

WEIXUAN DING

wxding.top

(+86) 157 2680 2730

Weixuan.Ding@outlook.com

EDUCATION

Wuhan University, Wuhan, China
School of Cyber Science and Engineering
Undergraduate Student in Cyberspace Security

September 2022 — June 2026 (Expected)

GPA: 3.77/4.00

89.81/100

SKILLS

Programming Languages	Python, C/C++, SQL, JavaScript, HTML/CSS, LaTeX
Libraries	Pytorch, Pandas, Matplotlib, Numpy, BeautifulSoup, Selenium
Frameworks	Vue, Node.js
Languages	Chinese(Native), English(Proficient)

RESEARCH EXPERIENCE

Data Security Lab, Wuhan University
Undergraduate Research Assistant

March 2024 - June 2024

- Research on Privacy-Preserving Federated LLMs with Heterogeneous Data Distributions
- Evaluated privacy-preserving techniques in Federated Learning for Large Language Models (LLMs), focusing on differential privacy approaches.
- Assessed the performance of methods such as FedProx, Bounded Local Update Regularization (BLUR), and Adaptive Noise Mechanism (ANDPFL), while exploring potential optimization strategies.

PROJECT EXPERIENCE

National College Student Blockchain Plus Application Competition August 2024 - Present
Team Member

- Design TrxLLM, a blockchain transaction risk monitoring system based on Graph Neural Networks (GNN) and Transformer.
- Assist in implementing large-scale models with GNN and Transformer to analyze complex dependencies in blockchain transaction data, improving model generalization and downstream task performance.
- Developed the frontend using Vite and Vue3, creating a user-friendly interface for real-time transaction display, risk evaluation, and transaction monitoring functionalities.

INTERESTS

Research Interests:

Adversarial Machine Learning, Privacy-preserving Machine Learning, Trustworthy AI, LLM

ACHIEVEMENTS

Model Student of Academic Records
The Third Prize Scholarship

Fall 2024

Fall 2024