Asim Waheed

Waterloo, ON, Canada | asim.waheed29@gmail.com
asimwaheed.com | GitHub | LinkedIn | OCRID:0009-0001-9618-1082

Education

PhD in Computer Science *Sep 2025 – Present*
University of Waterloo, Canada
Supervisors: Florian Kerschbaum, N. Asokan

M.Math in Computer Science *Sep 2021 – Aug 2023*
University of Waterloo, Canada
Supervisor: N. Asokan
Thesis: On Using Embeddings for Ownership Verification of Graph Neural Networks

BS in Computer Science *Aug 2016 – May 2020*
Lahore University of Management Sciences, Pakistan

Experience

Doctoral Researcher *Sep 2025 – Present*
University of Waterloo, Canada

Research Engineer *Oct 2023 – Aug 2025*
University of Waterloo, Canada
- Developed **Amulet**, a framework for trustworthy ML (technical report).
- Designed an Intel SGX–based framework for secure attestation of ML model properties.

Graduate Student Researcher *Sep 2021 – Aug 2023*
University of Waterloo, Canada
- Developed a defense against model-stealing attacks on graph neural networks (IEEE S&P 2024).
- Contributed to an NLP-based auditing framework for Android APIs (USENIX Security 2023).

Data Scientist *Sep 2020 – Aug 2021*
Data Science Dojo, USA (Remote)
- Led enterprise AI consulting projects using Azure Cognitive Services.
- Built production analytics and NLP systems.

Research Assistant *Sep 2019 – Aug 2020*
Lahore University of Management Sciences, Pakistan
- Conducted research on backdoor defenses in NLP models (USENIX Security 2021).
- Supported faculty research through infrastructure management and data pipeline development.

Machine Learning Engineer Intern *Jun 2018 – Aug 2018*

Paitoo (Food Technology Start-up), Pakistan

- Built text classification and recommendation systems.
- Deployed backend services using Docker and Kubernetes.

Publications

1. **Asim Waheed**, Vasisht Duddu, N. Asokan. *GrOVe: Ownership Verification of Graph Neural Networks using Embeddings*. IEEE S&P 2024. Proceedings arXiv:2304.08566.
2. Parjanya Vyas, **Asim Waheed**, Yousra Aafer, N. Asokan. *Auditing Framework APIs via Inferred App-side Security Specifications*. USENIX Security 2023. Proceedings.
3. **Asim Waheed**, Sara Qunaibi, Diogo Barradas, Zachary Weinberg. *Darwin's Theory of Censorship: Analysing the Evolution of Censored Topics with Dynamic Topic Models*. WPES 2022. Proceedings.
4. Ahmadreza Azizi, Ibrahim Asadullah Tahmid, **Asim Waheed**, Neal Mangaokar, Jiameng Pu, Mobin Javed, Chandan K. Reddy, Bimal Viswanath. *T-Miner: A Generative Approach to Defend Against Trojan Attacks on DNN-based Text Classification*. USENIX Security 2021. Proceedings arXiv:2103.04264.

Teaching & Mentoring

Teaching Assistant *2021 – 2023*

University of Waterloo

- CS458: Computer Security and Privacy
- CS480: Introduction to Machine Learning
- Multiple intro courses (CS105, CS135, CS246)

Teaching Assistant *2018 – 2020*

Lahore University of Management Sciences

- CS437: Deep Learning
- CS334: Principles and Techniques of Data Science

Mentor *Oct 2021 – Dec 2021*

GradApp Lab (voluntary)

- Advised undergraduate students on graduate school applications and career planning; mentee admitted to the University of Toronto and currently employed as a Data Scientist with the Ontario Government.

Academic Service

- **Artifact Evaluation Committee**, Privacy Enhancing Technologies Symposium (PoPETS) *2026*

Scholarships & Awards

- **David R. Cheriton Graduate Scholarship**, University of Waterloo (PhD) *2025–2027*
- **David R. Cheriton Graduate Scholarship**, University of Waterloo (M.Math) *2021–2023*
- **International Master's Award of Excellence**, University of Waterloo (MMath) *2021–2023*
- **Graduated with High Distinction**, Lahore University of Management Sciences *2020*
- **Dean's Honor List (all four years)**, Lahore University of Management Sciences *2016–2020*