Jing Xu

Curriculum Vitae

TU Delft, Postbus 5, 2600 AA Delft
The Netherlands
Visa State: Euro Blue Card
✱ *Born: 4 April, 1994*
📱 *+49 1747735811*
✉ *jingxu.buaa@gmail.com*
🌐 *https://www.linkedin.com/in/jing-xu-aa66871b0/*

About Me

Experienced machine learning scientist with over 5 years of experience in machine learning, security, and AI model development. Expertise in designing, training, and optimizing state-of-the-art models, analyzing large datasets, and deploying scalable and robust AI/ML models. Skilled in distributed training, model optimization, and data preprocessing using frameworks like PyTorch and TensorFlow. Passionate about developing AI-driven solutions and leveraging cutting-edge AI technologies to address real-world challenges.

Education

2019-2024 **PhD, Computer Science**, ***Delft University of Technology***, **The Netherlands**

- Research Focus: Machine Learning, Graph Neural Networks, Security.
- Thesis: *Exploring backdoor attacks on graph neural networks*.
- Supervisors: Prof. Inald Lagendijk, Prof. Frans A. Oliehoek and Dr. Stjepan Picek.
- Achievements: Published 10+ papers published at top-tier conferences & journals. Successfully defended in May 2024.

2016-2019 **MSc, Optical Engineering**, ***Beihang University***, **China**

- Specialization: Electrical Engineering, Signal Processing, Computer Vision
- Thesis: Research on Multi-Source Information Fusion in the All-Source Navigation and Positioning System based on the Factor Graph
- GPA: **3.857/4.0**-RANK: **top 5%**

2012-2016 **BSc, Electrical Engineering**, ***Shanghai University***, **China**

- Specialization: Computer Vision, Signal Processing, Automata
- Thesis: Coin Automatic Recognition System based on Computer Vision
- GPA:**3.86/4.0**-RANK: **1/931**

Work Experience

2023.11-present **Researcher**, ***CISPA, SprintML Lab***, **Germany**

- Developed privacy-preserving machine learning mechanisms to protect sensitive data in Large Language Models (LLMs) during training, fine-tuning, or soft prompt tuning.
- Implemented ML pipelines using tools such as Git, Docker, and GitLab, ensuring efficient deployment and scaling of production models.
- Collaborated with cross-functional teams to design and deploy machine learning solutions that address security risks.
- Mentored junior researchers in developing machine learning models and contributed to multiple research publications.

2019 **Researcher Intern**, ***Momo Technology Company, Deep Learning Lab***, **China**

- Developed data pipelines and automated workflows for processing and curating large datasets used in model training and evaluation.
- Developed GAN-based methods for face recognition and object detection.
- Developed deep learning models for object detection against spoofing, ensuring model robustness and applicability in high-performance environments.

Skills

Developer Tools: Linux, Slurm, Docker, VS Code, Git, GitLab, tmux, SSH, Jupyter

Libraries: Python, C++, PyTorch, TensorFlow, Hugging Face Transformers, Scikit-learn

Data Processing & Analysis: Pandas, NumPy, Matplotlib, Data Pipelines

Model Evaluation & Optimization: Hyperparameter Tuning, Accuracy Metrics

Algorithms: LLMs, vision-language models, GNNs, GANs, Fine-tuning models

Language: Mandarin–Native, English–Fluent, German–Beginner

Selected Projects

2024 **Differentially Private Graph Prompt Learning**

- First study to demonstrate private information can leak from graph prompts.
- Developed privacy-preserving machine learning models for secure data handling in production environments.

2024 **Private Soft-prompt Transfer**

- Explored secure soft-prompt transfer techniques for privacy-preserving LLMs.
- Proposed a novel method to transfer private prompts between LLMs using only public data.

2023 **Protect Ownership of Graph Neural Networks**

- Developed a watermarking framework to verify ownership of graph neural networks, ensuring model integrity and security.
- Conducted hypothesis testing to provide statistical analysis for verifying model ownership in practice.

2020-2023 **Exploring Security of Graph Neural Networks**

- Designed explainability-based backdoor attacks against GNNs, where the performance of our attack can be better explained and visualized.
- Applied federated learning to train GNNs over isolated private graph data.
- Designed multiple novel backdoor attacks to enhance the development of more secure and robust GNN models.

Honors

2018 BUAA Outstanding Graduate Student, Outstanding Member

2017 BUAA First Prize Scholarship (two consecutive years)

2016 SHU Outstanding Graduate Student, Outstanding Student, Outstanding Member

2015 SHU First Prize Scholarship (three consecutive years), GuangHua Scholarship

Hobbies

Boarding Games: Seven Wonders, Splendor, Wingspan, Ticket to Ride, Machi Koro, ...

Switch/PS Games: Zelda, Hogwarts Legacy

Cooking: Bakery, Chinese food

Outdoor Sports: Hiking, Tennis