Pritam Dash

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

RESEARCH INTEREST

AI and Systems, Trustworthy AI, Secure Systems.

EDUCATION

PhD in Electrical and Computer Engineering Sep 2020 – Present	University of British Columbia, Canada Advisor: Dr. Karthik Pattabiraman
MASc in Electrical and Computer Engineering Sep 2018 – Aug 2020	University of British Columbia, Canada Advisor : Dr. Karthik Pattabiraman
MS in Software Engineering (BS+MS Integrated Program) Jul 2011-May 2016	Vellore Institute of Technology, India

AWARDS AND HONORS

- NSF/ACM SIGBED Rising Star Award – 2024 link. (awarded to 40 young researchers worldwide).
- UBC Solutions Scholars Award for interdisciplinary research in AI and climate – 2024.
- UBC President’s Academic Excellence Award – 2022-2024.
- UBC Faculty of Applied Sciences graduate award – 2020-2024.
- Best paper award at IEEE/IFIP DSN’2021 (flagship venue in the field of Dependable Computing research).
- Master’s thesis featured in SERENE-RISC as top ten cybersecurity development in Canada – 2020.
- 4YF Fellowship for doctoral studies at UBC (given to top 10 students in each graduating class) – 2020.
- DAAD Working Internship in Science and Engineering Fellowship – 2015.
- Indian Academy of Sciences Research Fellowship – 2014, 2015 (~120 students selected across India).

RESEARCH EXPERIENCE

Research Assistant at the University of British Columbia, Vancouver, Canada **Sept 2018 – Present**

Doctoral Research: Trustworthy AI (research featured in EurekaAlert, TechXplore, GlobalNews*)*

- 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 **transfer learning** framework for training Deep-RL policy, using low-dimensional latent state representations. This approach achieved **4X faster** convergence compared to conventional methods.
- Designed a robust **time series** modeling approach that achieves > 90% accuracy in anomaly classifications, with integrated graph-based **causal analysis** for root cause identification.

Machine Learning Security – Computer Vision

- Proposed methods to detect and mitigate physically realizable **adversarial patch** attacks against DNNs. This method demonstrated **80% reduction** in misclassification in computer vision benchmarks.

AI for Search and Information Retrieval

- Designed an AI agent using **LLM** and **RAG** to answer environmental science queries by synthesizing insights from climate reports for improved accuracy and relevance.
- Developed role-aware filtering to rank and tailor information based on the users’ profile.

Security Analysis and Testing

- Proposed a **physics-driven fuzz testing** technique to evaluate the resilience of distributed algorithms.
- Highlighted the limitations of **end-to-end encryption** protocols, and demonstrated how network **side channel leaks** can be exploited to launch active attacks to disrupt distributed systems’ operations.

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

Research Areas: Large Language Models, Search and Retrieval

- 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 (ISEC/IAIK) Graz University of Technology, Austria **Jan 2017 – Aug 2018**

Research Areas: Applied Cryptography, End-to-End Confidentiality, Privacy.

Involved in CREDENTIAL EU Horizon 2020 Project. Key contributions are as follows:

- 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).

Conferences

Pritam Dash, Ethan Chan, Karthik Pattabiraman, "SpecGuard: Specification Aware Recovery for Robotic Autonomous Vehicles from Physical Attacks", ACM SIGSAC Conference on Computer and Communications Security (CCS) 2024. *Acceptance Rate 16.7%.*

Pritam Dash, Guanpeng Li, Mehdi Karimibiuki, Karthik Pattabiraman, "Diagnosis-Guided Attack Recovery for Securing Robotic Vehicles from Sensor Deception Attacks", ACM ASIA CCS 2024. *Acceptance Rate 21%.*

Elaine Yao, **Pritam Dash**, Karthik Pattabiraman, "SwarmFuzz: Discovering GPS Spoofing Attacks in Drone Swarms", IEEE/IFIP DSN 2023. *Acceptance Rate 20%*.

Zitao Chen, **Pritam Dash**, Karthik Pattabiraman, "Jujutsu: A Two-stage Defense against Adversarial Patch Attacks on DNNs", ACM ASIA CCS 2023. *Acceptance Rate 16%*.

Pritam Dash, Guanpeng Li, Zitao Chen, Mehdi Karimibiuki, Karthik Pattabiraman, "PID-Piper: Recovering Robotic Vehicles from Physical Attacks", IEEE/IFIP Dependable Systems and Networks (DSN) 2021. *Acceptance Rate 16.4%*. **Best paper award** Talk

Pritam Dash, Mehdi Karimibiuki, and Karthik Pattabiraman, "Out of Control: Stealthy Attacks on Robotic Vehicles Protected by Control-Based Techniques", ACM ACSAC 2019. *Acceptance Rate 22.6%*. Work featured in EurekaAlert, TechXplore, GlobalNews.

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.

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

TECHNICAL SKILLS

Tools and Technologies	C, C++, Java, Python, JavaScript, Matlab, Git, AWS, Docker, ROS2.
AI Technologies	PyTorch, Stable-Baselines, Hugging Face, LangChain, Gym, MuJoCo, Isaac Sim.

Date: July 15, 2025
Place: Vancouver, Canada

Pritam Dash