

Prathamesh Kalamkar

Backend & AI Infrastructure Engineer

Dublin, Ireland prathamesh7744@gmail.com github.com/prathamesh-git9 linkedin.com/in/prathamesh-kalamkar
research and engineering portfolio

PROFILE

Backend engineer with 3.5+ years across Java, Spring Boot, Python, REST APIs, production support, and AI workflow infrastructure. Builds reliable tool-execution systems with explicit authority, idempotency, crash recovery, validation, observability, and deterministic tests. Current research examines whether security oracles used to evaluate AI-generated code measure executable behaviour or superficial form.

EXPERIENCE

Independent Software Engineer — AI and Automation Systems Jan 2025–present

- Built Python services and workflow engines for tool-calling agents with structured outputs, durable state, retries, validation, human-review gates, and evidence-rich audit records.
- Developed GitHub-integrated developer tooling and OpenAPI migration infrastructure with least-privilege access, signed provider intent, bounded source transforms, and fail-closed coverage reporting.

Software Engineer — matriXploit Pvt. Ltd. Jun 2022–Jul 2024

- Built and maintained backend services using Java, Spring Boot, Python, SQL, and REST APIs; delivered features, production fixes, authentication refactors, diagnostics, and regression checks.
- Worked with QA and support teams on root-cause analysis, code review, release readiness, and production follow-up across shared systems.

Software Engineer Intern — PhysicsWallah Oct–Dec 2024

Implemented Java and Spring Boot backend features, investigated API behaviour, and supported testing and release readiness for high-usage product workflows.

Technical Support Engineer — matriXploit Pvt. Ltd. Jan–Jun 2022

Investigated application failures through SQL, logs, reproducible cases, and structured escalation; maintained reusable troubleshooting evidence for engineering teams.

SELECTED ENGINEERING AND RESEARCH

SODA security-oracle benchmark

Reproducible construct-validity audit: 96 execution-labelled variants plus 140 real CVE fix pairs from 65 projects; CI, provenance, frozen protocol, and public v0.1.0 artifact.

PatchPilot

Provider-to-customer API migration system built for YC's Self-Maintaining APIs request: fans signed releases through repository-scoped GitHub App tokens, verifies customer-pinned keys, generates bounded JS/TS/Python patches, and opens reviewable PRs. 118 tests.

Effect Broker

Durable correctness boundary for side-effecting agent tools using stable intent, idempotency contracts, authoritative reconciliation, crash recovery, and explicit unknown outcomes.

Agent Redteam

Authorised adversarial testing and runtime guardrails for LLM agents with planted-evidence oracles, recomputable risk vectors, causal proof records, and offline regression suites.

EDUCATION

MSc Cybersecurity, First Class Honours — Dublin Business School 2024–2025

BSc Computer Science, First Class — Savitribai Phule Pune University 2021–2024

TECHNICAL SKILLS

Backend	Python, Java, Spring Boot, FastAPI, REST APIs, SQL, PostgreSQL, SQLite
AI systems	tool calling, MCP, agent workflows, structured outputs, RAG, evaluation harnesses, guardrails
Reliability	idempotency, durable execution, event sourcing, retries, audit trails, observability, pytest
Platform	GitHub Actions, Docker, Kubernetes, AWS, Azure, Terraform, CI/CD

Project evidence, limitations, reproducible commands, and source repositories are linked from the portfolio. Research artifacts are not represented as peer-reviewed publications.