

Pritam Dash

Vancouver, BC • E-mail: pdash@ece.ubc.ca • Web: dashpritam.github.io • LinkedIn [/in/pritamdash](https://in.pritamdash)

RESEARCH INTEREST

Trustworthy AI, Secure Systems.

RESEARCH EXPERIENCE

Doctoral Candidate at the University of British Columbia, Vancouver, Canada

Sep 2018 – 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.
- This work resulted in filing **two US patents** in the area of LLM and recommendation systems.

Research Engineer at (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 transparent assessment of **GDPR compliance** in cloud services. This work is now used by EuroCloud's StarAudit Certification ([StarAudit](#), [CREDENTIAL](#)).

SELECTED PUBLICATIONS

Talks **Pritam Dash**, "Detection is not Enough: Attack Resilience for Safe and Robust Autonomous Robotic Vehicles", Usenix Enigma 2022. [Talk](#) (Exemplary talk mention [link](#)).

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%.
Zitao Chen, **Pritam Dash**, Karthik Pattabiraman, "Jujutsu: A Two-stage Defense against Adversarial Patch Attacks on DNNs", ACM AsiaCCS 2023. Acceptance Rate 16%.
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** [Talk](#)

Patents **Pritam Dash**, Arno Schneuwly, Saeid Allahdadian, Matteo Casserini, Felix Schmidt, "Training Syntax-aware Language Models with AST Path Prediction". [link](#)

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 – 2024 [link](#). (awarded to 40 young 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

Tools and Technologies C++, Java, Python, JavaScript, Matlab, AWS, Docker, ROS2.

AI and Simulation PyTorch, Spark, Hugging Face, LangChain, Stable-Baselines, Gym, Isaac Sim.