Saranya Vijayakumar

saranyav@andrew.cmu.edu • +1 (914) 648-0021 • 626 Hastings Street, Pittsburgh PA 15206

Education

Carnegie Mellon University — Pittsburgh

Ph.D., Computer Science — *Expected graduation 2026*

M.S., Computer Science Research — *2025 via Ph.D program*

Advisors: Professors Christos Faloutsos & Matt Fredrikson

Harvard University — Cambridge

A.B., Joint Concentration in Computer Science & Government — *2018*
Thesis: "Interpretability Through Interrogation: Fairness in the Context of Criminal Sentencing"
Bachelor's Advisors: Professors Cynthia Dwork & Jim Waldo

Conference Publications

[1] Prototype-Integrated Representation Learning for Novelty Detection
Saranya Vijayakumar, Christos Faloutsos, Matt Fredrikson
Under Review — *2025*

[2] Evaluating LLM-Supported Malware Evasion: A Red Team Benchmark for Code Obfuscation and Antivirus Bypass
Saranya Vijayakumar, Christos Faloutsos, Matt Fredrikson
Under Review — *2025*

[3] Leveraging Large Language Models for Enhanced Membership Inference and Reidentification in Topics API Analyses
Saranya Vijayakumar, Norman Sadeh
Under Review — *2025*

[4] Mechanistically Interpreting a Transformer-based 2-SAT Solver: An Axiomatic Approach
Nils Palumbo, Ravi Mangal, Zifan Wang, Saranya Vijayakumar, Corina Pasareanau, Somesh Jha
International Conference on Machine Learning (ICML) — *Vancouver, 2025*

[5] Aligned LLMs Are Not Aligned Browser Agents
Priyanshu Kumar, Saranya Vijayakumar, Elaine Lau, Tu Trinh, Zifan Wang, Matt Fredrikson
The International Conference on Learning Representations (ICLR)) (Paper) — *Singapore, 2025*

[6] Grounding Neural Inference with Satisfiability Modulo Theories
Saranya Vijayakumar, Zifan Wang, Kaiji Lu, Vijay Ganesh, Somesh Jha, Matt Fredrikson
NeurIPS (Spotlight) (Talk) — *Vancouver, 2023*

[7] CallMine: Fraud Detection and Visualization of Million-Scale Call Graphs
Mirela Cazzolato, Saranya Vijayakumar, Meng-Chieh Lee, Namyong Park, Catalina Vajiac, Christos Faloutsos
The Conference on Information and Knowledge Management (CIKM) — *Birmingham, 2023*

Workshop Publications and Conference Contributions

[1] Through the Lens of LLMs: Unveiling Differential Privacy Challenges
USENIX Conference on Privacy Engineering Practice and Respect — *Santa Clara, 2024*

[2] Anomaly Detection and Visualization of Large-Scale Call Graphs
AAAI-23 Demonstrations Program — *Washington DC, 2023*

[3] TgraphSpot: Fast and Effective Anomaly Detection for Time-Evolving Graphs
2022 IEEE International Conference on Big Data Industry and Government Program — *Osaka, 2022*

[4] Interpretability Through Interrogation: Fairness in the Context of Criminal Sentencing — *2018*

[5] Algorithmic Decision-Making — *Harvard Political Review, 2017*

[6] A Worldwide Survey of Encryption Products
Bruce Schneier, Kathleen Seidel, and Saranya Vijayakumar. — *Berkman Center Research Publication, 2015*

Invited Talks

[1] 17-416/17-716, AI Governance (Masters/PhD level) — Carnegie Mellon University
Guest Lecture on LLM Security and Alignment — *Spring 2025*

[2] 17-331/17-631, Information Security, Privacy, Public Policy — Carnegie Mellon University
Guest Lecture on Vulnerabilities of ML — *Fall 2024*

[3] 17-416/17-716, AI Governance (Masters/PhD level) — Carnegie Mellon University
Guest Lecture on ML Security and Privacy — *Spring 2024*

[4] 17-331/17-631, Information Security, Privacy, Public Policy — Carnegie Mellon University
Guest Lecture on ML Security and Adversarial Robustness — *Fall 2023*

[5] Dagstuhl Seminar: Machine Learning and Logical Reasoning: The New Frontier — Germany, 2022

[6] CRA-WP Grad Cohort 2022 — New Orleans, 2022

[7] Cylab Partners Conference — Pittsburgh, 2022

[8] Alumni Committee for Harvard Women in Computer Science — 2022

Selected Fellowships and Awards

Best Poster Award — New Orleans, 2024

GFDS Program — NSA

CRA-W Grad Cohort for Women — New Orleans, 2022

National Defense Science & Engineering Graduate Fellowship Program — Army Research Office, 2022 – 2025

Tech in the World Fellow, Partners in Health — Lima, 2018

The Ernst Kitzinger Prize, Lowell House — Harvard University, 2018

Microsoft Scholarship, Grace Hopper Celebration of Women in Computing — Orlando, 2017

Director's Internship, Harvard Kennedy School Institute of Politics — New York, 2015

Teaching Experience

17-331/631, Information, Security, Privacy & Policy (Masters level) — Carnegie Mellon University
Teaching Assistant — *Fall 2023*
Created homework assignments, graded assignments, and held office hours. Gave a lecture on ML/security. Course included applied cryptography, authentication & security protocols, web & network attacks, and ML security & privacy.

15-294, Rapid Prototyping (undergraduate level) — Carnegie Mellon University
Teaching Assistant — *Spring 2023*
Taught lecture, graded assignments, and redesigned the syllabus and course schedule to accommodate interactive learning and new assignments. Course focused on SolidWorks.

15-394, Intermediate Rapid Prototyping — Carnegie Mellon University
Teaching Assistant — *Spring 2023*
Taught lecture, graded assignments, and redesigned homework assignment for students to design automata in SolidWorks with linear bushing, rotational motion, and rendering/motion analysis components. Course focused on Rhino, Grasshopper, and Kangaroo 2 physics-based simulation.

Future Faculty Program — Carnegie Mellon University
Participant — *2021 – 2023*
Eberly Center for Teaching Excellence & Educational Innovation. Participated in seminars aimed at helping graduate students develop and document their teaching skills in preparation for a faculty career. Completed a lesson plan review and teaching observation with Eberly experts; redesigned Rapid Prototyping syllabus; completed a teaching philosophy project

Industry Collaborations

Inria/Proof techniques for security protocols (PESTO)
Nancy, France

Visiting Scholar *October – November 2024*

Formal verification project: Studying the security properties and transcript consistency of a secure messaging platform used by the French government. Studied under Charlie Jacomme and Steve Kremer.

Mobileum/Adaptive, Intelligent and Distributed Assurance Platform (AIDA)
Braga, Portugal

Collaborator *2021 – 2026*

- Collaborated with Mobileum, a global provider of telecom analytics solutions, on industry-scale fraud detection research. Mobileum offers risk management, roaming, and network analytics to over 900 telecom operators worldwide.
- Analyzed real-world call graph data to develop scalable anomaly detection techniques.
- Published multiple peer-reviewed publications and demos, including deployment-ready systems for detecting telecom fraud on million-scale graphs.

Goldman Sachs/Algorithmic Trading (GSET)
New York

Data Scientist, Electronic Trading *2018 – 2021*

- Covered quantitative hedge funds and asset managers in a client-facing data science role.
- Performed trade cost analyses using Python, Slang (Goldman's proprietary language), SQL, and KDB Q and communicated algorithmic recommendations to stakeholders.
- Designed and implemented experiments with the software engineering team & strategized on new features and methodologies.
- Published research pieces sent to over one thousand clients, focusing on market microstructure and electronic trading statistics.

Beto O'Rourke for U.S. Senate
Austin

Data Scientist, Distributed Organizing *Summer 2018*

- Collaborated with the data team and campaign director to create Python models predicting voter turnout and support.
- Presented my findings on persuasion tactics and priority counties for grassroots organizing to the chief of staff.
- Strategized student turnout and started grassroots offices around Texas.
- Canvassed in San Antonio with the Field Director to organize and fundraise.

Booz Allen Hamilton
Virginia Square, Herndon & Boston, MA

Cybersecurity Intern *Summer 2017*

- Worked on autonomous swarming behavior in team of six.
- Created the functionality for semi-autonomous navigation of the ground robots in ROS and using Python and C++.
- Investigated and created prevention methods against security threats by creating a proof-of-work demonstrating how a potential hacker could use GPS spoofing to override a military-grade GPS-enabled robot. Implemented PCA for GPS anomaly detection.

Digital Solutions Intern *Winter 2017*

- Collaborated with intern team to perform impact analysis on the MBTA using data provided by the MBTA to evaluate pricing strategies based on revenue and equity.
- Studied the fairness of public transit fares in Boston by examining surge pricing, subsidies to low-income individuals and students, and distance-based fares.

Conference Service

NeurIPS, Reviewer	NeurIPS 2025
ICML, Reviewer	ICML 2025
ICLR, Reviewer	ICLR 2025
KDD, Reviewer	KDD 2025
ICLR, Reviewer	ICLR 2024
NeurIPS, Reviewer	NeurIPS 2023 Workshop: New Frontiers in Graph Learning
NeurIPS, Reviewer	NeurIPS 2024
Peer Reviewer	Georgetown Center for Security and Emerging Technology (CSET), 2024

Selected Service

Women in CSD, Founder — Carnegie Mellon University, 2022 – Present

- Organizer of a weekly lunch and other programming for over 90 women and non-binary members of Computer Science Department and broader School of Computer Science.

Introductory Course, Organizer — Carnegie Mellon University, Summer 2022

- Organized Introductory Course events, which introduces new Ph.D. students to the department.

Alumni Association Executive Committee, Member — Riverdale Country School, 2022 - Present

- Sustain loyalty and enthusiasm among peers by developing programs, initiatives, and events that promote the general welfare of the school and by encouraging alumni participation in activities and philanthropic support.
- Class Correspondent (2014 - present): Solicit class notes & serve as part of Reunion Committee

Harvard University, Member — Boston & New York, 2018 - Present

- Schools & Scholarships Committee (2018 - Present): interview Harvard College applicants yearly
- Participation chair for class of 2018 fifth year reunion (2023)

Cyber Defense Club, Finance & Communications Chair — Harvard University, 2017 – 2018

- Qualified for the New England regional finals of the National Collegiate Cyber Defense Competition.
- Led weekly meetings.

Girls Who Code, Leader — Harvard University, 2016 - 2017

- Wrote the curriculum and led classes for 20 middle school girls, coordinated female Harvard mentors.
- Collaborated with Harvard Kennedy School and Business School students to make Girls Who Code more inclusive to girls in different parts of Boston.
- Worked with the Harvard EdLabs to host programs in Allston, MA.

Digital Literacy Project, Education & Community Outreach Chairs — Harvard University, 2014 - 2017

- Taught computer science weekly at underserved schools in Boston.
- Expanded the curriculum to create second course in HTML and CSS and created partnerships with Boston public schools.

Skills

Technical specialties: Java, Python, C, R, Tensorflow, Sklearn, ROS, HTML+CSS, PHP, Swift, Git, Parse, OpenMRS, Stata, LaTeX. Linux administration skills: bash, Apache, MySQL, VMware, & KDB Q.

Natural languages: English, Tamil, Spanish (*working proficiency*), Japanese (*limited working proficiency*).