

Chaitanya Rahalkar

Personal Website: rahalkar.dev

GitHub: github.com/chaitanyarahalkar

LinkedIn: [/in/chaitanyarahalkar](https://in/chaitanyarahalkar)

Email : chaitanyarahalkar4@gmail.com

Research: [Google Scholar](#)

EDUCATION

- **Georgia Institute of Technology** Atlanta, GA
Master of Science in Cybersecurity — GPA - 4/4 January 2021 – December 2022
- **Savitribai Phule Pune University** Pune, India
Bachelor of Engineering in Computer Engineering — GPA - 9.6/10 July 2016 – June 2020

EXPERIENCE

PROFESSIONAL EXPERIENCE

- **OmniChat AI (tryomni.chat)** Remote, US
Founder & CEO Aug 2023 – Present
 - Built a multimodal autonomous-agent platform + unified API (text/image/audio/video) and shipped agent engine, no-code builder, and self-serve onboarding/pricing/upgrade flows for enterprise customers.
 - Designed and operated the multimodal infrastructure (vision/speech/LLM) with sub-200ms latency and 99.9% uptime; instrumented analytics to improve activation, retention, and expansion.
 - Drove 21K+ beta signups and \$132K+ enterprise API revenue last year and raised 40,000 USD/30,000GBP in funding in our pre-seed round.
- **Block Inc. (f.k.a. Square Inc.)** Remote, US
Software Security Engineer (L5) June 2024 – Present
 - Led security data-platform modernization and logging cost optimization across GCP/AWS, delivering approximately \$1M annualized savings (93% GCS storage reduction/\$800K) via lifecycle redesign, Pub/Sub + BigQuery efficiencies, and decommissioning legacy pipelines.
 - Owned security data lake + FleetDM (device management + security platform) modernization: migrated 15,000+ hosts to vendor-managed FleetDM in AWS, built Terraform infra + GitOps query management, enabled Osquery in AWS AMIs for EC2 VMs, and improved pipeline reliability by replacing Cloudproxy with GCP↔AWS PrivateLink (\$50K/year savings) while expanding log coverage into Panther SIEM system.
- **Praetorian Security** Remote, US
Security Engineer III January 2023 - May 2024
 - Conducted 100+ in-depth security assessments across the company's SaaS platform, ensuring product resilience, compliance readiness, and alignment with customer security expectations.
 - Designed and refined 50+ threat models and product security reports, directly shaping product roadmaps and influencing engineering priorities.
 - Identified and remediated 200+ critical vulnerabilities across web, mobile, and connected device applications, strengthening the security of flagship products used by enterprise and consumer clients.
 - Built and enhanced core modules for internal security products, including a vulnerability management and assessment platform and a source code secrets detection tool, embedding scalable security capabilities directly into the product ecosystem.
- **Meta (previously Facebook)** Seattle, WA
Security Engineering Intern May 2022 - August 2022
 - Designed and developed coverage-guided fuzzing harnesses using LLVM Libfuzzer for Meta's Continuous Fuzzing platform, Lionhead. Identified and reported over 10 security vulnerabilities in Meta's production code and tooling systems through fuzzing, code reviews, and audits.
 - Assisted in the development of an automated fuzzing harness generation system, enhancing the scope of coverage-guided fuzzing across 100,000+ API endpoints, and demonstrating scalability and efficiency in security testing.

- Conceptualized and designed a comprehensive fuzzing metrics system and associated visualization dashboard to provide insight into coverage and fuzzing performance, aiding in strategic decision making and process optimization.

- **BosLeo LLC**

Pune, India

Security Engineer bosleo.com

July 2020 - July 2021

- Worked on the development of Anti-Virus, Anti-Phishing, Software Sandboxing, and Application Firewall components, strengthening the company's Endpoint Protection Platform (EPP) and directly improving endpoint threat prevention coverage by 35%.
- Architected and implemented a network-based intrusion detection system (NIDS) with advanced intrusion analytics, successfully simulating, detecting, and analyzing 100+ attack scenarios; reduced false positives by 20% and enabled proactive threat detection at scale.
- Designed and modeled a software-defined perimeter prototype aligned with Zero Trust Network Architecture principles, enhancing secure access management and reducing unauthorized lateral movement risks across enterprise environments.

- **RhythmFlows Solutions Pvt. Ltd.**

Pune, India

Security Software Engineer rhythmflows.com

Jan 2019 - Jan 2022

- Built a configurable multi-way reconciliation platform with rule-driven transforms; validated best-in-class throughput (180M transactions processed in 12 hours) with audit-friendly traceability.
- Added reconciliation analytics for quality/anomaly triage
- Performed security audits across backend and Cordova iOS/Android for a video-on-demand platform serving 500k+ users.

CONFERENCE REVIEWING AND JUDGING

- International Conference on Cyber Warfare and Security 2025 (ICWS 2025) ([link](#))
- The Intelligent Cybersecurity Conference 2025 (ICSC 2025) ([link](#))
- International Conference on Electrical, Computer and Energy Technologies (ICECET 2025), Paris – Session C-IX: Big Data & Cryptography ([link](#))
- International Conference on Artificial Intelligence, Computer, Data Sciences and Applications (ACDSA 2025), Antalya
- Globee Cybersecurity Awards ([link](#))

ACADEMIC WORK

1. Rahalkar, Chaitanya, and Anushka Virgaonkar. "Reconciling Safety and Privacy: A Systematic Review of Moderation in End-to-End Encrypted Messaging." 2025 13th International Symposium on Digital Forensics and Security (ISDFS), IEEE 2025, pp. 1–7. ([paper](#)).
2. Virgaonkar, Anushka, and Chaitanya Rahalkar. "On Adding Context to Automated .NET Malware Analysis." *International Conference on Information Warfare and Security*, vol. 20, 24 Mar. 2025, pp. 492–500. ([paper](#)).
3. Rahalkar, Chaitanya. "A Diamond Model Analysis on Twitter's Biggest Hack." International Journal of Scientific Research in Science, Engineering and Technology, vol. 11, no. 6, Technoscience Academy, December 2024, pp. 315–320 ([paper](#)).
4. Rahalkar, Chaitanya, and Anushka Virgaonkar. "Achieving Secure, Transparent, and Performant File Transfer: A Relay-Based PAKE Protocol" 6th International Conference on Electrical, Computer and Energy Technologies (ICECET 2025) ([paper](#))
5. Rahalkar, Chaitanya, and Anushka Virgaonkar. "Evolution of the Tor Network: An Empirical Analysis of Usage Patterns and Infrastructure" The Intelligent Cybersecurity Conference (ICSC2025), IEEE 2025, pp. 312-318. ([paper](#))

6. Rahalkar, Chaitanya, and Anushka Virgaonkar. "Evaluating Privacy-Preserving Strategies in Bitcoin and Beyond" The Intelligent Cybersecurity Conference (ICSC2025), IEEE 2025, pp. 162-168. ([paper](#))
7. Rahalkar, Chaitanya. "Automated Fuzzing Harness Generation for Library APIs and Binary Protocol Parsers." arXiv preprint arXiv:2306.15596, 2023 ([paper](#)).
8. Rahalkar, Chaitanya & Virgaonkar, Anushka & Gujar, Dhaval & Patkar, Sumedh. (2020). End-to-End Lung Cancer Diagnosis on Computed Tomography Scans using 3D CNN and Explainable AI. International Journal of Computer Applications. 176. 1-6. 10.5120/ijca2020920111. ([paper](#))
9. Rahalkar, Chaitanya, and Dhaval Gujar. "Content Addressed Peer-to-Peer File System for the Web with Blockchain-based Metadata Integrity." IEEE International Conference on Advances in Computing, Communication and Control. IEEE, 2019 ([paper](#))
10. Oak, Rajvardhan, Chaitanya Rahalkar, and Dhaval Gujar. "Poster: Using Generative Adversarial Networks for Secure Pseudorandom Number Generation." Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security. ACM, 2019 ([paper](#))
11. Rahalkar, Chaitanya, and Dhaval Gujar. "A Secure Password Manager." International Journal of Computer Applications 975: 8887. ([paper](#))

BOOKS

- Cybersecurity for Startups: Your Blueprint for Growing Securely in the Digital Age [securityblueprint.store](#), [Amazon Books](#)

INVITED TALKS & PRESENTATIONS

1. Breaking Down Buffer Overflow Exploits: From Vulnerability to Patch (BSides SLC Security Conference, 2025) - [session](#), [video](#), [slides](#)
2. AI-Driven Phishing Attacks (SANS AI Cybersecurity Summit, 2025) - [slides](#), [video](#), [credentials](#)
3. Killer CLIs: Building platform tools developers actually want to use (PlatformCon, 2025) - [session + video](#), [slides](#)
4. Scaling DevOps in Complex Environments: Challenges, Failures, and Successes (DevOpsDay Austin, 2025) - [session](#), [video](#), [slides](#)
5. The Linguistics of Large Language Models: What Your AI's Mistakes Reveal and Navigating AI Security: Protecting Your Organization in the Era of Generative AI (Tech STL FinTech Summit, 2025) - [session i](#), [slides i](#), [session ii](#), [slides ii](#)
6. Secure Coding Training: A Critical Foundation for Modern Security (Cleveland Convene Security Conference, 2025) - [session](#)
7. Agentic CI/CD: from Pull Request to Production without the Paper Cuts (GitNation AI Coding Summit, 2025) - [session](#)
8. Kubernetes Runtime Security (CNCF Kubernetes Austin, 2025) - [session](#)
9. Supply Chain Poisoning: Breaking Trust in Modern Software Delivery (BSides Nashville Security Conference, 2025) - [session](#), [slides](#)
10. The Linguistics of Large Language Models: What Your AI's Mistakes Reveal (AI Saturday Houston #1108, 2025) - [slides](#), [session](#)
11. Weaving Zero-Trust into Web DNA: Architecting the Unbreachable (2000K Tulsa Developer Conference, 2025) - [session](#), [slides](#)

MENTORSHIP

- Mentors in Tech Mentor, 2024-2025 - [credential](#)
- Software Development Mentor, CodeDay 2025 - [credential](#)
- Develop for Good Program Mentor, 2025 - [credential](#)