Junyuan Hong

Michigan State University – 428 S Shaw Ln, East Lansing, Michigan, US 48823

+1 517 668 5790 • hongju12@msu.edu • https://jyhong.gitlab.io

Education

Michigan State University (MSU) **East Lansing, USA**
Ph.D. student, Computer Science and Engineering *2018.9–Now*
Advisor: Prof. Jiayu Zhou

University of Science and Technology of China (USTC) **Hefei, P.R.China**
M.Eng., Computer Science *2015.9–2018.6*
Advisor: Prof. Huanhuan Chen

University of Science and Technology of China **Hefei, P.R.China**
B.Sci., Physics, Computer Science minor *2011.9–2015.6*

Research Interests

Federated Learning: Distributed machine learning algorithms that respect users' privacy, personality, data biases, device heterogeneity and run-time dynamics.
Privacy-preserving Learning: Theory and algorithms for performance improvement and convergence analysis in privacy-preserving learning.

Research Experiences

Privacy and Security in Edge Machine Learning **2022.2–2022.8**
Research Intern *PPML Project, Sony AI*
During this intern, I work on developing new algorithms that can effectively train a model that can adapt to edge devices without leaking privacy and with robustness.

Federated Learning with Non-iid Data **2020–2022**
Research Assistant *ILLIDAN Lab, MSU*
Facing the need of learning from non-iid data and concern of privacy, we strive to develop novel federated learning algorithms to debias and transfer knowledge between users from different groups or environment.

- *ICML'22* (accepted): We propose a novel FL algorithm that is reslient to random drop of parameters at communication.
- *ICLR'22* (accepted): We exploit the FL with clients that have heterogeneous computation capacities and develop an algorithm that can achieve better performance complying clients' computation limitations.
- *KDD'21* (accepted): We leverage the federated averaging of a group discriminator to transfer the critiron on locally sensed bias, such that we can debias the trained classifiers.
- *ICML'21* (accepted): We use a locally trained generative model to transfer the local data knowledge, which mitigate the data scacity in some user ends.
- *ArXiv*: Considering the heterogeneous devices used by different clients, we provide a clean/noise-data-decoupled method for sharing robustness between users who only do standard training (cheap) or do adversarial training (expensive robustness learning).

Private Machine Learning **2018–2020**
Research Assistant *ILLIDAN Lab, MSU*

Machine learning models could be vulnerable to leaking private training information. To defend against attacks, we are designing advanced algorithms to efficiently protect data without heavily decreasing model utility.

- *FAccT'22* (accepted): We use a principled method to analyze the utility effect of privacy parameters per iteration and prove the optimal privacy-budget schedule for PL-class losses.
- *AAAI'21* (accepted): We meta-learn to schedule the privacy-utility balance at each gradient-descent iteration such that a better final model can be trained under privacy budget constraints.

Data Augmentation for Subspace Data **2016–2018**

Research Assistant *USTC-Birmingham Joint Research Inst. (UBRI)*

We extend the implicit data augmentation method to kernel-based classifiers through dual optimization and apply the method to classifying subspace representations of data, e.g. action videos.

- *ACM SIGKDD'18* (accepted as oral): We propose the Disturbance Grassmann Kernels on the Grassmann manifold by implicitly augmenting subspaces.

Model-based Kernel Method for Time Series Classification **2015–2016**

Research Assistant *UBRI*

We utilize a special type of Recurrent Neural Network, in which neural signals simulate natural spiking, to represent time series in model space for classification. As second author (*ECML'16*), I contribute a lot to codes and advise to apply the model to **event-based time series**.

Publications

Junyuan Hong, Lingjuan Lyu, Jiayu Zhou, and Spranger Micheal. Outsourcing training without uploading data via efficient collaborative open-source sampling. In *NeurIPS*, 2022.

Junyuan Hong, Haotao Wang, Zhangyang Wang, and Jiayu Zhou. Efficient split-mix federated learning for on-demand and in-situ customization. *ICLR*, 2022.

Junyuan Hong, Zhangyang Wang, and Jiayu Zhou. Dynamic privacy budget allocation improves data efficiency of differentially private gradient descent. In *FAccT*, 2022.

Haotao Wang, **Junyuan Hong**, Aston Zhang, Jiayu Zhou, and Wang Zhangyang. Trap and replace: Defending backdoor attacks by trapping them into an easy-to-replace subnetwork. In *NeurIPS*, 2022.

Zhuangdi Zhu, **Junyuan Hong**, Steve Drew, and Jiayu Zhou. Resilient and communication efficient learning for heterogeneous federated systems. In *Proceedings of the 39-th International Conference on Machine Learning*, 2022.

Junyuan Hong, Haotao Wang, Zhangyang Wang, and Jiayu Zhou. Federated robustness propagation: Sharing adversarial robustness in federated learning. *arXiv preprint arXiv:2106.10196*, 2021.

Junyuan Hong, Haotao Wang, Zhangyang Wang, and Jiayu Zhou. Learning model-based privacy protection under budget constraints. In *Proceedings of the 35-th AAAI Conference on Artificial Intelligence*, 2021.

Junyuan Hong, Zhuangdi Zhu, Shuyang Yu, Zhangyang Wang, Hiroko Dodge, and Jiayu Zhou. Federated adversarial debiasing for fair and transferable representations. In *Proceedings of the 27th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (SIGKDD 2021)*, 2021.

Zhuangdi Zhu, **Junyuan Hong**, and Jiayu Zhou. Data-free knowledge distillation for heterogeneous federated learning. In *Proceedings of the 38-th International Conference on Machine Learning*, 2021.

Yang Li, **Junyuan Hong**, and Huanhuan Chen. Short sequence classification through discriminable linear dynamical system. *IEEE Transactions on Neural Networks and Learning Systems (TNNLS)*, 2019.

Junyuan Hong, Yang Li, and Huanhuan Chen. Variant grassmann manifolds: A representation augmentation method for action recognition. *ACM Transactions on Knowledge Discovery from Data (TKDD)*, 2019.

Junyuan Hong, Huanhuan Chen, and Feng Lin. Disturbance Grassmann kernels for subspace-based learning. In *Proceedings of the 24th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (SIGKDD 2018)*, 2018.

Yang Li, **Junyuan Hong**, and Huanhuan Chen. Sequential data classification in the space of liquid state machines. In *the European Conference on Machine Learning and Principles and Practice of Knowledge Discovery in Databases (ECML PKDD)*, 2016.

Selected Honors and Awards

Carl V. Page Memorial Graduate Fellowship: Michigan State University 2021

Student Travel Award: SIGKDD 2018 2018

Outstanding Freshman Scholarship: University of Science and Technology of China 2015

Talks and Poster Presentations

TrustML Young Scientist Seminars, RIKEN AIP: Online Talk 2022

Split-Mix Federated Learning for Model Customization
ICLR 2022: Poster 2022

Efficient Split-Mix Federated Learning for On-demand and In-situ Model Customization
FAccT 2022: Oral presentation 2022

Dynamic privacy budget allocation improves data efficiency of differentially private gradient descent
SIGKDD 2021: Oral presentation 2021

Federated adversarial debiasing for fair and transferable representations.
AAAI 2021: Poster 2021

Learning model-based privacy protection under budget constraints.
SIGKDD 2018: Oral presentation 2018

Disturbance Grassmann kernels for subspace-based learning.

Selected Projects

Cinema Manager System **2015.8**

Software Designer and Engineer *Works Applications (WAP), Shanghai*

(5-day internship) This project aims to design software for cinema managers, which should be efficient for their daily work. The whole internship is of English-based communication.

- Software design and documentation composing;
- Implement software using Java in one day and demonstrate it to WAP engineer;
- Get job offer from Works Applications.

Underworld Detection Project **2014–2015**

Engineer and Manager *USTC-Birmingham Joint Research Institute (UBRI)*

This project aims to detect underground infrastructure by combining physics and computer technologies. Both **hardware** and **software** works are included.

- As the manager, I distribute and schedule works to teammates, achieving a stable and efficacious cooperation;
- As the engineer, I designed the 1st generation of the cable detectors with my teammates:
  - The outdoor underground cable detector;
  - The indoor cable portable detector.

Professional Activities

Journal Review:

- NeuroComputing, TKDD

Program Committee Member (or Equivalent) for Conferences:

- NeurIPS2022, ICML2022, KDD2022, WSDM2022, AISTATS2022, AAAI2022, AAAI2021, IJCAI2019

Teaching Experiences

CSE 404: Introduction to Machine Learning, 2020 Fall