WEIXUAN DING

wxding.top
(+86) 157 2680 2730
Weixuan.Ding@outlook.com

EDUCATION

Wuhan University, Wuhan, China — *September 2022 — June 2026 (Expected)*
School of Cyber Science and Engineering — GPA: 3.77/4.00
Undergraduate Student in Cyberspace Security — 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(Proficent)

RESEARCH EXPERIENCE

University of Louisville — October 2024 - Present
Undergraduate Research Intern — *Advisor: Zeyan Liu*

- Research on generating unrestricted adversarial examples via generative models.
- Explore the potential of diffusion-based models in multimodal adversarial attack tasks.

Data Security Lab, Wuhan University — March 2024 - June 2024
Undergraduate Research Intern

- 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 Information Security Contest — October 2024 - Present
Team Member

- Design an efficient deepfake detection system based on identity inconsistency.
- Distill a Transformer-based model for efficient inference on edge computing devices using locally stored user image resources.

National College Student Blockchain + Application Competition — August 2024 - October 2024
Team Member

- Design TrxLLM, a blockchain transaction risk monitoring system based on Graph Neural Networks (GNN) and Transformer, to analyze complex dependencies in blockchain transaction data.
- Developed the frontend using Vite and Vue3, creating a user-friendly interface for real-time transaction display, risk evaluation, and transaction monitoring functionalities.

ACHIEVEMENTS

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

INTERESTS

Research Interests:

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