NANJUN ZHOU

Apt.635, Block C12, South China University of Technology, Guangzhou, China 510000
Mobile: +86 18066111058 ***Email: arbiter0102@gmail.com***

EDUCATION

South China University of Technology (SCUT) **Guangzhou, China**
Bachelor of Engineering in Computer Science & Technology *(Expected Jul.2025)* Jul.2021-Present
Elite Class (<u>a selective Honors Program: only 23 out of around 500 computer science students)</u>

- **Weighted Average GPA: 89.05/100**
- **Relevant Coursework:** Mathematical Analysis I & II; Linear Algebra and Analytic Geometry; Discrete Mathematics; Data Structure; The Design and Analysis of Computer Algorithms; Computer Organization and Architecture; Computer Networks; Operating System; Software Engineering; Database.

SKILLS

Programming:	Python, C++, Java, SQL, Ruby, HTML, JSON
Software & Tools:	Linux, Docker, GitHub, MATLAB, SPSS, Stata, Qt, LaTex, VMWare, WireShark, MobaXterm

PUBLICATIONS

- **Nanjun Zhou**, Weilin Lin and Liu Li. Gradient Norm-based Fine-Tuning for Backdoor Defense in Automatic Speech Recognition. In *ICASSP 2025 (**CCF-B**)*

RESEARCH EXPERIENCE

Backdoor Learning for Diffusion Models **Guangzhou, China**
Research Assistant (Under guidance of Professor Li Liu, HKUST-GZ SV4G Lab) Sep.2024-Jan.2025

- Independently conducted survey on backdoor attacks and defenses for **Diffusion Models**, including both **unconditional generation** and **text-to-image generation;**
- Reproduced **three existing backdoor attacks** and **two defenses** for unconditional diffusion models and proposed the first **comprehensive benchmark** for backdoor learning in diffusion models (submitted to IJCAI 2025 as the second author);
- Proposed two useful **analysis tools** for the benchmark: **Assimilation Visualization** and **Activation Norm**.

Backdoor Defense for Automatic Speech Recognition **Guangzhou, China**
Research Assistant (Under guidance of Professor Li Liu, HKUST-GZ SV4G Lab) Mar.2024-Sep.2024

- Independently surveyed and reproduced **seven existing attack methods** and organize these programs into a unified framework using **PyTorch**, reaching good attacking effects;
- Observed that the backdoor-related neurons in the victim models exhibit higher gradient values during training;
- Proposed **Gradient Norm-based Fine-tuning**, the **first effective model-level defense method** against backdoored models in the audio domain, reaching **state-of-the-art** performance.

Backdoor Defense for Deep Neural Networks **Guangzhou, China**
Researcher (Under guidance of Professor Patrick Chan, SCUT) Jul.2023-June.2024

- Worked with 2 teammates to survey the existing **backdoor attacks and defenses** in **computer vision** domain;
- Developed a backdoor attack and defense **framework** that incorporates **multiple backdoor attack** and **defense methods**, across **various datasets** and **models**, achieving effective attack and defense results;
- Guiding underclassmen in developing a new backdoor defense method based on **adversarial sample generation**.

WORKING EXPERIENCE

ZTE Corporation **Shenzhen, China**
Software Development Engineer Intern Sep.2024-Dec.2024

- Developed **Python** scripts to process business data lists in batches, converting business reports to a standard JSON structure and writing them into the **metadata platform**, a knowledge base of iGPT agent;
- Developed the data querying functionality of **Data Agent** using **Python** based on **LangChain**, converting natural language queries to SQL to retrieve analytical data from databases in various domains within company;
- Developed a data testing script and a testing interface for the Data Agent based on **Flask**, ensuring data integrity and authority validation for the interface;
- Developed a data cleaning script using **BeautifulSoup**, converting the HTML codes of the requirements documents into a standard JSON structure and text paragraphs, making it easier for LLMs to understand.

E-surfing Internet of Things Technology, China Telecom **Guangzhou, China**
AI Application Intern Jul.2024-Sep.2024

- Deployed LLMs privately using LLM services including **Ollama** and **Xinference** for constructing an intelligent agent;
- Deployed an RAG service **RAGFlow**; built a local knowledge base and tuned the parameters of LLMs to test the performance of the RAG system, reaching **an accuracy of over 85%**;
- Developed a dialog program to test the **API functions** of RAGFlow, aiming to communicate with a chatbot on RAGFlow;

- Built a question-intent dataset using **data augment technique**, and trained **a Bert classifier** with the dataset for the **intent recognition task** using **PyTorch**, achieving **an accuracy of over 99%**.

Hong Kong University of Science and Technology (Guangzhou) **Guangzhou, China**
Research Assistant (Guided by Professor Li Liu) Jan.2024-Present

- Conducting research on **Trustworthy Machine Learning;**
- Invited guest speakers via email and designing even schedule for AIAA6102 AI Seminar in 2024 Spring semester;
- Assisted the team in general operations and finance work, such as coordinating and collecting employee onboarding materials and other information.

HONORS & AWARDS

• SCUT University Scholarship: Second Prize	Dec. 2024
• 2023 MathorCup Mathematical Contest in Modeling: Third Prize	Jun. 2023
• 2022 Asia and Pacific Mathematical Contest in Modeling (APMCM): Third Prize	Jan. 2023
• 2022 National Mathematical Modeling Contest (Guangdong): Third Prize	Oct. 2022
• School Merit Student	Dec. 2022
• SCUT University Scholarship: Third Prize	Dec. 2022