Yanzhao Wu

266 Ferst Drive, Room 3337, Atlanta, Georgia, 30332, USA
yanzhaowu@gatech.edu +1 404-279-2853 yanzhaowu.me

Education

Georgia Institute of Technology **Aug. 2017 – May 2022 (expected)**
Ph.D. in Computer Science (GPA: 3.92/4.00) *Atlanta, GA, USA*

University of Science and Technology of China (USTC) **Sep. 2013 – Jul. 2017**
Bachelor in Computer Science and Technology (GPA: 3.80/4.30) *Hefei, Anhui, China*

Research Interests

- Systems for Machine Learning
- Machine Learning for Systems
- Big Data Systems & Analytics
- Edge AI Systems

Experience

Georgia Institute of Technology **Aug. 2017 – May 2022 (expected)**
Graduate Research Assistant *Atlanta, GA, USA*

- **EVA (Edge Video Analytics):** Build an efficient framework for supporting various object detection/tracking models and achieving high performance on multiple edge devices.
- **EnsembleBench:** Design an ensemble framework for improving DNN accuracy and optimizing inference robustness.
- **LRBench:** Improve the deep learning training efficiency via semi-automatic hyper-parameter tuning.
- **GTDLBench:** Propose a performance benchmark to measure and optimize mainstream deep learning frameworks.

Facebook, Inc **Summer 2020, Summer 2021**
Software Engineer Intern *Menlo Park, CA, USA*

- **Data-efficient Learning:** Study the data efficiency of DNN ensemble models and design effective subsampling strategies to improve data efficiency for training ML models. (Summer 2021)
- **PipeDLRM:** Apply pipeline parallelism into Facebook deep learning recommendation models to accelerate distributed recommendation model training. (Summer 2020)

IBM Research **Summer 2018, Summer 2019**
Research Intern *San Jose, CA, USA*

- **Performance Analysis:** Conduct a comprehensive performance analysis of the IBM Comanche storage system with different storage devices, such as persistent memory and SSD, on popular deep learning workloads. (Summer 2019)
- **Direct-to-GPU Storage System:** Integrate the Direct-to-GPU storage system into Caffe to obtain over 2× performance improvement by reducing the overhead of data transmission. (Summer 2018)

Publications

- **Yanzhao Wu**, Ling Liu, Zhongwei Xie, Ka-Ho Chow, and Wenqi Wei. "Boosting Ensemble Accuracy by Revisiting Ensemble Diversity Metrics." (CVPR 2021)
- Wenqi Wei, Ling Liu, **Yanzhao Wu**, Gong Su, and Arun Iyenger. "Gradient-Leakage Resilient Federated Learning." (ICDCS 2021)
- Zhongwei Xie, Ling Liu, **Yanzhao Wu**, Lin Li, Luo Zhong. "Learning TFIDF Enhanced Joint Embedding for Recipe-Image Cross-Modal Retrieval Service." (IEEE TSC 2021)
- **Yanzhao Wu**, Ling Liu, Zhongwei Xie, Juhyun Bae, Ka-Ho Chow, Wenqi Wei. "Promoting High Diversity Ensemble Learning with EnsembleBench." (IEEE CogMI 2020)
- Zhongwei Xie, Ling Liu, **Yanzhao Wu**, Lin Li, Luo Zhong. "Cross-Modal Joint Embedding with Diverse Semantics." (IEEE CogMI 2020)
- Semih Sahin, Ling Liu, Wenqi Cao, Qi Zhang, Juhyun Bae, **Yanzhao Wu**. "Memory Abstraction and Optimization for Distributed Executors." (IEEE CIC 2020)
- Wenqi Wei, Ling Liu, Margaret Loper, Ka-Ho Chow, Mehmet Emre Gursoy, Stacey Truex, **Yanzhao Wu**. "Adversarial Deception in Deep Learning: Analysis and Mitigation." (IEEE TPS 2020)
- Ka-Ho Chow, Ling Liu, Margaret Loper, Juhyun Bae, Mehmet Emre Gursoy, Stacey Truex, Wenqi Wei, **Yanzhao Wu**. "Adversarial Objectness Gradient Attacks in Real-time Object Detection Systems." (IEEE TPS 2020)

- Juhyun Bae, Gong Su, Arun Iyengar, **Yanzhao Wu** and Ling Liu. "Efficient Orchestration of Host and Remote Shared Memory for Memory Intensive Workloads." (MemSys 2020)
- Ka-Ho Chow, Ling Liu, Mehmet Emre Gursoy, Stacey Truex, Wenqi Wei and **Yanzhao Wu**. "Understanding Object Detection Through An Adversarial Lens." (ESORICS 2020)
- Wenqi Wei, Ling Liu, Margaret Loper, Ka-Ho Chow, Mehmet Emre Gursoy, Stacey Truex and **Yanzhao Wu**. "A Framework for Evaluating Client Privacy Leakages in Federated Learning." (ESORICS 2020)
- Wenqi Wei, Ling Liu, Margaret Loper, Ka Ho Chow, Emre Gursoy, Stacey Truex, **Yanzhao Wu**. "Cross-layer Strategic Ensemble Defense against Adversarial Examples." (IEEE ICNC 2020)
- **Yanzhao Wu**, Ling Liu, Juhyun Bae, Ka-Ho Chow, Arun Iyengar, Calton Pu, Wenqi Wei, Lei Yu, Qi Zhang. "Demystifying Learning Rate Policies for High Accuracy Training of Deep Neural Networks." (IEEE BigData 2019)
- Ka-Ho Chow, Wenqi Wei, **Yanzhao Wu**, Ling Liu. "Denoising and Verification Cross-Layer Ensemble Against Black-box Adversarial Attacks." (IEEE BigData 2019)
- Ling Liu, Wenqi Wei, Ka-Ho Chow, Margaret Loper, Emre Gursoy, Stacey Truex, **Yanzhao Wu**. "Deep Neural Network Ensembles against Deception: Ensemble Diversity, Accuracy and Robustness." (IEEE MASS 2019)
- **Yanzhao Wu**, Ling Liu, Calton Pu, Wenqi Cao, Semih Sahin, Wenqi Wei, Qi Zhang. "A Comparative Measurement Study of Deep Learning as a Service Framework." (IEEE TSC 2019)
- Ling Liu, Wenqi Cao, Semih Sahin, Qi Zhang, Juhyun Bae, **Yanzhao Wu**. "Memory Disaggregation: Research Problems and Opportunities." (ICDCS 2019)
- **Yanzhao Wu**, Wenqi Cao, Semih Sahin, and Ling Liu. "Experimental Characterizations and Analysis of Deep Learning Frameworks." (IEEE BigData 2018)
- Ling Liu, **Yanzhao Wu**, Wenqi Wei, Wenqi Cao, Semih Sahin, and Qi Zhang. "Benchmarking Deep Learning Frameworks: Design Considerations, Metrics and Beyond." (ICDCS 2018)
- Pengcheng Wang, Jeffrey Svajlenko, **Yanzhao Wu**, Yun Xu and Chanchal K. Roy. "CCAligner: A Token Based Large-Gap Clone Detector." (ICSE 2018)

Teaching

Georgia Institute of Technology

Graduate Teaching Assistant

- CS6220 Big Data Systems and Analytics (Fall 2021)
- CS6675/CS4675 Advanced Internet Computing Systems and Application Development (Spring 2018, Spring 2019, Spring 2020, Spring 2021)
- CS6235/CS4220 Embedded Systems and Real-Time Systems (Fall 2018)

University of Science and Technology of China

Undergraduate Teaching Assistant

- CS1001A Computer Programming A (Fall 2015)

Reviewer

- Conference: ICDE 2018, UCC 2018, BDCAT 2018, ICDCS 2019, WWW 2021
- Journal: IEEE TKDE, ACM TOIT

Open-source Projects

- DP-Ensemble: Leveraging FQ-diversity metrics to identify high diversity ensemble teams with high performance.
- PipeDLRM: Using pipeline parallelism for training deep learning recommendation models.
- EnsembleBench: A set of tools for building high-quality ensembles for machine learning and deep learning models.
- LRBench: A semi-automatic learning rate tuning tool to improve the DNN training efficiency and accuracy.
- GTDLBench: A performance benchmark to measure and optimize mainstream deep learning frameworks.
- Comanche: Accelerating deep learning with Direct-to-GPU storage with a modified Caffe and DeepBench.
- CCAligner: A token based code clone detector for detecting large-gap copy-and-paste source codes.
- PRISM: Building the LTS and Game model checkers for PRISM, a widely applied model checker for system analysis.