

ANUDEEP DAS

anudeep.das@uwaterloo.ca · (437)234-1117

EDUCATION

University of Waterloo Candidate for Doctor of Philosophy (PhD) Computer Science Co-advised by Profs. N. Asokan & Florian Kerschbaum	Waterloo, ON, Canada 09/2024 - Ongoing
University of Waterloo Bachelor's Computer Science (BCS) Honours Co-op	Waterloo, ON, Canada 06/2024

AWARDS AND GRANTS

Cybersecurity and Privacy Excellence Graduate Scholarship - \$10 000	06/2026
Queen Elizabeth II Graduate Scholarship in Science & Technology - \$15 000	05/2026
President's Graduate Scholarship - \$5 000	05/2026
Coefficient Giving (formerly Open Philanthropy) Gift - \$80 416 Research on LLM backdoors.	09/2025
David R. Cheriton Scholarship - \$10 000/year x 2 years	09/2025
Undergraduate Research Fellowship - \$7 500	01/2023
Math Undergraduate Research Award - \$6 000	01/2023
President's Research Award - \$1 500	05/2022
President's Scholarship of Distinction - \$2 000	09/2018

PUBLICATIONS AND MANUSCRIPTS

Functional and Secure Code Generation with Task Vectors Wang F., Das, A. , Nagappan M., Asokan, N. <i>arXiv.org</i> , 2025	2026
Backdooring Bias in Large Language Models Das, A. , Chantasantitam, P., Singh, G., He, L., Ponomarenko, M., & Kerschbaum, F. <i>arXiv.org</i> , 2025	2026
Do Concept Replacement Techniques Really Erase Unacceptable Concepts Das, A. , Singh, G., Chantasantitam, P., & Asokan, N. <i>arXiv.org</i> , 2025	2025
Espresso: Robust Concept Filtering in Text-to-Image Models Das, A. , Duddu, V., Zhang R., & Asokan, N. <i>Proceedings of the Fifteenth ACM Conference on Data and Application Security and Privacy (CODASPY)</i> [Best Paper Award], 2025	2025
Attesting Distributional Properties of Training Data for Machine Learning Duddu, V., Das, A. , Khayata, N., Yalame, H., Schneider, T., & Asokan, N. <i>29th European Symposium on Research in Computer Security (ESORICS)</i> , 2023	2023
Accord: application-driven networking in the datacentre Mortazavi, S. H., Shafieirad, H., Bahnasy, M., Munir, A., Cheng, Y., Das, A. , & Ganjali, Y. <i>Proceedings of the 14th IEEE/ACM International Conference on Utility and Cloud Computing</i> , 2021	2021

RESEARCH EXPERIENCE

Undergraduate Research Fellow University of Waterloo	Waterloo, ON 01/2023 - 04/2023
- Advised by N. Asokan and Vasisht Duddu. - Developed a novel, adversarially robust method for privately attesting confidential machine learning (ML) training data using ML and multi-party computation (MPC) techniques.	

Undergraduate Research Assistant
University of Waterloo

Waterloo, ON
09/2022 - 12/2022

- Began preliminary work for attestation project.

Undergraduate Research Assistant
University of Waterloo

Waterloo, ON
05/2022 - 08/2022

- Advised by Jesse Hoey and Zahra Sheikhabaee.
- Worked on reinforcement learning with Bayesian non-parametric models.

Network Automation ML Research Engineer
Huawei Technologies Co., Ltd.

Waterloo, ON
09/2020 - 12/2020

- Advised by Yashar Ganjali and Mahmoud Bahnasy.
- Designed and implemented a novel routing strategy using a Deep Q-Network (DQN) reinforcement learning model developed with PyTorch and NetworkX; the approach performed at 98% effectiveness.

WORK EXPERIENCE

Lead Machine Learning Architect
Shoplogix

Oakville, ON
01/2024 - 09/2024

- Led all ML implementation and deployment efforts to determine best specifications for go-to-market strategy.
- Developed Shoplogix's first AI product, an AI chat agent, using custom Large Language Models (LLMs), orchestrated in Amazon ECS.

Data Engineer
Shoplogix

Oakville, ON
05/2023 - 08/2023

- Optimized the running time of an ELT pipeline by 1200% (from 3 hours to 15 minutes).
- Leveraged AWS Lambda functions, SQS, S3, and PostgreSQL to architect two new ELT pipelines from scratch, unlocking valuable new KPI's.

Machine Learning Engineer
VTS

Toronto, ON
09/2021 - 12/2021

- Successfully designed and productionalized the company's first NLP ML pipeline using Amazon Sagemaker, S3, ECR, AWS Lambda, and CircleCI; unlocked valuable new data insights for clients.
- Employed the ULMFiT transfer learning methodology to construct a content classifier on top of Fast.AI's AWD-LSTM implementation; this NLP model performed with 95% accuracy.

Machine Learning Software Developer
BlackBerry Limited

Mississauga, ON
01/2020 - 04/2020

- Successfully developed a feature which detects Man-in-the-Middle (MiTM) attacks by leveraging C++ CURL and SSL libraries; this feature was added into the proprietary Mobile Threat Detection Android and iOS apps.

TEACHING ASSISTANTSHIPS

CS 446/646: Software Design and Architecture
University of Waterloo

04/2025 - 09/2025

CS 135: Designing Functional Programs
University of Waterloo

09/2024 - 12/2024

VOLUNTEER EXPERIENCE

Artifact Reviewer *PoPets*

09/2025 - 07/2026

[[Distinguished Artifact Reviewer](#)]

Reviewer *CPI Graduate Student Conference*

01/2025 - 03/2025