Ganyu Wang

Home Page Personal WesternU LinkedIn Github Scholar

Education

University of Western Ontario **Sept. 2021 - Present**
Ph.D Student in Computer Science

Ontario Tech University **Sept. 2019 - July. 2021**
M.Sc in Computer Science (Thesis-based)

University of Electronic Science and Technology of China **Sept. 2015 - Jul. 2019**
B.Sc in Computer Science and Technology *Overall GPA: 3.84/4.00 (87.02/100)*
*Yingcai Honors College (**for top 5% undergraduates**)*

Projects and Publications

Optimization Efficiency and Privacy in Vertical Federated Learning **Apr. 2022 - Jan. 2024**

- Developed a novel Vertical Federated Learning framework (a large-scale distributed machine learning framework) combining different optimization approaches to improve convergence and maintain privacy.
- Proposed theoretical analysis on the convergence and the differential privacy guarantees of the framework
- Experimentally demonstrated significant communication cost reductions.
- This series of works are published in the **top-tier conference (NeruIPS-2024)**[1] and **journal (MLJ)** [3].

Kernelized AUC Maximization in Vertical Federated Learning **Jun. 2023 - Jul. 2024**

- Contributed to the development of the Asynchronous Vertical Federated Kernelized AUC Maximization (AVFKAM)
- Published in the **top-tier conference, KDD-2024** [4].

Adversarial Attack in Speech Recognition **Nov. 2019 - Jul. 2021**

- Proposed and implemented SegmentPerturb, an innovative method that crafts hidden voice commands by probing target **Automatic Speech Recognition (ASR)** systems [2]. Conducted experiments on a wide variety of ASRs, such as Google ASR, Microsoft Azure ASR, and IBM ASR.

Projects in Progress

- **Online Learning** in Vertical Federated Learning. Submitted to ICLR-2025.
- **Black-box Prompt Learning** for Cloud-based Large Language Models in Federated Learning. Led a project investigating prompt learning techniques on **cloud-based large language models (LLMs) such as GPT**. Developed strategies for optimizing prompt learning in a black-box setting, leveraging the **OpenAI API** without access to the model's internal architecture or gradients. Submitted to ICLR-2025.

TLDR: I innovate in designing algorithms that address engineering challenges, performing theoretical analysis and practical implementation, and specializing in machine learning, distributed learning, and emerging trends in LLMs. I also have experience in conducting research on Speech Recognition, including signal processing, novel model architecture, and model APIs.

Research Interest

Machine Learning, Distributed System Application, Optimization, LLM, Differential Privacy, Speech Recognition

Serves as Reviewer

AISTATS-2024, ICML-2024, KDD-2024, ICLR-2025

Technical Skills

Languages: Python, R, C++, Java, TypeScript, HTML, SQL, VHDL, LaTeX
Clouds & Platforms: OpenAI API, AWS, Amplify, Vite, React, Material UI, Linux
Developer Tools: VS Code, GitHub, Android Studio, Matlab
***Music**: Piano – 10 years of learning experience.

TLDR: I have a solid foundation in computer science fundamentals and quickly master new programming tools, platforms, APIs, and related skills. My music-learning experience also sharpens my intuition when conducting research in related areas.

Work Experiences

Wilfrid Laurier University **Jan. 2022 - May 2022**
Lecturer for CP421A - Data Mining: Designed and taught the course.

References

[1] **Wang, Ganyu**, Bin Gu, Qingsong Zhang, Xiang Li, Boyu Wang, and Charles X Ling. A unified solution for privacy and communication efficiency in vertical federated learning. *Advances in Neural Information Processing Systems*, 36, 2024.

[2] **Wang, Ganyu** and Miguel Vargas Martin. Segmentperturb: Effective black-box hidden voice attack on commercial asr systems via selective deletion. In *2021 18th International Conference on Privacy, Security and Trust (PST)*, pages 1–12. IEEE, 2021.

[3] **Wang, Ganyu**, Qingsong Zhang, Xiang Li, Boyu Wang, Bin Gu, and Charles X Ling. Secure and fast asynchronous vertical federated learning via cascaded hybrid optimization. *Machine Learning*, 113(9):6413–6451, 2024.

[4] Ke Zhang, **Wang, Ganyu**, Han Li, Yulong Wang, Hong Chen, and Bin Gu. Asynchronous vertical federated learning for kernelized auc maximization. In *Proceedings of the 30th ACM SIGKDD Conference on Knowledge Discovery and Data Mining*, pages 4244–4255, 2024.