Hong Kong University of Science and Technology
Clear Water Bay, Kowloon
Hong Kong, China
yhuanggn@connect.ust.hk | 616290511@qq.com
+86-18758068101

Yuchen Huang

PhD Student, Department of Computer Science and Engineering, HKUST

Education

Department of Computer Science and Engineering, Hong Kong University of Science and Technology, Hong Kong, China
PhD Student, Computer Science and Engineering
advised by Prof.Wei Wang *Sept.2023 - Present*

College of Information Science and Electronic Engineering, Zhejiang University, China
Bachelor of Engineering, Electronic Science and Technology
GPA: 91.67/100
Rank: 2/92 *Sept.2019 - Jul.2023*

Research Interests

Large Language Model, Privacy-Preserving Machine Learning

Awards & Achievements

Awarded **Hong Kong PhD Fellowship(HKPF)** in 2023
Awarded **Outstanding Graduates of Zhejiang Province** in 2023
Awarded **Outstanding Graduates of Zhejiang University** in 2023
Awarded the **National Scholarship** in 2019-20 and 2020-21
Awarded the **The First-Class Scholarship of Zhejiang University** in 2019-20, 2020-21 and 2021-22

Research Experience

Membership Inference Attacks against Large Language Models
Supervisor : Prof. Wei Wang, HKUST *Feb.2024 - Present*

- Exploring privacy issues of Large Language Models.

Defending Byzantine Attacks in Non-iid Federated Learning Scenario
Supervisor : Prof. Yang Liu, AIR, Tsinghua University *July.2023 - Aug.2023*

- Based on the fact that updated gradients from Byzantine attackers may be similar to normal gradients in non-iid FL scenario, we design a strategy utilizing clustering algorithm to improve utility.

Asynchronous Decentralized Federated Learning towards Non-iid Data
Supervisor : Prof. Ying Liu, Zhejiang University *Nov.2022 - May.2023*

- Propose a decentralized federated learning approach based on multi-source knowledge transfer
- Optimize the communication efficiency by introducing an event-triggered model sending strategy and the asynchronous communication mechanism.

Byzantine-Robust Federated Bayesian Personalized Ranking Using Multi-Krum Aggregation
Supervisor : Prof. Qinming He, Zhejiang University *Jul.2021 - May.2022*

- Design an optimized model based on Bayesian Personalized Ranking by using the framework of federated learning while applying Multi-Krum aggregation to keep system Byzantine-Robust.
- Write a program in pytorch to experiment the accuracy of the model with PAT dataset.
- Write the patent specification.