

Saurabh Mahapatra

Full Stack Engineer

CONTACT

Gurgaon, India | +91 7768917067 | saurabhm121102@gmail.com | github.com/saurabhm02 | linkedin.com/in/saurabhm02

SKILLS

Languages: Python, Go, Java, JavaScript, TypeScript, SQL

Frontend: React 18, Next.js, TypeScript, Context API (state management), Component-Based UI Development

Backend: FastAPI, Spring Boot, Node.js, REST APIs, Prisma ORM, JWT, Microservices, WebSockets, Full-Stack Development, Backend Development

Database: PostgreSQL, MongoDB, Redis

Cloud / DevOps: AWS (Lambda, SQS, Step Functions, EventBridge, CDK, S3), Docker, Serverless, CI/CD

AI / ML: LLMs (OpenAI GPT-4, Anthropic Claude, Google Gemini), Computer Vision, Semantic Search, Vector Embeddings, Prompt-Injection Defense, Multi-modal Pipelines

Tools & Practices: System Design, Distributed Systems, Multi-tenant Architecture, Multi-tenant Data Isolation, Data Structures & Algorithms (DSA), OOP, Git, Agile, Data Pipelines, Message Queues, Application Security, Testing (Go race-detector tests, k6 load testing), Monitoring & Observability (Prometheus)

EDUCATION

Lovely Professional University - B.Tech, Computer Science and Engineering

2021 - 2025 | Phagwara, Punjab | GPA: 8.2 / 10

EXPERIENCE

Marxx.ai - Software Engineer

Sep 2025 - Present | Gurgaon, India

- Owned the core Python/FastAPI backend and data-ingestion layer as one of the first engineers, processing 1M+ Meta ad records daily at under 3-minute end-to-end latency.
- Architected the FastAPI backend for a full-stack AI ad-intelligence SaaS platform integrating a React 18/TypeScript frontend, scaling it to 20+ clients including Spinny and Hero and driving INR 1.5L/month in recurring revenue.
- Designed serverless AWS pipelines with Lambda, SQS, and Step Functions, ingesting data from 500+ brands daily with schema validation and structured logging for reliability.
- Led integration of 5 LLM providers (GPT-4, Claude, Gemini) and vision models with the founders, shipping semantic search and AI creative analysis to 20+ clients.

Recur Club - Software Developer Intern

Aug 2024 - Aug 2025 | Gurgaon, India

- Engineered an ETL pipeline in Java, AWS Lambda, and Node.js to run AML, PEP, and sanctions checks on PAN/DIN records, cutting verification time 65% (45 to 15 min) across 800+ monthly checks.
- Developed a Groovy Backend-for-Frontend service with the Aggregator pattern, merging 4 API calls into 1 per page view and cutting page load from 2s to 1.4s (25% fewer network calls).
- Created a Python/Flask monitoring platform with the staff engineer and CTO to score company profiles and trigger Slack alerts on failures, saving analysts ~14 hrs/week (70%).
- Delivered a document-processing pipeline for AICA (Recur Club's AI Credit Analyst) to handle 5,000+ borrower documents - Aadhaar, PAN, and financial records - during underwriting.
- Diagnosed and fixed data discrepancies in the bank-ingestion system on live client support calls, keeping underwriting data accurate in real time.

PROJECTS

Distributed Rate Limiter | Go, Redis, PostgreSQL, Docker, Prometheus | GitHub

- Built a multi-tenant rate limiter in Go using Token Bucket and Sliding Window algorithms with atomic, race-safe Redis Lua scripts, sustaining sub-1.5ms p95 latency at 2,000 req/s across allow and deny paths (load-tested with k6).
- Exposed a documented, read-only config API with SHA-256-hashed keys and Prometheus metrics, verifying correctness with Go race-detector tests.

AdmitDesk | Next.js, React, PostgreSQL, Prisma, AWS S3 | Live · GitHub

- Built the AdmitDesk frontend end-to-end in React/Next.js - UI components, page layouts, and state management via Context API/hooks - powering self-serve college signup and applicant triage workflows for admissions staff, on top of a PostgreSQL/Prisma backend.
- Enforced tenant data isolation with branded TypeScript ID types at the repository layer, eliminating cross-tenant data leakage at compile time.
- Integrated an LLM-powered assistant (Anthropic/OpenAI) with a custom prompt-injection defense for per-applicant Q&A, and added rate limiting that caught a header-spoofing vulnerability before launch.