MING YIN

✉ Email 🌐 Website in LinkedIn GitHub

Education

University of Science and Technology of China (USTC) Sept 2020 - Present

School of the Gifted Young, Computer Science

Major GPA: 3.81 (88.29/100) Overall GPA: 3.6 (86.42/100) TOEFL: 105 (R: 29, L: 29, S: 20, W: 27)

Relevant Coursework:

Introduction to Computing Systems A(98), Computer Organization(90), Computer System(A), A Guide to Formal Methods(90), Fundamentals of Scientific Programming with Python(A), Advances in Computer Graphics(95), Principles and Techniques of Compiler(90), Stochastic Processes B(92), Function of Complex Variable B(90)

Research Intersets

Security, Trustworthy Machine Learning, Large Language Models, Optimization, Federated Learning

Publications

*** indicates equal contribution.**

1. Robust Federated Learning Mitigates Client-side Training Data Distribution Inference Attacks

Yichang Xu*, **Ming Yin***, Minghong Fang and Neil Gong

Submitted to The 2024 ACM Web Conference

2. Poisoning Federated Recommender Systems with Fake Users

Ming Yin*, Yichang Xu*, Minghong Fang and Neil Gong

Submitted to The 2024 ACM Web Conference

Research Experience

Robust Federated Learning Mitigates Client-side Data Inference Attacks Mar 2023 - June 2023

Advisor: Prof. Neil Gong, Duke University

Motivation: Existing defense mechanisms are ineffective in defending against client-side inference attacks.

- Introduced InferGuard, an innovative defense designed to protect against client-side inference attacks.
- Proposed adaptive attack using PGD.
- InferGuard effectively mitigates client-side inference attacks, outperforming all the baselines.

Poisoning Federated Recommender Systems with Fake Users July 2023 - Oct 2023

Advisor: Prof. Neil Gong, Duke University

Motivation: Existing attacks on federated recommender systems (FedRecs) necessitate supplementary system information other than the received item embedding, such as genuine users' local training data or the popularity distribution of items.

- Introduced PoisonFRS, a novel poisoning attack that needs no extra information about FedRecs.
- Conducted extensive experiments and proved PoisonFRS is effective even when the proportion of fake users is extremely low, a scenario where all the baselines are ineffective.
- Demonstrated the superior concealment of PoisonFRS.

Large Language Model Toxic Content Detection Nov 2023 - Present

Advisor: Prof. Weiming Zhang, USTC

Motivation: Currently, Large Language Models (LLM) still have limited ability to detect toxic content, including sensitive keywords, euphemisms, and anti-prefixes.

- Used GPT-4 to label small datasets and compare them with the results generated by the toxic content detection classifier.
- Trained the toxic content detection classifier through knowledge distillation.
- Aim to surpass the current state of the art in toxic content detection.

Skills

Programming	Python, C, C++, Java, Assembly, Verilog, HTML, CSS, SQL
AI Toolkits	Pytorch, Tensorflow, MXNet
Miscellaneous	Linux, LaTeX, Markdown, Git

Selected Honors

Excellent Student Scholarship Gold (TOP 3%)	Oct 2020
Anhui Collegiate Programming Contest (Second Place)	Oct 2021
Excellent Student Scholarship Bronze (TOP 20%)	Oct 2022
Qiangwei Progress Scholarship (52/1000)	Oct 2023
Excellent Student Scholarship Gold (TOP 3%)	Oct 2023

Extracurricular Activities & Leadership

Class Committee, School of the Gifted Young, USTC Sept 2020 - Present

- Organized activities such as the Mid-Autumn Festival Gala and the New Year's Eve Gala.
- Played a key role in promoting student-faculty communication.

USTC Admissions Volunteer June 2021 - July 2021

- Held presentations to promote USTC.
- Assisted high school students with inquiries and helped them apply to USTC.