Pritam Dash

Vancouver, BC • **E-mail:** pdash@ece.ubc.ca • **Web**: dashpritam.github.io • **LinkedIn** /in/pritamdash

SUMMARY - PhD Candidate in AI and Systems. Proven track record of developing scalable learning frameworks for LLMs, Deep-RL agents and time-series models. Work recognized through top-tier publications, awards, and patents. Passionate about translating AI research into real-world impact.

RESEARCH EXPERIENCE

PhD Candidate at the University of British Columbia, Vancouver, Canada — Sep 2020 – Present

- Proposed a **multimodal adversarial training** framework for AI agents that enables **2X faster** policy learning while improving safety compliance and minimizing system's disruption under adversarial conditions.
- Proposed a robust **time series** modeling approach that achieves > 90% accuracy in anomaly classifications, with integrated graph-based **causal analysis** for root cause identification.
- Designed methods to **classify and detect** physically realizable **adversarial patch** attacks against DNNs. This method demonstrated > **80% reduction** in misclassification in computer vision benchmarks.

Research Intern at Oracle Labs, Vancouver, Canada — Jul 2022 – Dec 2022

- Proposed a pre-training approach to improve **zero-shot performance** of LLMs in code automation tasks.
- Designed an LLM based **recommendation system** that integrates with developer environments to proactively provide ranked and relevant solutions by eliminating the need for manual prompts.

Research Engineer at (ISEC/IAIK) Graz University of Technology, Austria — Jan 2017 – Aug 2018

- Designed a crypto framework for end-to-end confidentiality (IAIK-JCE extension) in **federated identity management** cloud services. This approach is **used by three services providers** in Germany and Italy.
- Led the efforts in designing approaches for assessment of **GDPR compliance** in cloud services. This work is now used by EuroCloud's StarAudit Certification (StarAudit, CREDENTIAL).

SELECTED PUBLICATIONS

Talks

"*Detection is not Enough: Attack Recovery for Securing Robotic Vehicles*", USENIX Enigma 2022.

"*Crash, Fail-safe, or Recover*", VehicleSec at USENIX Security 2025.

Conferences

Pritam Dash, Ethan Chan, Karthik Pattabiraman, "*SpecGuard: Specification Aware Recovery for Robotic Autonomous Vehicles from Physical Attacks*", ACM CCS 2024. *Acceptance Rate 16.7%.*

Pritam Dash, Guanpeng Li, .., Karthik Pattabiraman, "*PID-Piper: Recovering Robotic Vehicles from Physical Attacks*", IEEE/IFIP DSN 2021. *Acceptance Rate 16.4%*. **Best paper award**

Patents

Pritam Dash, Arno Schneuwly, Saeid Allahdadian, Matteo Casserini, Felix Schmidt, "*Training Syntax-aware Language Models with AST Path Prediction*".

Arno Schneuwly, Saeid Allahdadian, **Pritam Dash**, Matteo Casserini, Felix Schmidt, Eric Sedlar, "*doc4code: An AI-driven Documentation Recommender System to aid Programmers*".

EDUCATION

PhD in Electrical and Computer Engineering, University of British Columbia — Sep 2020 – Present

MASc in Electrical and Computer Engineering, University of British Columbia — Sep 2018 – Aug 2020

AWARDS AND HONORS

- NSF/ACM SIGBED Rising Star Award in CPS – 2024 link. (Top 40 early career researchers worldwide).
- Master's thesis featured in SERENE-RISC as top ten cybersecurity development in Canada – 2020.
- Four Year Fellowship (4YF) for doctoral studies. Given to the top 10 students in each incoming class – 2020.
- Indian Academy of Sciences Research Fellowship – 2014, 2015 (~120 students selected across India).

TECHNICAL SKILLS

Programming	C++, Java, Python, Matlab
AI Technologies	PyTorch, TensorFlow, ONNX, Hugging Face, LangChain, Stable-Baselines, Gym
Systems and Infra	Docker, AWS, Spark, Isaac Sim, ROS2