Dongting Li

CURRICULUM VITAE

PERSONAL DETAILS

Full Name	Dongting Li
Gender	Male
Date and Place of Birth	08/11/2003, China
Citizenship	China
Mobile	0430050959
Email address	leedontip@gmail.com

EDUCATION

Course /Degree Name	**Educational Institution**	**Start date (Month/Year)**	**End date (Month/Year)**	**Course Grade (indicated as a percentage)**	**Duration of research component**
Bachelor of Engineering (Honours) - Software Engineering	University of Technology, Sydney	08/2024	08/2026	86.00%	1 year
Computer Science and Technology (Sino-foreign Cooperative Education Program)	Northeastern University-China	09/2022	06/2026	86.34%	2 months

RESEARCH EXPERIENCE

Duration	**Organization**	**Job title**
September 2024 - Current	DL Sec. With Apps. Griffith & UTS Joint Research Group	Researcher under Prof Leo Yu Zhang and Prof Yanjun Zhang.

Research Details:

Focus: *Trustworthy and Secure Artificial Intelligence (Backdoor Attack & Defense against Deep Reinforcement Learning)*

- Joined the research group while completing my undergraduate Honours degree, engaging in a research-intensive project on trustworthy AI with a primary focus on deep learning security and its extended application domains.

• Conducted in-depth research on adversarial machine learning, model robustness, and defensive paradigms, gaining hands-on experience with empirical evaluations, security benchmarking, and vulnerability assessments. • Assisted with peer-review activities for major conferences such as AAAI and ICLR, gaining exposure to scholarly evaluation standards and research quality assessment. • Supported the review process for ICICS 2025, contributing to the assessment of technical validity, experimental rigour, and presentation quality of submitted manuscripts. • Developed the ability to source knowledge across academic literature, security standards, and applied ML systems, and apply this knowledge to research, engineering practice, and security analysis.
Outputs: • Ongoing collaborative research project under preparation for publication in the area of secure and trustworthy deep learning systems. • Internal review reports and recommendation summaries for conference submissions (5 Papers).

SKILLS AND COMPETENCIES

Technical Skills:

Research on trustworthy artificial intelligence and reinforcement learning primarily requires researchers to have a solid grasp of fundamental computer science knowledge and artificial intelligence techniques. Specifically, I possess the following crucial skills:

- **Backdoor Attack and Defense Methodologies** — Competency in implementing poisoning-based backdoor attacks, empirical trigger analysis, defence evaluation pipelines, and robustness benchmarking across varied model architectures.
- **Deep Reinforcement Learning Security Analysis** — Skilled in assessing DRL agents under threat models, performing vulnerability evaluation, and analysing failure modes in policy optimisation under adversarial conditions.
- **Deep Learning Frameworks & Model Engineering** — Proficient with PyTorch/TensorFlow for model development, experiment orchestration, and controlled evaluations of model behaviour under security-critical scenarios.
- **Data Handling and Experimental Reproducibility** — Skilled in dataset curation for adversarial and backdoor experiments, ensuring controlled experimental conditions, reproducibility, and structured documentation.
- **Programming & Tooling** — Solid command of Python for research prototyping, automation, and experiment scripting; familiarity with security-oriented tools and ML system debugging practices.

Other Skills:

- **Language skill** — Fluent Chinese and English (Demonstrated by having completed 11 UTS courses in English-speaking environments)
- **Teamwork and communication skills** — Demonstrated by successfully developing a website with team members from Software Innovation Studio.

GRANTS AND AWARDS

Award Name	Date/Month/Year	Provider	Award Prize
Third-class scholarship at the school level	08/10/2024	Northeastern University-China	￥500 (RMB)
Details: This scholarship is awarded once per semester, based on the student's academic performance that semester. I achieved excellent grades in the second semester of my sophomore year (ranking in the top 14.66% of my major), thus securing the award.			