ABHIJITH SHARMA

abhijith.sharma.ubc@gmail.com | 236-338-1319 | LinkedIn | Google Scholar | GitHub

SUMMARY

- Skilled Machine Learning (ML) Engineer with a Master's degree in Computer Science and 3 years of experience
- Passionate about building safe and trustworthy AI that goes beyond typical accuracy metrics to prioritize robustness and fairness
- Dedicated to enhancing AI reliability through rigorous testing, validation, and continuous improvement processes
- Specializes in computer vision with high proficiency in deep learning frameworks like PyTorch and ML libraries like Scikit-learn
- Creative and analytical; Dedicated to applying innovative ML solutions to solve challenging problems and drive business success

TECHNICAL SKILLS

- **Programming languages:** Python, C, PySpark, SQL, R, Embedded C
- **ML Toolkit:** PyTorch, Tensorflow/Keras, Pandas, NumPy, SkLearn, Tableau, Flask, Streamlit
- **Others:** Azure (Databricks, Storage) Hadoop, Linux, Shell Scripting, Docker, MATLAB

EDUCATION

Master of Science, Computer Science **GPA: 4.33/4.33**
The University of British Columbia *Sep 2021 to Aug 2023*

WORK EXPERIENCE

Associate Research Engineer **Waterloo, Canada**
University of Waterloo Research *Nov 2023 to present*

- ***NSERC Alliance grant with AVL***: Developing adversarial testing framework: AVATAR, integrated with CARLA for validating robustness of object detection models in real-time for autonomous driving.
- ***Palitronica***: Implemented parameter-less and DB-SCAN inspired algorithm for identifying specific counterfeited electronic parts with 99% accuracy. Contributing to ML operations for developing pipeline for an in-house safety-critical network/IC analyzer.

Data Science - MITACS Accelerate Intern **Remote, Canada**
TrojAI Inc. *Jan 2022 to Aug 2023*

- Surveyed and compiled 100+ existing physical adversarial threats and their counter measures into a comprehensive review paper.
- Demonstrated 3 novel Multi-Patch threat to state-of-the-art CNN defenses, having superior potency than single patch attack.
- Improved CNN's confidence by at least 3 times against natural corruptions (snow, fog) by placing generative artifacts in scene.
- Developed the first model-agnostic defense against Multi-Patch attacks using total-variation-based image resurfacing, achieving up to a 20% improvement in accuracy

Decision Analytics Associate **Pune, India**
ZS Associates *Dec 2020 to May 2021*

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

RESEARCH EXPERIENCE

Graduate Research Assistant **Kelowna, Canada**
The University of British Columbia (Intelligent Data Science Lab) *Sep 2021 to Aug 2023*

- Proposed subset selection of vulnerable samples for soft adversarial training against norm-based attacks while retain natural accuracy. Work got selected as a position paper at ICAART' 22. [Paper Link]
- Conducted in-depth research on identifying and mitigating physical attacks on deep-learning systems for visual tasks for my Master's thesis, under the guidance of Dr. Apurva Narayan, contributing to enhanced security measures in AI systems. [Thesis Link]

AWARDS

- **MITACS Accelerate Award** with TrojAI Inc. to research defenses against the adversarial attacks for visual tasks. - (2022-23)
- **MITACS Globalink Graduate Fellowship** for the returning MITACS Glabalink Research Interns for masters in Canada. - 2021
- **UBC Dean's Entrance Scholarship:** Merit based award for incoming graduate students at UBC. - 2021
- **Gold Medalist:** Highest GPA at the department level for bachelors degree at COEP. - 2020
- **COEP Alumni Excellence Award** for the academic excellence at department level. - (2017-20)

SELECTED PUBLICATIONS

- **A. Sharma**, P. Munz, and A. Narayan. "Assist Is Just As Important as the Goal: Image Resurfacing To Aid Model's Robust Prediction." *In IEEE/CVF Winter Conference on Applications of Computer Vision **(WACV)**, 2024*.
- **A. Sharma**, P. Munz, and A. Narayan. "Naturalistic support artifacts to boost network confidence." *In Proceedings of the International Joint Conference on Neural Networks **(IJCNN)**, 2023*.
- **A. Sharma**, Y.Bian, V.Nanda, P. Munz, and A. Narayan. "Vulnerability of cnns against multi-patch attacks." *In Proceedings of the Secure and Trustworthy Cyber-Physical Systems **(SaT-CPS)**, 2023*.
- **Sharma** et al. (2022) "Adversarial patch attacks and defences in vision-based tasks: A survey."*Preprint arXiv:2206.08304, 2022*