Yukun **Jiang**

SCHOOL OF CYBER SCIENCE & ENGINEERING · SICHUAN UNIVERSITY

☐ (+86) 130-8806-2284　|　✉ ashbringer0926@gmail.com

Research Interest

My research interest includes Privacy Preservation, Deep Learning, and IoT Security. Recently, I am focusing on building secure, robust, and efficient federated learning to face the challenges of Byzantine attacks and Non-IID data.

Education

Sichuan University (985 Project, Chengdu, China)　　　　　　　　　　　　　　　*Sep. 2018 - Jul. 2022 (expected)*
B.E. IN *Cyber Security*　　　　　　　　　　　　　　　　　　　　　　　　　　　*GPA: 3.66/4 (87.64/100)*
Core A/A+ courses: Applied Cryptography, Database System and Security, Data Mining for Cybersecurity, Cybersecurity Practice, Cybersecurity Comprehensive Experiment, Computer Communication and Networks, Computer Organization and Architecture, Assembly Language Programming, Web App. Dev., etc.

Publications

Yukun Jiang, Xiaoyu Cao, Chen Hao, Neil Gong: FedER: Communication-Efficient Byzantine-Robust Federated Learning. In Proceedings of International Conference on Learning Representations 2022 Workshop on Socially Responsible Machine Learning (ICLR 2022-SRML).

Beibei Li, **Yukun Jiang**, Qingqi Pei, Tao Li, Liang Liu, Rongxing Lu: FEEL: Federated End-to-End Learning with Non-IID Data for Vehicular Ad Hoc Networks. Major revision in IEEE Transactions on Intelligent Transportation Systems (T-ITS).

Beibei Li, **Yukun Jiang**, Wenbin Sun, Weina Niu, Peiran Wang: FedVANET: Efficient Federated Learning with Non-IID Data for Vehicular Ad Hoc Networks. In Proceedings of IEEE Global Communications Conference 2021 (GLOBECOM 2021).

Beibei Li, Yaxin Shi, Yuqing Guo, Qinglei Kong, **Yukun Jiang**: Incentive-Based Adaptive Federated Knowledge Distillation for Cross-Silo Applications. In Proceedings of IEEE International Conference on Computer Communications Workshops (INFOCOM 2022 WORKSHOPS)

Beibei Li, Peiran Wang, Hanyuan Huang, Shang Ma, **Yukun Jiang**: FLPhish: Reputation-Based Phishing Byzantine Defense in Ensemble Federated Learning. In Proceedings of IEEE Symposium on Computers and Communications 2021 (ISCC 2021).　　　**Best Paper Award**

Research Experience

Novel Byzantine Defense Method for Federated Learning　　　　　　　　　　　　　*Jul. 2021 – Nov. 2021*
ADVISOR: *Prof. Neil Gong* (DUKE UNIV.)
- Proposed a novel Byzantine-robust FL method that could reduce high communication cost of the state-of-the-art method while maintaining or even enhancing robustness, which is helpful for resource-constrained clients to conduct FL in adversarial settings.

Efficient Federated Learning with Non-IID Data for IoV　　　　　　　　　　　　　*Dec. 2020 – Jul. 2021*
ADVISOR: *Prof. Beibei Li* (SICHUAN UNIV.) & *Prof. Rongxing Lu* (UNIV. OF NEW BRUNSWICK)
- Leading projects aiming at alleviating the accuracy degeneration caused by data's Non-IIDness under various scenarios, which is a common feature of data-private learning.
- Proposed a hierarchical inner-cluster federated learning algorithm and a weighted inter-cluster cycling update algorithm, which are able to accelerate convergence, improve the model accuracy by around 10% under Non-IID data distributions, and reduce the redundant intra-cluster P2P communication overhead, while maintaining the premise of data privacy.　　　**Accepted by IEEE GLOBECOM 2021**
- Designed an efficient and secure federated end-to-end learning framework that can be implemented in vehicular ad hoc networks (VANETs), which supports the federated training of context prediction for self-driving cars.　　　**Major revision in IEEE T-ITS**

Reputation-based Phishing Byzantine Defense in Ensemble Federated Learning　　　　　*Dec. 2020 – May. 2021*
ADVISOR: *Prof. Beibei Li*
- Developed a novel federated learning architecture named Ensemble Federated Learning and a reputation-based robust Byzantine defense scheme called FLPhish based on our proposed 'phishing' method.　　　**Published in IEEE ISCC 2021**

Skills

Common　Python, C/C++, LaTeX, (Kali) Linux, SQL, Assembly, Java, HTML, etc.
AI & Security　PyTorch, TensorFlow, Sklearn, Burpsuite, Metasploit, Bettercap, Mitmproxy, Nessus, SQLMap, etc.
Language　Chinese (native), English (IELTS 7.0)

Honors & Activities

Best Paper Award, IEEE Symposium on Computers and Communications 2021.　　　　　　　　　*Sep. 2021*

1st Prize, Outstanding Student Scholarship, Sichuan Univ.　　　　　　　　　　　　　　*Sep. 2021*

2nd Prize, Outstanding Student Scholarship, Sichuan Univ.　　　　　　　　　　　　　　*Sep. 2020*