Curriculum Vitæ

Junyuan Hong

University of Texas at Austin

Phone: +1 (517) 668-5790
E-mail: hongju12@msu.edu, Webpage: https://jyhong.gitlab.io

I am currently a joint postdoctoral fellow in the Institute for Foundations of Machine Learning (IFML) and Wireless Networking and Communications Group (WNCG) at UT Austin.

Education

Ph.D. in Computer Science and Engineering 2023
Michigan State University, East Lansing, MI, USA
Supervisor: Dr. Jiayu Zhou
Committee: Dr. Anil K. Jain, Dr. Sijia Liu, Dr. Zhangyang Wang, Dr. Jiayu Zhou
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 '23 - Present **Joint Postdoctoral Fellow**, IFML&WNCG at University of Texas, Austin, TX, USA
Host: Dr. Zhangyang Wang
(1) The privacy of foundation models;
(2) Enhancing the trustworthiness of foundation models with privacy constraints.

Aug '18 - 2023 **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.

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 '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

2023	The 3rd place in the U.S.-U.K. Privacy-Enhancing Technologies (PETs) prize challenge.
	Dissertation Completion Fellowship, Michigan State University
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 (* indicates equal contributions)

[ICML'23] **Junyuan Hong***, Yi Zeng*, Shuyang Yu*, Lingjuan Lyu, Ruoxi Jia, Jiayu Zhou. Revisiting Data-Free Knowledge Distillation with Poisoned Teachers. *Proceedings of Fortieth International Conference on Machine Learning.*

[ICLR'23] **Junyuan Hong**, Lingjuan Lyu, Jiayu Zhou, Michael Spranger. MECTA: Memory-Economic Continual Test-Time Model Adaptation. *Proceedings of the Eleventh International Conference on Learning Representations.*

[ICLR'23] Shuyang Yu, **Junyuan Hong**, Haotao Wang, Zhangyang Wang and Jiayu Zhou. Turning the Curse of Heterogeneity in Federated Learning into a Blessing for Out-of-Distribution Detection. *Proceedings of the Eleventh International Conference on Learning Representations.*

[TMLR'23] Haotao Wang, **Junyuan Hong**, Jiayu Zhou, and Zhangyang Wang. How Robust is Your Fairness? Evaluating and Sustaining Fairness under Unseen Distribution Shifts. *Transactions on Machine Learning Research.*

[AAAI'23] **Junyuan Hong**, Haotao Wang, Zhangyang Wang, and Jiayu Zhou. Federated Robustness Propagation: Sharing Adversarial Robustness in Heterogeneous Federated Learning. *Proceedings of the Thirty-Seventh AAAI Conference on Artificial Intelligence.*

[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.*

[AD'20] **Junyuan Hong**, Jeffrey Kaye, Hiroko H Dodge, Jiayu Zhou. Detecting MCI using real-time, ecologically valid data capture methodology: How to improve scientific rigor in digital biomarker analyses. *Alzheimer's & Dementia*

[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. Yuyang Deng, Nidham Gazagnadou, **Junyuan Hong**, Mehrdad Mahdavi, Lingjuan Lyu. Rademacher Complexity Over Class for Adversarially Robust Domain Adaptation. (2023)
2. Haobo Zhang, **Junyuan Hong**, Fan Dong, Steve Drew, Liangjie Xue, Jiayu Zhou. A Privacy-Preserving Hybrid Federated Learning Framework for Financial Crime Detection. (2023)
3. **Junyuan Hong**, Haotao Wang, Zhangyang Wang and Jiayu Zhou. Precautionary Unfairness in Self-Supervised Contrastive Pre-training. (2022)

Teaching Experiences

Spring 2023	Lectures on privacy and federated learning at CSE847 (graduate level)

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

2023	(Invited Talk) MECTA: Memory-Economic Continual Test-Time Model Adaptation. *Computer Vision Talks*, April, 2023
	(Oral) Federated Robustness Propagation: Sharing Adversarial Robustness in Heterogeneous Federated Learning, *The Thirty-Seventh AAAI Conference on Artificial Intelligence* (AAAI 2023), Washington D.C., February 2023.
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.
2020	(Invited Talk) Dynamic Policies on Differential Private Learning, *VITA Seminars*, University of Texas at Austin, Virtual, March 2020.
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.

Media Covers

2023 At Summit for Democracy, the United States and the United Kingdom Announce Winners of Challenge to Drive Innovation in Privacy-enhancing Technologies That Reinforce Democratic Values, The White House

Privacy-enhancing Research Earns International Attention, MSU Engineering News

Privacy-Enhancing Research Earns International Attention, MSU Office Of Research And Innovation

Professional Activities

Program Chair:

- Lead Chair at the 1st International Workshop on Federated Learning for Distributed Data Mining co-located with ACM SIGKDD 2023. (`fl4data-mining.github.io`)

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

- Annual Conference on Neural Information Processing Systems (NeurIPS): 2022, 2023
- International Conference on Learning Representations (ICLR): 2023
- ACM SIGKDD Conference on Knowledge Discovery and Data Mining (KDD): 2022, 2023
- International Conference on Machine Learning (ICML): 2022, 2023
- 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 (TKDD): 2020
- Transactions on Knowledge and Data Engineering (TKDE): 2023

Volunteers:

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

Advising Students

Students co-advised with my advisor:

2020 - 2023 **Shuyang Yu**, Ph.D. student, Michigan State University
Research: Federated Learning, out-of-distribution data.

- (First author) Turning the Curse of Heterogeneity in Federated Learning into a Blessing for Out-of-Distribution Detection. *Featured as spotlight at ICLR'23*
- Revisiting Data-Free Knowledge Distillation with Poisoned Teachers. *ICML'23.*

- Federated Adversarial Debiasing for Fair and Transferable Representations. *ACM SIGKDD'21.*

2022 - 2023 **Haobo Zhang**, Ph.D. student, Michigan State University
Research: Privacy-Preserving Learning.

- Won 3rd place at U.S.-U.K. PETs (Privacy-enhancing technologies) Prize Challenge, 2023.
- Certifiable Gradient-Inversion Privacy, *Under Review.*