Junxiao Wang

Personal Mail: wangjunxiao@live.com
Work Mail: junxiao.wang@kaust.edu.sa
King Abdullah University of Science and Technology
Postdoctoral Fellow, http://jxiao.wang

Area of Expertise

AI and Systems: Distributed Machine Learning, AI Security and Privacy, Optimization of Inference.
My objective is to develop intelligent agents that are **ubiquitous** and **human-centric**, capable of learning from networked users in a manner that is considerate of limited data and resources.

Work Experience

King Abdullah University of Science and Technology, *Postdoctoral Fellow* 2023.02 - Now

Main Research Directions: Large Language Model, Optimization of Transformer Inference.
Lab: Provable Responsible AI and Data Analytics Laboratory Manager: Assistant Prof. Dr. Di Wang

The Hong Kong Polytechnic University, *Postdoctoral Fellow* 2021.03 - 2023.03

Main Research Directions: Federated Learning, Machine Unlearning.
Lab: Pervasive Edge Intelligence Laboratory Manager: Prof. Dr. Song Guo

Educational Background

Dalian University of Technology (Dalian, China), Computer Science, *PhD* 2016.09 - 2020.12
Queen Mary University of London (London, UK), Computer Science, *Visitor* 2018.10 - 2019.09
Dalian University of Technology (Dalian, China), Computer Science, *MEng* 2014.09 - 2017.07
Dalian Maritime University (Dalian, China), Software Engineering, *BEng* 2010.09 - 2014.06

Research Highlight

1. *Protecting Federated Learning users' Right to be Forgotten.*

Introduction: The European Union's General Data Protection Regulation (GDPR), which came into effect in 2018, means that "personal control" of data privacy has become increasingly important. For FL, users' right to be forgotten should completely eliminate the impact of personal data on the model. To this end, we proposed a framework that can realize the right to be forgotten, filling the gap in the field of compliance governance of FL.

Publication: ACM TheWebConf2022, IEEE Network2022.

2. *Ensure the privacy and security of shared model parameters in Federated Learning.*

Introduction: Gradient exchange is a commonly used communication method in FL. For a long time, it was believed that gradients can be safely shared, that is, training data will not be leaked due to gradient exchange. However, in fact, private training data can be obtained through shared gradients. We conducted a series of research on the risk of gradient exchange in FL.

Publication: IEEE INFOCOM2022, IJCAI2022.

3. *Use Foundation Models to improve the efficiency of Federated Learning.*

Introduction: The performance and efficiency of FL depend on the effectiveness of local training parameters and their smooth aggregation. FL inherently requires a large number of communication rounds and labeled data for training, which is often not available to edge users. To this end, we proposed a FL architecture based on the foundation model and its prompt learning technique, and implemented a new type of FL personalization technique based on the new architecture.

Publication: ACM TheWebConf2023, IEEE TMC2023.

4. *Ensure the security, privacy and ethical copyright issues of large pre-trained AI models.*

Introduction: There are more and more large AI models appearing on the Internet, which can generate false data that is difficult for humans to distinguish, or carry hidden Trojans. We conducted a series of studies exploring potential risks and countermeasures.

Publication: ACM KDD2023, NeurIPS2023.

Publication List

1. **Junxiao Wang**, Song Guo, Xin Xie, Heng Qi. Federated Unlearning via Class-Discriminative Pruning. The ACM Web Conference (TheWebConf) 2022, Online. (acceptance rate∼17.7% [323/1,822])

2. **Junxiao Wang**, Song Guo, Xin Xie, Heng Qi. Protect Privacy from Gradient Leakage Attack in Federated Learning. IEEE International Conference on Computer Communications (INFOCOM) 2022, Online. (acceptance rate∼19.8% [224/1,129])
3. Peiran Dong, Song Guo, **Junxiao Wang** (Corresponding Author). Investigating Trojan Attacks on Pre-trained Language Model-powered Database Middleware. ACM SIGKDD Conference on Knowledge Discovery and Data Mining (KDD) 2023, Long Beach, CA, USA. (acceptance rate∼22.1% [313/1,416])
4. Tao Guo, Song Guo, **Junxiao Wang** (Corresponding Author). pFedPrompt: Learning Personalized Prompt for Vision-Language Models in Federated Learning. The ACM Web Conference (TheWebConf) 2023, Austin, Texas, USA. (acceptance rate∼19.2% [365/1,900])
5. Peiran Dong, Song Guo, **Junxiao Wang** (Corresponding Author), Bingjie Wang, Jiewei Zhang, Ziming Liu. Towards Test-Time Refusals via Concept Negation. The Annual Conference on Neural Information Processing Systems (NeurIPS), New Orleans, LA, USA. (acceptance rate∼26.1% [3,222/12,343])
6. Rui Zhang, Song Guo, **Junxiao Wang** (Corresponding Author), Xin Xie, Dacheng Tao. A Survey on Gradient Inversion: Attacks, Defenses and Future Directions. International Joint Conference on Artificial Intelligence (IJCAI) 2022, Vienna, Austria. (acceptance rate∼14.9% [679/4,535])
7. Tao Guo, Song Guo, **Junxiao Wang** (Corresponding Author), Xueyang Tang, Wenchao Xu. PromptFL: Let Federated Participants Cooperatively Learn Prompts Instead of Models - Federated Learning in Age of Foundation Model. IEEE Transactions on Mobile Computing (TMC) 2023.
8. **Junxiao Wang**, Heng Qi, Keqiu Li, Xiaobo Zhou. PRSFC-IoT: A Performance and Resource Aware Orchestration System of Service Function Chaining for Internet of Things. IEEE Internet of Things Journal (IoTJ) 2018.
9. Leijie Wu, Song Guo, **Junxiao Wang** (Corresponding Author), Zicong Hong, Jie Zhang, Yaohong Ding. Federated Unlearning: Guarantee the Right of Clients to Forget. IEEE Network 2022.
10. Yunfeng Fan, Wenchao Xu, Haozhao Wang, **Junxiao Wang**, Song Guo. PMR: Prototypical Modal Rebalance for Multimodal Learning. IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) 2023, Vancouver, Canada. (acceptance rate∼25.8% [2,360/9,155])
11. Xin Xie, Xiulong Liu, **Junxiao Wang**, Song Guo, Heng Qi, Keqiu Li. Efficient Integrity Authentication Scheme for Large-scale RFID Systems. IEEE Transactions on Mobile Computing (TMC) 2022.
12. **Junxiao Wang**, Heng Qi, Wenxin Li, Keqiu Li, Steve Uhlig, Yuxin Wang. Dynamic SDN Control Plane Request Assignment in NFV Datacenters. IEEE Transactions on Network Science and Engineering (TNSE) 2021.
13. **Junxiao Wang**, Heng Qi, Yang He, Wenxin Li, Keqiu Li. FlowTracer: An Effective Flow Trajectory Detection Solution Based on Probabilistic Packet Tagging in SDN-Enabled Networks. IEEE Transactions on Network and Service Management (TNSM) 2019.
14. **Junxiao Wang**, Heng Qi, Keqiu Li, Steve Uhlig. Click-UP: Towards the Software Upgrade of Click based Modular Network Function. IEEE Systems Journal (ISJ) 2020.
15. Heng Qi, **Junxiao Wang**, Wenxin Li, Yuxin Wang, Tie Qiu. A Blockchain-driven IIoT Traffic Classification Service for Edge Computing. IEEE Internet of Things Journal (IoTJ) 2021.
16. **Junxiao Wang**, Yuchen Huang, Heng Qi, Keqiu Li, Steve Uhlig. CLICK-UP: Towards Software Upgrades of Click-driven Stateful Network Element. ACM SIGCOMM Conference 2018 (Demo), Budapest, Hungary.

Academic Service

PC Member/Reviewer International Conference on Artificial Intelligence and Statistics (AISTATS) 2024
Reviewer International Conference on Computer Vision (ICCV) 2023
Reviewer IEEE Transactions on Mobile Computing (TMC)
Reviewer IEEE Transactions on Network Science and Engineering (TNSE)

Referees

Assistant Prof. Dr. Di Wang, CEMSE, KAUST, di.wang@kaust.edu.sa
Prof. Dr. Song Guo, CSE, HKUST, songguo@cse.ust.hk
Prof. Dr. Steve Uhlig, EECS, QMUL, steve.uhlig@qmul.ac.uk
Prof. Dr. Keqiu Li, CIC, TJU, keqiu@tju.edu.cn
Prof. Dr. Heng Qi, CS, DLUT, hengqi@dlut.edu.cn

Last updated: *09 November 2023*