

GANYU WANG

 [Home Page](#)  [Personal](#)  [WesternU](#)  [LinkedIn](#)  [GanyuWang](#)  [Scholar](#)

Education

Ph.D Candidate in Computer Science <i>University of Western Ontario</i>	Sept. 2021 - Expected May 2025
M.Sc in Computer Science (Thesis-based) <i>Ontario Tech University</i>	Sept. 2019 - July. 2021
B.Sc in Computer Science and Technology <i>University of Electronic Science and Technology of China</i> <i>Yingcai Honors College (for top 5% undergraduates)</i>	Sept. 2015 - Jul. 2019 <i>Overall GPA: 3.84/4.00 (87.02/100)</i>

Selected Research Projects

Optimization Efficiency and Privacy in Vertical Federated Learning <ul style="list-style-type: none">Published as the first author in the top-tier conference (NeruIPS-2023)[1] and journal (MLJ) [4].Developed a <i>novel VFL framework</i>, a large-scale distributed ML system, by pioneering a hybrid optimization approach that significantly improves efficiency while preserving privacy, addressing critical challenges in distributed ML system.Introduced <i>theoretical advancements</i> with novel analyses of optimization techniques and innovative implicit differential privacy guarantees, establishing new benchmarks in the field.Practically achieved a <i>substantial reduction in communication costs</i> through strategic algorithmic optimizations, paving the way for scalable AI solutions in resource-constrained large-scale distributed ML environments.	Apr. 2022 - Jan. 2024
Federated Black-box Discrete Prompt Tuning (BDPL) for Cloud-based LLM <ul style="list-style-type: none">Proposed a novel federated framework, designed to optimize query efficiency for Federated BDPL with cloud-based Large Language Models (LLMs).Conducted the <i>first theoretical analysis</i> of query efficiency in Federated BDPL, identifying the relationship between client activation strategies and cloud-based LLM service query costs.Demonstrated significant improvement of query-efficiency of our framework through experiments on both a benchmark model (RoBERTa) and a real-world scenario of cloud-based LLM (GPT-3.5 Turbo).	Dec. 2023 - Present
Event-Driven Online Vertical Federated Learning <ul style="list-style-type: none">This work has been accepted at the ICLR 2025 conference (top 5% review score).Proposed a novel event-driven framework for online learning in VFL.Addressed the real-world challenges including asynchronous data reception and non-stationary environments.Established the framework as a <i>scalable and efficient solution</i> for VFL in practical applications, paving the way for real-time collaboration in VFL.	Jan. 2023 - Oct. 2024

Research Interest: *Machine Learning, Large-scale Distributed System, Optimization, LLM, Differential Privacy.*

Professional Experiences

Full-Stack and Cloud Solutions Developer <i>Developing a full-stack application to support RFID IoT devices, enabling smart storage solutions.</i> <ul style="list-style-type: none">Utilized AWS for cloud development, integrating secure user authentication and real-time data processing.Interfaced with RFID devices for efficient inventory tracking and management.	Dec. 2023 - Present
Serves as Reviewer for Top-tier AI&ML conference <i>AISTATS-2024, ICML-2024, KDD-2024, AAAI-2025, ICLR-2025, ICML-2025.</i> <ul style="list-style-type: none">Contributed comprehensive, in-depth reviews for manuscripts submitted to top-tier ML conferences.	Oct. 2023 - Present
Lecturer for Course: Data Mining <i>Wilfrid Laurier University</i> <ul style="list-style-type: none">Designed and taught a comprehensive course on data mining, achieving exceptional student feedback for clarity, engagement, and practical application.	Jan. 2022 - May 2022

Technical Skills

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

- [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.