JIAYUN ZHANG

Email: jiayunzhang15@outlook.com ◇ Homepage: https://jiayunz.github.io/

EDUCATION

University of California San Diego — La Jolla, CA, U.S.A
Ph.D. Program in Computer Science and Engineering — Sep 2020 - Present

Fudan University — Shanghai, China
B.S. in Computer Science (with honors) — Sep 2015 - Jun 2020

University of Chicago — Chicago, IL, U.S.A
Research Assistant co-advised by Prof. Ben Y. Zhao and Prof. Heather Zheng. — Jan 2020 - Mar 2020

Aalto University — Espoo, Finland
Research Assistant advised by Prof. Yu Xiao. — Jun 2019 - Sep 2019

PUBLICATIONS

1. Huiying Li, Shawn Shan, Emily Wenger, **Jiayun Zhang**, Haitao Zheng, Ben Y. Zhao. "Blacklight: Defending Black-Box Adversarial Attacks on Deep Neural Networks." *arXiv preprint arXiv:2006.14042 (2020).* [pdf]
2. **Jiayun Zhang**, Qingyuan Gong, Yushan Liu, Yang Chen, Xin Wang. "Identifying Structural Hole Spanners in Online Social Networks Using Deep Learning." *In Submission.*
3. **Jiayun Zhang**, Qingyuan Gong, Yang Chen, Yu Xiao, Xin Wang, Aaron Yi Ding. "Understanding Work Rhythms in Software Development and Their Effects on Technical Performance." *In submission.*
4. **Jiayun Zhang**, Petr Byvshev, Yu Xiao. "Dataset: A video dataset of a wooden box assembly process." *To Appear: 3rd Workshop on Data Acquisition to Analysis (DATA'20).* [dataset]
5. Shawn Shan, Emily Wenger, **Jiayun Zhang**, Huiying Li, Haitao Zheng, Ben Y. Zhao. "Fawkes: Protecting Personal Privacy against Unauthorized Deep Learning Models." Proceedings of *the* 29^{th} *USENIX Security Symposium (USENIX Security)*, Boston, MA, Aug. 2020. [pdf]
6. **Jiayun Zhang**, Yang Chen, Qingyuan Gong, Aaron Yi Ding, Yu Xiao, Xin Wang, Pan Hui. "Understanding the Working Time of Developers in IT Companies in China and the United States." *IEEE Software. (DOI: 10.1109/MS.2020.2988022).* [pdf]
7. Qingyuan Gong, **Jiayun Zhang**, Yang Chen, Qi Li, Yu Xiao, Xin Wang, Pan Hui. "Detecting Malicious Accounts in Online Developer Communities Using Deep Learning." Proceedings of *the* 28^{th} *ACM International Conference on Information and Knowledge Management (CIKM)*, Beijing, China, Nov. 2019. [pdf]
8. Qingyuan Gong, **Jiayun Zhang**, Xin Wang, Yang Chen. "Identifying Structural Hole Spanners in Online Social Networks Using Machine Learning." Proceedings of *the ACM SIGCOMM 2019 Conference Posters and Demos*, Beijing, China, Aug. 2019. [pdf]
9. Yihan Ma, Hua Sun, Yang Chen, **Jiayun Zhang**, Yang Xu, Xin Wang, Pan Hui. "DeepLoc: A Location Preference Prediction System for Online Lodging Platforms." Proceedings of *the 14th CCF Chinese Conference on Computer Supported Cooperative Work (ChineseCSCW)*, Kunming, China, Aug. 2019. [pdf]

RESEARCH EXPERIENCE

Security and Privacy on Deep Neural Networks — Jan 2020 – Jun 2020
co-advised by Prof. Ben Y. Zhao and Prof. Haitao Zheng, University of Chicago

- **Defending Black-Box Adversarial Attacks on Deep Neural Networks** — Mar 2020 – Jun 2020
  - Collaborated in building Blacklight, a defense that detects query-based black-box attacks using an efficient similarity engine operating on probabilistic content fingerprints.
- **Protecting Personal Privacy against Unauthorized Deep Learning Models** Jan 2020 – Feb 2020

- Collaborated in building Fawkes, a system that allow individuals to inoculate themselves against unauthorized facial recognition models by adding imperceptible pixel-level changes to their photos.
- Contributed to a paper published by **USENIX Security'20**.

User Behavior Analysis in Online Social Networks May 2018 – Jun 2020
advised by Prof. Yang Chen, Fudan University

◦ **Identifying Structural Hole Spanners in Online Social Networks** Mar 2019 – May 2020
- Proposed a deep learning-based system for identifying structural hole spanners in online social networks with TextCNN and GBDT2NN; leveraged the cross-site linking function to enhance the identification; achieved a test AUC value of 0.854 on the Foursquare and Twitter datasets.
- Contributed to a paper submitted to **CIKM'20** and a poster published in **SIGCOMM Posters and Demos'19**.

◦ **Malicious User Identification in Version Control Systems** Jun 2018 – Jun 2019
- Collected a user-centric dataset including the information of over 10 million GitHub Users. [code][dataset]
- Proposed GitSec, a deep learning-based system with Phased LSTM and attention mechanism to detect malicious accounts on VCS; achieved a test AUC value of 0.938 on the GitHub dataset.
- Contributed to a paper published in **CIKM'19**.

◦ **Discovering Work Patterns of Developers** Jan 2019 – Sep 2019
- Performed clustering analysis on commit behaviors to identify representative work rhythms of developers.
- Analyzed the relationship between work rhythms and demographics, collaboration role and productivity.
- Conducted a user survey to understand the situation of working overtime from developers' perspectives.
- Contributed to a first-authored paper accepted by **IEEE Software**.

A Video and Sensor Dataset of a Wooden Box Assembly Process Jun 2019 – Sep 2019
advised by Prof. Yu Xiao, Aalto University

- Acquired video and sensor data of the wooden box assembly process with multiple cameras and a sensor glove; performed data labeling, processing and analysis.
- Contributed to a first-authored paper accepted by **DATA'20**.

INDUSTRIAL EXPERIENCE

VMware Information Technology (China) Co., Ltd. Shanghai, China
MTS (Member of Technical Staff) Intern Apr 2018 – Oct 2018

- Developed a log analysis system for automatically detecting the causes of program failures. 67 types of error causes was detected with an accuracy of 0.936 on real-time data from an internal bug reporting platform.
- Developed web APIs for an internal cloud resource platform to support the use of virtual machine templates.
- Participated in the implementation of Template Validation Service, a system for security verification of virtual machine templates uploaded to database.

SELECTED AWARDS

2020 Outstanding Graduate of Fudan University
2020 Chun-Tsung Scholar (Research Program Funded by Nobel Laureate Dr. Tsung-Dao Lee)
2019 The First Prize of Shanghai Open Data Innovation Research Competition (Top 1 among 65 teams)
2019 Best Student Award, Mobile Systems and Networking Group at Fudan University (1 out of 32)
2019 Second Class Scholarship for Outstanding Students in Fudan University (Top 10%)
2018 Xiyuan Scholar (Undergraduate Research Program at Fudan University)
2016 & 2018 Third Class Scholarship for Outstanding Students in Fudan University

SKILLS

Programming: Python, C/C++, Ruby, C#, HTML/CSS, JavaScript, SQL.
Packages and Tools: Pytorch, Tensorflow, Scikit-learn, Matlab, Django, Bootstrap, Unity, Blender etc.
Standard Language Tests: TOEFL 104 (Reading 28, Listening 24, Speaking 24, Writing 28)