Abhijith Sharma

☎ +971-054-770-0935 ✉ abhijith.sharma.ubc@gmail.com Scholar LinkedIn Website Abu Dhabi, UAE

Focused towards building efficient decision-making AI agents under uncertainty, with a broader goal of enhancing their reliability and trustworthiness. Interested in developing robust validation strategies for a reliable AI deployment in real-world.

Work Experience

Machine Learning Research Associate II | *MBZUAI* — Abu Dhabi, UAE
Supervisor: Dr. Salem Lahlou — Dec 2024 - Jun 2025

- Worked towards evaluating privacy risks of spiking neural networks against membership inference attack
- Contributed to open source torchgfn by implementing graphical environment for generative flow network analysis.
- Implemented an agentic framework for diverse music melody generation using GFlowNet finetuning of LLMs.

Machine Learning Research Associate | *University of Waterloo AI Institute* — ON, Canada
Supervisors: Dr. Sebastian Fischmeister, Dr. Nasser Azad — Sep 2023 - Nov 2024
In collaboration with AVL, Graz, Austria and Transport Canada

- Responsible for building adversarial test features for AVL Scenius to evaluate visual AI models in autonomous driving.
- Developed a CARLA based test framework for adversarial evaluation of object detection models in real-time.
- Proposed a kernel density estimation based classifier to distinguish between regular & adversarial vehicle in the scene.
- Demonstrated the efficacy of test framework by conducting real-world experiments in the outdoor environment.

Data Science Intern | *TrojAI Inc.* — BC, Canada
MITACS Accelerate Researcher — Oct 2021 - Aug 2023

- Surveyed 100+ physical adversarial threats and their defenses into a comprehensive review paper.
- Demonstrated 3 novel techniques for designing a Multi-Patch threat against state-of-the-art CNN defenses
- Developed model-agnostic defense utilizing scene's total-variation to mitigate Multi-Patch attacks in a single scan

Decision Analytics Associate | *ZS Associates* — Pune, India
Market Research Team — Dec 2020 - May 2021

- Designed surveys to evaluate client's product pricing for the launch of a medical equipment in US.
- Developed statistical models and custom analyses in R, Python, Tableau to investigate business needs.
- Leveraged data analytics and hypothesis testing to guide market research team for decision-making

Education

Ph.D. in Machine Learning | *Mohamed Bin Zayed University of Artificial Intelligence* — Abu Dhabi, UAE
Research: Agentic AI Auditing and Safety, Intelligent Fuzz Verification of Multi-Agent Systems — Aug 2025 - Present
Supervisor: Dr. Salem Lahlou and Dr. Nils Lukas

M.Sc. in Computer Science | *University of British Columbia* — BC, Canada
Thesis: Towards Safeguarding Convolutional Neural Networks Against Physical Corruptions — Sep 2021 - Sep 2023
Supervisor: Dr. Apurva Narayan and Dr. John Braun — **GPA:** 4.33/4.33

B.Tech in Electrical Engineering | *College of Engineering, Pune* — Pune, India
Thesis: Hardware Implementation of Model Predictive Controller — Aug 2016 - May 2020
Supervisor: Dr. D.N Sonawane — **GPA:** 9.21/10 *(Gold Medal)*

Technical Skills

Programming	Python, C, PySpark, R, Embedded C, SQL
ML Libraries	PyTorch, Tensorflow/Keras, Pandas, NumPy, SkLearn, Tableau, Flask, Streamlit
Tools	Git, GitHub, MySQL, VSCode, LaTeX
Others	Azure (Databricks, Storage) Hadoop, Linux, Shell Scripting, Docker, MATLAB

Scholarships and Awards

- **MBZUAI PhD Scholarship:** To carry out research and cover living expenses during PhD. AED 840K (2025-29)
- **MITACS Accelerate Award:** Scholarship to research defenses against the adversarial attacks. CA$50K (2021-23)
- **MITACS Globalink Graduate Fellowship:** For returning MITACS scholars for masters in Canada. CA$15K (2021)
- **UBC Dean's Entrance Scholarship:** Merit based award for incoming graduate students at UBC. CA$5K (2021)
- **Gold Medalist:** Highest GPA at the department level for bachelors degree at COEP. - (2020)
- **COEP Alumni Excellence Award:** Based on overall academic excellence at the department level. INR 50K (2017-20)
- **Globalink Research Award:** Grant to conduct research at Canadian university as a visiting scholar. CA$10K (2019)

Publications

- I. Malek, A. Laajil, **A. Sharma**, S. Lahlou, and E. Moulines, "Loss-guided auxiliary agents for overcoming mode collapse in gflownets," *Proceedings of the AAAI Conference on Artificial Intelligence*, 2026
- **A. Sharma**, J. Guan, C. Tian, and S. Lahlou, "On the privacy risks of spiking neural networks: A membership inference analysis," in *Proceedings of the 41th Uncertainty in Artificial Intelligence (UAI)*, 2025
- **A. Sharma**, A. Narayan, N. L. Azad, S. Fischmeister, and S. Marksteiner, "AVATAR: Autonomous vehicle assessment through testing of adversarial patches in real-time," *IEEE Transactions on Intelligent Vehicles*, 2024
- **A. Sharma**, P. Munz, and A. Narayan, "Assist is just as important as the goal: Image resurfacing to aid model's robust prediction," in *Proceedings of the IEEE/CVF Winter Conference on Applications of Computer Vision*, pp. 3833–3842, 2024
- D. Kumar, **A. Sharma**, and A. Narayan, "Attacking CNNs in histopathology with SNAP: Sporadic and naturalistic adversarial patches," in *Proceedings of the AAAI Conference on Artificial Intelligence*, vol. 38, pp. 23550–23551, 2024
- **A. Sharma**, P. Munz, and A. Narayan, "NSA: Naturalistic support artifact to boost network confidence," in *2023 International Joint Conference on Neural Networks (IJCNN)*, pp. 1–8, IEEE, 2023
- **A. Sharma**, Y. Bian, V. Nanda, P. Munz, and A. Narayan, "Vulnerability of CNNs against multi-patch attacks," in *Proceedings of the 2023 ACM Workshop on Secure and Trustworthy Cyber-Physical Systems (SaT-CPS)*, 2023
- **A. Sharma**, Y. Bian, P. Munz, and A. Narayan, "Adversarial patch attacks and defences in vision-based tasks: A survey," *arXiv preprint arXiv:2206.08304*, 2022
- **A. Sharma** and A. Narayan, "Soft adversarial training can retain natural accuracy," in *Proceedings of the 14th International Conference on Agents and Artificial Intelligence (ICAART)*, 2022

Research Experience

MITACS Globalink Intern | *University of British Columbia* — BC, Canada

Supervisor: Dr. Ryozo Nagamune - Control Engineering Lab — May 2019 - Aug 2019

- Made small scale wind turbine setup operational by modifying existing motor drivers and calibrating sensors
- Developed data-driven model of turbine using data collected by running it in the wind tunnel under varying conditions.
- Designed feedback control of pitch and yaw system for maximum power point tracking.

Control Subsystem Member | *COEP Satellite's Initiative* — Pune, India

Team Mission: Design of a Nano-Sat with the objective of solar sailing in lower earth orbit (LEO) — Aug 2017 - Mar 2020

- Developed an early-stage sun sensor prototype to determine satellite's relative orientation to sun.
- Designed a modified PID algorithm for satellite's reaction wheel control to ensure stable and efficient orbit maneuvering.

Teaching Experience

Graduate Teaching Assistant | *Introduction to Operating Systems* — BC, Canada

Department of Computer Science, University of British Columbia — Jan 2022 - Apr 2022
Instructor: Dr. Apurva Narayan

- Conducted weekly lab sessions, graded exams and assignments. Assisted in designing lab tutorials.

Graduate Teaching Assistant | *Introduction to Data Analytics* — BC, Canada

Department of Computer Science, University of British Columbia — May 2022 - Aug 2022
Instructor: Dr. Youry Khmelevsky

- Conducted weekly lab sessions with tutorials on data analytics using R and Python