# Curriculum Vitae: Karthik Pattabiraman

**Address:** Fred Kaiser Building, Univ. of British Columbia, 2332 Main Mall, Vancouver, BC Canada V6T 1Z4.
**Email:** karthikp@ece.ubc.ca **Alternate Email**: Karthik.Pattabiraman@gmail.com
**Phone:** (604)-827-4245 (Office) **Webpage: http://blogs.ubc.ca/karthik/**

**Research Interests:** Dependable Computer Systems, Cybersecurity, Cyber-Physical Systems, Software Engineering.

**Education**

| | | |
|---|---|---|
| PhD in Computer Science | University of Illinois (Urbana Champaign)<br>*Advisor: Ravishankar K. Iyer* | May 2009 |
| MS in Computer Science | University of Illinois (Urbana Champaign)<br>*Advisor: Daniel A. Reed* | Dec 2004 |
| B.Tech in Information Technology | University of Madras (Chennai, India) | Jul 2001 |

**Work Experience (post PhD)**

- Associate Head, Graduate Affairs, Dept. of Electrical and Computer Engineering, Univ. of British Columbia, July'23 - July'24.
- Professor, Dept. of Electrical and Computer Engineering, Univ. of British Columbia, July 2020 - present.
- Associate Professor, Dept. of Electrical and Computer Engineering, Univ. of British Columbia, July 2015 - Jun 2020.
- Assistant Professor, Dept. of Electrical and Computer Engineering, Univ. of British Columbia, Jan 2010- Jun 2015.
- Post-Doctoral Researcher, Microsoft Research (MSR), Research in Software Engineering (RiSE) Group, Jan-Dec 2009.

**Awards and Recognitions**

**External awards**

- IEEE Computer Society's Distinguished Contributor Recognition, class of 2022. *"recognizes those members who have made technical contributions, through either applied or pure computing, to the Computing Profession, Computing Community, and Humanity,*". One of 19 members who received this recognition worldwide in 2022.
- Distinguished member of the Association of Computing Machinery (ACM), 2021 - " *recognizes those ACM members with at least 15 years of professional experience and 5 years of Professional Membership in the last 10 years who have achieved significant accomplishments or have made a significant impact on the computing field.*" One of 61 members who received this recognition worldwide in 2021.
- *Inaugural* Rising Star in Dependability award, 2020, awarded jointly by the IEEE Technical Committee on Fault Tolerant Computing (TC-FTC) and IFIP Working Group on Dependable Computing and Fault-tolerance, to "*recognize a junior researcher, from academia or industry, who demonstrates outstanding potential for creative ideas and innovative research in the field of dependable and resilient computer systems and networks."*
- Member of the IFIP WG 10.4 on Dependable Computing and Fault Tolerance (January 2015 onwards). The WG 10.4 consists of over 60 eminent experts in the field of fault-tolerant and dependable computing from academia and industry, and membership is by election. *I was elected as the vice-chair in 2019, and re-elected in 2022.*
- University of Illinois's (UIUC) Computer Science Department Distinguished Alumni Award – Early Career Educator Category, 2018. This award "*honors computer science alumni or faculty members who have attained early career milestones and show great promise toward continued contributions to computer science education and research.*" I was one of two alumni to receive the award that year.

- NSERC Discovery Accelerator Grant Supplement (DAS) Award for 2015. "*The DAS Program provides substantial and timely resources to researchers who have a superior research program that is highly rated in terms of originality and innovation, and who show strong potential to become international leaders within their field.*" One of 125 awarded across all fields of science and engineering out of more than 3000 applications across Canada.

- *William C. Carter* award in 2008 by the IEEE Technical Committee on Fault-Tolerant Computing (TC-FTC) and the IFIP Working Group on Dependable Computing and Fault Tolerance (WG 10.4). The William C. Carter Award is presented annually since 1997 "*to recognize an individual who has made a significant contribution to the field of dependable computing through his or her graduate dissertation research*". The award is given to one student a year.

- Listed in the DSN conference hall of fame (I'm listed in the top 10 among over 100 researchers worldwide). DSN is the top conference in the area of dependable computing, and the hall of fame reflects the number of publications in the conference since 1988 (Available at: https://engineering.purdue.edu/~sbagchi/dsn-hof.html)

**Internal awards won at UBC**

- UBC Killam award in 2020 for excellence in mentoring, to "*recognize faculty members' outstanding ability to foster the intellectual, professional, and personal development of graduate students*. " I won the award in the mid-career category (less than 12 years in the first faculty position) - one award was given across all of UBC.

- UBC Killam Faculty Research Prize, 2018 in the Sciences and Engineering category *"in recognition of outstanding research and scholarly contributions*". One of 5 faculty members across all of UBC - I was the only winner in the "Junior" category (less than 12 years since PhD).

- Killam Research Fellowship at UBC for 2016. This fellowship is awarded on a competitive basis to 10 researchers each year across all of UBC based on research achievements (for salary supplement during a sabbatical).

**Awards won by my students**

- Bo Fang (co-supervised with Matei Ripeanu) won the William C. Carter PhD dissertation award for best PhD thesis in Dependability in 2020. This award is aimed at "*recognizing an individual who has made a significant contribution to the field of dependable and secure computing throughout his or her PhD dissertation*." One award is given each year. His thesis also received an *honorable mention* at the SIGHPC dissertation award, 2020 (i.e., runner up), and was nominated by UBC for the ACM doctoral dissertation award (1 of 2 nominees across UBC).

- Guanpeng Li received Standard Performance Evaluation Corporation (SPEC) Kaivalya Dixit Distinguished Dissertation award in 2019. This award "*aims to recognize outstanding doctoral dissertations in the field of computer benchmarking, performance evaluation, and experimental system analysis in general*". One award is given each year.

- Saba Alimadadi (co-supervised with Ali Mesbah) won an NSERC Postdoctoral Fellowship, where she was placed first in Canada in the Computer Science division (among over 100 applicants) in 2018.

**Paper awards**

- Paper published at International Conference for High-Performance Computing, Storage and Networking (SC), 2017 chosen for IEEE Top Picks in Test and Reliability (TPTR), 2023 workshop. The workshop "*collects and presents the most impactful publications in the past 6 years in the areas of VLSI test and reliability*." (1 of 13 papers)
- Paper published at IEEE/IFIP International Conference for Dependable Systems and Networks (DSN), 2021 chosen for IEEE Top Picks in Test and Reliability (TPTR), 2024 workshop. The workshop "*collects and presents the most impactful publications in the past 6 years in the areas of VLSI test and reliability*." (1 of 8 papers)
- Best paper award for paper at the ACM International Workshop on Edge Systems, Analytics and Networking (Edgesys'23) - one paper out of 24 submissions. This was co-authored with my faculty colleague and student.
- "Best of SELSE" award at IEEE Workshop on Silicon Errors in Logic, System Effects (SELSE'23 paper) - one of three papers chosen) - invited to present the paper at DSN'23. This was co-authored with my students.

- Best demo award at IEEE/ACM International Symposium on Edge Computing (SEC), 2021. (1 award given)
- Best paper award candidate at AISafety Workshop, 2021 for paper co-authored with my student and colleagues at Intel (one of four papers).
- Best paper award at IEEE/IFIP International Conference on Dependable Systems and Networks (DSN'21), for a paper co-authored with my students (1 out of nearly 300 papers won the award).
- Best paper award at the IEEE International Conference on Quality, Reliability and Security (QRS), 2021. One of three papers won the award among nearly 300 submissions. This was co-authored with my students and faculty colleagues.
- Best paper runner up award at IEEE/IFIP International Conference on Dependable Systems and Networks (DSN'21) for another paper co-authored with my students (1 of 2 papers). This is the first time since the award's inception that both the award and the runner up went to papers from the same group.
- Best Paper at the ACM Transactions on Embedded Computing Systems (TECS) in 2020 - this was awarded to one paper published in the journal in the years 2018-2020. The paper was co-authored with my student.
- Paper at ACSAC'19 was rated one of the top 10 cybersecurity innovations in Canada for the year 2019 by SERENE-RISC. This paper was co-authored with my PhD student. It also received extensive media coverage.
- Paper at International Conference for High-Performance Computing, Storage and Networking (SC), 2019 was a finalist for the SC reproducibility challenge (1 of 3 papers chosen among more than 300 papers submitted to the conference). This is the top venue in the area of high-performance computing. The paper was co-authored with my students.
- Best paper award runner up at the IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), 2018. One of two papers that won the award among more than 250 submissions. The paper was co-authored with students and colleagues from Nvidia research.
- Paper at ISSRE'14 was chosen as the "Highlights of ISSRE" in ISSRE 2019 – one of 26 papers among 1074 published in 30 years of the IEEE International Symposium on Software Reliability Engineering (ISSRE). These are papers that have had "*great influence and impact in the community*". The paper was co-authored with my student and a colleague from the SUNY Buffalo supercomputing center.
- Distinguished paper awards at the European Dependable Computing Conference (EDCC), 2015 and 2016. One of three papers from more than 50 submissions in each year. Both papers were co-authored with my students.
- ACM SIGSOFT Distinguished paper award at the IEEE/ACM International Conference on Software Engineering (ICSE) 2014, one of nine papers that received the award (out of nearly 500 submissions). This is the top venue in the area of software engineering. This paper was co-authored with my students and faculty colleague.
- Best paper award runner up at the IEEE International Conference on Software Testing, Verification and Validation (ICST) 2013. (one of 2 papers among more than 150 submissions). This paper was co-authored with my students and faculty colleague.
- Best paper award nominee at the IEEE International Conference on Software Testing, Verification and Validation (ICST) 2012 (one of 6 papers among more than 150 submissions). This paper was co-authored with my students and faculty colleagues.

**Selected Activities**

- Steering Committee Member
  - IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), 2021-2023, and 2023-2025. One of twelve members of the Steering Committee.
  - IEEE Pacific Rim International Symposium on Dependable Computing (PRDC), 2015-2023. One of ten members of the Steering Committee.
  - Workshop on Dependable and Secure Machine Learning (DSML), 2021, co-held with the IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), 2021. (One of the seven members of the SC). I co-founded this workshop with 2 others, and served as one of the program co-chairs for the first four years of the workshop. DSML had the largest attendance among all DSN workshops for the last three years (2019-2021).
  - Trustworthy Machine Learning (TrustML) cluster at UBC (one of three steering committee members).

- Associate editor
    - IEEE Transactions on Computers (TC), 2022-present.
    - Springer Software Quality Journal (SQJ), 2022-present.

- Guest co-editor of a special issue of
    - IEEE Transactions on Dependable and Secure Computing (TDSC), 2018 (one of three co-editors).
    - IEEE Transactions on Reliability (TR), 2019 on Software Reliability Engineering (one of two co-editors).

- Conference Organization
    - Co-chair of the Inaugural Artifact Evaluation Track at IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), 2024. (one of two co-chairs). I was also a member of the artifact policy committee earlier that was responsible for introducing this track at DSN, and I played a key role in formulating the policy charter.
    - Co-chair for Disrupt 23, a new track at the IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), 2023. (one of two co-chairs)
    - Program co-chair for the International Symposium on Reliable Distributed Systems (SRDS), 2022. (one of two co-chairs)
    - Track co-chair for IEEE/ACM Conference on Design Automation and Test in Europe (DATE), 2021, 2022 and 2023 - Dependability and System-Level Test Track (one of two co-chairs). This was a new track in DATE in 2021.
    - Program co-chair of the International Workshop on Dependable and Secure Machine Learning (DSML), co-held with the IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), 2020. (one of seven co-chairs) –
    - Program coordinator for IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), 2020.
    - New Faculty Symposium Co-Chair for IEEE International Conference on Software Reliability Engineering (ISSRE), 2020 and 2021. (First time for ISSRE) - one of two co-chairs. I conceptualized and started this track at ISSRE.
    - Program co-chair for the IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), 2019. (one of two co-chairs)
    - Program co-chair of the second International Workshop on Dependable and Secure Machine Learning (DSML), co-held with the IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), 2019. (one of five co-chairs)
    - Program co-chair of the first International Workshop on Dependable and Secure Machine Learning (DSML), co-held with the IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), 2018. (one of three co-chairs)
    - Publications co-chair for the IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), 2018. (one of two co-chairs)
    - Program co-chair of the IEEE Workshop on Silicon Errors in Logic, System Effects (SELSE), 2018. (one of two co-chairs)
    - Program co-chair for the IEEE International Symposium on Software Reliability Engineering (ISSRE), 2017. (one of two co-chairs)
    - Program chair for the 16$^{th}$ IEEE International Workshop on Assurance in Distributed Systems and Networks (ADSN), 2017. Held in conjunction with the IEEE International Conference on Distributed Computing Systems (ICDCS), 2017.
    - Industry track co-chair for the IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), 2017. (one of two co-chairs)
    - Program co-coordinator: IEEE International Symposium on Software Reliability Engineering (ISSRE), 2016.
    - Workshops co-chair of the IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), 2016. (one of two co-chairs)
    - Finance chair of the 14$^{th}$ ACM/IFIP/Usenix International Conference on Middleware, 2015.
    - Local Chair of 1$^{st}$ IEEE International Conference on Software Quality, Reliability and Security (QRS), 2015.
    - Publicity co-chair of the 11$^{th}$ European Dependable Computing Conference (EDCC), 2015.
    - Publications chair of the 8$^{th}$ IEEE/ACM International Symposium of Network On Chips (NOCS), 2015

- Fast abstracts chair, IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), 2014.
- Student Track chair, IEEE International Symposium on Software Reliability Engineering (ISSRE), 2014.
- General chair of the IEEE Pacific Rim International Symposium on Dependable Computing (PRDC), 2013.
- Program co-chair of the first and second workshops on *Compiler and Architectural Techniques for Application Reliability and Security* (CATARS), held in conjunction with the IEEE International Conference on Dependable Systems and Networks (DSN), 2008 and 2009. (one of two co-chairs)

- Award and other Committees
  - Chair of the Committee for the Rising Star in Dependability award, 2024 (sponsored jointly by the IEEE and the IFIP).
  - Member of IFIP WG 10.4 committee to formulate the working group's charter (2022-2023).
  - Canadian Association of Graduate Studies (CAGS) committee for Award for Outstanding Graduate Mentorship, 2021. One of eight members across all disciplines in Canada.
  - UBC-wide Faculty Research Awards Committee (2021-2024) - one of 12 faculty members across UBC. The committee is responsible for adjudication and awarding of faculty research excellence awards across UBC.
  - William Carter award, 2021 - awarded by the IEEE Technical Committee on Fault Tolerant Computing (TC-FTC) and the IFIP Working Group on Dependable Computing and Fault Tolerance (WG 10.4). One of five members.
  - Panel for best papers in ACM International Conference on High-Performance and Distributed Computing (HPDC), 2020.
  - Expert Panel of Special issue of Journal of Software Systems (JSS), to select the best papers from ISSRE 2016.

- Tutorials Delivered
  - "LLTFI and the art of Fault Injection"
    - IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), 2024.
  - "Injecting faults for fun and insight" (2 hours): course on "Towards More Reliable Software" offered by Prof. Kishor Trivedi to the Ground Based Strategic Defense Program, US, 2021 (one of 15 invited tutorial presenters).
  - "LLFI and the art of Fault Injection"
    - IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), 2017.
    - IEEE International Symposium on Software Reliability Engineering (ISSRE), 2019.
  - "Modern Web Applications' Reliability Engineering"
    - IEEE International Symposium on Software Reliability Engineering (ISSRE), 2014, and 2016.
    - IEEE International Conference on Quality, Reliability and Security (QRS), 2015.

- Selected Technical Program Committee member (excluding PC chair roles)
  - IEEE International Conference on Dependable Systems and Networks (DSN), 2010-2012, 2015-2022, 2025.
  - IEEE International Symposium on Software Reliability Engineering (ISSRE), 2012, 2016-2019. 2020-24 (Program Board)
  - ACM Symposium on Applied Computing (SAC), 2024. Safe, Secure and Robust AI Track (S2RAI).
  - IEEE International Symposium on Reliable Distributed Systems (SRDS), 2023.
  - IEEE International Conference on Distributed Computing Systems (ICDCS), 2020-2023.
  - ACM International Conference on High-Performance and Distributed Computing (HPDC), 2019-2021.
  - IEEE International Symposium on Parallel and Distributed Systems (IPDPS), 2021.
  - IEEE International Conference on Rebooting Computing (ICRC), 2020.
  - IEEE International Conference on Parallel Processing (ICPP), 2020, 2021.
  - IEEE/ACM International Conference on Automated Software Engineering (ASE), 2019.
  - IEEE/ACM International Conference on Design Automation (DAC), 2018.
  - International Conference on Computer Safety, Reliability and Security (SafeComp), 2016.

- IEEE International Conference on Cloud Computing (Cloud), 2015, 2016.
- IEEE International Online Testing Symposium (IOLTS), 2014, 2015.
- IEEE International High Assurance Systems Symposium (HASE), 2010-2017.
- IEEE Workshop on Silicon Errors in Logic, System Effects (SELSE), 2011-2014.
- European Dependable Computing Conference (EDCC), 2017-2021, 2025.
- IEEE Pacific Rim International Symposium on Dependable Computing (PRDC), 2012, 2015-2017.

- Reviewer for the following journals:
    - IEEE Transactions on Dependable and Secure Computing (TDSC)
    - ACM Journal on Emerging Technologies in Computing (JETC)
    - IEEE Transactions on CAD (TCAD)
    - IEEE Transactions on Cloud Computing
    - IEEE Transactions on Software Engineering (TSE)
    - Elsevier Journal on Software Testing and Verification (STVR)
    - Elsevier Journal on Software Practice and Experience (SPE)

- External examiner:
    - Andy Hwang, PhD, University of Toronto, October 2022.
    - P. Sareena, PhD, Indian Institute of Technology (IIT), Madras, September 2022.
    - Bushra Aloraini, PhD, University of Waterloo, September 2020.
    - Bin Nie, PhD, College of William and Mary, April 2019.
    - Oliver Schwan, PhD, TU Darmstadt, March 2019.
    - Mohammad Shahrear Iqbal, PhD, Queen's University, November 2017.
    - Jonah Kaplan, MASc, McGill University, Canada. December 2015.

- Member of the IEEE Standards committee on “P2975.3: Recommended Practice for Software Framework for Industrial Artificial Intelligence(AI) At-the-Edge” (2023).

- Consulting activities (only selected activities are listed)
    - Los Alamos National Labs (LANL), January 2018 to February 2018.
    - Futurewei, a wholly owned subsidiary of Huawei, June 2016 to August 2016.

- Internal Service (UBC ECE department): Space Committee (2011), Scholarship Committee (2012, 2013, 2014 – chair, 2019), Graduate Experience Committee (2013), Merit/PSA Committee (2013), Curriculum Committee (2015, 2016), Research Facilities Support Grant Committee (2017), External awards committee (2018-2023), Faculty recruiting Committee (2018, 2019): Teaching evaluation committee (2020-21), Faculty Recruiting committee (2022, 2023, 2024 - chair).

- Senior Member of the IEEE (since 2015), Senior member of the ACM (since 2019), and a member of the Usenix (since 2010)

- Professional Engineer (P.Eng.) registered with the Association of Professional Engineers and Geoscientists of British Columbia (APEGBC), Canada, since 2011.

- Maintainer of the “www.dependability.org” website and moderator of the FTTC mailing list for the dependability community (since 2024). Also, responsible for maintaining the cloud servers for web hosting and other activities of the community.

**Teaching Accomplishments**

I have taught 10 courses at UBC, six of which I created from scratch (CPEN400A, CPEN 322, CPEN 400P, EECE571K, EECE571R, and EECE571P), and three of which I revamped considerably (EECE 210, EECE 315, and EECE 513). CPEN400A is one of the most popular electives in the department, and has the highest registration among all ECE electives with over 120 students (based on enrolment numbers as of September 2020). It's now been renamed as CPEN 322 (since 2021). CPEN 400P is a new course I introduced in 2022 and focuses on program analysis for reliability and security - it's the first time a course on advanced program analysis has been taught at the undergraduate level in any N. American university. I have also won 2 Teaching and Learning Enhancement Grants (2011, 2012) from UBC for improving the undergraduate curriculum, as co-PI.

1. Undergraduate courses (total of 5 courses taught over 6 years)
    a. Software Engineering (EECE 310) – Taught three times
    b. Software Design (EECE 309/210) – Taught twice
    c. Software Architecture (EECE 417) – Taught twice
    d. Operating Systems (EECE 315) – Taught once
    e. Building Modern Web Applications (CPEN 400A) – Created, and Taught five times
    f. Software construction 2 (CPEN 322) - Created and taught twice (previously CPEN400A)
    g, Program Analysis for Reliability and Security Engineering (CPEN 400P) - Created and taught thrice

2. Graduate Courses (total of 4 courses)
    a. Design of Fault-tolerant Systems (EECE 513) –Taught three times
    b. Program Analysis and Optimization (EECE 571P) – Created and Taught three times
    c. Error Resilient Computing Systems (EECE 513) – Created and Taught twice
    d. Security and Reliability of Internet of Things (EECE 571K/R) – Created and taught thrice
    e. Dependable and Secure Autonomous Systems (EECE 571P) - Created and taught thrice

3. Other: Taught in the Vancouver Summer Programme (VSP), a UBC-affiliated institute for 1 month intensive course on "Principles of the Modern Internet", along with a colleague. July-August, 2017, 2018, 2019, 2022, 2023 to international students.

**Research Accomplishments**

1. **Good Enough Dependability:** This has been the mainstay of my research programme at UBC since I joined in 2010. Together with my students, I proposed the idea of trading off protection overhead for fault coverage in applications by systematically modeling error propagation, and reasoning about which errors are the most impactful. Prior to this approach, the default approach was "all-or-nothing" protection, which was used only in a few highly critical systems such as banking and healthcare, due to its high cost. In contrast, the good enough approach can be customized based on the application's needs. Our main contribution has been to identify the important portions of an application for protection using both analytical modeling and empirical techniques, without requiring any support from the programmer. The good enough approach has since become the mainstream approach for dependability, and has been adopted by many companies as well. This line of work has received a best-paper nomination at DSN'18, and a distinguished paper award at EDCC'16.

2. **Empirical Studies of Reliability:** Along with my graduate students and colleagues at MSR and UBC, I pioneered the area of empirical studies of JavaScript-based web applications' reliability. Our papers in this area showed that even mature, production websites exhibit significant numbers of JavaScript errors, and that the majority of these errors are caused by the interaction of the JavaScript code with the Document Object Model (DOM). The latter result flies in the

face of conventional wisdom which rules that JavaScript errors occur due to the loosely typed nature of the language. This work has shaped many of the web application engineering tools we have since developed and released. We also performed empirical studies of cloud application reliability, which received an impact paper award at ISSRE'14.

3. **Fault Injectors**: My group at UBC has developed many fault injectors to evaluate the error resilience of programs. One of our main products in this space is LLFI, a fault injector based on the LLVM compiler that is highly configurable and allows easy mapping of the fault propagation results to the program's code. LLFI supports a wide variety of failure modes in hardware and software, and is used by both researchers and industry. For example, Cisco Systems funded a project to adopt LLFI in their internal quality assurance process. It has also been used by IBM Research and Nvidia. Another fault injector developed by our group, GPU-Qin, to evaluate the error resilience of GPGPU applications, has been used by academic research groups, national labs, and industry research labs such as Nvidia and AMD.

4. **Tools for web application engineering:** We have developed a number of tools and techniques for web applications' engineering based on the insights from our empirical studies. These have been published in top-tier international venues, and are being used by other researchers in the area. One such tool, Clematis, developed in collaboration with the SALT Lab at UBC, has won the SIGSOFT distinguished paper award at ICSE'14. We have also won best paper nominations/runner-up awards at ICST'12, and ICST'13.

5. **Internet of Things (IoT) Security:** In this line of work, we have developed a systematic framework for reasoning about the security of IoT devices such as smart meters, insulin pumps, drones etc. We have built a formal model for capturing the key behavioral properties of an IoT device, and then use the model to drive automated attack generation against the device. We have also built intrusion detection systems (IDSes) to efficiently detect attacks against IoT devices. Finally, we have built efficient recovery techniques from attacks for robotic vehicles such as drones. This work has received significant press coverage, as well as distinguished paper awards at EDCC'15, ACM TECS, and DSN'21.

6. **Dependability of Machine Learning:** This is also a recent area I have been exploring with my students and colleagues at Nvidia, Intel and Los Alamos National Labs. We investigate the resilience of Machine Learning (ML) algorithms deployed on special purpose hardware platforms to soft errors. Our paper on the reliability of deep neural network (DNN) accelerators has been adopted by Nvidia research in their product. This paper published at SC'17 also received a top picks in Test and Reliability award in 2023. We have also built a fault injection tool for ML programs written using the TensorFlow framework, called TensorFI, in collaboration with Los Alamos National Labs. Recently, we built BinFI, a tool for optimizing fault injections into ML programs deployed in safety-critical systems such as self-driving cars, and Ranger, a technique for protecting DNNs from silent data corruption causing faults. This work has received awards such as finalist for "Reproducibility Challenge" at SC'19, best paper award runner up at DSN'21, best paper award finalist at AISafety'21, and best paper award at QRS'21. The Ranger system published at DSN'21 has been adopted by Intel in their OpenVino 2022 framework (https://www.intel.com/content/www/us/en/developer/articles/release-notes/openvino-relnotes.html). Ranger also received a top picks in Test and Reliability award in 2024.

7. **Edge Computing Dependability and Programmability:** In this line of work, we aim to make edge computing systems more dependable and programmable. To this end, have built middleware systems for coordinating tasks in edge systems transparent to the programmer (ThingsJS, OneOS) - these have won best demo awards at SEC, a best paper award at EdgeSys 2023 and have been used by other research groups. We have explored techniques to predict failures and performance in these systems. Finally, in collaboration with the NetSysLab at UBC, we have worked on techniques to characterize the performance variations that are endemic to edge systems, and to build middleware systems to mitigate the impact of the performance variations on the application. This work has also received a best paper award at the EdgeSys'23 workshop.

8. **Blockchain and smart contracts' security:** In this line of work, we have investigated the efficacy of static analysis tools in detecting vulnerabilities in smart contracts. We found that existing tools are highly ineffective in finding even simple vulnerabilities. Consequently, we have focused on building static analysis tools for detecting targeted vulnerabilities. We are also exploring detecting price oracle manipulation vulnerabilities in the blockchain ecosystem.

**Selected Recent Talks (2010 to current)**

- *In Autonomy We Trust, Building Trustworthy Autonomous Systems for a Safer Future*
    - Singapore Management University (SMU), Singapore, September 2024.
    - Singapore University of Technology and Design (SUTD), Singapore, September 2024.
    - Illinois Advanced Research Computing Center (ARC), Singapore, September 2024.
    - Indian Institute of Technology (IIT) Madras, Chennai India. September 2024.
    - IBM Research T.J. Watson (virtual), November 2024.
- *Error-Resilient Machine Learning for HPC: Challenges and Opportunities,* Featured talk at the Workshop on Fault Tolerance in High-Performance Computing at Extreme Scale (FTXS), 2024. Co-held with SC 2024.
- *Security Challenges and Opportunities in Decentralized Finance (DeFI),* Nanyang Technological University (NTU) Blockchain Symposium, September 2024.
- *Secure and Resilient Cyber-Physical Systems for Critical Infrastructure,* Big Data Research Center (BDRC) Workshop on Cybersecurity, Laval Univ., September 2024.
- *Building Error-Resilient and Attack-Resilient ML-Enabled CPS,* Invited presentation at the IFIP WG 10.4 Workshop on AI-Enabled Cyber Physical Systems, Georgia, US. February 2024.
- *Fault Injection is Dead, Long Live Fault Injection,* Keynote talk at the 1st International Workshop on Verification and Validation of Dependable Cyber-Physical Systems (VERDI'23), Co-held with the DSN'23 conference.
- *Improving the Dependability and Security of Smart Contracts and Machine Learning (ML) Systems,* Informatics Dept., Monash Univ., Melbourne, Cyber-security seminar, 2023.
- *From Padawan to Jedi Knight: The nine trials of a PhD student*, Keynote talk at the Doctoral Symposium of the IEEE International Symposium on Software Reliability Engineering (ISSRE), 2022.
- *In Autonomy We Trust, Building Trustworthy Autonomous Systems for a Safer Future*, Lakehead University, Computer Science, Invited departmental seminar, October 2022.
- *Characterizing and Improving the Resilience of Machine Learning Applications,* Intel Munich, September 2022.
- *Building Error Resilient Machine Learning Systems from Unreliable Components,*
    - TTTech Austria, September 2022
    - Nvidia Research, USA, December 2022
    - Western University, Canada, March 2023
    - University of Coimbra, Portugal, June 2023
    - University of Lisbon, Portugal, July 2023
- *Detection is not Enough: Low-cost Attack Recovery for Autonomous Robotic Vehicles,* IFIP WG 10.4 workshop on Intelligent Vehicle Dependability and Security, Alexandria, Maryland. June 2022.
- *The Barbarians are at the Gates: Security Vulnerabilities of the IoT and their Implications,* Invited Talk at Meeting of Chartered Engineers Pacific (CEP), Vancouver. March 2022.
- *Detection is Not Enough: Low Cost Attack Recovery for Robotic Vehicle Systems*, Workshop on hardware and IoT security, CMC Microsystems, February 2022.
- *Failure Data Everywhere, but not a Failure in Sight! The joys and frustrations of analyzing open data sources,* Workshop on Reliability and Security Data Analysis (RSDA), 2021. Co-held with the IEEE International Symposium on Software Reliability Engineering (ISSRE), 2021. (Keynote)
- *Detection is not Enough: Low-cost Error and Attack Recovery in Autonomous Systems,* Invited Guest lecture at the University of Illinois at Urbana Champaign (UIUC), October 2021.
- *Stopping the Barbarians at the Gate: Protecting End User Devices from Security Attacks,*
    - IFIP WG 10.4 workshop on Cyber-Physical Systems Security and Reliability, Italy. January 2020.
    - International Workshop on Governing Adaptive & Unplanned Systems of Systems (GauSS), 2020, Co-held with the IEEE International Symposium on Software Reliability Engineering (ISSRE), 2020. (Keynote)

- *Error Resilient Machine Learning for Safety-critical Applications*
    - IOLTS 2020. Special session on Dependable Machine Learning (remote).
    - MLPerf working Group Meeting, March 2020 (remote).
    - IFIP WG 10.4 meeting on Machine learning dependability, June 2019.
    - Chinese University of Hong Kong, July 2019.
    - AMD Research, October 2019.
    - Workshop on Robust and Trustworthy Machine Learning, November 2019 (invited).
- *Resilience and Security in Cyber-Physical Systems: Self-Driving Cars and Smart Devices,*
    - Johns Hopkins University, March 2019.
    - University of Virginia, March 2019.
- *Error Resilience of Deep Neural Network Accelerators and Applications*, Trends in HPC Workshop, co-held with the HPDC PC meeting, Arlington, Virginia, March 2019.
- *Building Reliable Software for the Web, IoT and Beyond,*
    - Zhejiang University, China. May 2018.
    - Technische Universitat, Darmstadt, Germany, June 2018.
- *Modeling Hardware Error Propagation In Programs for Low Cost Dependability,* Northeastern University, 2018.
- *Resilience & Security of Cyber-Physical Systems: Self-Driving Cars and Smart Devices,* Microsoft Research, 2017.
- *Tolerating Hardware Faults in Commodity Software: Problems, Solutions and a Roadmap,* Workshop on Silicon Errors in Logic, System Effects (SELSE), 2017, Boston, US. *Opening Keynote Talk.*
- *Why do Modern Web Applications Fail and What Can we Do About it?,*
    - CS department, Univ of Utah, 2016.
    - CS department, Univ of Massachusetts, Amherst, 2018.
- *Security and Reliability of the Internet of Things: A Smart Meter Case Study,* Microsoft Research, 2016.
- *Does Error Resilience matter in the age of Approximate Computing?* Invited Panelist at Workshop on Silicon Errors in Logic, Systems Effects (SELSE), 2016 on "Resilience and Probabilistic Computing".
- *Error Resilient Systems and Approximate Computing: Conjoined Twins Separated at Birth?* Dagstuhl workshop on Approximate and Probabilistic Computing, November 2015 (invited).
- *Good Enough Dependability: A new paradigm for Dependable Systems Design,*
    - Purdue University, West Lafayette, Indiana, November 2017.
    - *o* University of Illinois at Urbana-Champaign, October 2017.
    - Indian Institute of Technology (IIT), Madras, August 2017.
    - Universitat De Polytechnica, Valencia (UPV), Jan 2017.
    - University of Virginia (U. Va.), March 2016.
    - University of Illinois at Chicago (UIC), Feb 2016.
    - Rutgers, State University of New Jersey, October 2016. ECE Colloquium.
    - Microsoft Research, August 2015.
    - University of Maryland (College Park), February 2015.
    - Technische Universität Darmstadt, November 2014.
- *Application-level Error Resilience: Tolerating Hardware Faults through Software Techniques,* Nvidia, 2015.
- *Good Enough Dependability: Providing Security and Reliability at Low Cost for Embedded Devices*, Qualcomm Research Silicon Valley, May 2015.
- *Helping Developers Understand, Analyze and Synthesize JavaScript Code in Web Applications,* Intel, May 2015.
- *Tolerating Silent Data Corruption (SDC) causing Hardware Faults through Software Techniques,*
    - Electrical and Computer Engineering, Georgia Tech, Computer Engineering Seminar, June 2014.

  - IBM T.J. Watson Research, New York, August 2014.
  - AMD Research, Boston, August 2014.
- *Invited Panelist: "Towards 21st Century High Assurance Engineering",* 15th IEEE High Assurance System Engineering (HASE), 2014, Miami, Florida. (one of four panelists)
- *How I learned to Stop Worrying and Love the DOM,*
  - IFIP WG 2.4 Meeting, Victoria (April 2016)
  - Microsoft Research, Redmond (August, 2014)
  - Intel, Santa Clara (May 2013)
  - Microsoft Research, India (August 2013)
  - IBM Research, India (August 2013)
- *Why do Web Applications Fail and What can we do about it?,*
  - Intel, Santa Clara, September 2012.
  - CS department Colloquium, Queen's University, August 2012.
  - ECE department, University of Illinois at Urbana-Champaign (UIUC), May 2012.
  - Microsoft Research, Redmond, June, 2011.
- *Good Enough Software Systems: Tolerating (most) Hardware Errors in Software,*
  - CS department Colloquium, University of Pittsburgh, Feb 2012.
  - CS department Colloquium, McGill University, Montreal, Quebec, March 2011.
  - IEEE Vancouver Computer Society Seminar, May 2010.

**Press Coverage of Research**

1. **Drones and Rovers Security (December 2019)**

a. EurekAlert (https://www.eurekalert.org/pub_releases/2019-11/uobc-urh112719.php)

b. TechXplore (https://techxplore.com/news/2019-11-highlights-safeguard-drones-robotic-cars.html)

c. GlobalNews BC (https://globalnews.ca/news/6235460/ubc-drone-hacking-research/)

d. Market Associates (https://themarketassociates.com/2019/12/03/the-need-to-secure-drones-and-automated-vehicles-against-cyber-attacks/)

e. HelpNet (https://www.helpnetsecurity.com/2019/12/02/hacking-robotic-vehicles/)

f. SERENE RISC digest (September 2020) https://www.serene-risc.ca/public/media/files/prod/page_files/11/14_SERENE-RISC-Vol3-Iss1.pdf

2. **Smart meter security (June 2019)**

a. UBC (https://news.ubc.ca/2019/06/06/ubc-researchers-find-ways-to-hackproof-smart-meters/)

b. TheStraight (https://www.straight.com/tech/1250511/smart-meters-your-home-are-target-hackers-says-ubc-researcher)

c. EurekaAlert (https://www.eurekalert.org/pub_releases/2019-06/uobc-urf060519.php)

d. E&T (https://eandt.theiet.org/content/articles/2019/06/system-developed-to-boost-smart-meter-resilience-to-cyber-attacks/)

e. ScienceDaily (https://www.sciencedaily.com/releases/2019/06/190606101822.htm)

f. TechXplore (https://techxplore.com/news/2019-06-ways-hackproof-smart-meters.html)

3. **Expert Opinion**

a. GlobalNews BC: https://globalnews.ca/news/4356375/google-titan-key/

b. Vancouver Sun: https://vancouversun.com/news/local-news/covid-19-zoombombers-hitting-with-regularity-as-apps-like-zoom-gain-in-popularity/wcm/f25c8e68-10f8-4998-8487-2f3d1b3f5f07/

c. Spice Radio Vancouver: https://soundcloud.com/user-244969524-696484203/ubc-prof-talks-about-cybersecurity-in-the-time-of-covid-19-and-the-rising-trend-of-zoom-bombing?ref=clipboard&p=i&c=0

d. Business in Vancouver, *AI adoption may expose businesses to cybersecurity risk*

**Research Funding (Includes grants currently held and held in the past – amounts are specified in CAD[1])**

1. Building Error-Resilient Applications on Many-Core Platforms, NSERC Discovery Grant, 2010-2015, $120,000
2. Microsoft Research, Unrestricted Gift, 2010, $17,000.
3. Teaching and Learning Enhancement Fund, University of British Columbia, 2011 (co-PI with 2 others), $39,000.
4. WATERS: A computational Infrastructure for Web Application Testing, Energy-Efficiency, Reliability and Security, Leaders Opportunity Funds (LOF), Canada Foundation for Innovation (CFI), 2011 (PI, 1 co-PI), $280,000
5. Shared-memory Multiprocessor for Parallel Algorithms and Architectures, NSERC Research Tools and Infrastructure Grant (RTI), 2011. (Co-PI with six others). $80,000.
6. Leveraging Dynamic Co-Processor Platforms for High-Performance Computing Applications, NSERC Engage Grant, 2011 (Sole PI). $22,750. (Industry partner: Secodix, Vancouver).
7. Assessing the Error Reporting Capabilities of the Freescale QoRIQ Platform, NSERC Engage Grant, 2011 (Sole PI), 24,675. (Industry partner: Freescale).
8. Nokia Research, Unrestricted Gift, 2012. $15,000.
9. Teaching and Learning Enhancement Fund, University of British Columbia, 2012 (co-PI, 1 PI) $31,000.
10. Automatic Code Partitioning for XPU Acceleration, MITACS Accelerate Grant, 2012 (Sole PI), $30,000.
11. Hardening Software to Detect Hardware Faults, NSERC Engage Grant, 2012 (Sole PI). $25,000. (Industry partner: Cisco).
12. Systematic Software Analysis and Maintenance Techniques for Web 2.0 Applications, NSERC Strategic Project Grant, 2012-2015 (Co-PI with three others), $480,000. My share: $120,000
13. Unifying Static and Dynamic Analysis Techniques for Checking Non-Functional Properties, Lockheed Martin Research Grant, 2012-2013 (Co-PI with four others), $180,000.
14. Secure and Trusted Network Terminals for Smart vehicular Networks, DIVA Strategic Network Grant, 2010-2015 (Multiple PIs, my portion is $20,000 a year).
15. Software Robustness Assessment through Fault Injection, Research Grant, Cisco Systems, 2013-2015 (Sole PI). $120,000.
16. Hardware Fault Injection for GPGPU Applications, NSERC Engage Grant, 2013 (Sole PI). $25,000. (Industry partner: AMD).
17. Nvidia Equipment Donation, 2013. $3000 market value.
18. Programming Techniques for QUBO compatible processors II, MITACS Accelerate Grant (Sole PI), 2013. $30,000. (Industry partner: 1-Qbit, Vancouver).
19. Intel, Unrestricted Gift, 2012-2016 (PI, one co-PI), $270,000. My share: $135,000. NOTE: The funding was awarded each year on a competitive basis for four years in a row.
20. AMD, Unrestricted gift, 2014. $8000.
21. Building Error-Resilient Applications on Next Generation Computing Platforms, NSERC Discovery Grant, 2015-2020, $250,000 (Awarded an additional Discovery Accelerator (DAS) Supplement of $120,000 for 2015-2018).
22. Low-cost Security for Internet of Things (IoT) Security, NSERC Engage Grant, 2015 (Sole PI), $25,000. (Industry partner: Sierra Wireless).

[1] Unlike most US Government agencies, grant amounts from most Canadian Government agencies (e.g., NSERC) do not include overheads (i.e., indirect costs of research). Also, student tuition fees and faculty summer salaries are typically not included in the grant amounts, so grant sizes tend to be smaller as well.

23. Error Propagation Analysis for GPGPU Applications, NSERC Engage Grant, 2015 (Sole PI), $23,000. (Industry partner: Nvidia).
24. Automatic Secure Code Migration for the Web of Things, Intel Research, 2016-2019 (PI, 1 Co-PI). $210,000. My share: $105,000.
25. Error-Resilient Machine Learning Systems, NSERC Strategic Grant, 2017-2020 (Co-PI, 4 other co-PIs). $720,000. My share: $180,000
26. Designing Efficient and Resilient Deep Learning Accelerators using an AI Supercomputer, NSERC RTI Grant, 2018 (Co-PI, 4 other co-PIs). $150,000. (Equipment grant)
27. Invariant-Driven Intrusion Detection System for Cyber-Physical Systems, NSERC Engage Grant, 2018. (Industry Partner: General Dynamics, Canada). $25,000 (sole PI).
28. Automatic, Secure, Code Migration in the Heterogeneous world of the Internet of Things (IoT), NSERC CRD Grant, 2019-2022. (PI, Co-PI: 2 Others) $254,400. My share: $90,000.
29. Huawei-UBC AI System-On-Chip (SoC) Program, 2019. $71,400 (sole PI).
30. Huawei-UBC Software Engineering Research Program, 2019. $72,800 (sole PI).
31. Resilient, Secure, and Programmable Next-Generation Internet of Things (IoT), NSERC Discovery Grant, 2020-2025, $240,000 (sole PI).
32. Unrestricted Gift, Intel Research, 2020. $64,000 (sole PI).
33. Discovery Grants Department of National Defense (DND) Research Supplement. $120,000 (sole PI). 2020-2023
34. Huawei-UBC AI System-On-Chip (SoC) Program, 2021-2022. $156,400 (sole PI).
35. Huawei-UBC Software Engineering Research Program, 2021. $81,000 (sole PI).
36. Robust and Resilient Machine Learning for Connected Health-Care Systems, National Research Council (NRC), Canada $300,000 (sole PI), 2022-2025
37. Trustworthy Machine Learning Systems, Grants for Catalyzing Research Clusters (GCRC), UBC VPRI Research Excellence Initiative (co-PI, one of three core members of the cluster). $100,000.
38. Toward Situational-aware and Adaptive 5G Networks for Defense and Security: A Machine Learning Approach, Ideas DND proposal, (co-PI with four others. PI: Vincent Wong). 2022-2025. Total amount: $1.5 Million, My share: $251,187.
39. Software-hardware strategies for enhancing ML application resilience, Meta Research Proposal on Silent Data Corruptions at Scale (Co-PI, PI: Prashant Nair), $65,000 CAD. 2022. Five proposals out of 62 submitted proposals received the award.
40. Dependable and Secure Cyber-Physical Systems Lab, NSERC RTI grant. $145,000. 2024-2025. (co-PI with two others, PI: Arpan Gujarati). My share: $48,000.
41. ICS Security in the Age of Internet 4.0, National Center for Cybersecurity (NCC), $500,000 (co-PI, PI: Aastha Mehta). My share: $250,000
42. Novel methods for Quantifying and Improving Privacy in Machine Learning, National Center for Cybersecurity (NCC), $495,000 (co-PI with two others, PI: Simon Oya). My share: $161,000.

**Current Graduate Students (PhD/MASc)**

**Post-doc:**

1. Gargi Mitra, from 2023. Distinguished reviewer award at CCS'24.

**PhD:**

1. Pritam Dash, from 2020. Four Year Fellowship (FYF) awardee. Best paper award at DSN'21. Rising star in CPS, 2024.

2. Abraham Chan, from 2020. NSERC PGS(D) and Four Year Fellowship (FYF) awardee. (Co-advised with Sathish Gopalakrishnan). Best paper award at QRS'21. Best of SELSE'23.

3. Kumseok Jung, from 2021. (Co-advised with Sathish Gopalakrishnan). Interned at Microsoft Research. Best Demo Award at SEC'21.

4. Zitao Chen, from 2021. Four Year Fellowship (FYF) awardee. Best paper award and runner up award at DSN'21. SC'19 reproducibility initiative finalist. UBC Public Scholars Initiative (PSI) awardee, 2022. Brandwajn awardee from UBC ECE, 2023 and 2024. DaaD Fellowship, 2024. IEEE Top Picks in Test and Reliability (TPTR), 2024.

5. Mohsen Salehi, PhD, from 2021. Four Year Fellowship (FYF) awardee.

6. Rui Xi, PhD, from 2022. (Co-advised with Zehua Wang). UBC Blockchain Pathways Fellowship.

7. Mohammad ElNawawy, from 2022. Four Year Fellowship (FYF) awardee.

**MASc:**

8. Seyedmani Sadati, MASc, from 2023.

9. Yuqi Liu, MASc, from 2024.

**Former Graduate Students and Post-docs**

**Post-doc:**

1. Julien Gascon-Samson. NSERC Postdoctoral Fellow, 2016-2018. Currently assistant professor of Computer Science at the Ecole Technologie Superieure (ETS), Montreal. Marcelle Gauvreau Engineering chair.

**PhD students:**

1. Asem Ghaleb, PhD, 2023. (co-advised with Julia Rubin). Four Year Fellowship (FYF) awardee. First Position: Research Engineer, Huawei, Vancouver.

2. Mohammad Rafiuzzaman, PhD, 2023. (co-advised with Sathish Gopalakrishnan). International Doctoral Fellowship (IDF) awardee. First position: Instructor at British Columbia Institute of Technology (BCIT), Vancouver.

3. Mehdi Karimibiuki, PhD, 2020 (co-advised with Andre Ivanov). Four Year Fellowship (FYF) awardee. First position: Senior Security Engineer, Sierra Wireless, Vancouver. Current Position: CTO, Fractional Inc., Vancouver.

4. Bo Fang, PhD, PhD 2020, MASc from 2011-2014 (co-advised with Matei Ripeanu). Interned at Los Alamos National Labs (LANL), Pacific Northwest National Labs (PNNL). J.K. Zee Fellowship. (received the NSERC Postdoctoral Fellowship in 2020 - ranked #2 in CS). First Position: Postdoctoral researcher at Pacific Northwestern National Labs. Winner of **William C Carter Dissertation award**, 2020 and **honorable mention for the ACM SIGHPC dissertation award**, 2020. **Nominated by UBC for the ACM Doctoral Dissertation award, 2020.**

5. Guanpeng Li, PhD, 2019. Four Year Fellowship (FYF) awardee. Interned at Nvidia Research. Distinguished paper runner up at DSN 2018 (received the NSERC Postdoctoral Fellowship in 2019). Current Position: Assistant Professor, University of Iowa (U Iowa), Computer Science department. First Position: Post-doctoral researcher, University of Illinois (UIUC). Winner of the **SPEC Kaivalya Dixit Distinguished Dissertation Award**, 2019. IEEE TCHPC Early Career award, 2024.

6. Farid Molazem Tabrizi, PhD, 2017. Interned at Fortinet, Vancouver, and Google, Mountain View. Distinguished paper award at EDCC 2015. Best paper award at TECS 2020. First Position: Google, US.

7. Saba Alimadadi, PhD, 2017 (co-advised with Ali Mesbah), Distinguished paper award at ICSE 2014. Interned at SAP Vancouver. Current Position: Assistant professor, Simon Fraser University (SFU), Computer Science department. First Position: Post-doctoral researcher at Northeastern University, US (received the NSERC Postdoctoral Fellowship in 2018 – **ranked #1 in the Computer Science division**).

8. Frolin Ocariza, PhD, 2016 (co-advised with Ali Mesbah), MASc, 2012: NSERC CGS(D) and FYF awardee. Interned at Microsoft Research, Redmond, and Fujitsu Labs, America. First position: SAP, Vancouver.

9. Shabnam Mirshokraie, PhD, 2015 (co-advised with Ali Mesbah), Best paper runner up at ICST 2013. First Position: Co-founder of a Startup in Stealth mode. Current Position: Software Engineer, Salesforce

10. Layali Rashid, PhD, 2013 (co-advised with Sathish Gopalakrishnan), NSERC CGS(D) and FYF awardee. Interned at Microsoft Research, Redmond. First position: Qualcomm, US. Current Position: Deep Learning Architect, Nvidia, US.

**Masters students (thesis):**

1. Jiesheng Wei, MASc, 2012. First position: Microsoft, Canada. Currently: Meta, US

2. Anna Thomas, MASc, 2013. First position: IBM Canada. Currently: Azul Systems, US

3. Majid Dadashi, MASc, 2014. First position: 1-QBit, Canada. Currently: Salesforce, Vancouver

4. Xin Chen, MASc, 2014. Impact paper award at ISSRE'14. First position: CCB Fintech, China.

5. Sheldon Sequira, MASc, 2014 (co-advised with Ali Mesbah), Distinguished paper award at ICSE'14. First Position: SAP, Vancouver.

6. Kartik Bajaj, MASc, 2014 (co-advised with Ali Mesbah), FYF awardee, MITACS Globalink Fellowship and FYF awardee. Vancouver. First Position: Hootesuite, Vancouver. Currently: WonderFI, Vancouver.

7. Qining Lu, MASc, 2015. First position: Google, Canada.

8. Nithya Narayanamurthy, MASc, 2015. Distinguished paper award at EDCC 2016. First Position: Oracle Labs, Vancouver. Currently: Amazon, Vancouver.

9. Abraham Chan, MASc, 2017. First Position: Huawei, Canada. Currently: PhD student at UBC.

10. Maryam Raiyat Aliabadi, MASc, 2018. First Position: PhD student, Shahid Beheshti Univ., Currently: Post-doc, UBC CS

11. Ekta Aggarwal, MASc, 2019 (co-advised with Andre Ivanov). First position: Clio. Current position: Amazon, Vancouver.

12. Lucas Palazzi, MASc, 2019. First Position: Data Realm Inc.

13. Zitao Chen, MASc, 2020. Best Paper Award Nominee at DSN'21 (twice), Finalist for SC'19 reproducibility challenge, Best paper award winner and runner up at DSN'21 (different papers). First Position: PhD student, UBC.

14. Abdul Rehman Anwer, MASc, 2020. First Position: Huawei, Canada.

15. Aarti Kashyap, MASc, 2020. Invited to attend Heidelberg Laureate Forum. First Position: PhD student, UBC CS.

16. Pritam Dash, MASc, 2020. First Position: PhD student, UBC.

17. Kumseok Jung, MASc, 2021. First Position: PhD student, UBC.
18. Niranjhana Narayanan, MASc, 2021. First Position: Neat Inc, Norway.
19. Rui Xi, MASc, 2022. First Position: PhD student, UBC.
20. Ali Asgari, MASc, 2022 (co-advised with Prashant Nair). Best paper nominee at AISafety'21. First Position: Electronic Arts, Vancouver.
21. Udit Agarwal, MASc, 2023. Best of SELSE'23. First Position: Huawei, Vancouver.
22. Elaine Yao, MASc, 2023. First Position: Fortinet, Vancouver.
23. Amirhossein Ahmadi, MASc, 2024. (co-advised with Matei Ripeanu). Best Paper at EdgeSys'23. First Position: Huawei, Vancouver.
24. Mohammadreza Hallajiyan, MASc, 2024.First Position: TBD.

**M.Eng students (non-thesis):**

1. Jose Thomas, 2018 first position: Lotlinx Canada.
2. Ahmed Effat, 2019, first position: Abebooks, Canada.
3. Bill Yan, first position: Unknown
4. Dan Jin, first position: Intel, Canada

**Visiting PhD students:**

1. Behrooz Sangchoolie, Chalmers University of Technology, Gothenburg, Sweden (May-Aug 2016). Co-authored paper at DSN'17. Current Position: Researcher, Research Institutes of Sweden (RiSE).
2. Yong Yang, PhD student at Peking University, China. (Feb – Aug 2019). Co-authored paper at ISSRE'20. Current Position: Post-doctoral researcher, Peking University, China.
3. Arpan Gujarati, PhD student, MPI-SWS, Germany (joint with Sathish Gopalakrishnan, Feb-March 2020). Current Position: Assistant Professor, Computer Science Dept., UBC. Winner of ACM SIGBED dissertation award.
4. Gargi Mitra, PhD student, IIT Madras (September 2021 - December 2021). Current Position: Post-Doctoral Researcher, UBC. MITACS-SCI Fellowship.

**Other:**

1. Phil Tribyaukthal, May 2015 - August 2015
2. Nanda Kumar Velayuthan, June-Sep 2016. Research Programmer Intern.
3. Anushree Bannadbhavi, May - December 2022. Research Programmer Intern.

**Undergraduate students:** I have mentored a total of 35 undergraduate students as summer interns or undergraduate project advisees at UBCs. Seven of these students were NSERC USRA interns (equivalent of NSF REUs in Canada). Six of these undergraduate students have co-authored papers with me during their undergraduate studies - these are indicated with a '*'.

a. Ranbir Sharma, UBC (May - December 2024).
b. Zachary Tseng, UBC (May - December 2024).
c. Luke Mattson, UBC (May - August 2024).
d. Mohanna Shahrad, McGill University (Sep - Dec 2023).
e. Chengkai He, UBC (Sep - Dec 2023).
f. Joshua Chiu, UBC (Sep 2023 - Apr 2024).
g. Jerry Shao, UBC (Sep - Dec 2023).
h. *Shashwat Jaiswal, IIT Bhilai (May - August 2023), MITACS Globalink.
i. James Liang, UBC (May - August 2023).
j. *Ethan Chan, UBC (May - August 2023). NSERC USRA intern.
k. Patrick Creighton, UBC (January to April 2023). NSERC USRA intern.
l. Himanshu, HMR Institute of Management and IT, (July 2022 to October 2022), MITACS Globalink.
m. Ashikka Gupta, Vellore Institute of Technology (VIT), (July 2022- September 2022), MITACS Globalink.
n. Yuanzhi (Gigi) Ma, University of British Columbia (May 2021 - Aug 2021), NSERC USRA Intern.
o. Brennan Cathcart, University of British Columbia (January 2021 - April 2021).
p. Daniel Kong, University of British Columbia (May 2020 - August 2020), NSERC USRA intern.
q. Alicia Tang, University of British Columbia (May 2018 – Nov 2018). UBC Work-learn Intern.
r. Amira Said, National Institute of Applied Sciences and Tech., Tunisia (May - July 2018). MITACS Globalink.
s. Selina Suen, University of British Columbia (January 2018 – Nov 2018). UBC Work-learn Intern.
t. Atif Mahmud, University of British Columbia (January – April 2018).
u. *Armin Rezalen-Asel, University of British Columbia (May - July 2017). NSERC USRA intern.
v. Wiem Badreddine, National Institute of Applied Sciences and Technology, Tunisia (May to August 2017). MITACS Globalink.
w. *Shivanshu Goyal, University of British Columbia. (May to July 2017).
x. Yilun Song, University of British Columbia (September-December 2016). Honor's thesis.
y. *Amita Kamath, National Institute of Technology (NIT), Surathkal, India (May - July 2016). MITACS Globalink Intern.
z. Siddharth Sharma, Birla Institute of Technology and Sciences (BITS), Pilani, India (May - July 2015). MITACS Globalink Intern.
aa. Dinesh Gurjar, Indian Institute of Technology, Rajasthan, Jodhpur, India (May – July 2015), co-supervised with Jose Marti and K.D. Shrivastava.
bb. Gaurav Shastri, Indian Institute of Technology, Rajasthan, Jodhpur, India (May-July 2015), co-supervised with Jose Marti and K.D. Shrivastava.
cc. Phil Tribunyakthul, University of British Columbia (Jan – August 2015).
dd. Abraham Chan, University of British Columbia (Jan – April 2015). Honor's thesis.
ee. Erin Bush, University of British Columbia (May-Aug 2014) – NSERC USRA intern (Co-supervised with Ali Mesbah).
ff. Yilun Song, University of British Columbia (May – Aug 2014) – International USRA intern
gg. Chung-Chi Yen, University of British Columbia (May – Aug 2014).
hh. Aniruddh Ramrakhyani, Indian Institute of Technology, Rajasthan, Jodhpur, India (May – July 2014), co-supervised with Jose Marti and K.D. Shrivastava.

ii. Rohith Yeravothula, Indian Institute of Technology, Rajasthan, Jodhpur, India (May – July 2014), co-supervised with Jose Marti and K.D. Shrivastava. MSc at Univ of Southern California (USC).

jj. *Guanpeng Li, University of British Columbia (May - Dec 2013)

kk. Mohamed Ali, University of British Columbia (May – Aug 2013) – NSERC USRA intern (Co-supervised with Ali Mesbah)

ll. Sam Coulter, University of British Columbia (May 2013 – Aug 2014).

mm. Rinku Meena, Indian Institute of Technology Rajasthan, Jodhpur, India (May – August 2013).

nn. Rajat Jain, Indian Institute of Technology Rajasthan, Jodhpur, India (May – August 2013).

oo. Aditie Garg, National Institute of Technology (NIT), India (May to August 2013) – MITACS Globalink.

pp. Denis Abalakov, University of British Columbia (May to August, 2012)

qq. Anurag Mittal, Indian Institute of Technology Rajasthan, Jodhpur, India. (May to July 2012)

rr. Shayoni Seth, Birla Institute of Technology and Science (BITS), India. (May to July 2012) - MITACS.Globalink (Co-supervised with Ali Mesbah)

ss. Kevin Cho, University of British Columbia (UBC). (Jun to Aug 2012 and May to Aug 2013).

**Publications (in chronological order): Names of students and postdocs who I have (co-)advised are in bold font.**

**Choice of Venues:** My research spans multiple sub-areas of computer science and engineering, and consequently I publish in venues that straddle multiple domains. For example, my papers have been published in venues in the domains of dependable computing, cybersecurity, embedded systems, high-performance computing, software engineering and hardware reliability. In each of these domains, I choose to publish my work in top-tier conferences as opposed to journals, as this is the defacto norm in my field - note that conference papers are archival, full length and rigorously peer-reviewed in these areas. On occasion, I also publish my work in top-tier journals - these are often expanded versions of conference papers (with at least 30% new material).

**Authorship convention:** In my area, students and trainees who worked with me are usually listed as first authors, while my name goes last as the lead PI. In case there are multiple supervisors or lead PI, we usually follow the order of seniority in terms of contributions, i.e., those who contributed more go earlier. Finally, industry collaborators are usually listed in the end. Finally, if a student is co-advised with another colleague, then both the supervisors are listed last (the order varies from paper to paper).

**According to Google Scholar, my h-index = 43 (https://scholar.google.ca/citations?user=p_V9YWgAAAAJ&hl=en)**

*(a) Journals: In my area of computer systems, conference papers are often more prestigious and rigorous than journal papers. Also, many journal papers are expanded versions of the conference papers – these are included below.*

*TECS* [1] *Co-Approximator: Enabling Performance Prediction in Colocated Applications*, **Mohammad Rafiuzzaman,** Sathish Gopalakrishnan and Karthik Pattabiraman, ACM Transactions on Embedded Computing Systems (TECS). Acceptance Date: May 2024.

*TCPS* [2] *Characterizing and Improving Resilience of Accelerators to Memory Errors in Autonomous Robots,* Deval Shah, Zi Yu Xue, Karthik Pattabiraman and Tor Aamodt. ACM Transactions on Cyber-Physical Systems (TCPS), Acceptance Date: September 2023.

*JPDC* [3] *Mixed Precision Support in HPC Applications: What About Reliability?,* Alessio Netti, Yang Peng, Patrik Omland, Michael Paulitsch, Jorge Parra, Gustavo Espinosa, **Udit Agarwal, Abraham Chan,** and Karthik Pattabiraman, Journal of Parallel and Distributed Computing (JPDC). Acceptance Date: August 2023.

*SPE* [4] *A Large-scale Empirical Study of Low-level Function Use in Ethereum Smart Contracts and Automated Replacement,* **Rui Xi** and Karthik Pattabiraman, Wiley Journal of Software Practice and Experience (SPE). Acceptance Date: October 2022.

*TDSC* [5] *Fault Injection for TensorFlow Applications*, **Niranjhana Narayanan, Zitao Chen, Bo Fang, Guanpeng Li,** Karthik Pattabiraman, and Nathan DeBardeleben, IEEE Transactions on Dependable and Secure Computing (TDSC). Acceptance Date: May 2022.

*SPE* [6] *ThingsMigrate: Platform Independent Migration of Stateful JavaScript Applications,* **Kumseok Jung, Julien Gascon-Samson, Shivanshu Goyal, Armin Rezalean-Asel,** Karthik Pattabiraman, Wiley Journal of Software Practice and Experience (SPE). Acceptance Date: December 2020.

*DTRAP* [7] *Stealthy Attacks Against Robotic Vehicles Protected by Control-based Intrusion Detection Techniques,* **Pritam Dash, Mehdi Karimibiuki,** and Karthik Pattabiraman, ACM Journal on Digital Threats: Research and Practice (DTRAP), 2020. Acceptance date: October 2020.

*TDSC* [8] *An Empirical Study of the Impact of Single and Multiple Bit-Flip Errors in Programs,* **Behrooz Sangchoolie,** Karthik Pattabiraman and Johan Karlsson, IEEE Transactions on Dependable and Secure Computing (TDSC). 2022.

*TDSC* [9] *Improving the accuracy of IR-level Fault Injection,* **Lucas Palazzi, Guanpeng Li, Bo Fang,** and Karthik Pattabiraman, IEEE Transactions on Dependable and Secure Computing (TDSC). 2022.

*TECS* [10] *Design-Level and Code-Level Security Analysis of IoT Devices*, **Farid Molazem Tabrizi** and Karthik Pattabiraman, ACM Transactions on Embedded Computing Systems (TECS). 2020. **Won Best Paper Award among all papers published in the journal for the years 2018-2020**

*TECS* [11] *Configurable Detection of SDC-causing Errors in Programs,* **Qining Lu, Guanpeng Li,** Karthik Pattabiraman, Meeta Gupta and Jude Rivers, ACM Transactions on Embedded Computing Systems (TECS), 2017.

*TSE* [12] *A Study of Causes and Consequences of Client-Side JavaScript Bugs,* **Frolin Ocariza, Kartik Bajaj,** Karthik Pattabiraman and Ali Mesbah, IEEE Transactions on Software Engineering (TSE), 2017.

*TPDS* [13] *A Systematic Methodology for Evaluating the Error Resilience of GPGPU Applications,* **Bo Fang,** Karthik Pattabiraman, Matei Ripeanu, and Sudhanva Gurumurthi, IEEE Transactions on Parallel and Distributed Systems (TPDS). 2016.

*TOSEM* [14] *Understanding JavaScript Event-Based Interactions with Clematis,* **Saba Alimadadi,** Ali Mesbah and Karthik Pattabiraman, ACM Transactions on Software Engineering and Methodology (TOSEM), 2016.

*TECS* [15] *Error Detector Placement for Soft-Computing Applications,* **Anna Thomas** and Karthik Pattabiraman, ACM Transactions on Embedded Computing Systems (TECS), 2016.

*STVR* [16] *Automatic Fault Localization for Client-Side JavaScript*, **Frolin Ocariza**, **Guanpeng Li**, Karthik Pattabiraman and Ali Mesbah, Journal of Software Testing, Verification and Reliability (STVR), 2016.

*TSE* [17] *Guided Mutation Testing for JavaScript Web Applications*, **Shabnam Mirshokraie,** Ali Mesbah and Karthik Pattabiraman, IEEE Transactions on Software Engineering (TSE), 41(5), 429-444 (2015).

*TR* [18] *Characterizing the Impact of Intermittent Hardware Faults on Programs*, **Layali Rashid**, Karthik Pattabiraman and Sathish Gopalakrishnan, IEEE Transactions on Reliability (TR), 2015.

*JCS* [19] *Modular Protections against Non-control Data Attacks,* Cole Schlesinger, Karthik Pattabiraman, Nikhil Swamy, David Walker, and Benjamin Zorn, Journal of Computer Security (JCS), 2014. **Invited as one of the best papers from CSF'11.**

*TC* [20] *SymPLFIED: Symbolic Program Level Fault Injection and Error Detection,* Karthik Pattabiraman, Nitin Nakka, Zbigniew Kalbarczyk and Ravishankar K Iyer, IEEE Transactions on Computers (TC) , 2013.

*TC* [21] *Efficient Runtime Detection and Toleration of Asymmetric Races*, Paruj Ratanaworabhan, Martin Burtscher, Darko Kirovski, Benjamin Zorn, Rahul Nagpal, Karthik Pattabiraman, IEEE Transactions on Computers (TC), 2012.

*TDSC* [22] *Automated Derivation of Application-specific Error Detectors using Dynamic Analysis*, Karthik Pattabiraman, Giacinto Paolo Saggese, Daniel Chen, Zbigniew Kalbarczyk and Ravishankar Iyer, IEEE Transactions on Dependable and Secure Computing (TDSC), 2011.

*TDSC* [23] *Automated Derivation of Application-aware Error Detectors using Static Analysis,* Karthik Pattabiraman, Zbigniew Kalbarczyk and Ravishankar Iyer, IEEE Transactions on Dependable and Secure Computing (TDSC), 2011.

(b) *Conference Proceedings (Acceptance rates provided where known: see note above): Publications in tier-1 conferences are indicated with a '*'. These are highly competitive venues with low acceptance rates.* ***Total tier-1 papers = 40.***

*NDSS'25** [1] *A Method to Facilitate Membership Inference Attacks in Deep Learning Models,* **Zitao Chen** and Karthik Pattabiraman. To appear in the Proceedings of the Network and Distributed Systems Security Symposium (NDSS), 2025. (Acceptance rate: TBD)

*CCS'24** [2] *AutoPatch: Automated Generation of Hotpatches for Real-Time Embedded Devices,* **Mohsen Salehi** and Karthik Pattabiraman. Proceedings of the ACM Conference on Computer and Communications Security (CCS), 2024. (Acceptance rate: 16.7%)

*CCS'24** [3] *SpecGuard: Specification Aware Recovery for Robotic Autonomous Vehicles from Physical Attacks,* **Pritam Dash, Ethan Chan** and Karthik Pattabiraman. Proceedings of the ACM Conference on Computer and Communications Security (CCS), 2024. (Acceptance rate: 16.7%)

| | | |
|---|---|---|
| *S&P'24* (Oakland)* | [4] | *POMABuster: Detecting Price Oracle Manipulation Attacks in Decentralized Finance,* **Rui Xi,** Zehua Wang, and Karthik Pattabiraman.Proceedings of the IEEE Symposium on Security and Privacy (S&P), 2024 (Oakland). (Acceptance rate: 17.8%). |
| *CHASE'24* | [5] | *Systematically Assessing the Security Risks of AI/ML-enabled Connected Healthcare Systems,* **Mohammad ElNawawy, Mohammadreza Hallajiyan, Gargi Mitra**, Shahrear Iqbal, and Karthik Pattabiraman*,* Proceedings of the IEEE/ACM International Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE), 2024. (Acceptance Rate: 28.4%). |
| *IoTDI'24* | [6] | *ImmunoPlane: Middleware for Providing Adaptivity to Distributed Internet-of-Things Applications,* **Kumseok Jung, Gargi Mitra,** Sathish Gopalakrishnan, and Karthik Pattabiraman, Proceedings of the IEEE/ACM Conference on Internet of Things Design and Implementation (IoTDI), 2024. (Acceptance Rate: 36.7%) |
| *AsiaCCS'24* | [7] | *Diagnosis-guided Attack Recovery for Securing Robotic Vehicles from Sensor Deception Attacks,* **Pritam Dash,** Guanpeng Li, **Mehdi Karimibiuki**, and Karthik Pattabiraman, Proceedings of the ACM Asia Conference on Computer and Communications Security (AsiaCCS), 2024. (Acceptance Rate: 21.9%) |
| *NDSS'24** | [8] | *Overconfidence is a Dangerous Thing: Mitigating Membership Inference Attacks by Enforcing Less Confident Prediction,* **Zitao Chen** and Karthik Pattabiraman, Proceedings of the International Network and Distributed Systems Symposium (NDSS), 2024 (Acceptance rate: 15%). **Artifacts Available, Functional and Reproduced.** |
| *SEC'23* | [9] | *Edge Engine: A Thermal-Aware Optimization Framework for Edge Inference,* **Amirhossein Ahmadi,** Hazem Abdelhafez, Karthik Pattabiraman and Matei Ripeanu, Proceedings of the ACM/IEEE International Symposium on Edge Computing (SEC), 2023. (Acceptance Rate: 25%) |
| *ISSRE'23* | [10] | *Resilience Assessment of Large Language Models under Transient Hardware Faults,* **Udit Agarwal, Abraham Chan**, and Karthik Pattabiraman. Proceedings of the IEEE International Symposium on Software Reliability Engineering (ISSRE), 2023. (Acceptance Rate: 28.5%). **Artifacts Available and Reviewed.** |
| *ISSRE'23* | [11] | *Evaluating the Effect of Common Annotation Faults on Object Detection Techniques,* **Abraham Chan,** Arpan Gujarati, Karthik Pattabiraman and Sathish Gopalakrishnan. Proceedings of the IEEE International Symposium on Software Reliability Engineering (ISSRE), 2023. (Acceptance Rate: 28.5%). **Artifacts Available and Reviewed.** |
| *SC'23** | [12] | *Structural Coding: A Low-Cost Scheme to Protect CNNs from Large-Granularity Memory Faults,* **Ali Asgari**, Florian Geissler, Syed Qutub, Michael Paulitsch, Prashant Nair, and Karthik Pattabiraman. Proceedings of the International Conference for High Performance Computing, Networking, Storage, and Analysis (SC), 2023. *(Acceptance Rate: 23.9%).* **Artifacts Available and Functional.** |
| *SafeComp'23* | [13] | *A Low-cost Strategic Monitoring Approach for Scalable and Interpretable Error Detection in Deep Neural Networks,* Florian Geissler, Syed Qutub, Michael Paulitsch and Karthik Pattabiraman, Proceedings of the International Conference on Computer Safety, Reliability and Security (SafeComp), 2023. (Acceptance Rate: 20%) |

| | | |
|---|---|---|
| *DSN'23** | [14] | *SwarmFuzz: Discovering GPS Spoofing Attacks in Drone Swarms,* **Yingao (Elaine) Yao, Pritam Das**h, and Karthik Pattabiraman, Proceedings of the IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), 2023. (Acceptance Rate: 20%). |
| *ICSE'23** | [15] | *AChecker*, *Statically Detecting Smart Contract Access Control Vulnerabilities,* **Asem Ghaleb**, Julia Rubin, and Karthik Pattabiraman, Proceedings of the IEEE/ACM International Conference on Software Engineering (ICSE), 2023. (Acceptance Rate: 26%). **Artifacts Available and Reusable** |
| *AsiaCCS'23* | [16] | *Jujutsu: A Two-stage Defense against Adversarial Patch Attacks on Deep Neural Networks*, **Zitao Chen, Pritam Dash,** and Karthik Pattabiraman, Proceedings of the 18th ACM Asia Conference on Computer and Communications Security (ACM ASIACCS), 2023. (Acceptance Rate: 16%) |
| *SEC'22* | [17] | *Characterizing Variability in Heterogeneous Edge Systems: A Methodology & Case Study*, Hazem A. Abdelhafez, Hassan Halawa, Amr Almoallim, **Amirhossein Ahmadi**, Karthik Pattabiraman, and Matei Ripeanu. Proceedings of the ACM/IEEE Symposium on Edge Computing (SEC), 2022. (Acceptance Rate: 27%) |
| *ISSRE'22* | [18] | *LLTFI: Framework Agnostic Fault Injection for Machine Learning Applications (Tools and Artifact Track),* **Udit Agarwal, Abraham Chan**, and Karthik Pattabiraman, Proceedings of the IEEE International Symposium on Software Reliability Engineering (ISSRE), 2022. (Acceptance Rate: 29%). |
| *ISSTA'22** | [19] | *eTainter: Detecting Gas-Related Vulnerabilities in Smart Contracts,* **Asem Ghaleb,** Julia Rubin, and Karthik Pattabiraman, Proceedings of the ACM International Conference on Software Testing and Analysis (ISSTA), 2022. (Acceptance Rate: 24.5%). **Artifacts Functional and Reusable.** |
| *DSN'22** | [20] | *The Fault in our Data Stars: Studying Mitigation Techniques against Training Data Faults in ML applications,* **Abraham Chan,** Arpan Gujarati, Karthik Pattabiraman, and Sathish Gopalakrishnan, Proceedings of the IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), 2022. (Acceptance Rate: 18.7%) |
| *IOTDI 22* | [21] | Π-*configurator: Enabling Efficient Configuration of Pipelined Applications on the Edge,* **Mohammad Rafiuzzaman,** Sathish Gopalakrishnan, and Karthik Pattabiraman, Proceedings of the ACM/IEEE International Conference on Internet of Things Design and Implementation, 2022 (IoTDI'22). (Acceptance Rate: 33%). |
| *SANER'22* | [22] | *When They Go Low: Automated Replacement of Low-level Functions in Ethereum Smart Contracts ,* **Rui Xi** and Karthik Pattabiraman, Proceedings of the IEEE International Conference on Software Analysis, Evolution and Reengineering (SANER), 2022. (Acceptance Rate: 36%). |
| *QRS'21* | [23] | *Understanding the Resilience of Neural Network Ensembles against Faulty Training Data,* **Abraham Chan, Niranjhana Narayananan,** Arpan Gujarati, Karthik Pattabiraman, and Sathish Gopalakrishnan, Proceedings of the IEEE International Symposium on Quality, Reliability and Security (QRS), 2021. Full paper (Acceptance Rate: 25.1%). **Best Paper Award (one of three papers from > 300 submissions).** |
| *SEC'21* | [24] | *OneOS: Middleware for Running Edge Computing Applications as Distributed POSIX pipelines*, **Kumseok Jung, Julien Gascon-Samson,** and Karthik Pattabiraman, Proceedings of the ACM/IEEE |

Symposium on Edge Computing (SEC), 2021. (Acceptance Rate: 27.5%). **Won best demo award (1 award given).**

*SEC'21* [25] *MIRAGE: Machine Learning-based Modeling of Identical Replicas of the Jetson AGX Embedded Platform,* Hazem A. Abdelhafez, Hassan Halawa, Mohamed Ahmed, Karthik Pattabiraman, and Matei Ripeanu. Proceedings of the ACM/IEEE Symposium on Edge Computing (SEC), 2021. (Acceptance Rate: 27.5%)

*PRDC'21* [26] *Are you for Real? Authentication in Dynamic IoT Systems,* **Mehdi Karimibiuki,** Karthik Pattabiraman, and Andre Ivanov, Proceedings of the IEEE Pacific Rim International Symposium on Dependable Computing (PRDC), 2021. (Acceptance Rate: 43%.)

*DSN'21** [27] *A Low Cost Fault Corrector for Deep Neural Networks through Range Restriction,* **Zitao Chen, Guanpeng Li,** and Karthik Pattabiraman, Proceedings of the IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), 2021. (Acceptance Rate: 16.3%). **Best Paper Award Runner up (1 of 2 papers from nearly 300 submissions). Chosen as IEEE Top Picks in Test and Reliability, 2024.**

*DSN'21** [28] *PID-Piper: Recovering Robotic Vehicles from Physical Attacks,* **Pritam Dash, Guanpeng Li, Zitao Chen, Mehdi Karimibiuki,** and Karthik Pattabiraman, Proceedings of the IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), 2021. (Acceptance Rate: 16.3%). **Best Paper Award (1 paper of nearly 300 submissions). Chosen for IEEE Top Picks in Test and Reliability, 2024.**

*ISSRE'20* [29] *TensorFI: A Flexible Fault Injection Framework for TensorFlow Applications,* **Zitao Chen, Niranjhana Narayanan, Bo Fang, Guanpeng Li,** Karthik Pattabiraman, and Nathan DeBardeleben, Proceedings of the IEEE International Symposium on Software Reliability Engineering (ISSRE), 2020. (Acceptance Rate: 25.6%).

*ISSRE'20* [30] *How Far Have We Come in Detecting Anomalies in Distributed Systems? An Empirical Study with a Statement-level Fault Injection Method,* **Yong Yang,** Yifan Wu, Karthik Pattabiraman, Long Wang, and Ying Li, Proceedings of the IEEE International Symposium on Software Reliability Engineering (ISSRE), 2020. (Acceptance Rate: 25.6%).

*SC'20** [31] *GPU-TRIDENT: Efficient Modeling of Error Propagation in GPU Programs,* **Abdul Rehman Anwer, Guanpeng Li**, Karthik Pattabiraman, Michael Sullivan, Timothy Tsai and Siva Hari. Proceedings of the IEEE/ACM International Conference for High-Performance Computing, Storage and Networking (SC), 2020. (Acceptance Rate: 25.1%)

*ISSTA'20** [32] *How Effective are Smart Contract Analysis Tools ? Evaluating Smart Contract Static Analysis Tools Using Bug Injection,* **Asem Ghaleb** and Karthik Pattabiraman, Proceedings of the ACM International Conference on Software Testing and Analysis (ISSTA), 2020. (Acceptance Rate: 26%). **Artifacts Functional Badge.**

*DSN'20** [33] *Trace Sanitizer: Eliminating the Effects of Non-Determinism on Error Propagation Analysis,* Habib Saissi, Stefan Winter, Oliver Schwan, **Karthik Pattabiraman,** and Neeraj Suri, Proceedings of

IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), 2020. (Acceptance Rate: 16.5%).

*ACSAC' 19* [34] *Out of Control: Stealthy Attacks on Robotic Vehicles Protected by Control-Based Techniques,* **Pritam Dash, Mehdi Karimibiuki,** and Karthik Pattabiraman, Proceedings of the Annual Computer Security Applications Conference (ACSAC), 2019. (Acceptance Rate: 22.6%). **Artifacts Reusable Badge. Rated 1 of 10 top cyber-security innovations in Canada for the year 2019 by SERENE-RISC. Media coverage.**

*ISSRE'19* [35] *A tale of two injectors: An end-to-end comparison of IR-level and Assembly-level Fault Injection*, **Lucas Palazzi, Guanpeng Li, Bo Fang,** and Karthik Pattabiraman, Proceedings of the IEEE International Conference on Software Reliability Engineering (ISSRE), 2019. (Acceptance Rate: 31.5%).

*SC'19** [36] *BinFI: An Efficient Fault Injector for Safety-Critical Machine Learning Systems*, **Zitao Chen, Guanpeng Li,** Karthik Pattabiraman, and Nathan DeBardeleben, Proceedings of the IEEE/ACM International Conference for High-Performance Computing, Storage and Networking (SC), 2019. (Acceptance Rate: 21%). **Finalist for SC 20 reproducibility challenge (one of three papers).**

*ICS'19** [37] *BonVoision: Leveraging Spatial Data Smoothness for Recovery from Memory Soft Errors,* **Bo Fang,** Karthik Pattabiraman, Matei Ripeanu and Sriram Krishnamoorthy, Proceedings of the ACM International Conference on Supercomputing (ICS), 2019. (Acceptance Rate: 23.2%).

*SAC'19* [38] *Failure Prediction in the Internet of Things due to Memory Exhaustion,* **Mohammad Rafiuzzaman, Julien Gascon-Samson,** Karthik Pattabiraman, and Sathish Gopalakrishnan, Proceedings of the ACM/SIGAPP Symposium on Applied Computing (SAC), 2019. Dependable, Adaptive and Secure Distributed Systems Track. (Acceptance rate: 27.5%)

*PRDC'19* [39] *DynPolAC: Dynamic Policy-based Access Control for IoT Systems,* **Mehdi Karimibiuki, Ekta Aggarwal,** Karthik Pattabiraman, and Andre Ivanov, Proceedings of the IEEE International Conference on Pacific Rim Dependable Computing (PRDC), 2018. (Acceptance Rate: 45%).

*ECOOP' 18* [40] *ThingsMigrate: Platform-Independent Migration of Stateful JavaScript IoT Applications,* **Julien Gascon-Samson, Kumseok Jung, Shivanshu Goyal, Armin Rezalean-Asel,** Karthik Pattabiraman, Proceedings of the European Conference on Object Oriented Programming (ECOOP), 2018. (Acceptance Rate: 39%).

*DSN'18** [41] *Modeling Soft Error Propagation in Programs*, **Guanpeng Li,** Karthik Pattabiraman, Siva Hari, Michael Sullivan and Timothy Tsai, Proceedings of the IFIP/IEEE International Conference on Dependable Systems and Networks (DSN), 2018 (Acceptance rate for regular papers: 25%). **Best Paper Award Runner up.**

*DSN'18** [42] *Modeling Input-Dependent Error Propagation in Programs*, **Guanpeng Li, and** Karthik Pattabiraman, Proceedings of the IFIP/IEEE International Conference on Dependable Systems and Networks (DSN), 2018 (Acceptance rate for regular papers: 25%).

| | | |
|---|---|---|
| *ICSE'18** | [43] | *Inferring Hierarchical Motifs from Execution Traces,* **Saba Alimadadi,** Ali Mesbah and Karthik Pattabiraman, Proceedings of the ACM/IEEE International Conference on Software Engineering (ICSE), 2018 (Acceptance Rate: 21%). |
| *ASE'17* | [44] | *Detecting Unknown Inconsistencies in Web Applications,* **Frolin Ocariza**, Karthik Pattabiraman, and Ali Mesbah, Proceedings of the ACM/IEEE International Conference on Automated Software Engineering (ASE), 2017. (Acceptance Rate: 21%) |
| *SC'17** | [45] | *Understanding Error Propagation in Deep Learning Neural Network (DNN) Accelerators and Applications,* **Guanpeng Li,** Siva Hari, Michael Sullivan, Timothy Tsai, Karthik Pattabiraman, Steve Keckler, and Joel Emer, Proceedings of the International Conference for High-Performance Computing, Storage and Networking (SC), 2017. (Acceptance Rate: 19%). **Chosen for IEEE Top Picks in Test and Reliability, 2023.** |
| *FSE'17** | [46] | *ARTINALI: Dynamic Invariant Detection for Cyber-Physical System Security*, **Maryam Raiyat Aliabadi, Amita Kamath, Julien Gascon-Samson**, and Karthik Pattabiraman, Proceedings of the ACM SIGSOFT Symposium on Foundations of Software Engineering (FSE), 2017. (Acceptance Rate: 24.5%) |
| *HPDC'17** | [47] | *LetGo: A Lightweight Continuous Framework for HPC Applications Under Failures,* **Bo Fang,** Qiang Guan, Nathan Debardeleben**,** Karthik Pattabiraman, and Matei Ripeanu, Proceedings of the ACM International Symposium on High-Performance Parallel and Distributed Computing (HPDC), 2017. (Acceptance Rate: 19%) |
| *DSN'17** | [48] | *One Bit is (Not) Enough: An Empirical Study of the Impact of Single and Multiple Bit Flip Errors,* **Behrooz Sangchoolie,** Karthik Pattabiraman and Johan Karlsson, Proceedings of the IEEE International Conference on Dependable Systems and Networks (DSN), 2017. (Acceptance Rate: 23%) |
| *ICST'17* | [49] | *IPA: Error Propagation Analysis of Multi-Threaded Programs Using Likely Invariants*, **Abraham Chan,** Stefan Winter, Habib Saissi, Karthik Pattabiraman and Neeraj Suri, Proceedings of the IEEE International Conference on Software Testing, Verification and Validation (ICST), 2017. (Acceptance Rate: 27%) |
| *ACSAC' 16* | [50] | *Formal Security Analysis of Smart Embedded Systems*, **Farid Molazem Tabrizi** and Karthik Pattabiraman, Proceedings of the Annual Computer Security Applications Conference (ACSAC), 2016. (Acceptance Rate: 23%). |
| *SC'16** | [51] | *Understanding Error Propagation in GPGPU Applications,* **Guanpeng Li,** Karthik Pattabiraman, Chen-Yong Cher and Pradip Bose, Proceedings of the International Conference for High-Performance Computing, Storage and Networking (SC), 2016. (Acceptance Rate: 18%). |
| *EDCC'16* | [52] | *Finding Resilience-Friendly Compiler Optimizations Using Meta-Heuristic Search Techniques,* **Nithya Narayanamurthy,** Karthik Pattabiraman and Matei Ripeanu, Proceedings of the European Dependable Computing Conference (EDCC), 2016. (Acceptance Rate: 41%). **Best Paper Award (1 of 3).** |

| | | |
|---|---|---|
| *SafeComp'16* | [53] | *FIDL: A Fault Injection Description Language for Compiler-Based Tools*, **Maryam Raiyat Ailabadi** and Karthik Pattabiraman, Proceedings of the 35th International Conference on Computer Safety, Reliability and Security (SafeComp), 2016. (Acceptance Rate: 35%) |
| *DSN'16** | [54] | *ePVF: An Enhanced Program Vulnerability Factor Methodology for Cross-Layer Resilience Analysis,* **Bo Fang, Qining Lu,** Karthik Pattabiraman, Matei Ripeanu and Sudhanva Gurumurthi, Proceedings of the IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), 2016. (Acceptance Rate: 21%) |
| *ICST'16* | [55] | *Atrina: Inferring Unit Oracles from GUI Test Cases*, **Shabnam Mirshokraie,** Ali Mesbah and Karthik Pattabiraman, Proceedings of the IEEE International Conference on Software Testing, Verification and Validation (ICST), 2016. (Acceptance Rate: 27%) |
| *ICSE'16** | [56] | *Understanding Asynchronous Interactions in Full-Stack JavaScript,* **Saba Alimadadi,** Ali Mesbah and Karthik Pattabiraman, Proceedings of the IEEE/ACM International Conference on Software Engineering (ICSE), 2016. (Acceptance Rate: 19%) |
| *ISSRE' 15* | [57] | *Experience Report: An Application-Specific Checkpointing Technique for Minimizing Checkpoint Corruption*, ***Guanpeng Li,*** Karthik Pattabiraman, Chen-Yong Cher and Pradip Bose, Proceedings of the IEEE International Symposium on Software Reliability Engineering (ISSRE), 2015. (Acceptance Rate: 32%) |
| *ASE'15* | [58] | *Synthesizing Web Element Locators,* ***Kartik Bajaj*****,** Karthik Pattabiraman and Ali Mesbah, Proceedings of the IEEE/ACM International Conference on Automated Software Engineering (ASE), 2015. (Acceptance Rate: 20.6%) |
| *EDCC'15* | [59] | *Flexible Intrusion Detection Systems for Memory-Constrained Embedded Systems,* ***Farid Tabrizi*** and Karthik Pattabiraman, Proceedings of the 11th European Conference on Dependable Computing (EDCC), 2015. (Acceptance Rate: 46%)**. Distinguished paper award – one of three from 54 submissions.** |
| *ECOOP '15* | [60] | *Hybrid Change-Impact Analysis for JavaScript Applications*, ***Saba Alimadadi*****,** Ali Mesbah and Karthik Pattabiraman, Proceedings of the European Conference on Object Oriented Programming (ECOOP), 2015. (Acceptance rate: 22.8%) |
| *ISSRE'15* | [61] | *Fine Grained Characterization of Faults Causing Long Latency Crashes in Programs,* ***Guanpeng Li*****, Qining Lu,** and Karthik Pattabiraman, Proceedings of the IEEE/IFIP International Conference on Dependable Systems (DSN), 2015. **(**Acceptance Rate: 22.5%) |
| *ICST'15* | [62] | *JSEFT: Automated JavaScript Unit Test Generation,* ***Shabnam Mirshokraie*****,** Ali Mesbah and Karthik Pattabiraman, Proceedings of the IEEE International Conference on Software Testing, Verification and Validation (ICST), 2015. (Acceptance Rate: 25%). **Invited as one of the best papers in the conference to the Journal on Software Testing and Verification (STVR).** |

*ICSE'15** [63] *Finding Inconsistencies in JavaScript MVC Applications*, ***Frolin Ocariza*****,** Karthik Pattabiraman and Ali Mesbah, Proceedings of the IEEE/ACM International Conference on Software Engineering (ICSE), 2015. (Acceptance Rate: 18.5%)

*ISSRE'14* [64] *Failure Analysis of Jobs in Compute Clouds: A Google Cluster Case Study***, Xin Chen**, Charng-da Lu and *Karthik Pattabiraman*, Proceedings of the 25th IEEE International Symposium on Software Reliability Engineering (ISSRE), 2014. (Acceptance rate: 25%). **Chosen as one of the "highlights of ISSRE" – one of 26 papers chosen from over 1000 papers in the 30 year history of the ISSRE conference (in 2019).**

*ASE'14* [65] *DOMpletion: DOM-Aware JavaScript Code Completion*, ***Kartik Bajaj*****,** Karthik Pattabiraman and Ali Mesbah, Proceedings of the ACM International Conference on Automated Software Engineering (ASE), 2014. (Acceptance Rate: 20%)

*CASES'14* [66] *SDCTune: A Model for Predicting the SDC Proneness of an Application for Configurable Protection*, **Qining Lu**, *Karthik Pattabiraman*, Meeta S. Gupta and Jude A. Rivers, International Conference on Compilers, Architecture and Synthesis for Embedded Systems (CASES), 2014. (Acceptance Rate: 30%)

*DSN'14** [67] *Integrated Hardware-Software Diagnosis for Intermittent Hardware Faults,* ***Majid Dadashi,*** **Layali Rashid,** Karthik Pattabiraman and Sathish Gopalakrishnan, Proceedings of the IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), 2014. (Acceptance Rate: 30%)

*DSN'14** [68] *Quantifying the Accuracy of High-Level Fault Injection Techniques for Hardware Faults,* **Jiesheng Wei, Anna Thomas, Guanpeng Li,** and *Karthik Pattabiraman*, Proceedings of the IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), 2014. (Acceptance Rate: 30%)

*ICSE'14** [69] *Vejovis: Suggesting Fixes for JavaScript Faults,* ***Frolin Ocariza*****,** Karthik Pattabiraman and Ali Mesbah, Proceedings of the IEEE/ACM International Conference on Software Engineering (ICSE), 2014, Hyderabad, India (Acceptance Rate: 20%).

*ICSE'14** [70] *Understanding JavaScript Event-Based Interactions,* ***Saba Alimadadi*****, Sheldon Sequira,** Ali Mesbah and Karthik Pattabiraman, Proceedings of the IEEE/ACM International Conference on Software Engineering (ICSE), 2014, Hyderabad, India (Acceptance Rate: 20%). **ACM SIGSOFT Distinguished Paper Award (9 of nearly 500 submissions)**

*MSR'14* [71] *Mining Questions Asked by Web Developers,* **Kartik Bajaj,** Karthik Pattabiraman and Ali Mesbah, Proceedings of the 11th Working Conference on Mining Software Repositories (MSR), 2014. (Acceptance Rate: 34%)

*ISPASS'14* [72] *GPU-Qin: A Methodology for Evaluating the Error Resilience of GPGPU Applications,* ***Bo Fang*****,** Karthik Pattabiraman, Matei Ripeanu and Sudhanva Gurumurthi, Proceedings of the IEEE International Symposium on Performance Analysis of Systems and Software (ISPASS), 2014. (Acceptance Rate: 30%)

*HASE'14* [73] *Model-based Intrusion Detection for Smart Meters*, **Farid M. Tabrizi** and *Karthik Pattabiraman*, Proceedings of the IEEE International Symposium on High Assurance Systems Engineering (HASE), 2014. Miami, USA (Acceptance rate: 30%)

| | | |
|---|---|---|
| *ASE'13* | [74] | *Pythia: Generating Test Cases with Oracles for JavaScript Applications,* ***Shabnam Mirshokraie****,* Ali Mesbah and Karthik Pattabiraman, Proceedings of the ACM/IEEE International Conference on Automated Software Engineering (ASE), New Ideas Track, 2013. October 2013 (Acceptance rate: 23%) |
| *ESEM'13* | [75] | *An Empirical Study of Client-Side JavaScript Bugs*, ***Frolin Ocariza*****, Kartik Bajaj,** Karthik Pattabiraman and Ali Mesbah, Proceedings of the IEEE International Symposium on Empirical Software Engineering and Measurement (ESEM), 2013 (Acceptance rate: 28 %) |
| *DSN'13** | [76] | *Error Detector Placement for Soft Computation,* ***Anna Thomas*** and Karthik Pattabiraman, Proceedings of the IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), 2013. (Acceptance Rate: 20%) |
| *ICST'13* | [77] | *Efficient JavaScript Mutation Testing*, ***Shabnam Mirshokraie****,* Ali Mesbah and Karthik Pattabiraman, Proceedings of the IEEE International Conference on Software Testing, Verification and Validation (ICST), 2013. (Acceptance Rate: 25 %). **Best paper runner up award at the conference of over 150 submissions.** |
| *QEST'12* | [78] | *Intermittent Hardware Errors Recovery: Modeling and Evaluation*, ***Layali Rashid***, Karthik Pattabiraman and Sathish Gopalakrishnan, Proceedings of the International Conference on Quantitative Evaluation of Systems (QEST), 2012. |
| *DSN'12** | [79] | *BlockWatch: Leveraging Similarity in Parallel Programs for Error Detection,* ***Jiesheng Wei*** and Karthik Pattabiraman, Proceedings of the IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), 2012. (*Acceptance rate: 17%).* |
| *ICST'12* | [80] | *AutoFlox: An Automatic Fault Localizer For JavaScript,* ***Frolin Ocariza***, Karthik Pattabiraman and Ali Mesbah, IEEE International Conference on Software Testing, Verification and Validation (ICST), 2012. (*Acceptance rate: 27%)*. **Nominated for best paper award (one of six), among more than 150 submissions**. |
| *ISSRE'11* | [81] | *JavaScript Errors in the Wild: An Empirical Study*, ***Frolin Ocariza****,* Karthik Pattabiraman and Benjamin Zorn, Proceedings of IEEE International Symposium on Software Reliability Engineering (ISSRE), 2011 (*Acceptance Rate: 25%)* |
| *CSF'11* | [82] | *Modular Protections against Non-control Data Attacks, Cole Schlesinger*, Karthik Pattabiraman, Nikhil Swamy, David Walker and Benjamin Zorn, Proceedings of the IEEE Computer Security Foundations (CSF) Symposium, 2011 (*Acceptance Rate: 26%)*. **Invited for a special issue by Journal of Computer Security (JCS)** |
| *ASPLOS' 11** | [83] | *Flikker: Saving DRAM Refresh-power through Critical Data Partitioning,* ***Song Liu***, Karthik Pattabiraman, Thomas Moscibroda and Benjamin Zorn*,* Proceedings of the ACM International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS) *,* 2011. *(Acceptance Rate: 20%)* |

| | | |
|---|---|---|
| *PRDC'10* | [84] | *Modeling the Propagation of Intermittent Hardware Faults in Programs*, ***Layali Rashid***, Karthik Pattabiraman and Sathish Gopalakrishnan, Proceedings of the IEEE Pacific Rim International Symposium on Dependable Computing (PRDC), 2010. (Acceptance rate: 41.5%). |
| *ISSRE'10* | [85] | *DoDOM: Leveraging DOM Invariants for Robustness Testing of Web 2.0 Applications*, *Karthik Pattabiraman* and Benjamin Zorn, Proceedings of the IEEE International Symposium on Software Reliability Engineering (ISSRE), 2010. (Acceptance rate: 32 %). |
| *DSN'09** | [86] | *An End-to-end Approach for the Automatic Derivation of Application-aware Error Detectors*, Galen Lyle, Shelley Chen, *Karthik Pattabiraman***,** Zbigniew Kalbarczyk and Ravishankar Iyer, Proceedings of the IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), 2009. (Acceptance rate: 25%). |
| *SEC'09* | [87] | *Discovering Application-level Insider attacks using Symbolic Execution*, Karthik Pattabiraman, Nithin Nakka, Zbigniew Kalbarczyk and *Ravishankar Iyer*, Proceedings of the IFIP International Information Security Conference (SEC), 2009. (Acceptance Rate: 22%) |
| *PPoPP'09* | [88] | *ToleRace: Detecting and Tolerating Asymmetric Races, Paruj Ratanaworabhan*, Martin Burtscher, Darko Kirovski, Benjamin Zorn, Karthik Pattabiraman and Rahul Nagpal, Proceedings of the ACM SIGPLAN Symposium on Principles and Practice of Parallel Programming (PPoPP), 2009. (Acceptance Rate: 24%) |
| *DSN'08** | [89] | *SymPLFIED: Symbolic Program Level Fault-Injection and Error Detection Framework, Karthik Pattabiraman*, Nithin Nakka, Zbigniew Kalbarczyk and Ravishankar Iyer, Proceedings of the IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), 2008. (Acceptance Rate: 25%). |
| *EuroSys '08** | [90] | *Samurai: Protecting Critical Heap Data in Unsafe Languages,* Karthik Pattabiraman, Vinod Grover and *Benjamin Zorn*, Proceedings of ACM European Systems Conference (EuroSys), 2008. (Acceptance Rate: 18%) |
| *IOLTS'07* | [91] | *Automated Derivation of Application-Aware Error Detectors using Static Analysis*, Karthik Pattabiraman, Zbigniew Kalbarczyk and *Ravishankar Iyer*, Proceedings of IEEE International Online Test Symposium (IOLTS), 2007 |
| *DSN'07** | [92] | *Processor-level Selective Replication*, *Nithin Nakka*, Karthik Pattabiraman and Ravishankar Iyer, Proceedings of the IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), 2007. (Acceptance Rate: 25%) |
| *EDCC'06* | [93] | *Dynamic Derivation of Application-Specific Error Detectors and their Hardware Implementation***,** Karthik Pattabiraman, Giacinto Paulo Saggesse, Daniel Chen, Zbigniew Kalbarczyk, and Ravishankar Iyer, Proceedings of the European Dependable Computing Conference (EDCC), 2006. (Acceptance Rate: 27%) |
| *PRDC'05* | [94] | *Application-Based Metrics for Strategic Placement of Detectors*, *Karthik Pattabiraman*, Zbigniew Kalbarczyk and Ravishankar Iyer, Proceedings of the IEEE Symposium on Pacific Rim Dependable Computing (PRDC), 2005. (Acceptance Rate: 36.5%) |

*DSN'05** [95] *Modeling Coordinated Checkpointing for Large-Scale Supercomputers*, *Long Wang*, Karthik Pattabiraman, Larry Votta, Chris Vick, Alan Wood, Zbigniew Kalbarczyk and Ravishankar Iyer, Proceedings of the IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), 2005. (Acceptance Rate: 25%)

*SEC'04* [96] *Formal Reasoning of Various Categories of Widely Exploited Security Vulnerabilities by Pointer Taintedness Semantics*, Shuo Chen, Karthik Pattabiraman, Zbigniew Kalbarczyk and *Ravishankar Iyer*, Proceedings of the IFIP International Information Security Conference (SEC), 2004. (Acceptance Rate: 22%)

*(c) Books edited*

[1] *System Dependability and Analytics: Approaching System Dependability from Data, System and Analytics Perspective*s, Edited by Long Wang, Karthik Pattabiraman, Catello Di Martino, Arjun Athreya, Saurabh Bagchi, Springer Series in Reliability Engineering, Springer Nature, 2022.

(d) *Selected Workshop/Demo/Poster Papers (Number of pages given, where applicable)*

*[1]* *Hierarchical Unlearning Framework for Multi-Class Classification,* **Abraham Chan**, Arpan Gujarati, Karthik Pattabiraman and Sathish Gopalakrishnan. Workshop in Fine Tuning in Modern Machine Learning (FiTML), co-held with the International Conferences on Neural Information Processing Systems (NeurIPS), 2024. (6 pages)

[2] *Targeting the Blind Spot: Evaluating Modern ICS Security Against A Novel Denial of Service (DoS) Attack,* **Gargi Mitra, Pritam Dash, Yingao (Elaine) Yao**, Aastha Mehta, Karthik Pattabiraman, International Workshop on Re-design Industrial Control Systems with Security (RICSS'24), co-held with CCS'24. (8 pages)

[3] *SAM: Foreseeing Inference-Time False Data Injection Attacks on ML-enabled Medical Devices,* **Mohammadreza Hallajiyan, Athish Pranav Dharmalingam, Gargi Mitra**, Homa Alemzadeh, Shahrear Iqbal and Karthik Pattabiraman. To appear in the CyberSecurity in Healthcare Workshop (HealthSec'24), co-held with CCS'24. (8 pages)

[4] *Global Clipper: Enhancing Safety and Reliability of Transformer-based Object Detection Models,* Qutub Syed, Michael Paulitsch, Karthik Pattabiraman, Korbinian Hagn1, Fabian Oboril, Cornelius Buerkle, Kay-Ulrich Scholl, Gereon Hinz and Alois Knoll, To appear in the IJCAI-AISafety Workshop, 2024. (Acceptance Rate: TBD). 10 pages.

[5] *Harnessing Explainability to Improve ML Ensemble Resilience,* **Abraham Chan,** Arpan Gujarati**,** Karthik Pattabiraman, and Sathish Gopalakrishnan*,* Disrupt track of the IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), 2024. (Acceptance Rate: 45%). (5 pages)

[6] *Hot Under the Hood: An Analysis of Ambient Temperature Impact on Heterogeneous Edge Platforms,* **Amirhossein Ahmadi,** Hazem AbdelHafez, **Shashwat Jaiswal**, Karthik Pattabiraman, and Matei Ripeanu, IEEE/ACM International Workshop on Edge Systems, Analytics and Networking (EdgeSys), 2023. Co-located with Eurosys'23 (Acceptance Rate: 42%). **Best Paper Award.** (6 pages)

[7] *Towards Reliability Assessment of Systolic Arrays against Stuck-at Faults,* **Udit Agarwal, Abraham Chan, Ali Asgari** and Karthik Pattabiraman, IEEE Workshop on Silicon Errors in Logic, System Effects (SELSE), 2023. **Chosen as "Best of SELSE'23" and invited to present at DSN'23 - one of three papers.** (6 pages)

[8] *Poster: May the Swarm Be With You: Sensor Spoofing Attacks Against Drone Swarms.* **Yingao (Elaine) Yao, Pritam Dash**, Karthik Pattabiraman. ACM SIGSAC Conference on Computer and Communications Security (CCS), 2022.

[9] *Poster AutoPatch: Automatic Hotpatching of Real-Time Embedded Devices.* **Mohsen Salehi**, Karthik Pattabiraman, ACM SIGSAC Conference on Computer and Communications Security (CCS), 2022.

[10] *Poster: EdgeShell - A language for composing edge applications.* **Kumseok Jung,** Julien Gascon-Samson, and Karthik Pattabiraman, IEEE/ACM International Symposium on Edge Computing (SEC), 2022.

[11] *Towards Building Resilient Ensembles against Training Data Faults,* **Abraham Chan,** Arpan Gujarati, Karthik Pattabiraman, and Sathish Gopalakrishnan, 5th International Workshop on Dependable and Secure Machine Learning (DSML), 2022, Co-located with the IEEE/IFIP Intl. conference on Dependable Systems and Networks (DSN), 2022. (1-page talk abstract).

[12] *Demo: Recovering Autonomous Robotic Vehicles from Physical Attacks,* **Pritam Dash** and Karthik Pattabiraman, Proceedings of the 4th International Workshop on Automotive and Autonomous Vehicle Security (AutoSec 2022) co-located with NDSS 2022. (2 pages)

[13] *Demo: OneOS - Middleware for Running Edge Computing Applications as Distributed POSIX Pipelines*, **Kumseok Jung, Julien Gascon-Samson,** Karthik Pattabiraman, ACM/IEEE Symposium on Edge Computing (SEC), 2021. Demo Track. (2 pages). **Best Demo Award at the conference (1 paper received the award).**

[14] *(WiP) Low Level Tensor Fault Injector (LLTFI)*, **Abraham Chan, Udit Agarwal,** and Karthik Pattabiraman, IEEE Workshop on Software Certification (WoSoCER), 2021. co-located with ISSRE 2021 (6 pages).

[15] *Towards a safety case for hardware-fault tolerance in convolutional neural networks using activation range supervision,* Florian Geissler, Syed Qutub, Sayanta Roychowdhury, **Ali Asgari,** Yang Peng, Akash Dhamasia, Ralf Graefe, Karthik Pattabiraman and Michael Paulitsch, Workshop on AISafety, 2021, co-located with IJCAI 2021 (7 pages). **Best Paper Award Nominee (1 of 4 papers nominated for the award).**

[16] *Snowflakes at the Edge: A Study of Variability among NVIDIA Jetson AGX Xavier Boards,* Hazem Abdelhafez, Hassan Halawa, Karthik Pattabiraman, and Matei Ripeanu, Proceedings of the International Workshop on Edge Systems, Analytics and Networking (EdgeSys), 2021. Co-located with Eurosys 2021. (6 pages)

[17] *TF-DM: Tool for Studying ML Model Resilience to Data Faults*, **Niranhana Narayanan** and Karthik Pattabiraman, Proceedings of the 2nd International Workshop on Testing for Deep Learning and Deep Learning for Testing (DeepTest 2021), colocated with ICSE 2021. (4 pages)

[18] *Demo Paper: Impact of Stealthy Attacks on Autonomous Robotic Vehicle Missions*, **Pritam Dash, Mehdi Karimibiuki,** and Karthik Pattabiraman, Proceedings of the 3rd International Workshop on Automotive and Autonomous Vehicle Security (AutoSec 2021) co-located with NDSS 2021. (2 pages)

[19] *New Wine in an Old Bottle: N-Version Programming for Machine Learning Components,* **Arpan Gujarati,** Sathish Gopalakrishnan and Karthik Pattabiraman, Proceedings of the International Workshop on Software Certification (WoSoCER), co-held with the IEEE International Symposium on Software Reliability Engineering (ISSRE), 2020. (4 pages)

[20] *Towards Predicting the Impact of Roll-Forward Failure Recovery for HPC Applications*, **Bo Fang**, Jieyang Chen, Karthik Pattabiraman, Matei Ripeanu, Sriram Krishnamoorthy, Fast abstract at the IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), 2019. (2 pages).

[21] *OneOS: IoT Platform based on POSIX and Actors,* **Kumseok Jung, Julien Gascon-Samson,** and Karthik Pattabiraman, 2nd Usenix workshop on Hot Topics in Edge Computing (HotEdge), 2019. (7 pages).

[22] *Towards analytically evaluating the error resilience of GPU Programs,* ***Abdul Rehman Anwer,*** **Guanpeng Li**, *Karthik Pattabiraman, Siva Kumar Sastry Hari, Michael Sullivan and Timothy Tsai, IEEE Workshop on Silicon Errors in Logic, System Effects (SELSE), 2019. (6 pages).*

[23] *ThingsJS: Towards a Distributed and Self-Adaptable Cloud Edge Middleware,* **Julien Gascon-Samson, Kumseok Jung,** and Karthik Pattabiraman, Poster presentation at the ACM/IEEE Symposium on Edge Computing (SEC), 2018. (2 pages)

[24] *ThingsMigrate - Platform-Independent Live-Migration of JavaScript Processes,* **Kumseok Jung, Julien Gascon-Samson,** and Karthik Pattabiraman, Demo presentation at the ACM/IEEE Symposium on Edge Computing (SEC), 2018. (2 pages)

[25] *CORGIDS: A Correlation-based Generic Intrusion Detection System,* Ekta Aggarwal, Mehdi Karimbuiki, Karthik Pattabiraman and Andre Ivanov, 5th ACM International Workshop on Cyber-Physical System Security (CPS-SPC), co-located with the ACM International Conference on Computer and Communications Security (CCS), 2018. (11 pages)

[26] *TensorFI: A Configurable Fault Injector for TensorFlow Applications,* Guanpeng Li, Karthik Pattabiraman, and Nathan DeBardeleben, 8th IEEE International Workshop on Software Certification (WoSoCER), 2018, co-located with the IEEE International Symposium on Software Reliability Engineering (ISSRE), 2018.

[27] *SmartJS: Dynamic and Self-Adaptable Runtime Middleware for Next-Generation IoT Systems,* **Julien Gascon-Samson, Mohammad Rafiuzzaman** and Karthik Pattabiraman, Poster Paper, ACM SIGPLAN Conference on Systems, Programming, Languages and Applications: Software for Humanity (SPLASH) (2 pages).

[28] *ThingsJS: Towards a Flexible and Self-Adaptable Middleware for Dynamic and Heterogeneous IoT Environments,* **Julien-Gascon Samson, Mohammad Rafiuzzaman**, and Karthik Pattabiraman, Workshop on Middleware and Applications for the Internet of Things (M4IoT), co-located with the ACM/IFIP/Usenix Middleware Conference, 2017 (6 pages).

[29] *SDC is in the Eye of the Beholder: A Survey and Preliminary Study***, Bo Fang**, Panruo Wu, Qiang Guan, Nathan Debardeleben, Laura Monroe, Sean Blanchard, Zhizong Chen, Karthik Pattabiraman, and Matei Ripeanu, International Workshop on Reliability and Security Data Analysis (RSDA), September 2016 (4 pages). Held in conjunction with the IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), 2016.

[30] *Intrusion Detection Systems for Embedded Systems*, **Farid Molazem Tabrizi** and Karthik Pattabiraman, Doctoral student Symposium Track of the ACM Middleware Conference (Middleware), 2015. (6 pages).

[31] *A Fault Injection Description Language (FIDL) for Compiler-based Tools,* **Maryam Raiyat,** Karthik Pattabiraman and Nematollah Bidokhti, Industry Track of the IEEE International Symposium on Software Reliability Engineering (ISSRE), 2015. (1 page – refereed based on abstract)

[32] *LED: Tool for Synthesizing Web Element Locators,* **Kartik Bajaj,** Karthik Pattabiraman and Ali Mesbah, Tools Track of the IEEE/ACM International Conference on Automated Software Engineering (ASE), 2015. (3 pages)

[33] *LLFI: An Intermediate Code Level Fault Injector for Hardware Faults,* **Qining Lu, Mostafa Farahani, Jiesheng Wei, Anna Thomas** and *Karthik Pattabiraman*, Proceedings of IEEE International Conference on Quality, Reliability and Security (QRS), August 2015. Short paper. (6 pages)

[34] *Failure Prediction of Jobs in Compute Clouds: A Google Cluster Case Study,* **Xin Chen,** Charng-da Lu and Karthik Pattabiraman, International Workshop on Reliability and Security Data Analysis (RSDA), 2014 (6 pages). Held in conjunction with the IEEE International Symposium on Software Reliability Engineering (ISSRE), 2014. (6 pages)

[35] *Soft-LLFI: A Comprehensive Framework for Software Fault Injection,* **Maryam Raiyat,** Karthik Pattabiraman and Nematollah Bidokhti, Industry Track of the IEEE International Symposium on Software Reliability Engineering (ISSRE), 2014.

[36] *Evaluating the Error Resilience of Parallel Programs,* ***Bo Fang*****,** Karthik Pattabiraman, Matei Ripeanu and Sudhanva Gurumurthi, Workshop on Fault Tolerance for High-Performance at Extreme Scale (FTXS), 2014 (6 pages). In conjunction with DSN 2014.

[37] *Effect of Compiler Optimizations on the Error Resilience of Soft Computing Applications,* **Anna Thomas** and *Karthik Pattabiraman*, First Workshop on Algorithm and Application Error Resilience (AER), 2013, in conjunction with ICS 2013 (8 pages).

[38] *Predicting Job Completion Times Using System Logs in Supercomputers,* ***Xin Chen*****,** Charng-da Lu and Karthik Pattabiraman, IEEE Workshop on Reliable and Security Data Analysis (RSDA), 2013, in conjunction with DSN 2013 (6 pages).

[39] *LLFI: An Intermediate Code Level Injector for Soft Computing Applications*, ***Anna Thomas*** and Karthik Pattabiraman, IEEE Workshop on Silicon Errors in Logic, System Effects (SELSE), 2013. (6 pages).

[40] *SCRIBE: A Hardware Infrastructure Enabling Fine-Grained Software Error Diagnosis,* **Majid Dadashi, Layali Rashid**, *Karthik Pattabiraman*, Workshop on Silicon Errors in Logic, System Effects (SELSE), 2013. (6 pages).

[41] *Towards Building Error Resilient GPGPU Applications,* ***Bo Fang*****, Jiesheng Wei**, Karthik Pattabiraman, Matei Ripeanu, 3rd IEEE Workshop on Resilient Architecture (WRA) in conjunction with MICRO 2012. (6 pages).

[42] *A Model for Security Analysis of Smart Meters*, ***Farid M. Tabrizi*** and Karthik Pattabiraman, 6th Workshop on Recent Advances in Intrusion Tolerance and Resilience (WRAITS), 2012, held with DSN 2012. (6 pages).

[43] *DIEBA: Diagnosing Intermittent Errors by Backtracing Application Failures,* **Layali Rashid,** *Karthik Pattabiraman* and Sathish Gopalakrishnan, Workshop on Silicon Errors in Logic, System Effects (SELSE), 2012. (6 pages).

[44] *BlockWatch: Leveraging Similarity in Parallel Programs for Error Detection,* **Jiesheng Wei** and *Karthik Pattabiraman,* Workshop on Silicon Errors in Logic, System Effects (SELSE), 2012. (6 pages).

[45] *Comparing the Effects of Intermittent and Transient Hardware Faults on Programs*, ***Jiesheng Wei*****, Layali Rashid,** Karthik Pattabiraman, Sathish Gopalakrishnan, Workshop on Dependable and Secure Nano-computing (WDSN), 2011, in conjunction with DSN 2011 (6 pages).

[46] *Towards Understanding the Effects of Intermittent Hardware Faults on Programs,* ***Layali Rashid*****,** Karthik Pattabiraman and Sathish Gopalakrishnan, Workshop on Dependable and Secure Nanocomputing (WDSN), 2010, in conjunction with DSN 2010 (6 pages).

[47] *Formal Diagnosis of Hardware Transient Errors in Programs,* ***Layali Rashid*****,** Karthik Pattabiraman and Sathish Gopalakrishnan, Workshop on Silicon Errors in Logic, System Effects (SELSE), 2010 (6 pages).

[48] *Hardware Implementation of Information Flow Signatures Derived via Program Analysis,* Paul Dabrowski, William Healey, *Karthik Pattabiraman*, Shelley Chen, Zbigniew Kalbarczyk, Ravishankar Iyer, Workshop on Dependable and Secure Nano-computing (WDSN), 2008, In conjunction with DSN 2008 (6 pages).

[49] *Critical Variable Recomputation for Transient Error Detection,* Karthik Pattabiraman, Zbigniew Kalbarczyk and *Ravishankar K. Iyer*, Workshop on Silicon Errors in Logic, System Effects (SELSE), 2007. (6 pages).

[50] *FPGA Hardware Implementation of Statically Derived Application-aware Error Detectors, Peter Klemperer*, Shelley Chen, Karthik Pattabiraman, Zbigniew Kalbarczyk and Ravishankar Iyer, Workshop on Dependable and Secure Nano-computing (WDSN), In conjunction with DSN 2007. (6 pages).

[51] *Tolerace: Tolerating and Detecting Asymmetric Races (Position Paper*), Rahul Nagpal, Karthik Pattabiraman, Darko Kirovski, Benjamin Zorn, Workshop on Software Tools for Multi-core Systems (STMCS), 2007 (4 pages), in conjunction with PPoPP 2007.

[52] *Processor-level Selective Replication*, *Nithin Nakka*, Karthik Pattabiraman, Zbigniew Kalbarczyk, Ravishankar Iyer, Workshop on Silicon Errors in Logic, System Effects (SELSE), 2006. (6 pages).

[53] *Automated Derivation and Hardware Implementation of Application-Specific Error Detectors*, *Karthik Pattabiraman*, Giacinto Paulo Saggesse, Daniel Chen, Zbigniew Kalbarczyk and Ravishankar Iyer, Workshop on Reliability Issues in High-Performance Computing (HPCRI), 2005, in conjunction with HPCA'05 (6 pages).

*(e) Invited contributions (non-refereed or lightly refereed)*

[1] *Application Aware Reliability and Security: The Trusted Illiac Experience,* Karthik Pattabiraman, Chapter in the book "System Dependability and Analytics: Approaching System Dependability from Data, System and Analytics Perspectives", Springer Nature, 2022. Editors: L Wang, K Pattabiraman, C Di Martino, A Athreya, S Bagchi.

[2] *Introduction: Dependability Assessment*, Preface to dependability assessment section of the book "System Dependability and Analytics: Approaching System Dependability from Data, System and Analytics Perspectives", Springer Nature, 2022. Editors: L Wang, K Pattabiraman, C Di Martino, A Athreya, S Bagchi.

[3] *Error Resilient Machine Learning for Safety Critical Systems: Position Paper,* Karthik Pattabiraman, **Guanpeng Li**, and **Zitao Chen,** Special Session on Dependable Machine Learning, IEE International Online Testing Symposium (IOLTS), 2020.

[4] *Fault Injection at the Instruction Set Architecture (ISA) Level,* Karthik Pattabiraman and **Guanpeng Li,** Chapter in the "*Cross Layer Reliability of Computer Systems",* Editors: Giorgio De Natale, Dimitros Gizoupolous, Stefano De Carlo, Alberto Benso, and Ramon Canal, The Institution of Engineering and Technology (IET). Publication date May 2020.

[5] *GPUs: Combining high-performance with high-reliability,* L. Bautista Gomez, F. Cappello, L. Carro, N. DeBardeleben, **B. Fang**, S. Gurumurthi, K. Pattabiraman, P. Rech, M. Sonza Reorda, Embedded tutorial paper, Proceedings of the International Symposium on Design Automation and Test in Europe (DATE), 2014.

[6] *Towards Application-aware Security and Reliability*, Ravishankar Iyer, Zbigniew Kalbarczyk, Karthik Pattabiraman, Wen-Mei Hwu, William Healey, Peter Klemperer and Reza Farivar, IEEE Security and Privacy (S&P) Magazine, 2007.

*(f) Patents*

[1] *Critical Memory,* with Benjamin Zorn and Vinod Grover, Microsoft Corporation, 2011. Granted 2016.

[2] *Critical Memory using Replication,* with Benjamin Zorn, Vinod Grover, Microsoft Corporation, 2011. Granted 2016.

[3] *Providing Hardware Resources having Different Reliabilities for Use by an Application***,** with Benjamin Zorn, Thomas Moscibroda and Song Liu, Microsoft Corporation, 2016. Granted 2020.

[4] *Leveraging On-Chip Variability,* Benjamin Zorn, Darko Kirovski, Ray Bittner, and Karthik Pattabiraman, Microsoft Corporation, 2016. Granted 2020.

*(g) Selected Software Artifacts Released (Most of these are released under a BSD/MIT/Illinois open source license)*

[1] *LLTFI:* LLVM-based fault injector for regular and ML programs. Available:

*https://github.com/DependableSystemsLab/LLTFI*

[2] *LLFI*: A fault injector based on the LLVM compiler: Available:

https://github.com/DependableSystemsLab/LLFI

[3] OneOS: Overlay Network Operating Systems

*https://github.com/DependableSystemsLab/OneOS*

[4] PC Meeting Web Dashboard: For running PC meetings - used for DSN'19 , DSN'20, DSN'21, HPDC'19, SRDS'22.

https://github.com/DependableSystemsLab/PCMeetingDashboar3