Pritam Dash

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

RESEARCH EXPERIENCE

Doctoral Candidate at the University of British Columbia, Vancouver, Canada **Sep 2018 – Present**

- Proposed a method for designing **safe Deep-RL** agent that is resilient even under adversarial conditions (faults, attacks) by incorporating temporal logic-based invariants and game-theoretic adversarial training.
- Designed a **robust time series** modeling approach to detect and mitigate sensor anomalies against autonomous vehicles (AV). Work on AV security featured in EurekaAlert, TechXplore, GlobalNews.
- Proposed methods to detect and mitigate physically realizable **adversarial patch** attacks against DNNs. This method demonstrated **80% reduction** in misclassification in computer vision benchmark.

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.

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", filed with US Patent Office.

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 for research in Cyber-Physical Systems – 2024.
- 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.
- DAAD working internship in science and engineering fellowship – 2015.
- Indian Academy of Sciences research fellowship – 2014, 2015 (~120 students selected across India).

TECHNICAL SKILLS

Programming Language	C++, Python, JavaScript, Matlab.
Tool and Technologies	PyTorch, Keras, Stable-Baselines, Gazebo, Gym, Docker, AWS, Docker, ROS2.