# Aditya Saligrama

(774) 270-7173 | aditya@saligrama.io | saligrama.io | github.com/saligrama | linkedin.com/in/saligrama

## Education

**Stanford University** Sep 2020 – Jun 2024

*B.S. and M.S. Candidate in Computer Science | GPA 3.9* *Stanford, CA*

- Coursework includes Cryptography, Computer and Network Security, Modern Internet Infrastructure, Parallel Computing, Embedded Operating Systems, Compilers, Algorithms, Machine Learning, Natural Language Understanding, Blockchain

## Experience

### I. Work experience

**Software Engineering Intern** at **Lacework** Jun 2022 – Sep 2022 at *San Jose, CA*

- Engineered end-to-end virtualization of benchmarking system on Spark, reducing data import time by 20x vs. Snowflake
- Contributed enhanced Snowflake and Spark parsing support to SQLGlot, an open-source SQL parser and transpiler; 3 PRs merged

**Engineering Intern** at **Uptycs** Nov. 2020 – Apr. 2021 at *Waltham, MA*

- Wrote and deployed production feature to Osquery monitoring software to inspect and detect malware in Java packages
- Code now open-source; functionality used to detect and patch client software with Log4Shell vulnerabilities (10.0 severity CVE)

**Security Consultant** Jun 2022 – Present

- Evaluating and strengthening initial setup and ongoing security of tech stack (incl. Firebase, AWS Lambda) for Stanford startups

**Research Science Institute Intern** at **Akamai Technologies** Jun 2019 – Aug 2019 at *Cambridge, MA*

- Engineered realtime garbage collection monitoring system for Go programs with per-thread granularity
- Detailed flagging of stop-the-world pauses used for profiling and boosting performance across Akamai Labs codebase

### II. Teaching, leadership, and competition experience

**Teaching Assistant** at **Stanford University** Sep 2022 – Dec 2022 at *Stanford, CA*

*TA for INTLPOL 268 (Hack Lab) taught by Alex Stamos, Riana Pfefferkorn*

- Taught two discussion sections (44 students) for Stanford's intro cyber security, law, and policy course; 170 students enrolled
- Built course GCP infra; created labs including encrypted WiFi PCAP cracking and leaking data from insecure Firebase chat app

**Vice President and CCDC Linux Lead** at **Stanford Applied Cybersecurity** Jan 2021 – Present at *Stanford, CA*

- Securing systems against external red teams in CCDC and DOE Cyberforce competition environments; 3rd place national finish
- Found and disclosed security vulnerabilities to 10+ startups, leading to data-protecting fixes; work covered in Stanford Daily
- Directed workshops on security basics for beginners and application security for entrepreneurs
- Presented on vuln-finding in Firebase apps; contributed Google OAuth login support to open-source Firebase exploration tool

### III. Research projects and experience

- **Software patching dynamics** *(Stanford)*: Exploring how and when organizations patch vulnerable software on the internet
- **Parallel, human-interpretable ML** *(Harvard)*: Achieved linear speedup on CORELS increasing tractability of 250k+ sample datasets; short paper featured at SysML 2018 (57% acceptance rate); implemented R API and Node.js web UI
- **Rust concurrency evaluation** *(MIT)*: Developed fast, lock-free Rust concurrent hashmap with 140+ stars on GitHub
- **Adversarial machine learning** *(MIT)*: Designed ensemble schemes that increase accuracy while preserving adversarial robustness vs. single model; paper presented at ICLR 2020 workshop (44% acceptance rate)
- **Political polarity detection** *(Independent)*: Implemented novel two-step classification scheme for political bias increasing accuracy on long articles by 13%; paper published at AAAI 2020 student abstract program (48% acceptance rate)
- **Virtual assistants for customer support queries** *(Stanford)*: Created virtual assistant pipeline to classify customer support requests with GPT-3 data augmentation; increased sample data size by 4x

## Skills

- **Languages**: C, C++, Python, Java, Go, Rust, JavaScript, HTML/CSS, SQL, ARM and x86 assembly, Bash, Markdown, LaTeX
- **Frameworks**: Django, Node.js, React.js, Next.js, PyTorch, Tensorflow, Hugo, Bootstrap
- **Technologies and Developer Tools**: Git, Unix, Docker, Packer, Osquery, AWS, GCP
- **Security Tools and Techniques**: Burp Suite, Wireshark, Metasploit, Network Scanning, Security Research, Vulnerability Disclosure

## Publications

**A. Saligrama**, G. Leclerc. Revisiting Ensembles in an Adversarial Context: Improving Natural Accuracy. *ICLR:TML'20*, 2020.
**A. Saligrama**. KnowBias: Detecting Political Polarity in Long Text Content. *AAAI:SAP'20*, 2020.
**A. Saligrama**. KnowBias: A Novel AI Method to Detect Polarity in Online Content. *arXiv:1905.00724*, 2019.
**A. Saligrama**, A. Shen, J. Gjengset. A Practical Analysis of Rust's Concurrency Story. *arXiv:1904.12210*, 2019.
N. Larus-Stone, E. Angelino, D. Alabi, M. Seltzer, V. Kaxiras, **A. Saligrama**, C. Rudin.
Systems Optimizations for Learning Certifiably Optimal Rule Lists. *SysML (now MLSys) Conference*, 2018.

## Selected Awards and Honors

- 3rd place team, National CCDC, 1st place, Western Regional CCDC (2022); 2nd place, NCCDC Wild Card and WRCCDC (2021)
- USA Computing Olympiad, Gold Division (2018 – 2020)