Aarti S. Kashyap

Personal Data

web: https://grep-aarkash.github.io/
Phone: +1 236 987 6003(Canada), +91 9930 645 411(India)
email: kaarti.sr@gmail.com

Research Interests

Formal verification; Machine-Learning; Security; Cyber-physical systems; Programming Languages.

I am interested in designing scalable verification techniques for systems.

Education

August 2018 - current — Master of Applied Science in Electrical and Computer Engineering,
University of British Columbia, Vancouver
Advisor: Prof. Karthik Pattabiraman

July 2018 — B.Tech in Information Technology,
College of Engineering, Pune, India

Research Internships

2017 | Summer Intern, NTT DATA R&D, Tokyo
Development of function for remote forensic tools
Supervisor: Shinichiro Fuji and Shota Togasaki

2016 | Summer Intern , Interface Design Associates Pvt Ltd., Mumbai
Machine learning
Supervisor: K. Srinivasan Iyer and Dr. B. Vaidyanathan

2016 | Winter Intern , Interface Design Associates Pvt Ltd., Mumbai
Linux Device Drivers (LDD) and Real Time Kernel implementation.
Supervisor: K. Srinivasan Iyer and Dr. B. Vaidyanathan

Open source contributions

2017 | Debian Packaging
npm modules packaging
https://qa.debian.org/developer.php?login=kaarti.sr@gmail.com

2017 | Represented the FOSS Community (Mozilla and Debian) at TIFR,Khodak
Talk on Embedded systems such as Raspberry pi and Beaglebone Black
Runner up prize for the talk.

2017 | Lintian project
Localization for Hindi support.

Research Projects

2019 | Formal security analysis of security in Deep-neural networks for safety-critical systems
MASc. Thesis
Using Mixed Integer Linear Programming(MILP) to encode Deep Neural networks in order to verify security properties for safety-critical systems such as Artifical Pancreas Systems.

2019 | Fault injector for Autonomous Vehicles
SenFI
Fault-injector for detecting the failure rates caused due to sensor faults in Autonomous vehicles.

2019 | Compiler correctness
Compositional correctness
Compositional compiler correctness for source language - Simply typed lambda calculus(STLC) and target language - STLC with recursive types using logical relations. - https://github.com/grep-aarkash/Compiler-Theory

2019 | Static analysis of placement of Linux security modules (LSMs)
Camflow
Static analysis to determine the completeness of information flow policy for Linux kernel v4.20. - https://github.com/grep-aarkash/LSM-based-provenance-capture

2018 | Using theorem provers for verifying equivalence of storage systems)
Storage-Why3
Applying theorem provers such as Z3, CVC4 and Alt-ergo for equivalence checking of different storage systems in the Why3 environment.

2018 | Building an architectural platform for edge computing
Things-JS
ThingsJS is a comprehensive platform for designing and deploying high-level edge applications written in JavaScript onto the IoT devices themselves, in combination with the cloud. http://thingsjs.io/

2018 | Intrusion Detection Systems(IDS)
IDS using Ontology based methodologies
Comparison of Ontology based approaches and Machine learning based approaches for constructing IDS. - https://github.com/grep-aarkash/Ontology-based-IDS-for-DOS-Attacks

2016 | Fingerprint scanner
Fingerprint scanner for college attendance
Exploring feasibility and scalability of fingerprint scanners in a practical environment.

Other-Projects

https://github.com/grep-aarkash

Awards and Grants

2019 | PLMW (Programming Languages Mentoring Workshop) at SPLASH'19

2019-20 | International student award (ITA)

2019 | Logic Mentoring Workshop(LMW) for LICS'19

2019 | ACM SIGPLAN PAC for PLDI'19

2019 | Travel grant to attend Student Mentoring Workshop (SMeW) at ICSE 2019.

2018-19 | International student award (ITA)

2018 | Credit Suisse 48 Hour Hackathon
Stock Market Prediction
Top 5 teams

2018 | Women's Excellence Award
Credit Suisse
Runner-up

Posters and Presentations

2019 | Safety guarantees in Cyber-physical Systems using neural networks for modelling
Dependable Day - UBC, 2019

2019 | Ontology based IDS for slow-DOS attacks
CS-CAN student symposium, 2019

Sub-reviewer

2019 | Software Quality, Reliability, and Security
QRS, 2019

2019 | OThe 28th International Symposium on High-Performance Parallel and Distributed Computing
HPDC, 2019

Graduate level courses

2019 | CPSC 508
Advanced Operating Systems

2019 | CPSC 539B
Compiler Theory - Topics in Programming Languages

2019 | EECE 571K
Security and Reliability of Internet of Things

2018 | CPSC 513
Introduction to Formal Verification and Analysis

2018 | CPEN 642
Cybersecurity Research Seminar

Teaching experience

2019 | CPEN 400A
Topics in Computer Engineering - BLDG MDRN WEBAPP
Lab sessions
UBC

2019 | Package B
Building Web Applications
Tutorials and lab sessions
Vancouver Summer Program(VSP)

2019 | CPEN 421
Software project management
Tutorials and lab sessions
UBC

2018 | CPEN 400A
Topics in Computer Engineering - BLDG MDRN WEBAPP
Lab sessions
UBC