

Jie Peng

✉ jie.peng1004@gmail.com 🔗 <https://jiepeng104.github.io/>

Education

Harbin Institute of Technology

Sept 2018 – June 2022

Bachelor of Engineering in Computer Science and Information Security

- GPA: 3.73/4.00
- **Coursework:** Set Theory and Graph Theory (93/100), Computer System (94/100), Introduction to machine learning (93/100), Cryptography Theory and Practice (96/100), Information Content Security (95/100)

Harbin Institute of Technology

Sept 2022 – Jan 2025

Master of Engineering in Computer Security

- GPA: 3.34/4.00
- **Advisors:** Prof. Hui He and Prof. Weizhe Zhang
- **Coursework:** Combinatorial Optimization and Convex Optimization (97/100), Data Mining: Algorithms and Applications (98/100), Network and Information Security (94/100)

Publications

- **Jie Peng**, Hui He, Jing Zhao, Haoyu He, Hengji Dong, Jin Cao and Weizhe Zhang. “Circumventing Backdoor Space via Weight Symmetry”. (**Under Review**)
- **Jie Peng**, Hongwei Yang, Hui He, Jing Zhao, Haoyu He, Hengji Dong and Weizhe Zhang. “LS²: Boosting Hidden Separation for Backdoor Defense with Learning Speed-driven Label Smoothing”. (**Under Review**)
- Jing Zhao, Hongwei Yang, Hui He, **Jie Peng**, Weizhe Zhang, Jiangqun Ni, Arun Kumar Sangaiah, and Aniello Castiglione. “Backdoor Two-Stream Video Models on Federated Learning”. ACM Transactions on Multimedia Computing, Communications, and Applications (**TOMM**) [🔗](#)

Industry Experience

State Key Laboratory of Communication Content Cognition (Beijing)

April 2023 - Sept 2023

- Developed back-end services using Spring Boot and MyBatis for a social media analytics platform, enhancing data processing capabilities.
- Created a web crawler for Twitter using Selenium, collecting over one million data points and user information to train machine learning models, increasing data volume by 50%.
- Tools Used: Java, Python, Selenium

Shanghai Pudong Development Bank (SPD BANK, Shanghai)

Mar 2024 – June 2024

- Participated in developing a Graph-based Anomaly Detection algorithm within a federated learning setting to identify financial fraud patterns while maintaining data privacy
- Implemented the solution using FATE (Federated AI Technology Enabler), enabling secure and efficient collaboration between multiple financial institutions.
- Tools Used: Python, FATE (Federated AI Technology Enabler)

Additional Information

Skilled at: C, Java, Python, SQL, L^AT_EX

Languages: Mandarin (native), English (Proficient, IELTS band score 7)