




Sahil Wadhwani

Los Angeles, CA | wadhwanisahil9@gmail.com | +1 (213) 275-8066 |  www.sahilw.dev |  Sahil Wadhwani |  Sahil Wadhwani

Education

University of Southern California, MS in Computer Science

Jan 2025 – Dec 2026 (*Expected*)

- GPA: 3.66 / 4.0

- **Coursework:** Digital Forensics, Applied Cryptography, Database Systems, Web Technologies, Algorithms

Pune University, Bachelor of Engineering in Computer Science

Jun 2020 – May 2024

- GPA: 9.04 / 10.0

- **Coursework:** Computer Networks & Security, Blockchain Technology, Systems Programming & Operating Systems, Machine Learning & Applications, Software Engineering & Project Management

Experience

Associate Software Developer, Coditas – Pune, India

Jan 2024 – Dec 2024

- Developed **secure, production-grade REST APIs in Go (Golang)** for a live stock trading platform, handling 10,000+ daily requests with **low-latency, real-time execution**.
- Integrated **Redis caching** to optimize analytics queries, reducing response time by **25%** and improving system reliability under high load.
- Refactored fragmented microservices into a **unified, access-controlled watchlist service** using PostgreSQL, reducing the **attack surface** and improving backend maintainability by enforcing **secure design patterns at scale**.

Software Development Intern (Security Engineering), EzConverse Media – India

Aug 2023 – Nov 2023

- Built a **Vulnerability Management System** using React.js, Node.js, and MongoDB. Integrated Nmap and Nikto to **automate scanning**, ingest CVEs, and **visualize threats in real time** with Chart.js.
- Designed **secure-by-default REST APIs** with **input validation, role-based access control (RBAC)**, and **JWT/Firebase Auth**, aligned with **secure SDLC principles** for authentication and authorization.
- Participated in **threat modeling** and **secure code reviews**; performed **vulnerability assessments** using Burp Suite, Metasploit, and Nmap, leading to the remediation of **10+ critical security flaws**.
- Enhanced dashboard telemetry with **audit trails, severity tags**, and **scan timestamps**, reducing **incident triage time by 30%** and improving **post-incident forensics at scale**.

Skills and Certifications

Programming Languages: Python, Go, Java, JavaScript, TypeScript, C++ , Bash, SQL

Security Tools & Technologies: Nmap, Nikto, Metasploit, Burp Suite, Wireshark, Snort, Splunk, Nessus, OpenSSL, JWT, OAuth 2.0, Firebase Auth, Secure API Design

Security Concepts & Practices: Encryption (AES, TLS), Authentication Protocols, Network Security, Threat Modeling, Secure Software Development Lifecycle (SDLC)

Cloud, DevOps & Infrastructure: GCP (IAM, VPC, Cloud Armor), AWS (EC2), Docker, Jenkins, Redis, PostgreSQL, MongoDB, Git

Frameworks & Development: React.js, Node.js, Next.js, Express, Flask

Certifications: CEH v12, CCNA, TryHackMe: Security Engineer Path, AWS Security Fundamentals

Technical Projects

AI-Powered Threat Hunting & Incident Response Platform

[\[Source Code\]](#)

- Engineered an end-to-end security platform using **FastAPI, PostgreSQL, Redis, Docker**, and **Next.js** to ingest & normalize logs, apply **deterministic YAML rules + ML-based anomaly detection**, and enrich with **GeoIP/threat intel**, enabling real-time detection of brute force, geo-anomaly, and rare admin actions.
- Built **SOC-ready workflows** with **JWT auth (Argon2id)**, RBAC, case management, and **one-click responders** (block IP, disable account), exposed via a **dashboard & events explorer** with drill-downs, timelines, and explainable AI insights.

Certificate Verification using Blockchain

[\[Journal Publication\]](#) [\[Source Code\]](#)

- Designed a **decentralized certificate validator** with **Solidity, IPFS**, and **cryptographic signature verification** for data integrity and provenance.
- Implemented **RBAC with audit logs and revocation**; deployed a **Dockerized Streamlit DApp** with **Web3.py** and Firebase Auth.