Pritam Dash

2366 Main Mall, Vancouver, BC V6T 1Z4, Canada • **E-mail:** pdash@ece.ubc.ca • **Web**: dashpritam.github.io

RESEARCH INTEREST

Machine Learning, Embodied AI, Security and Reliability.

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

- 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.
- The University of British Columbia Four Year Fellowship (4YF) for doctoral studies – 2020. Given to the top 10 students in each incoming class of graduate students.
- 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 designing safe Deep-RL agents that incorporate temporal logic-based invariants and ensure resilience even under adversarial conditions (e.g., failure, attacks).
- Designed a robust time series modeling approach to detect attacks against autonomous vehicles (AV) and generate recovery signals that allows AVs to operate safely despite malicious interventions.

Research Area: Machine Learning Security

- Proposed methods to detect and mitigate physically realizable adversarial attacks (patch attacks) against image classification models. This allows the models to predict robust outputs despite malicious inputs.

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

Research Area: AI for Code

- Designed a novel pre-training approach for Large Language Models (LLM) to enhance semantic understanding of source code. This approach improves zero-shot performance 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 (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, Guanpeng Li, Mehdi Karimibiuki, Karthik Pattabiraman, "Diagnosis-Guided Attack Recovery for Securing Robotic Vehicles from Sensor Deception Attacks", ACM ASIA CCS 2024 (to appear). *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 Deep Neural Networks", 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

Yingao Yao, **Pritam Dash**, Karthik Pattabiraman, "May the Swarm Be with You: Sensor Spoofing Attacks Against Drone Swarms". ACM CCS 2022

TECHNICAL SKILLS

AI and ML	Large Language Models, Deep-RL, Multi-modal Learning, Causal Inference, Time series modeling, Adversarial ML.
Robotics	Foundation models for robotics, Deep-RL for robot control, SLAM, Sensor Fusion and Control, ROS.
Systems and Security	Fault tolerance and resilience, Program analysis, Fuzz testing, Applied Cryptography, Identity and access management.
Tools and Technologies	C++, Python, Java, Spark, TensorFlow, PyTorch, Keras, Stable-Baselines

Date: January 15, 2024
Place: Vancouver, Canada

Pritam Dash