Ming Yin

✉ mingyin@mail.ustc.edu.cn
🌐 Personal Website

Education

University of Science and Technology of China Sept 2020 - Present
School of the Gifted Young, Computer Science
Major GPA: 3.81, Major Average Score: 88.29 Cumulative GPA: 3.6, Cumulative Average Score: 86.42
Rank 16/67 in School of the Gifted Young, CS Major
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 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 on FL.

- Introduced InferGuard, an innovative defense designed to protect against client-side inference attacks on FL.
- 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 - Sept 2023
Advisor: Prof. Neil Gong, Duke University

Motivation: Existing attacks on Federated Recommender Systems (FedRecs) necessitate extra information about FedRecs 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.
- 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, as the model updates from genuine and fake users are indistinguishable within the latent space.

Large Language Model Toxic Content Detection (Graduation Project) Oct 2023 - Present
Advisor: Prof. Weiming Zhang, USTC

Research Intersets

Security, Privacy, Trustworthy Machine Learning, Federated Learning

Publications

*** indicates an 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

Selected Honors

Excellent Student Scholarship Gold (TOP 3%)	Oct 2020
Anhui Collegiate Programming Contest (Second Place)	Oct 2021
Excellent Student Scholarship Bronze (TOP 30%)	Oct 2022
Qiangwei Progress Scholarship (52/1000)	Oct 2023
Excellent Student Scholarship Gold (TOP 3%)	Oct 2023

Skills

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