JUNJIE SU

(+86) 159 2004 1151 | *momoyeyu@outlook.com* | *homepage*

Research Interests: AI Agent, Trustworthy AI, Adversarial Machine Learning

EDUCATION

Beijing University of Posts and Telecommunications (BUPT), Beijing, China

Bachelor of Cyberspace Security *Sept, 2022 – Jul, 2026 (expected)*

- **GPA: 3.7/4.0**

Core Courses

- **Mathematics**: Linear Algebra (94), Discrete Mathematics (94), Mathematic Foundations of Information Security (95), Mathematical Modeling and Simulation (96)
- **CS**: C++ Programming (96), Python advanced language programming (96), Java Programming Design and Practice (93), Operating System (94), Computer Networks (93), Assembly language and reverse engineering (93), Database Technologies and Applications (93)

PUBLICATIONS & MANUSCRIPTS

1 **Junjie Su**, Weifei Jin, Yuxin Cao, Derui Wang, Kai Ye, and Jie Hao. "Mirage Fools the Ear, Mute Hides the Truth: Precise Targeted Adversarial Attacks on Polyphonic Sound Event Detection Systems." Submitted to The **41st Conference on Uncertainty in Artificial Intelligence (UAI), 2025.** *Under review.*

2 Weifei Jin, Yuxin Cao, **Junjie Su**, Derui Wang, Yedi Zhang, Minhui Xue, Jie Hao, Jin Song Dong, and Yixian Yang. "Whispering Under the Eaves: Protecting User Privacy Against Commercial and LLM-powered Automatic Speech Recognition Systems." To appear in the **34th USENIX Security Symposium (USENIX Security), 2025.** Seattle, WA, USA.

3 Weifei Jin, **Junjie Su**, Hejia Wang, Yulin Ye, and Jie Hao. "Boosting the Transferability of Audio Adversarial Examples with Acoustic Representation Optimization." Accepted to IEEE International Conference on Multimedia & Expo (ICME) 2025.

4 Weifei Jin, Yuxin Cao, **Junjie Su**, Qi Shen, Kai Ye, Derui Wang, Jie Hao, and Ziyao Liu. "Towards Evaluating the Robustness of Automatic Speech Recognition Systems via Audio Style Transfer." In Proceedings of the 2nd ACM Workshop on Secure and Trustworthy Deep Learning Systems (SecTL, AsiaCCS Workshop), 2024, pp. 47–55. Singapore.

RESEARCH EXPERIENCE

Beijing University of Posts and Telecommunications (BUPT), Beijing, China
National Engineering Research Center of Disaster Backup and Recovery,
School of Cyberspace Security *Jun, 2023 – Present*
Research Assistant, Advisor: Prof. Jie Hao

Project: Adversarial Attacks on End-to-End Audio Models Based on Deep Learning

- Designed the preservation loss constraint using context information and implemented the first adversarial attack against sound event detection system in audio surveillance scenario.
- Proposed a novel evaluation metric for assessing attack performance on general 2D classification tasks.
- Achieved state-of-the-art attack transferability compared to all existing methods on audio adversarial attacks against automatic speech recognition.

PROJECT EXPERIENCE

AI Table Tennis — Full-Process Intelligent Tournament System
Entrepreneurial Project | National Level
Software Engineer *Sept 2023 – Present*

- Developed a backend using SpringBoot, proficiently utilizing Java collection frameworks and concurrent programming to optimize data processing, combined with Redis caching and efficient SQL queries, reducing API response time by approximately 35%.
- Built an algorithm backend using Flask to encapsulate services such as skeletal recognition and object detection, interfacing with the SpringBoot main business backend via REST-API, encapsulating services at the Service layer to decouple business and algorithm logic, enhancing system modularity.
- Conducted in-depth user requirement research and multiple offline tests, optimized business logic targetedly, significantly increasing user engagement, with active users exceeding 1,500.

WORK EXPERIENCE

Antiy Technology Group Co., Ltd.
Technical Committee/Security Development Engineer (Intern) *Jul, 2024 – Aug, 2024*

- Developed the Android reverse analysis tool SmaliAnalyzer, optimizing the decompilation of try-catch blocks in the Smali language, and enabling the decompilation of code blocks into Java that some professional software like JEB Pro could not directly decompile.
- Utilized tools such as IDA, GDA, and JEB Pro to perform reverse analysis on Android applications, identifying logical vulnerabilities and stack overflow vulnerabilities.

STUDENT WORK

BUPT Table Tennis Association
President *Sept 2023 – Jul 2024*

- Led a core team of 40 as president, overseeing the planning and execution of all association activities.
- Promoted the association, growing the active membership to over 900 during my tenure.
- Successfully organized multiple large-scale events, including a inter-campus tournament, an eight-university friendly match (hosted and moderated), faculty-student friendlies, and college-level team competitions, demonstrating strong leadership and organizational skills.

SCHOLARSHIPS & AWARDS

- **2024** Won **National Bronze Award** in the China International College Students' Innovation and Entrepreneurship Competition (2024)
- **2024** Won **Second Prize** in the 9th National Cryptography Technology Competition
- **2024** Awarded **Second-Class Scholarship** at BUPT
- **2024** Recognized as **Active Contributor to Arts and Sports** at BUPT
- **2023** Awarded **Third-Class Scholarship** at BUPT

SKILLS

Proficient	Python, PyTorch, Jupyter, Java, SSM, SpringBoot, Markdown, LaTeX, Git.
Familiar	Linux, MySQL, Redis, C/C++, HTML, JavaScript, etc.