Department of Computer Science
University of Virginia
(+1) 4044650810
bxv6gs@virginia.com
Webpage
Github *Linkedin*

Zihan Guan

Education

2023–present **PhD, Computer Science**, *University of Virginia*, Charlottesville, VA.
Research interests: Differential Privacy; Machine Learning Security

2020–2021 : **Master of Science, Computing**, *Imperial College London*, London, UK.
Courses: Optimization Theory; Operations Research; Network and Web Security

2016–2020 : **Bachelor of Management, Logistics Management**, *Dalian University of Technology*, China.
GPA: **3.92/4.00**, Rank: **1/29**

Publications & Preprints

Conferences

2023 **Zihan Guan**, *Mengnan Du, Ninghao Liu*, XGBD: Explanation-guided Graph Backdoor Detection, In *26th European Conference on Artificial Intelligence (ECAI 2023)*.

2023 **Zihan Guan**, *Lichao Sun, Mengnan Du, Ninghao Liu*, Towards Synchronization in Backdoor Attacks, In *32nd ACM International Conference on Information and Knowledge Management (CIKM 2023)*.

Preprints

2023 **Zihan Guan**, Zihao Wu, Zhengliang Liu, Dufan Wu, Hui Ren, Quanzheng Li, Xiang Li, and Ninghao Liu. Cohortgpt: An enhanced gpt for participant recruitment in clinical study, 2023.

2023 **Zihan Guan**, Mengxuan Hu, Zhongliang Zhou, Jielu Zhang, Sheng Li, and Ninghao Liu. Badsam: Exploring security vulnerabilities of sam via backdoor attacks. *arXiv preprint arXiv:2305.03289*, 2023.

2023 Yucheng Shi, Mengnan Du, Xuansheng Wu, **Zihan Guan**, and Ninghao Liu. Black-box backdoor defense via zero-shot image purification, 2023.

Research Experience

University of Georgia, Research Assistant

Dec,2022 – Jun,2023 ***Backdoor Detection on Graph Neural Networks***.
Developing efficient methods for defending against backdoor attacks on the graph neural networks.
(A paper has been accepted by ECAI2023.)

Dec,2021 – Sep,2023 ***Feature Synchronization in Backdoor Attacks***.
Formulating the early-fitting phenomenon in backdoor attacks and proposed an enhanced backdoor attacks.
(A paper has been accepted by CIKM2023.)

Advisor : **Dr. Ninghao Liu**, *Assistant Professor, Department of Computer Science*, University of Georgia (*Personal Web-page*)

Imperial College London, Master Thesis

Mar,2021 – Aug,2021 ***Scalable Methods for Neural Network Verification***.
Improved an existing semi-definite-programming-based method for verifying neural network.
(The code has been released to the code page)

Advisor : **Dr. Yang Zheng**, *Assistant Professor, Department of Electrical and Computer Engineering*, University of California San Diego (*Personal Web-page*)

Dalian University of Technology, Bachelor Thesis

Mar 2020 – Aug,2020 ***A Two-stage Tabu Search Algorithm for Solving the Job-shop Scheduling Problem***.
Proposed a new two-stage tabu search algorithm that aims at improving the neighborhood structure searching efficiency.

Advisor : **Dr. Xuewen Huang**, *Associate Professor, School of Economics and Management*, Dalian University of Technology

Work Experience

Dec,2019 – Mar,2020 ***Mobu***, *Android Engineer (Intern)*, Shanghai, China.
Developed more than 10 APPs independently, including Compass, Booster and Mini Games; Participated in the development and release of the Apps in the overseas market.

Dec,2018 – Mar,2019 ***Accenture***, *Software Engineer (Intern)*, Dalian, China.
Engaged in BMW project in automobile industry, developing an internal inventory system; Responsible for the layout design and business logistics of the log-in page; Received and fed back to the client's demand, completed 2 rounds of iterative development.

Fellowships & Awards

2023 Receipt of ***UVA Computer Science Scholar*** for the first year Ph.D. study.

2020 Excellent Graduate Student (top 5%)

2019 ***Meritorious Winner*** of Mathematical Contest In Modeling contest.

2017-2018 Technology and Information Scholarship (top 5%)

2017-2019 Academic Excellence Scholarship (GPA top 5%)

2017-2018 Merit Student

Professional Services

2023 The 2023 Conference on Empirical Methods in Natural Language Processing (EMNLP), Reviewer

2023 26th European Conference on Artificial Intelligence (ECAI), Reviewer

Computer skills

Programming Languages: Python, PyTorch, keras, R, Advanced JAVA, Kotlin

Web Technologies: HTML 5, PHP, JSP, Javascript

Database: SQL, MySQL, Apache