MING YIN

✉ Email 🌐 Website LinkedIn GitHub

Education

School of the Gifted Young, **University of Science and Technology of China (USTC)** Sept 2020 - Present

Computer Science and Technology

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

Highlight Courses:

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

Research Interests

Trustworthy AI, Security, Large Language Models, Federated Learning

Publications

*** indicates equal contribution.**

1. Poisoning Federated Recommender Systems with Fake Users

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

Submitted to The 2024 ACM Web Conference

2. 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

Research Experiences

Robust Federated Learning Mitigates Client-side Data Inference Attacks Mar 2023 - Jun 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 an adaptive attack using Projected Gradient Descent (PGD).
- Outperformed all 10 baselines in mitigating multiple inference attacks with InferGuard, as demonstrated by 3 different evaluation metrics.

Poisoning Federated Recommender Systems with Fake Users Jul 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.

- Proposed PoisonFRS, a novel poisoning attack that needs no extra information about FedRecs.
- Conducted experiments on 4 real-world datasets, and PoisonFRS consistently surpassed all 8 baselines in promoting target items, regardless of the fake user proportion.
- Demonstrated the superior concealment of PoisonFRS with t-SNE analysis.

Large Language Model Toxic Content Detection Nov 2023 - Present

Advisor: Prof. Weiming Zhang, USTC

Motivation: Large language models (LLM) still have limited ability to detect toxic content, such as sensitive keywords, euphemisms, and anti-prefixes.

- Proposed a method that uses GPT-4 to label small datasets and compare them with the results generated by a toxic content detection classifier.
- Trained the toxic content detection classifier through knowledge distillation.
- Aim to optimize the performance of LLM in toxic content detection.

Selected Course Projects

USTC Chatbot Apr 2022 - Jun 2022

- Developed a chatbot using TensorFlow that can address inquiries and manage directives from USTCers.
- Used a pre-trained classifier to endow the chatbot with a fixed personality.

CminusF Compiler Oct 2022 - Dec 2022

- Implemented a compiler that translates CminusF code into machine code.
- Utilized Global Value Numbering (GVN) analysis to eliminate redundant generated code.

Skills

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

Honors & Awards

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

Extracurricular Activities & Leadership

High School Basketball League Mar 2019 - Jun 2019

- Played the small forward (SF) role in our team.
- Achieved the runner-up position in the league.

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

- Organized activities such as the Student Seminar and the New Year's Eve Gala.
- Promote student-faculty communication.

USTC Admissions Volunteer Jun 2021 - Jul 2021

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