

Pratham Panchariya

AI Engineer

Jaipur, Rajasthan, India • +91-7976614633 • prathampanchariya@gmail.com • linkedin.com/in/prathampanchariya/ • github.com/pratham5456

AI Engineer with hands-on experience securing production LLM and agentic systems — implementing guardrails, prompt filtering, output validation, and governance automation. Proven at mitigating AI risks (prompt injection, hallucinations, data leakage) with an enterprise compliance mindset.

WORK EXPERIENCE

SDE II | Founding AI Engineer

March 2023 – Present

GrackerAI

Embedded responsible AI controls into runtime LLM/agentic systems — designing guardrails, enforcing governance through code, and ensuring enterprise-grade safety and compliance across all AI applications.

- Implemented Guardrails AI for LLM output validation, prompt filtering, and misuse protection across production systems, reducing hallucination rates and mitigating prompt injection vulnerabilities
- Designed and enforced AI governance controls through code and automation; defined safety patterns and policy-as-code rules applied consistently across all AI agents in production
- Built audit trails and traceability mechanisms for AI agent decisions, providing full forensic visibility and meeting enterprise compliance requirements
- Identified and mitigated AI risk scenarios including prompt injection, data leakage, and model hallucinations across LLM-powered workflows; advised on failure modes and failure recovery strategies
- Built Kveeky (kveeky.com) and Gracker (gracker.com): AI platforms using React.js, FastAPI, Next.js with integrated safety controls — 500+ voices, 100K+ monthly visitors
- Developed MojoAuth (mojoauth.com) and SSOJet (ssojet.com): Enterprise IAM systems with OTP auth (Email, Phone, WhatsApp, TOTP), SSO (SAML, OIDC, SCIM) — demonstrating deep enterprise security and approval workflow experience
- Led AI-powered applications serving 500K+ users across 200+ countries, ensuring responsible AI usage, content safety, and compliance at scale

Back-end Developer

September 2022 – March 2023

FunctionUp

Focused on server-side development and API integration using Python and Node.js, building robust backend systems for AI-powered applications.

- Developed Python and Node.js backend applications with server-side optimization for AI model integration
- Built scalable backend architectures using Python (Flask/FastAPI) supporting real-time AI processing and seamless data flow
- Designed and implemented RESTful APIs and data processing pipelines with Python for automated workflows

Software Engineer

July 2021 – August 2022

India I Tech Services Private Limited

Contributed to backend and web application development projects, focusing on database management and backend integration in a collaborative team environment.

- Contributed to backend application development and web application projects at India I Tech Services
- Gained hands-on experience in JavaScript and REST API development, enhancing system functionality
- Collaborated on a large-scale project, focusing on database management and backend integration

TECHNICAL SKILLS

Programming Languages

Python (Proficient), JavaScript, Go

Generative AI & LLMs

GPT, Claude, LLaMA, Prompt Engineering, Fine-tuning

AI Frameworks

LangChain, Transformers, OpenAI SDK, Hugging Face, AutoGen, CrewAI

Vibe Coding & AI Dev Tools

Claude Code, OpenAI Codex, Antigravity, Microsoft Copilot, Cursor, Windsurf

Backend & APIs

FastAPI, Flask, Django, Node.js, RESTful APIs, GraphQL, Microservices

Databases

MongoDB, SQL, Redis, Supabase, Database Design & Optimization

AI Safety & Governance

Guardrails AI, OPA (Open Policy Agent), Rego, Prompt Filtering, Output Validation, Prompt Injection Defense, Hallucination Mitigation, AI Risk Assessment, Misuse Protection

RAG & Vector Databases

FAISS, Pinecone, Weaviate, Vector Search, Embedding Models, MCP

Cloud & DevOps

AWS, Cloudflare, Digital Ocean, Docker, Git, CI/CD

Specializations

AI Security & Governance, Responsible AI, Enterprise Compliance, IAM & Auth Systems, AI Agents, NLP, Agentic Workflows

EDUCATION

Lachoo Memorial College of Science & Technology

September 2018 – June 2021

Bachelor of Computer Science - BSc, Computer Science

Pratham Panchariya

Projects Portfolio

CURRENT AI PROJECTS (GRACKERAI)

Chronos-Engine — AI Governance Platform

[Guardrails AI](#) • [OPA/Rego](#) • [CrewAI](#) • [LangChain](#) • [Python](#)

Mar 2024 – Present • Production • GrackerAI (cross-functional team of 4)

Production AI agent governance platform enforcing safety controls, audit traceability, and responsible AI policies across multi-agent orchestration systems processing 50K+ agent tasks/month.

- Authored OPA policies in Rego to enforce AI governance constraints across all CrewAI agent pipelines — preventing off-policy outputs, data leakage, and privilege escalation
- Implemented Guardrails AI validators for prompt filtering and output validation across 8 production LLM endpoints, reducing policy violations by 70%
- Built append-only audit log and traceability system capturing every agent decision with structured metadata, enabling forensic review and compliance reporting
- Designed automated failure mode detection with circuit-breaker patterns for LLM risk scenarios (hallucinations, injection attempts, budget overrun)

[Internal Production System](#) • [GrackerAI](#)

AI Safety & Guardrails System

[Guardrails AI](#) • [OPA/Rego](#) • [Python](#) • [RAG](#) • [MCP](#) • [LangChain](#)

Jan 2024 – Present • Production • GrackerAI (sole engineer)

Enterprise-grade AI safety framework deployed across all GrackerAI LLM products, governing 200K+ monthly LLM calls with real-time policy enforcement and full auditability.

- Implemented OPA (Open Policy Agent) with Rego policies as the central rule engine — enforcing AI governance constraints, access control, and output safety across all LLM endpoints
- Integrated Guardrails AI validators for prompt injection defense, output validation, and misuse protection, reducing unsafe outputs by 85% in production
- Built RAG pipeline safety layer with MCP (Model Context Protocol) — embedded safety checks at retrieval, context assembly, and generation stages
- Created real-time audit and monitoring system tracking 95%+ of agent decisions with alerting on risk scenarios (injection attempts, PII leakage, hallucination spikes)

[Production System](#) • [GrackerAI](#) • [All AI Products](#)

Gracker - Content Intelligence

[Python](#) • [Next.js](#) • [Astro.js](#) • [MongoDB](#)

Autonomous content generation platform with 60+ proven portals generating 100K+ monthly visitors.

- Developed Astro.js frontend for high-performance static generation
- Built Next.js dashboard for content management and analytics
- Implemented RAG pipelines for content intelligence monitoring
- Created automated SEO-optimized content deployment system

[gracker.com](#)

Mojolndie - AI Blog Writer

[Python](#) • [Next.js](#) • [MongoDB](#)

AI-powered blog writing platform that learns brand voice and creates personalized content automatically.

- Built complete Next.js application with AI integration
- Implemented brand voice learning algorithms
- Created automated content publishing workflows
- Developed SEO optimization and analytics features

[mojolndie.com](#)

MojoAuth - OTP Authentication

[Python](#) • [Next.js](#) • [PostgreSQL](#)

Unified API for OTP authentication supporting Email, Phone, WhatsApp, and Authenticator OTP methods.

- Developed Next.js frontend with authentication flows
- Built React dashboard for API management
- Implemented javascript backend with microservices architecture
- Created comprehensive SDK and API documentation

[mojoauth.com](#)

SSOJet - Enterprise SSO

[Python](#) • [Astro.js](#) • [PostgreSQL](#)

Enterprise SSO solution supporting SAML, OIDC, and SCIM with seamless integration capabilities.

- Built Astro.js frontend for optimal performance
- Developed React dashboard for SSO management
- Implemented backend with enterprise security standards
- Created integration connectors for 100+ identity providers

[ssojet.com](#)

LogicBalls - AI Content Platform

[Python](#) • [FastAPI](#) • [React.js](#) • [MongoDB](#)

Visual ChatGPT platform supporting 500K+ users across 200+ countries with AI tools for content creation.

- Developed FastAPI backend infrastructure
- Implemented EJS templating for dynamic content
- Built React.js dashboard for user management
- Created 140+ AI tools for marketing and writing

[logicballs.com](#)

Kveeky - AI Voiceover Platform

[Python](#) • [FastAPI](#) • [React.js](#)

AI scriptwriter and voiceover artist platform supporting 500+ voices in 200+ languages with customizable voice parameters.

- Built responsive React.js frontend with voice customization controls
- Developed FastAPI backend for AI voice processing
- Integrated multiple AI voice models and language support
- Implemented real-time audio preview and download features

[kveeky.com](#)