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

CISPA Helmholtz Center for Information Security (Saarbrücken, Germany), Ph.D. in Computer Science *Oct. 2022 –*

Sichuan University (Chengdu, China), B.E. in *Cyber Security* *Sep. 2018 – Jul. 2022*

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.

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.

Wokring Experience

Tencent Cloud (Shenzhen, China) *Fed. 2022 –*

MENTOR: *Dr. Yong Cheng*

- Aim at designing novel label protection methods for Split L learning.

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*