Tiansheng Huang

PhD student at Georgia Institute of Technology
Email: thuang374@gatech.edu
Phone: (470)301-7963

Education

Georgia Institute of Technology, Atlanta, USA — Aug 2022 – Present

- Third year PhD student, School of computer science
- Program Advisor: Prof. Ling Liu

South China University of Technology, Guangzhou, China — Sept 2019 – June 2022

- M.S, School of computer science
- Program Advisor: Prof. Weiwei Lin
- Thesis: Application of Multi-arm Bandit Algorithms in Client Selection of Federated Learning

South China University of Technology, Guangzhou, China — Sept 2015 – June 2019

- B.S, School of computer science
- GPA: 3.75 (rank top 10%)

Research Interest

Current interest

- My current research interest lies in security/privacy aspect of machine learning, distributed machine learning and parallel and distributed computing.

Previous studied

- Multi-arm bandit
- Online learning
- Resource scheduling on cloud/edge computing

Industrial Experience

Dolby Advanced Technology Group, Atlanta, USA — May 2024 - August 2024

Research Intern

- Refine service delivery pipeline for LLMs/VLMs against harmful fine-tuning.
- Program Advisor: Gautam Bhattacharya, Pratik Joshi, Josh Kimball

JD explore academy, Beijing, China — March 2022 - June 2022

Research Intern

- Develop Personalized FL algorithms with factorization and sparse compression.
- Program Advisor: Li Shen

JD explore academy, Beijing, China — June, 2021 - Sept 2021

Research Intern

- Develop high efficiency sparse training algorithms for personalized FL.
- Program Advisor: Li Shen

Publications

Peer-review Conference

[1] F. Ilhan, G. Su, S. Tekin, **T. Huang**, S. Hu, L. Liu, “Resource-Efficient Transformer Pruning for Finetuning of Large Models”, **CVPR2024.**

[2] S.Hu, **T. Huang**, KH. Chow, W. Wei, Y. Wu, L. Liu. “ZipZap: Efficient Training of Language Models for Ethereum Fraud Detection”, **WWW2024.**

[3] F. Ilhan, KH. Chow, S. Hu, **T. Huang**, S. Tekin, W. Wei, Y. Wu, M. Lee, R.Kompella, H. Latapie, G. Liu, L. Liu, "Adaptive Deep Neural Network Inference Optimization with EENet," **WACV2024.**
[4] **T. Huang**, S. Hu, KH. Chow, F. Ilhan, S. Tekin, L. Liu, "Lockdown: Backdoor Defense for Federated Learning with Isolated Subspace Training," **NeurIPS2023.**
[5] Y. Sun, L. Shen, **T. Huang**, and D. Tao, "FedSpeed: Larger Local Interval, Less Communication Round, and Higher Generalization Accuracy," **ICLR2023.**
[6] F. Ilhan, SF Tekin, S Hu, **T. Huang**, KH Chow and L Liu, "Hierarchical Deep Neural Network Inference for Device-Edge-Cloud Systems[C]" **WWW2023.**
[7] S. Hu, **T. Huang**, F. İlhan, SF. Tekin, L. Liu, "Large Language Model-Powered Smart Contract Vulnerability Detection: New Perspectives" **IEEE TPS2023.**

Journal
[8] **T. Huang**, L. Shen, Y. Sun, W. Lin, and D. Tao, "Fusion of Global and Local Knowledge for Personalized Federated Learning," 2022, Transactions on Machine Learning Research (**TMLR**).
[9] **T. Huang**, W. Lin, L. Shen, K. Li and A. Y. Zomaya, "Stochastic Client Selection for Federated Learning with Volatile Clients," 2022, IEEE Internet of Things Journals (**IoT-J**).
[10] **T. Huang**, W. Lin, X. Hong , X. Wang, Q. Wu, R. Li, CH. Hsu, AY. Zomaya, "Adaptive Processor Frequency Adjustment for Mobile Edge Computing with Intermittent Energy Supply", 2021, IEEE Internet of Things Journals (**IoT-J**).
[11] **T. Huang**, W. Lin, W. Wu, L. He, K. Li and AY. Zomaya, "An Efficiency-boosting Client Selection Scheme for Federated Learning with Fairness Guarantee," 2020, IEEE Transactions on Parallel and Distributed Systems (**TPDS**).
[12] **T. Huang**, W. Lin, C. Xiong, R. Pan and J. Huang, "An Ant Colony Optimization Based Multi-objective Service Replicas Placement Strategy for Fog Computing," 2020, IEEE Transactions on Cybernetics (**TCYB**).

Under Submission
[13] **T. Huang**, S. Hu, W. Wei, L. Liu, "Silencer: pruning-aware backdoor defense for decentralized federated learning," Under Submission.
[15] **T. Huang**, S. Hu, L. Liu, "Vaccine: Perturbation-aware Alignment for Large Language Model," Under Submission.
[16] **T. Huang**, S. Hu, F. Ilhan, S. Tekin, L. Liu, "Lazy Safety Alignment for Large Language Models against Harmful Fine-tuning," Under Submission.
[17] **T. Huang,** G. Bhattacharya, P. Joshi, J. Kimball, L. Liu, "Antidote: Post-fine-tuning Safety Alignment for Large Language Models against Harmful Fine-tuning," Under Submission.
[18] **T. Huang**, S. Hu, F. Ilhan, S. Tekin, L. Liu, "Booster: Tackling Harmful Fine-tuning for Large Language Models via Attenuating Harmful Perturbation," Under Submission.

Projects

Area 1: Safety alignment for Large language models (Current focus)

1.1 Alignment-Stage defense for LLMs' harmful finetuning

-Uncover the reason of failure of safety alignment after fine-tuning an LLM on partially harmful data.
-Based on the reason of failure, which we name "harmful embedding drift", we develop an alignment stage defense solution, which "vaccinate" the model to be immune of harmful finetuning.

1.2 Finetuning-Stage defense for LLMs' harmful finetuning

- Develop a fine-tuning stage prototype solution for preserving safety alignment after harmful finetuning.

- Observed that *excess drift* towards the switching point might be the performance bottleneck for the prototype solution.
- Develop a refined solution by adding a proximal term to control the excess drift.

Area 2: Security aspect of Federated Learning (Previous study)

2.1 Backdoor Defense for Federated Learning with isolated subspace training

- First to identify poison coupling effect in federated learning.
- Invent isolated subspace training technique to decouple and filter the poisoned parameters.
- Source code available at https://github.com/LockdownAuthor/Lockdown.

2.2 Pruning-aware Backdoor Defense for Decentralized Federated Learning

- Theoretically identify empirical Fisher information as a reliable indicator of poisoned parameters.
- Empirically study the Fisher-guided pruning technique to purify the poisoned model .
- Invent a defense to boost pruning-awareness in the training phase.

Area 3: Efficient Federated Learning/Personalized Federated Learning (Previous study)

3.1 Efficient client selection in FL with multi-arm bandit

- Identify system heterogeneity/selection fairness/ cumulative participation as main factors for federated learning system performance.
- balance system heterogeneity/selection fairness/cumulative participation with UCB/stochastic multi-arm bandit algorithms.

3.2 Efficient PFL with low-rank+sparse

- Low-rank+sparse joint compression for personalized federated learning.
- Design a proximal algorithms.to solve the problem with theoretical guarantee.

3.3 Efficient PFL with dynamic sparse training

- Formulate the personalized models as a nested network in the global model.
- Propose a dynamic sparse training technique for training time acceleration in PFL.

Area 4: Resource scheduling in cloud/edge environment (Previous study)

4.1 Resource scheduling for renewable-energy supply edge devices

- Study computation offloading in a scenario that the edge devices are powered by renewable-energy supply.
- Formulate the problem as an event driven semi Markov decision process
- Solve the problem with a deep reinforcement learning technique.

4.2 Service replicas placement in Fog computing

- Study replicas placement problem in Fog computing
- Formulate the problem as a Mixed Integer Linear Problem
- Solve the problem with an ant colony algorithm.

Honor and Awards

- IEEE TPS 2023 student travel grant 2023
- National Scholarship (Top graduate scholarship in China) 2021
- National Scholarship 2020
- First-Class School Scholarship 2019

Academy Service

Conference Reviewer: NeurIPS (2023,2024), ICLR (2024,2025), ICML2024, AAAI2024
Journal Reviewer: Transactions on communications, Transactions on mobile computing, Transaction on Privacy, Transactions on Internet Computing