Pritam Dash

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

RESEARCH INTEREST

Security and Reliability, Trustworthy AI, Embodied AI.

EDUCATION

PhD in Electrical and Computer Engineering — University of British Columbia, Canada
Sep 2020 – Present — Advisor: Dr. Karthik Pattabiraman

MASc in Electrical and Computer Engineering — University of British Columbia, Canada
Sep 2018 – Aug 2020 — Advisor : Dr. Karthik Pattabiraman

MS in Software Engineering (BS+MS Integrated Program) — Vellore Institute of Technology, India
Jul 2011-May 2016

AWARDS AND HONORS

- NSF/ACM SIGBED Rising Star Award for research in Cyber-Physical Systems – 2024 link.
- President's Academic Excellence Award (UBC) – 2023.
- Exemplary talk mention at Usenix Enigma'2022 link
- 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**

Research Area: Trustworthy AI, Embodied AI (research featured in UBC, EurekaAlert, TechXplore, GlobalNews)

- Proposed a method for training robust and **safe Deep-RL** policies for robotic systems. This approach enhances resilience of robotic systems under adversarial conditions, such as **sensor faults and 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 robotic vehicles (RV). This approach enables the RV to operate safely despite malicious intervention.

Research Area: Machine Learning Security

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

Security Analysis and Testing

- Proposed a fuzzing technique to discover **GPS spoofing** vulnerabilities in swarm control algorithms.
- Highlighted the limitations of end-to-end encryption protocols in CPS, and demonstrated how side channel leaks can be exploited to launch active attacks to disrupt CPS operations.

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

Research Area: AI for Code, Large Language Models

- 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**

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).

Research Intern at Institute for Infocomm Research (I2R) – A*STAR, Singapore **Jan – Jun 2016**

- Developed game-based techniques for cyber security training and awareness.

Research Intern at Fraunhofer SIT, Darmstadt, Germany **Jun – Jul 2015**

- Investigated impact of code changes on security assurance cases of software.

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.

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.

Demo/ Poster **Pritam Dash**, and Karthik Pattabiraman, "Demo: Recovering Autonomous Robotic Vehicles from Physical Attacks". AutoSec @NDSS 2022

PROFESSIONAL SERVICES

Conferences Sub-reviewer for research track in DSN'22, DSN'21, DSN'20, ISSRE'22, ISSRE'21.

Mentorship Co-supervised a master student and two undergraduate students at UBC (2021-2023).

Date: August 15, 2024
Place: Vancouver, Canada

Pritam Dash