SAI RAKSHITH MUDA

Tracy, CA | (814) 780-1228 | rakshithmuda@gmail.com
github.com/rakshithmuda22 | linkedin.com/in/sai-rakshith-muda-09341a1b4 | rakshithmuda22.github.io | PyPI: llm-agentspec

EDUCATION

Pennsylvania State University, B.S. Computer Science, GPA 3.45 *May 2026*
Coursework: Operating Systems, Artificial Intelligence, Database Management Systems, Communication Networks, Theory of Computation

Universidad Técnica Federico Santa María, Study Abroad (Chile) *Mar 2023*
Seismic wave analysis research and field-ready microscope construction.

EXPERIENCE

Founder and Engineer, VitalMaa *2026 - Present*

- Building an AI health companion for Indian families as a solo engineer (Flutter, Supabase, Cloudflare Workers): an AI health coach that speaks English, Hindi, and Telugu on Sarvam AI's Indian-language models, backed by 36 Supabase Edge Functions behind a Cloudflare Worker proxy; 1,380+ commits.

Mathematics Department Proctor; Commons Desk Operations *Penn State University | Mar 2024 - Apr 2026*

- Ran secure exam logistics and handled confidential examination materials (to Dec 2025); managed student information systems and check-in procedures at a residence-hall front desk. Employee of the Month.

PROJECTS

Belay *Python, MCP, Claude Code hooks, Ollama | PyPI: agentbelay*

- Open-source firewall for AI agents: checks every tool call from Claude Code or any MCP client against a YAML policy before it runs (allow, ask, or block), including order-aware rules such as tests-must-pass-before-push; audit trail plus CI replay of recorded traces. 114 tests.
- In a prompt-injection test with a local model (qwen3:8b) and the real filesystem MCP server, 8/8 runs leaked a planted fake key without Belay and 0/8 with it; adds about 0.7 ms per MCP call.

AgentSpec *Python, pytest, OpenTelemetry | PyPI: llm-agentspec*

- Built and published a zero-dependency Python library for deterministic contracts on LLM agent tool calls (ordering, budgets, forbidden tools, argument rules, approval gates) with Anthropic, OpenAI, and OpenTelemetry adapters. 173 tests.
- Designed an incremental live guard that decides each proposed tool call in about 2.7 µs regardless of session length, versus 3.4 ms for a full re-check at 10,000 calls; a randomized differential test over 400 generated rule sets proves it matches the batch checker and caught an approval-bypass bug.

AgentProbe *Python, LangGraph, Tree-sitter, Hypothesis, Docker*

- Dockerized GitHub Action that runs three deterministic Tree-sitter analyzers as a LangGraph state graph to enforce architecture boundaries and naming rules on every pull request; differential property tests (Hypothesis) run in an isolated subprocess and report minimal counterexamples. Policy is read from the base commit so a PR cannot loosen its own rules. 149 tests.

Stacktrace Time Machine *Python, FastAPI, GitHub GraphQL, Redis*

- Stateless service that maps a Sentry crash to the pull request that last wrote the crashing line, via GitHub GraphQL blame pinned to the deployed release SHA (no clones). Built an SZZ-style eval on 223 real crashes from 12 open-source projects: 80% top-1 accuracy, versus 42% for the whole-function blame it first shipped with, so the default changed. 115 tests.

CodeSage *Python, FastAPI, Redis/RQ, Groq, Tree-sitter*

- Webhook-driven PR reviewer: four concurrent LLM agents (bugs, security, style, tests) post inline comments on the exact changed lines; the unified-diff mapper is validated against 25 randomized real `git diff` outputs. 136 tests.

TECHNICAL SKILLS

Languages: Python, TypeScript, Dart, Swift, C, SQL
AI and LLM: Claude API (tool use), Sarvam AI, Groq, LangGraph, MCP, Ollama, RAG, ChromaDB, retrieval evals
Backend: FastAPI, Flask, Pydantic, Supabase, PostgreSQL, Redis, MySQL, REST APIs, GitHub GraphQL API
Frontend: React, Flutter, SwiftUI, Tailwind CSS
Infrastructure and DevOps: Docker, GitHub Actions, CI/CD, Cloudflare Workers, Vercel, Deno
Testing and Tools: Git, pytest, Hypothesis, asyncio, Tree-sitter, Redis Queue (RQ), webhooks
Spoken: English (fluent), Hindi (native), Telugu (native)

CERTIFICATIONS

- **Introduction to DevOps** and **Getting Started with Git and GitHub**, IBM (Coursera), 2026
- **Claude 101**, **Claude Code in Action**, **Introduction to Agent Skills**, and **AI Fluency Framework & Foundations**, Anthropic Academy, 2026