Zhirui Zeng

✉ zhiruizeng@cqu.edu.cn · ☎ (+86) 133-7260-3242

Education

Chongqing University (CQU), Chongqing, China 2021 – Present

M.S. in Computer Science and Technology, expected June 2024

- **Faculty Mentors:** Prof. Shangwei Guo
- **Key Modules:** Graph Theory; Machine Learning; Digital Image Processing; Scientific Research Methods and Thesis Writing; Algorithm Analysis and Computational complexity.
- **GPA: 3.58** / 4.

Chongqing University (CQU), Chongqing, China 2017 – 2021

B.S. in Computer Science and Technology

- **Faculty Mentors:** Prof. Shigang Zhong
- **Key Modules:** Algorithms and Data Structures; Principle of Computer Composition; Operating System; Computer Network; Database System; Discrete Mathematics.
- **GPA: 3.38** / 4.

Research Interests

- Artificial Intelligence Security
- Large-scale Language Model Security
- Multimodal Model Security
- Adversarial Machine Learning
- Natural Language Process

Publications

1. Tao Xiang, **Zhirui Zeng**, Shangwei Guo , Jialing He, Qiao Zhang, Guowen Xu, and Tianwei Zhang. Contrast-then-Approximate: Analyzing Keyword Leakage of Generative Language Models.

- **Journal Name:** IEEE Transactions on Information Forensics and Security (TIFS)
- **Status:** Under Review

2. **Zhirui Zeng**, Lishuang Hu, Shangwei Guo, Jialing He, Tao Xiang, Tianwei Zhang. Are Our Texts Used for Augmenting BERT? Auditing Data Provenance for Discriminative Models.

- **Conference Name:** 2024 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)
- **Status:** Under Review

Experience

Objective evaluation theory of multimedia big data perception security Dec. 2022 – Nov. 2025

Role: Participant

Brief introduction: In view of the contradiction that multimedia big data is either unsafe to use or safe but unusable, we focus on the characteristics of multimedia data and study efficient and practical security and privacy protection technologies in the entire life cycle of multimedia big data storage, sharing, query, release, processing and analysis. Break through the conflicting dilemma between security and availability of multimedia big data.

- Investigate the distributed two-way access control encryption method to achieve data security in a distributed environment.
- The project belongs to National Key R&D Program of the Ministry of Science and Technology (Sub-project).
- Project Number: 2022YFB3103501

Research on Byzantine Fault Tolerance in Decentralized Federated Learning Based on System Characteristics Jan. 2022 – Dec. 2024

Role: Participant

Brief introduction: Decentralized federated learning is a type of learning system without central servers and is vulnerable to Byzantine attacks. Existing Byzantine attack and fault tolerance works have the following problems: it is impossible to attack all benign node in a decentralized system with a small number of Byzantine nodes; it cannot be guaranteed that all benign nodes uniformly and effectively resist existing Byzantine attacks; it does not provide privacy protection while resisting Byzantine attacks. This proposal aims to address the above problems in decentralized federated learning, including using network topology characteristics of decentralized systems to design efficient Byzantine attacks with a single malicious node; constructing a Byzantine fault tolerance aggregation rule based on iterative features to ensure that all benign nodes uniformly converge to the ideal deep learning model under Byzantine attacks; using differential privacy features and machine learning technologies to design an aggregation rule that meets both privacy protection and Byzantine fault tolerance.

- Investigate a method that combines differential privacy features and machine learning technologies to design an aggregation rule that satisfies both privacy protection and Byzantine fault tolerance.
- The project belongs to National Natural Science Foundation of China (Young Scientists Fund Program).
- Project Number: 62102052

RNN-Based Urban Natural Gas High-Pressure Pipeline Network Operation Status Risk Assessment System Projects Jun. 2019 – Jul. 2020

Role: Participant

Brief introduction: The pressure data of natural gas pipeline network operation is collected by the monitoring station every 20 minutes, so it has very obvious timing characteristics. Therefore, we choose RNN network to build an assessment system, which uses the pressure data of the first four hours to predict the pressure data of the next time point to judge the risk.

- Investigate previous urban natural gas high-pressure pipeline network operation status risk assessment system methods.
- Participate in the research of modeling the pipeline topology network and train the RNN model using pipeline pressure data.
- Project Number: s201910611368

Honors and Awards

Scholarship of Chongqing University.	Oct. 2022
Scholarship of Chongqing University.	Oct. 2021
Third Prize in China College Student Mathematics Competition	Nov. 2020

Skills

- Language: IELTS 6.5
- Programming Languages: C/C++, Python, Java and Html
- Platform: Linux
- Computer fundamentals: Basic knowledge of deep learning, basic knowledge of natural language process, basic knowledge of git command, and knowledge of language models
- Personal: Football, Guitar, Sing, Read