**Aofan Liu**

Base: **Shenzhen · On Site**

mailto:af.liu@stu.pku.edu.cn

Tel：13418788132

[GitHub Page: github.com/Fab-Liu](https://github.com/Fab-Liu)

**Education Background**

**Xiamen University（985, 211 Project） Software Engineering B.Eng.** 2020.09-2024.06

* Overall Ranking: Top 3%; Weighted GPA: 94.4/100; IELTS 7.0

**Peking University（985, 211 Project） Computer Science M.Sc** Until Now

* Directly admitted to Peking University for postgraduate study
* Research Interests: Model Retrieval, AI Security, and Privacy Protection

# Work Experience

**International Digital Economy Academy (IDEA)** 2024.09-2024.11

Shenzhen | Multimodal Group | Algorithm Intern **Algorithm Intern |**

* Designed and introduced the RepoAlign-Bench dataset to address the lack of standardized benchmarks in the code retrieval domain
* Developed a reflection-based RAG-aligned dual-tower model for semantic matching between natural language queries and code
* Improved the accuracy of code and documentation representation using Abstract Syntax Tree (AST) techniques and context augmentation

**Beijing Academy of Artificial Intelligence (BAAI)** 2024.01-2024.06

Beijing | Multimodal Group | **Algorithm Intern |**

* Participated in research on semi-automatic annotation technology for large-scale multimodal datasets
* Studied the security defense mechanisms for bypassing visual adversarial examples in aligning LLMs
* Contributed to optimizing conditional generation probabilities on small harmful datasets and research on multimodal model security
* Contributed to model **SFT** (Supervised Fine-Tuning) and **DPO** (Direct Preference Optimization) training processes based on **LLaMa Factory**, helping improve model accuracy by 5% on specific tasks

**Peking University V2X National Key Laboratory (PKU)** 2023.01-2023.10

Guangdong Province, Shenzhen | National Key Laboratory | **Research Assistant |**

* Independently built a fuzz database for over 60 CVEs (Common Vulnerabilities and Exposures) using AFLFuzz and LibFuzzer

**Xiamen University, Computational and Data Science Laboratory (XMU)** 2021.09-2022.01

Fujian Province, Xiamen | Computational and Data Science Laboratory **Research Assistant |**

* Participated in experimental design, implementation, management, and monitoring for several research papers
* Assisted senior researchers in drafting sections of multiple papers using LaTeX
* Coordinated remote server scheduling for the laboratory, tracked research progress of junior researchers, and summarized findings

# Academic Experience

**Research on NLPL Probing Tasks Based on Context Augmentation** 2024.09-2024.11

* Explored enhancing large language models (LLMs) in code understanding tasks by augmenting the comments section within code.
* Evaluated the impact of context augmentation on LLMs' natural language understanding, introducing enriched contextual information to assess performance in multimodal tasks.
* Leveraged a large open-source codebase with rich annotations and designed tasks to measure the effectiveness of context augmentation.
* Compared the performance of context-augmented methods with traditional approaches, such as using only code structure or comments.

**RefleXGen: Reflection-Based Controllable Code Generation (ICASSP)** 2024.06-2024.10

* Integrated Retrieval-Augmented Generation (RAG) techniques with self-reflection mechanisms in large language models (LLMs).
* Enhanced code generation safety without requiring model fine-tuning or specialized safety datasets.
* Built a dynamic knowledge base by incorporating historical feedback and secure code snippets, improving model's ability to generate secure code.

**VisualDAN: Exposing Vulnerabilities in VLMs with Visual-Driven DAN Commands** 2024.04-2024.06

* Evaluated the vulnerabilities in LLM security caused by visual input and explored the "jailbreaking" ability of visual adversarial examples
* Investigated the use of visual modality to output classic Jailbreak Prompt DAN series commands, achieving significant results
* Assessed the effects of attacks on various VLMs (e.g., MiniGPT-4, InstructBLIP, LLaVA) through experimental setups
* Conducted both manual and automated evaluations to determine the impact of adversarial examples on model outputs
* Compared the optimization loss and "jailbreaking" effects of visual versus text-based attacks, testing the effectiveness of existing defense technologies like DiffPure against visual adversarial examples

**PiCo: Jailbreaking Multimodal Large Language Models via Pictorial Text and Code Instruction** 2024.01-2024.04

* Investigated methods for jailbreaking aligned LLMs, including prompt injection, adversarial attacks, jailbreaks, and data poisoning
* Proposed the Toxicity and Helpfulness Evaluator, akin to F1-Score, for benchmarking and evaluating multimodal large models
* Focused on cross-modal attacks on MLLMs, particularly the security vulnerabilities of advanced models like Gemini-Pro and GPT-4
* PiCo successfully bypassed the security defenses of several advanced MLLMs, with an average attack success rate (ASR) of 56.27% on Gemini Pro Vision and 32.27% on GPT-4V

**Research on Semi-Automatic Annotation Technology for Large-Scale Multi-Modal Datasets** 2024.02-2024.04

* Contributed to building a promptable vision-based model capable of segmenting, recognizing, and describing any target within an image
* Developed a human-in-the-loop collaborative annotation framework based on a hybrid supervised large model, inspired by the SAM architecture
* Built a semi-automatic interactive annotation engine based on datasets like MSCoCo, CityScape, and Mapillary
* Improved annotation efficiency by 1-2 orders of magnitude and constructed a high-quality multimodal dataset of 500,000 images

**AccuracyFuzz: Targeted Fuzz Testing Tool Based on FineTuned Large Language Models** 2023.08-2024.01

* Developed a Transformer-based method to predict vulnerabilities at a finer granularity of the line level
* Used pre-trained CodeBERT models and self-attention mechanisms to achieve higher accuracy and efficiency
* Applied large models to conduct pattern testing of vulnerable software function locations
* This method significantly outperforms existing approaches in function-level prediction and line-level vulnerability detection, offering more precise and cost-effective vulnerability identification

**Competition& Project**

**18th CitiBank Cup Financial Innovation Application Competition | National First Prize** 2022.06–2023.04

* Developed a catalog storage program using Solidity
* Created a custom star image generation program using HTML/CSS and JavaScript
* Contributed to the development and debugging of a deep learning program for artistic image style transfer

**8th China International "Internet+" Innovation and Entrepreneurship Competition | National Third Prize** 2022.04-2022.10

* Led the development of the business plan and collaborated with business students to finalize the written plan and presentation materials.
* Used regression analysis and weighted averages to determine the initial launch plan for smart knee protectors
* Applied PEST and Ansoff Matrix models to analyze the potential and risks in the smart healthcare industry

# Club and Organizational Experience

**NASA Programming Challenge | North America | Team Leader** 2022.02-2022.04

* Led a diverse team of four members from China, Pakistan, the UK, and India.
* Authored a comprehensive 7,000+ word project proposal and app introduction document.
* Successfully developed a mobile application using Kotlin within a 72-hour timeframe in collaboration with the team.

**Blockchain Association, Xiamen University | Events Department | Deputy Director** 2021.09-2023.09

* Organized and participated in blockchain-themed lecture series co-hosted by Xiamen University and the Blockchain Association.
* Acquired foundational knowledge of the operational mechanisms of mainstream cryptocurrencies.
* Attended and contributed to the on-campus seminar, Blockchain + Finance, discussing the real-world applications of NFTs.

**AIESEC International Volunteer | University of Nottingham | Volunteer** 2021.08-2021.10

* Delivered 20 general English education sessions to refugee children from neighboring countries.
* Provided academic support to over 80 international students, including homework guidance and grading.
* Coordinated and managed schedules for 100+ global volunteers, ensuring smooth operations during the event.

# Professional skills

# Programming Languages

* Experienced in Python (version 3.x)
* Experienced in developing and maintaining web applications with frameworks such as **Django or Flask**
* Familiar with Python standard libraries and third-party libraries/frameworks such as **NumPy, Pandas, Django, Flask**, etc.

**Development Environment**

* Familiar with **Linux/Unix** operating systems, including basic command-line operations and system management
* Experienced with **Git**, familiar with platforms such as **GitHub** or GitLab, and get used to **Docker** containerization of applications

# Data Mining and Web Scraping

* Proficient in using the **Requests** library for HTTP requests
* Experienced with HTML/XML parsing using **BeautifulSoup** or LXML
* Familiar with JavaScript-rendered pages and using **Selenium** for data scraping
* Able to store scraped data in databases such as **SQLite, MySQL, MongoDB**, etc.

# Awards

* CitiBank Cup Financial Application Innovation Competition | National First Prize 2023.02-2023.06
* American Mathematical Contest in Modeling (MCM/ICM) | National First Prize 2023.02-2023.02
* Higher Education Press Cup National Mathematical Modeling Competition | National Second Prize 2022.11-2022.11
* 8th China International "Internet+" Innovation and Entrepreneurship Competition | National Third Prize 2022.04-2022.10
* 7th China International "Internet+" Innovation and Entrepreneurship Competition | National Silver Prize 2021.07-2021.10

**Skills and Specialties**

**Language Proficiency**：Chinese (native); English (IELTS 7.0);

**Hobbies and Interests**：Rock climbing, scuba diving, writing, video editing (PR, CapCut)