

Xilie Xu

+86-188-6127-2649
✉ xuxilie@comp.nus.edu.sg
☎ GodXuxilie
Google Scholar

Education Background

- Aug. 2021 - **Ph.D. Candidate**, Department of Computer Science, School of Computing, National University of Singapore, Singapore.
Supervised by Prof. Mohan Kankanhalli
○ Research topic: adversarial machine learning for good, such as non-parametric two-sample tests [1].
- Sep. 2017 - **Undergraduate**, Taishan College, Shandong University, Jinan, China.
- Jun. 2021 GPA 88.80/100 (ranking 5/16)
Taishan College is an elite program, which is committed to cultivating compound and creative elite students in science and engineering disciplines. The selection of this college is really competitive, admitting only about 15 students of CS major.

Research Experience

- Jun. 2019 - **Research Assistant in Research Center of Software and Data Engineering**, Shandong University, Jinan, China.
Jun. 2021
Supervised by Prof. Cui Lizhen and Dr. Zhang Jingfeng
○ Research topic: adversarial machine learning [2, 3, 4].

Publication

- [1] Xilie Xu*, Jingfeng Zhang*, Feng Liu, Masashi Sugiyama, and Mohan Kankanhalli. Adversarial attacks and defense for non-parametric two-sample tests. *ICML*, 2022.
- [2] Jingfeng Zhang*, Xilie Xu*, Bo Han, Gang Niu, Lizhen Cui, Masashi Sugiyama, and Mohan Kankanhalli. Attacks which do not kill training make adversarial learning stronger. In *International Conference on Machine Learning*, pages 11278–11287. PMLR, 2020.
- [3] Jingfeng Zhang*, Xilie Xu*, Bo Han, Tongliang Liu, Gang Niu, Lizhen Cui, and Masashi Sugiyama. Noilin: Improving adversarial training and correcting stereotype of noisy labels. *TMLR*, 2022.
- [4] Chen Chen*, Jingfeng Zhang*, Xilie Xu, Lingjuan Lyu, Chaochao Chen, Tianlei Hu, and Gang Chen. Decision boundary-aware data augmentation for adversarial training. *IEEE Transactions on Dependable and Secure Computing*, 2022.

⁰An asterisk (*) beside authors' names indicates equal contributions.

Internship Experience

- Jun. 2021 - **Research Intern**, Department of Ant Group-CRO Line-Security and Risk Management, Ant Z Space, Hangzhou, China.
Jul. 2021
Mentored by Dr. Lyu Lingjuan
- Research topic: adversarial machine learning and privacy.
 - Proposed an innovative proposal – a new method to protect model intellectual property and data privacy by preventing knowledge distillation.

Academic Activity

- Jul. 2019 **NUS School of Computing Summer Workshop 2019**, National University of Singapore, Singapore.
- Project “Save Shanghai: Garbage Classification” was awarded the first prize among about 100 competitive teams in the “Big Data and Cloud Computing” cluster.
- Sep. 2018 - **Research Assistant in Lab of Big Data Management and Analysis**, Shandong University, Qingdao, China.
May. 2019
Supervised by Prof. Peng Zhaohui
- Research project: Big data analysis in the context of manufacturing and how to utilize data from heterogeneous domains via transfer learning.

Award

- Oct. 2021 **Outstanding Reviewer Award**, NeurIPS 2021.
- Jun. 2021 **Outstanding Undergraduate Thesis Award**, Shandong University.
- Sep. 2020 **Specialty Scholarship (Research Innovation Award)**, *First Prize*, Shandong University.
- Sep. 2020 **Outstanding Student Scholarship**, *Second Prize*, Shandong University.
- Sep. 2019 **Outstanding Student Scholarship**, *Third Prize*, Shandong University.
- Oct. 2018 **the 10th Mathematics Competition of Chinese College Student**, *First Prize*, Chinese Mathematical Society.
- Sep. 2018 **Outstanding Student Scholarship**, *Third Prize*, Shandong University.
- Dec. 2017 **the 12th Certified Software Professional Examination**, *Top 10%*, CCF Computer Proficiency Certification.

Service

- Jun. 2022 **Serve as a reviewer for NeurIPS 2022.**
- Apr. 2022 **Serve as a student reviewing member of the Master of Computing admission**, School of Computing, National University of Singapore.
- Mar. 2022 **Serve as a reviewer for TMLR.**
- Feb. 2022 **Serve as a reviewer for ICML 2022.**
- Sep. 2021 **Serve as a reviewer for ICLR 2022.**
- May. 2021 **Serve as a reviewer for NeurIPS 2021.**