WEIXUAN DING

Weixuan.Ding@outlook.com
wxding.top

EDUCATION

Wuhan University, Wuhan, China — *September 2022 — June 2026 (Expected)*
School of Cyber Science and Engineering — GPA: 3.80/4.00
Undergraduate Student in Cyberspace Security — 90.37/100

RESEARCH EXPERIENCE

Client-side Ownership Protection for Federated LLMs — December 2024 - Present
Stevens Institute of Technology - Research Intern — *Advisor: Hao Wang*

- Formulate a novel threat model for model stealing and unauthorized distribution in federated LLMs, and conduct a systematic analysis of why existing watermarking approaches fail in this setting.
- Address the main challenges in federated LLM fingerprinting, investigate model behavior during aggregation, and establish efficient and robust black-box watermarking and verification mechanisms.
- Launch ongoing experimental research, handle federated fine-tuning and evaluation pipelines, and build practical expertise in large-scale model optimization, data analysis and experimental research planning.

Open-World Object Placement via Imaginary Search — October 2024 - May 2025
University of Louisville - Research Intern — *Advisor: Zeyan Liu*

- Conducted comprehensive research on open-world object placement, investigating how multimodal language models can efficiently reason on spatial relationships and scene context.
- Designed a training-free framework that integrates iterative decision-making, multimodal reasoning, and heuristic search for open-world visual reasoning.
- Achieved state-of-the-art performance on 2 benchmarks against 7 baseline methods, and produced a manuscript under review, providing insights in open-world visual reasoning.

PROJECT EXPERIENCE

Intelligent Risk Monitoring System in Decentralized Finance — August 2024 - October 2024
Team Member

- Collaborated in the design of TrxLLM, a blockchain transaction risk monitoring system that integrates graph neural networks and Transformer to analyze complex transaction dependencies and malicious behaviors.
- Developed the web system using Vue 3 and Vite to support real-time transaction visualization, address risk evaluation, and interactive monitoring functionalities for practical deployment.
- Validated system effectiveness through large-scale experiments on 80K transactions, achieving 92% accuracy in malicious transaction detection, 85% accuracy in address risk assessment.

ACHIEVEMENTS

First Prize in the National College Student Blockchain + Application Competition — *Fall 2024*
Yearly Model Student of Academic Records — *Fall 2024 & 2025*
Yearly Third-Class Scholarship — *Fall 2024 & 2025*

PUBLICATIONS

Under Review

- **W. Ding**, S Liu, H Pei, Z. Liu, "Presto: Efficient, Training-free, and Open-world Object Placement via Imaginary Search", 2025

SKILLS

Programming Languages	Python, C/C++, SQL
AI Stack	PyTorch, Transformers, PEFT, LangChain, vLLM
Tools	Matplotlib, NumPy, Pandas, Git, Docker, Vue
Languages	Chinese(Native), English(Proficent)