

VARUN GANDHI

Science and Engineering Complex, 4.421
Harvard University, Allston, MA 02134

vgandhi@g.harvard.edu
vargandhi.github.io

EDUCATION

- Ph.D., Computer Science, Harvard University**, Cambridge, MA Expected 2025
- **Thesis:** Programming Models and Isolation Mechanisms for Secure Remote Computation
 - **Committee:** Prof. Srinivas Devadas (MIT, Advisor), Prof. Stephen Chong (Harvard, Advisor), Prof. Margo I. Seltzer (UBC), and Prof. Eddie Kohler (Harvard)
- S.M., Computer Science, Harvard University**, Cambridge, MA 2022
- **Minor:** Public Policy, Harvard Kennedy School
 - **Thesis:** Rethinking Isolation Mechanisms for Datacenter Multitenancy
- M.Phil., Computer Science, University of Cambridge**, Cambridge, UK 2015
- **Thesis:** Mitigating OpenSSL Attacks in Mobile Devices
 - **Committee:** Prof. Alastair R. Beresford and Prof. Ross J. Anderson
- B.S., Computer Science, IIIT-Delhi**, New Delhi, India 2013
- Dean's Scholar
 - Undergraduate Student Visitor, Carnegie Mellon University, Pittsburgh, PA

CURRENT RESEARCH

My research is at the intersection of systems, computer architecture, and security, broadly centered around the design and application of hardware-enforced isolation mechanisms and programming models for verifiable computation to support secure multi-tenancy for datacenter workloads.

Varun Gandhi, Simon Langowski, Stephen Chong, and Srinivas Devadas.
"Rethinking Runtime Integrity Guarantees in Distributed AI Frameworks." In Progress

Varun Gandhi, Stephen Chong, and Srinivas Devadas.
"Rethinking Verifiable Execution for Confidential AI Compute." In Progress

SELECTED PUBLICATIONS AND PATENTS

Stefan Saroiu, **Varun Gandhi**, Alastair Wolman, and Landon Prentice Cox.
"Liveness guarantees in secure enclaves using health tickets." **U.S. Patent 12,067,111**. August 20, 2024

Stefan Saroiu, **Varun Gandhi**, Alastair Wolman, and Landon Prentice Cox.
"Automated recovery of far edge computing infrastructure in a 5g network." **U.S. Patent 11,900,127**. February 13, 2024

Varun Gandhi, Sarbartha Banerjee, Aniket Agrawal, Adil Ahmad, Sangho Lee, and Marcus Peinado.
"Rethinking System Audit Architectures for High Event Coverage and Synchronous Log Availability." In 32nd USENIX Security Symposium (**USENIX Security 2023**)

Varun Gandhi, and James Mickens.
"Rethinking Isolation Mechanisms for Datacenter Multitenancy." In 12th USENIX Workshop on Hot Topics in Cloud Computing (**HotCloud 2020**)

CONTRIBUTIONS ACKNOWLEDGED

Alessandro Acquisti, Ralph Gross, and Fred Stutzman.
"Face recognition and privacy in the age of augmented reality" **Journal of Privacy and Confidentiality**, 2014

INDUSTRY RESEARCH POSITIONS

Cloudflare Research Ph.D. Research Intern Mentors: Dr. Marwan Fayed and Thibault Meunier	<i>Austin, TX</i> Summer 2025
Cloud and Infrastructure Security Group, Microsoft Research Ph.D. Research Intern Mentors: Dr. Sangho Lee and Dr. Marcus Peinado	<i>Redmond, WA</i> Summer 2022
Intelligent Networked Systems, Microsoft Research Ph.D. Research Intern Mentors: Dr. Stefan Saroiu and Dr. Alec Wolman	<i>Redmond, WA</i> Summer 2021
Data Systems Group, Microsoft Research Pre-Doctoral Research Fellow Mentor: Dr. Philip Bernstein	<i>Redmond, WA</i> 2016-2017

TEACHING EXPERIENCE

Compilers (CS 153) Teaching Fellow for Prof. Stephen Chong	Harvard SEAS Fall 2023
Introduction to Distributed Systems (CS 262) Teaching Fellow for Prof. James H. Waldo	Harvard SEAS Spring 2023
Critical Thinking in Data Science (APCOMP 221) Teaching Fellow for Prof. Michael D. Smith	Harvard SEAS Spring 2020

INVITED TALKS

Harvard Graduate Women in STEM (HGWISE) Seminar, 2025	<i>Cambridge, MA</i>
Harvard Programming Languages Seminar, 2024	<i>Boston, MA</i>
32nd USENIX Security Symposium, 2023	<i>Anaheim, CA</i>
Microsoft Research Security Workshop, 2022	<i>Redmond, WA</i>
Microsoft Research Security Workshop, 2021	<i>Virtual</i>
12th Workshop on Hot Topics in Cloud Computing, 2020	<i>Virtual</i>

AWARDS AND HONORS

Nominee, IBM Ph.D. Fellowship, Harvard University	2024
USENIX Student Grant	2023
Harvard Derek C. Bok Certificate of Distinction in Teaching	2020
Harvard Ralph H. Watson Graduate Science and Engineering Fellowship	2017

SERVICE AND LEADERSHIP

Harvard AI Safety Student Team, Technical Member	2024-2025
Harvard CS-SPYS, Systems Seminar Group, Coordinator	2024
IEEE Security and Privacy, Shadow PC	2021
ACM EuroSys, Shadow PC	2021

SKILLS

Languages: C/C++, Rust, Python, Golang, Haskell, OCaml, Java, Lisp, Solidity, Circom, Verilog, Chisel, x86 Assembly

Technologies: Apache Spark, Ray, Hadoop, Docker, Kubernetes, git, AWS, Azure, Firesim, Linux, RISC-V, L^AT_EX