana-Champaign | *Research Intern* July. 2025 – Present
Advised by Prof. Tianyin Xu *Topic: Cloud System Reliability & SRE Agent*

- Developing a unified benchmark for AIOps Agents, where a holistic taxonomy of cluster failures can be simulated on the k8s cluster via specifically designed fault injection and recovery mechanism, forming problems for agents to solve. The benchmark is the first of its kind to deploy microservice cloud environments, inject faults, generate workloads, and export telemetry data, while orchestrating these components and providing interfaces for interacting with and evaluating agents.
  - Role in the project: Designed a series of problem in the benchmark based on reproducing metastable failures on microservices apps (First in this field); Designed and implemented a noise mechanism that simulates the noise in real production clusters via chaos engineering tools; Implemented a etcd snapshot module for the benchmark to recover cluster states after single problem runs to optimize evaluation performance by 26%.

RTIS Lab, North Carolina State University | *GEARS Research Program* Jan. 2025 – Apr. 2025
Advised by Prof. Zhishan Guo *Topic: Healthcare AI & Real-Time System*

- Developing a real-time system, which could be deployed on embedded devices (wearable devices) and consists of a series of deep learning models with different efficiencies that classify cardiovascular diseases (CVDs) based on electrocardiograms (ECGs). By monitoring the user's physiological data, it determines and schedules the appropriately sized model for diagnosis, enabling real-time CVD detection.
  - Role in the project: Designed, implemented and trained models of different scales that classify CVDs based on ECGs; Designed a more reasonable loss function for training; Achieved an accuracy of 96% on the Physionet dataset with low inference time.

Software Engineering Institute, Peking University | *Research Intern* Sept. 2024 – July. 2025
Advised by Prof. Yasha Wang *Topic: ML4DB*

- Worked on designing an error correction module for a text-to-SQL LLM, which detects semantic errors in the generated SQL query by comparing its latent embedding with that of the input natural language query, without executing the SQL query.
  - Role in the project: First, tried different methods to design the module and ran experiments to test them, including LLM-based few-shot learning and so on; Designed a rule-based translator that could parse SQL queries into AST, then finally translated into SQL plan-like intermediate representation; Trained a Graph Attention Network to extract the embedding of the AST-like IR, using it as the latent embedding of SQL. Via this method, we build an easy-to-train small model (0.4M parameter) that achieves 99+% recall rate with rather low inference time, while preserves a success rate comparable to SOTA LLMs.

COSEC Group, Nanjing University | *Research Intern* Sept. 2023 – Sept. 2024
Advised by Prof. Sheng Zhong and Prof. Jingyu Hua *Topic: LLM Security*

- Designed a novel experiential model that could explain the gradual shift in LLMs' responses to users' queries, including jailbreak attacks, and an efficient jailbreak method for generating toxic prompts that simulates gradient descent in a black-box approach. Relevant results have been accepted by IEEE S&P 2024 DLSP Workshop after being formed into a paper.
  - Role in the project: Designed and implemented multiple rounds of interactive experiment, gained results from analyzing the of feedback of LLM; Concluded and devised the experiential model that explains phenomena in jailbreaks and verified it; Undertook the task of writing and polishing this paper.

Project

Secure-npm (Snpm) June 2024 - Aug. 2024

- Project built during the summer research program advised by Prof. Nikos Vasilakis
- Designed and implemented a software system based on npm that installs and manages third-party software packages on npm platform with the techniques of containerization and compartmentalization, thus defending against supply chain attacks efficiently.
- Devised and implemented the remote procedure call module, where an HTTP server was created and applied so that users can call functions or properties of the module from outside the container efficiently; Undertook the task of writing and polishing the paper.

NJU Emulator (NEMU) Sept. 2023 - Jan. 2024

- Curricular project for Introduction to Computer System (honors class), one of the most difficult lessons specialized for Elite Program students
- Developed an emulator with C and assemble language, along with the supplementary runtime environment and a simple operating system on it, so that we can finally ran some small programs and even the famous video game *"Chinese Paladin"* on it
- Learned how to debug and organize the structure of huge developing projects and read the manuals, documentation and source codes of it (Eventually got 90+ scores in this lesson)

Skills

Programming Languages: C/C++, Python, Go, JavaScript, LaTeX, Verilog HDL
Tools: Git/GitHub, Kubernetes, VS Code, Vivado, Logisim, Vim, Unix Shell, Linux
Languages: Chinese (native), English (fluent, TOEFL iBT total: 110, listening: 29, reading: 30, speaking: 25, writing: 26)

Selected Awards

- Special Scholarship for Undergraduates in Basic Sciences (Elite Program only), Nanjing University Nov. 2024
- People's Scholarship, Nanjing University Oct. 2024
- People's Scholarship, Nanjing University Oct. 2023
- Excellent Volunteer Student Ambassador, Nanjing University Mar. 2023