305 N. University Street.
West Lafayette, IN, 47907, USA
+1-469-381-0501
zhan4057@purdue.edu
kaiyuanzhang.com
Last Updated: November 2022

Kaiyuan Zhang

Research Interests

My research interests focus on security and privacy in machine learning, specifically on federated learning.

Education

2020 – now **Purdue University**, *Computer Science*, West Lafayette, IN, USA.
Ph.D. Student, Advisor: Prof. Xiangyu Zhang
Committee Members: Prof. Berkay Celik, Prof. Rajiv Khanna

2018 – 2020 **University of Texas at Dallas**, *Computer Science*, Richardson, TX, USA.
Master of Science, Advisor: Prof. Wei Yang

2019 – 2020 **University of Illinois at Urbana-Champaign**, *Computer Science*, Urbana, IL, USA.
Visiting Graduate Student, Advisors: Prof. Tao Xie and Prof. Tianyin Xu

2013 – 2017 **Chang'an University**, *Network Engineering*, Xi'an, China.
Bachelor of Engineering

Publications

AROW'22 [3] FLIP: A Provable Defense Framework for Backdoor Mitigation in Federated Learning.
Kaiyuan Zhang, Guanhong Tao, Qiuling Xu, Siyuan Cheng, Shengwei An, Yingqi Liu, Shiwei Feng, Guangyu Shen, Pin-Yu Chen, Shiqing Ma, Xiangyu Zhang.
Under submission.
ECCV 2022 Workshop on Adversarial Robustness in the Real World (AROW), Best Paper Award.

TVCG'21 [2] DRGraph: An Efficient Graph Layout Algorithm for Large-scale Graphs by Dimensionality Reduction.
Minfeng Zhu, Wei Chen, Yuanzhe Hu, Yuxuan Hou, Liangjun Liu, **Kaiyuan Zhang**.
IEEE Transactions on Visualization and Computer Graphics, 2021.

JOV'19 [1] Enhancing statistical charts: toward better data visualization and analysis.
Xiaonan Luo, Yuan Yuan, **Kaiyuan Zhang**, Jiazhi Xia, Zhiguang Zhou, Liang Chang, Tianlong Gu. *Journal of Visualization*, 2019.

Teaching Experiences

Guest Lecture

Fall 2022 **CS 52900: Security Analytics**, *"Backdoor Attacks and Defenses on Neural Networks"*, Purdue University.

Teaching Assistant

Fall 2022 **CS 37300: Data Mining and Machine Learning**, *Purdue University*.

Spring 2022 **CS 37300: Data Mining and Machine Learning**, *Purdue University*.
Fall 2021 **CS 47300: Web Information Search And Management**, *Purdue University*.
Summer 2021 **CS 18200: Foundations of Computer Science**, *Purdue University*.
Spring 2021 **CS 37300: Data Mining and Machine Learning**, *Purdue University*.
Fall 2020 **CS 47300: Web Information Search And Management**, *Purdue University*.
Summer 2018 **Visual Analytics**, *Zhejiang University*.

Positions held

08/2020 – now **Purdue University**, *West Lafayette, IN, USA*.
Teaching Assistant
05/2019 – 05/2020 **University of Illinois at Urbana-Champaign**, *Urbana, IL, USA*.
Visiting Graduate Student, Advisor: Prof. Tao Xie and Prof. Tianyin Xu
12/2018 – 04/2019 **University of Texas at Dallas**, *Richardson, TX, USA*.
Research Assistant, Advisor: Prof. Wei Yang
02/2017 – 08/2018 **State Key Laboratory of CAD&CG, Zhejiang University**, *Hangzhou, China*.
Research Assistant, Advisor: Prof. Wei Chen

Selected Press

PurdueCS News Provable defense framework for backdoor mitigation in federated learning, 10/2022

Invited Talks

11/07/2022 **Backdoor Attacks and Defenses on Neural Networks**, Department of Computer Science, Purdue University, West Lafayette, IN, 2022.
10/23/2022 **FLIP: A Provable Defense Framework for Backdoor Mitigation in Federated Learning**, ECCV 2022 Workshop on Adversarial Robustness in the Real World (AROW), Best Paper Session, Virtual, 2022.

Professional Services

Organizer PurduePAML Machine Learning & Security Seminar, Purdue University, 2021 - 2022
Program Committee ICML Workshop on Adversarial Machine Learning Frontiers 2022
Reviewer IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP) 2023
Co-Reviewer ACM Conference on Computer and Communications Security (CCS), 2022, 2021
International Conference on Computer-Aided Verification (CAV), 2019
Student Volunteer ICML 2021, ICLR 2021, ECOOP/ISSTA 2021, CCS 2020, SIGMOD 2020
International Summer School on Visual Analytics, Zhejiang University, 2018, 2017, 2016
Representative Grade Appeals Graduate Student Committee, College of Science, Purdue University, 2021 - 2022

Honors and Awards

October 2022 **Best Paper Award at ECCV 2022 AROW Workshop**
September 2022 ECCV Student Conference Grant
April 2022 Purdue University Summer Research Grant Award

October 2020	ACM CCS Student Conference Grant
July 2017	Outstanding Undergraduate Thesis Award (5% in university)
November 2016	**China National Scholarship (0.2% in China)**
May 2016	3^{rd} Place in National College Students Cloud Computing Challenge, China
Dec 2015	2^{nd} Place in Regional Mathematical Contest in Modeling (MCM), China

Technical Skills

Courses	Statistical Machine Learning, Machine Learning Theory, Big Data Management and Analytics, Security Analytics, Operating System, Software Engineering, Computer Networks, Database Design, Data Structure, Design and Analysis of Algorithms
Languages	Python, C, C++, SQL
Libraries	Pytorch, NumPy, Pandas, Scikit-learn, Matplotlib, Pyplot, seaborn, ggplot2
Tools	Databricks, AWS, Google Cloud, Unix, Git, Vim, Subversion, Docker, LaTeX
Database	MySQL, Neo4j

References

Available upon a request.