Ganyu Wang

Home Page | Personal | WesternU | LinkedIn | Github | Scholar

Education

University of Western Ontario **Sept. 2021 - Summer 2025**
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)*

Selected Research Projects

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

- Developed a *novel VFL framework*, a large-scale distributed ML system, by pioneering a hybrid optimization approach that significantly accelerates convergence while preserving differential privacy, addressing critical challenges in optimization efficiency and secure multi-party collaboration.
- Introduced *theoretical advancements* with novel analyses of optimization techniques and innovative implicit differential privacy guarantees, establishing new benchmarks in the field.
- Achieved a *substantial reduction in communication costs* through strategic algorithmic optimizations, paving the way for scalable AI solutions in resource-constrained environments.
- This series of works are published in the **top-tier conference (NeruIPS-2024)**[1] and **journal (MLJ)** [4].

Federated Black-box Discrete Prompt Tuning for Cloud-based LLM **Dec. 2023 - Present**

- Proposed a novel federated framework, designed to optimize query efficiency for Federated Black-Box Discrete Prompt Learning (BDPL) with Large Language Models (LLMs).
- Conducted the first theoretical analysis of query efficiency in Federated BDPL, identifying the relationship between client activation strategies and cloud-based LLM service query costs.
- Demonstrated the effectiveness of our framework by achieving optimal query efficiency, validated through experiments on both a benchmark model (RoBERTa) and a real-world scenario of cloud-based LLM (GPT-3.5 Turbo).
- Prepared for submission to ICML 2025.

Online Vertical Federated Learning **Jan. 2023 - Oct. 2024**

- Proposed a novel event-driven framework for Online VFL, addressing real-world challenges including asynchronous data reception and non-stationary environments.
- *Enhanced model adaptability* for non-convex optimization in dynamic scenarios.
- Established the framework as a *scalable and efficient solution* for VFL in practical applications, paving the way for real-time collaboration of VFL.
- Recognized as a high-quality submission to **ICLR 2025**, receiving a high review score, with the final decision pending.

Research Interest: Machine Learning, Large Scale Distributed System, Optimization, LLM, Differential Privacy.

Experiences

Full-Stack and Cloud Solutions Developer (Start-up) **Dec. 2023 - Present**
Developing a full-stack application to support RFID IoT devices, enabling smart storage solutions.
Utilized AWS for cloud development, integrating secure user authentication and real-time data processing for scalable cloud solutions. Interfaced with RFID devices for efficient inventory tracking and management.

Serves as Reviewer for Top-tier AI&ML conference **Jan. 2024 - Present**
AISTATS-2024, ICML-2024, KDD-2024, AAAI-2025, ICLR-2025, ICML-2025.
I have provided comprehensive, in-depth reviews for manuscripts submitted to top-tier ML conferences, ensuring rigorous evaluation of their technical contributions, novelty, and potential impact.

Wilfrid Laurier University **Jan. 2022 - May 2022**
Lecturer for CP421A - Data Mining
Designed and delivered a comprehensive course on data mining, equipping fourth-year undergraduate students with a strong foundation in core concepts. Incorporated hands-on projects and real-world datasets to enhance practical understanding.

Technical Skills

Languages: Python (PyTorch&Tensorflow), R, C++, Java, TypeScript, HTML, SQL, VHDL, LaTeX
Clouds & Platforms: OpenAI API, AWS, Amplify, Vite, Vue, React, Material UI, Linux
Developer Tools: VS Code, GitHub, Android Studio, Matlab

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**, Miguel Martin, Patrick Hung, and Shane MacDonald. Towards classifying motor imagery using a consumer-grade brain-computer interface. In *2019 IEEE International Conference on Cognitive Computing (ICCC)*, pages 67–69. IEEE, 2019.

[3] **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.

[4] **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.

[5] 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.