Curriculum Vitæ

Junyuan Hong

Department of Computer Science and Engineering
Michigan State University

428 S Shaw Ln Rm 3312, East Lansing, MI 48824
Phone: +1 (517) 668-5790
E-mail: hongju12@msu.edu, Webpage: https://jyhong.gitlab.io

Education

Ph.D. in Computer Science and Engineering 2023
Michigan State University, East Lansing, MI, USA (expected)
Supervisor: Dr. Jiayu Zhou
Tentative thesis: Data-Centric Privacy-Preserving Machine Learning

M.S. in Computer Science 2018
University of Science and Technology of China, Hefei, China
Supervisor: Dr. Huanhuan Chen

B.S. in Physics with minor in Computer Science 2015
University of Science and Technology of China, Hefei, China

Research Interests

Trustworthy machine learning: Theory and algorithms for learning with privacy, fairness, robustness and explainability.

Distributed machine learning: Algorithms for scalable learning from distributed clients with heterogeneous data, hardware and objectives.

Research Experiences

Feb '22 - Aug '22 **Research Intern**, Sony AI, NY, USA
Mentor: Dr. Lingjuan Lyu
(1) Designed the privacy-preserving cloud training algoirthms that require low computation costs and low privacy risks for edge devices.
(2) Designed memory-efficient model adaptation algorithms for dynamically-changing test-time environments, which can fit into edge devices.

Aug '18 - Now **Research Assistant**, Michigan State University, MI, USA
Supervisor: Dr. Jiayu Zhou
(1) Empirically and theoretically studied the dynamic privacy allocation for improving the model performance by centralized differentially-private learning.
(2) Developed algorithms for reducing social biases (unfairness) or distributional biases in federated learning with lower privacy risks;
(3) Developed training algorithms and models customizable by clients dynamically during training and testing in federated learning.

Aug '15 - Jun '18 **Research Assistant**, University of Science and Technology of China, Hefei, China
Supervisor: Huanhuan Chen

(1) Designed the hardware and software prototype for detecting underground cables;
(2) Developed implicit data-augmentation optimization algorithms for subspace data with applications to human action recognition.

Honors & Awards

2021	Carl V. Page Memorial Graduate Fellowship, Michigan State University
2018	Student Travel Award, SIGKDD
2015	Outstanding Freshman Scholarship, University of Science and Technology of China

Publications

Refereed Publications

[NeurIPS'22] **Junyuan Hong**, Lingjuan Lyu, and Jiayu Zhou, Micheal Spranger. Outsourcing Training without Uploading Data via Efficient Collaborative Open-Source Sampling. *Proceedings of the Thirty-seventh Conference on Neural Information Processing Systems.*

[NeurIPS'22] Hatao Wang, **Junyuan Hong**, Aston Zhang, Jiayu Zhou and Zhangyang Wang. Trap and Replace: Defending Backdoor Attacks by Trapping Them into an Easy-to-Replace Subnetwork. *Proceedings of the Thirty-seventh Conference on Neural Information Processing Systems.*

[FAccT'22] **Junyuan Hong**, Zhangyang Wang, and Jiayu Zhou. Dynamic Privacy Budget Allocation Improves Data Efficiency of Differentially Private Gradient Descent. *Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency.*

[ICLR'22] **Junyuan Hong**, Haotao Wang, Zhangyang Wang, and Jiayu Zhou. Efficient Split-Mix Federated Learning for On-Demand and In-Situ Customization. *Proceedings of the Tenth International Conference on Learning Representations.*

[ICML'22] Zhuangdi Zhu, **Junyuan Hong**, Steve Drew, and Jiayu Zhou. Resilient and Communication Efficient Learning for Heterogeneous Federated Systems. *Proceedings of Thirty-ninth International Conference on Machine Learning.*

[KDD'21] **Junyuan Hong**, Zhuangdi Zhu, Shuyang Yu, Zhangyang Wang, Hiroko Dodge, and Jiayu Zhou. Federated Adversarial Debiasing for Fair and Transferable Representations. *Proceedings of the 27th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining.*

[ICML'21] Zhuangdi Zhu, **Junyuan Hong**, and Jiayu Zhou. Data-Free Knowledge Distillation for Heterogeneous Federated Learning. *Proceedings of Thirty-eighth International Conference on Machine Learning.*

[AAAI'21] **Junyuan Hong**, Haotao Wang, Zhangyang Wang, and Jiayu Zhou. Learning Model-Based Privacy Protection under Budget Constraints. *Proceedings of the Thirty-Fifth AAAI Conference on Artificial Intelligence.*

[KDD'18] **Junyuan Hong**, Huanhuan Chen and Feng Lin. Disturbance Grassmann Kernels for Subspace-Based Learning. *Proceedings of the 24th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining.*

[ECML'16] Yang Li, **Junyuan Hong** and Huanhuan Chen. Sequential Data Classification in the Space of Liquid State Machines. *Proceedings of the European Conference on Machine Learning and Principles and Practice of Knowledge Discovery in Databases.*

[TKDD'19] **Junyuan Hong**, Yang Li and Huanhuan Chen. Variant Grassmann Manifolds: A Representation Augmentation Method for Action Recognition. *ACM Transactions on Knowledge Discovery from Data*.

[TNNLS'19] Yang Li, **Junyuan Hong** and Huanhuan Chen. Short Sequence Classification Through Discriminable Linear Dynamical System. *IEEE Transactions on Neural Networks and Learning Systems*.

Preprints

1. Haotao Wang, **Junyuan Hong**, Jiayu Zhou, and Zhangyang Wang. How Robust is Your Fairness? Evaluating and Sustaining Fairness under Unseen Distribution Shifts. *arXiv:2207.01168* (2022)

2. **Junyuan Hong**, Haotao Wang, Zhangyang Wang, and Jiayu Zhou. Federated Robustness Propagation: Sharing Adversarial Robustness in Federated Learning. *arXiv:2106.10196* (2021)

Teaching Experiences

Spring 2021

Teaching Assistant, "CSE847: Machine Learning" (graduate level), Michigan State University
Lectures on privacy and federated learning

Fall 2020

Teaching Assistant, "CSE404: Introduction to Machine Learning" (undergraduate level), Michigan State University

Invited Talks & Presentations

2022

(Poster) Outsourcing Training without Uploading Data via Efficient Collaborative Open-Source Sampling. *The Thirty-seventh Conference on Neural Information Processing Systems* (NeurIPS 2022), November, 2022.

(Invited Talk) Split-Mix Federated Learning for Model Customization, *TrustML Young Scientist Seminars*, RIKEN, July, 2022

(Poster) Efficient Split-Mix Federated Learning for On-demand and In-situ Model Customization, *The Tenth International Conference on Learning Representations* (ICLR 2022), Virtual, April, 2022.

(Poster) Efficient Split-Mix Federated Learning for On-demand and In-situ Model Customization, *Engineering Graduate Research Symposium*, Michigan State University, April, 2022.

(Invited Talk) Efficient Split-Mix Federated Learning for On-demand and In-situ Model Customization, *Sony AI Journal Club*, Virtual, February, 2022.

(Oral) Dynamic privacy budget allocation improves data efficiency of differentially private gradient descent, *The 2022 ACM Conference on Fairness, Accountability, and Transparency* (FAccT 2022), Virtual, June 2022.

2021

(Talk) Federated adversarial debiasing for fair and transferable representations, *CSE Graduate Seminar*, Michigan State University, October, 2021

(Oral) Federated adversarial debiasing for fair and transferable representations, *The 27th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining* (SIGKDD 2021), Virtual, August 2021.

(Poster) Learning model-based privacy protection under budget constraints, *The Thirty-Fifth AAAI Conference on Artificial Intelligence* (AAAI 2021), Virtual, February 2021.

2018 (Oral) Disturbance Grassmann kernels for subspace-based learning, *The 24th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining* (SIGKDD 2018), London, August 2018.

Professional Activities

Technical Program Committee Member (or Equivalent Reviewer) for Conferences or Journals:

- Annual Conference on Neural Information Processing Systems (NeurIPS): 2022
- International Conference on Learning Representations (ICLR): 2023
- ACM SIGKDD Conference on Knowledge Discovery and Data Mining (KDD): 2022
- International Conference on Machine Learning (ICML): 2022
- International Conference on Artificial Intelligence and Statistics (AISTATS): 2022, 2023
- International Conference on Web Search and Data Mining (WSDM): 2022
- AAAI Conference on Artificial Intelligence (AAAI): 2021, 2022, 2023
- International Joint Conference on Artificial Intelligence (IJCAI): 2019
- NeuroComputing: 2021, 2022
- ACM Transactions on Knowledge Discovery from Data: 2020

Volunteers:

- ACM SIGKDD Conference on Knowledge Discovery and Data Mining (KDD): 2018, 2021

Advising Students

- Shuyang Yu, Michigan State University, 2020-2022, Federated Learning
- Haobo Zhang, Michigan State University, 2022, Privacy-Preserving Learning