Jerry Wang

Email: 111306078@g.nccu.edu.tw | Website: pen9rum-github-io.vercel.app
LinkedIn: linkedin.com/in/teddyagee | GitHub: github.com/pen9rum

RESEARCH INTERESTS

Deep Learning · Information Retrieval · Adversarial Machine Learning · Trustworthy AI · Theory of Mind in AI · Multimodal Learning· Deep Reinforcement Learning · Reasoning in LLM·Reasoning in structured knowledge

EDUCATION

National ChengChi University (NCCU) Taipei, Taiwan
Bachelor of Commerce in Management Information Systems Sept. 2022 – Present
Double Major in Bachelor of Science in Artificial Intelligence Applications

- GPA: 3.92/4.0 (CS courses GPA: 4.0)

Honor & Awards

Deliman AI Scholarship, NCCU 2025

College Student Research Grant by the National Science and Technology Council 2025
Project: *Adversarial Example Generation for Automated Testing of Reinforced Retrieval-Augmented Generation and Expert-Mixture Models Using the PyCT Framework*

1st Place – Google DevJam Hackathon 2025 Group Gemini API 2025
Project: Gemini-powered Abroad Application Assistant

Finalist – Government Presidential Hackathon 2024
Project: Electric bus energy optimization system based on Genetic Algorithms (GA) and Large Language Models (LLM)

2nd Place – AWS Generative AI Applications Hackathon 2024
Project: Energy optimization solutions for AWS

3rd Place – Meichu Hackathon- Kronos Research 2022
Project: Trading strategy variant based on SMA

Top 3 – ACT Influential Plan– Business Technology Application Competition 2022
Project: Python-based Line Chatbot for handicapped

PUBLICATION

Wang, J., and Yu, F. "Gradient-Free Adversarial Prompt Optimization for RAG Systems via Differential Evolution." Under review at KDD 2026 (Research Track).

Wang, J., and Yu, F. *"DeRAG: Black-box Adversarial Attacks on Retrieval-Augmented Generation Applications via Prompt Injection."* Accepted at KDD 2025 (Workshop on Prompt Optimization).

Kuan-wu Chu, Joanna Qiong-yue Chen, **Jerry Wang,** …, Lyn Chao-ling Chen, *" Social Temperature: Real-Time Social Activity Monitoring Based on Deep Learning Methods"* , Accepted at 2024 International Computer Symposium ,IEEE

Wang, J., and Liu, T. Y. "Observer, Not Player: Simulating Theory of Mind in Large Language Models through Game Observation." Under review at NeurIPS 2025 Workshop on LAW.

Yao, Y.C and **Wang, J.** "BEARing the Game: Basketball Event Analysis with Recurrent Networks." Under review at TANet 2026

RESEARCH EXPERIENCE

Graph Lab, Stony Brook University Remote(New York, U.S.A)
Research Assistant, Advisor: Prof. Tengfei Ma Aug 2025 – Present
Onging Publication: CocoRAG — Dynamic Graph RAG with Coconut-Enhanced Reasoning

- Developing a dynamic Graph RAG system enhanced with improved Chain-of-Thought prompting (Coconut) for more robust reasoning.
- Targeted to evaluate on Knowledge Graph QA tasks to evaluate the effectiveness

Reinforcement Gaming Lab, Academia Sinica
Research Assistant, Advisor: Prof. Ti-Rong, Wu July 2025 – Present
Project: A stochastic MCTS based Go Variant based on Deep Reinforcement Learning

- Developing under stochastic environment on GO under AlphaZero Structure, adding mechanisms to adapt on more complexed gaming environment
- Modified traditional MCTS tree archictecture to accommodate a multi-turn gaming environment

Future Media Lab, NCCU
Research Assistant, Advisor: Prof. Prof. Chen, Lyn Chao-ling Jan. 2024 – Sep 2025
Project: 0Real-Time Social Activity Monitoring Based on Deep Learning Methods

- Developed a novel approach for measuring social temperature through a real-time deep learning multi-modal model including sound and emotion recognition assist with YOLO and DeepFace
- Utilized OpenAI Whisper model in Speech-to-Text conversion to retrieve texts from audio signals, and Voice Activity Detector for distinguishing speech from ambient noise

Project : BEARing the Game: Basketball Event Analysis with Recurrent Networks

- Developed a novel prediction framework that augments LSTM networks , improving NBA player performance prediction accuracy by over 10%.

Software Security Lab, NCCU
Research Assistant, Advisor: Prof. Prof. Fang Yu July 2024 – Present
Project: Gradient-Free Adversarial Prompt Optimization for RAG Systems via Differential Evolution

- Developed DeRAG, a novel black-box attack leveraging Differential Evolution to generate adversarial prompt suffixes that mislead retrieval in RAG-based QA systems
- Achieved state-of-the-art attack success (e.g., 100%@Top-10 on MS MARCO, >70%@Top-20 on SciFact) while minimizing token perturbations and maintaining stealthiness
- Proposed a prompt optimizing method to both improved the success rate over 10% on multiple GPT modern models by tuning general Jailbreaking adversarial prompts

Projects: Observer, Not Player: Simulating Theory of Mind in Large Language Models through Game Observation

- Developed an interactive evaluation mechanism for LLM reasoning in games via defined metrics for enabling real-time visualization, failure analysis, and reproducible evaluation.

Project: Extension Development for Deep Learning Network Concolic Testing

- Enhanced deep neural network testing by integrating VGG16, LeNet, and ResNet-based structures, which allows a larger model of Original PyCT

WORK EXPERIENCE

Binance Remote(Taipei, Taiwan)
QA Engineer (Accelator Program), AI and Data Service team Sep. 2025 – Present

- Evaluating risk check agent for AI safety, created over 1,000 test cases and auto pipeline on AWS SageMaker
- Designed red teaming singal turn and multi-turn prompts to attack internal bot for bot robustness

Carousell Taipei, Taiwan
Testing Engineer Intern Feb. 2025 – Jun 2025
Project: AI-powered Chatbot Development based on Gemini API and Golang

- Implemented automation testing using Golang and Jenkins to enhance testing efficiency over 12%
- Optimized and managed Trinity for iOS and Android, streamlining version control, deployment, and secure integration of secrets via Vault while using Gemini and Copilot to increase efficiency.

Delta Electronics Taipei, Taiwan
Software Engineer Intern Jan. 2024 – Feb. 2024
Project: Car Motoring pipeline data evaluation and report automation system

- Built a Python-based automation system for company progress tracking, enhancing efficiency by 15% across the entire workflow, with the assistance of C to mock experiments on car motoring via Infineon Board to enhance system performance

TEACHING EXPERIENCE

Teaching Assistant, NCCU Sept. 2024 – Jan. 2025
Course: Data Structures

- Taught Java-based data structures to a class of over 100 students, ensuring strong foundational knowledge, and developed an automated grading system with Python to reduce TA workload
- Supervised final projects, integrating modern web architecture, accelerated development speed by 35% through structured guidance

LEADERSHIP

Google Developer Student Clubs (GDSC), NCCU
Project Lead, Vice President July 2023– July 2025

- irected and mentored teams of 10+ members while leading a community of 500+ participants, overseeing 10+ AI and software development projects from planning to technical execution.
- Managed course content focusing on Deep Learning, Retrieval-Augmented Generation (RAG), and Python fundamentals to provide insights on latest technology

Reviwer in Efficient Reasoning Workshop, NeurIPS **2025**

SKILLS

AI/ ML Framework : TensorFlow / PyTorch /AutoML / Amazon Bedrock/ Amazon Sage Maker / Vertex AI/ YOLO
Full-stack web design: Python / Java / Golang / C / SQL /HTML/CSS /JS / React/ React Native/ Fast API/Spring Boot
Databases and Others: Firebase / MySQL / MongoDB/ Google Cloud Platform/ Docker/ K8S/ FAISS

REFERENCE

Prof. Yu Fang , Dept of Management in Information Systems, NCCU
Mail:yuf@nccu.edu.tw

Prof. Chen, Lyn Chao-ling, Dept of NCCU AI Center, NCCU
Mail:lynchen@ntu.edu.tw

Prof. Tsaih, Rua-Huan Dept of Management in Information Systems, NCCU
Mail:tsaih001@nccu.edu.tw