# Paawan Desai

paawankdesai@gmail.com • linkedin.com/in/paawan-desai • paawankdesai.com • github.com/paawandesai

## EDUCATION

**The University of Texas at Austin, Cockrell School of Engineering** — **Austin, TX**
*Bachelor of Science in Electrical and Computer Engineering, Minor in Entrepreneurship* — *May 2025*

## WORK EXPERIENCE

**Gauntlet AI** — **Austin, TX**
*AI Engineering Fellow, Cohort 7 (selected from 2,000+ applicants, ~2% admit)* — *September 2026 – Present*

- Fine-tuned Qwen3-4B (LoRA) to write exact 94-character NACHA ACH files from plain-language specs: 99/100 exact on holdout (base 0/50), 18/20 on the hardest specs vs. 17/20 for Claude Opus 5.5; on Hugging Face
- Built a clinical co-pilot in OpenEMR that drafts pre-visit briefs from FHIR records and lab PDFs, checking every claim in code; cut report latency from ~90 s to 7–8 s; a 98-case eval gate blocked 22/22 planted regressions
- Built an adversarial eval platform that attacks the deployed co-pilot with code-first oracles (10/11 verdicts decided without an LLM), confirming 3 vulnerabilities, including 2 critical cross-patient record leaks
- Shipped a call-center agent (Claude Haiku 5.5, 7 narrow tools, pgvector RAG) that routed 31/31 calls needing a human to a person and held 46/46 attacks; chose Haiku at ~$0.04 per 100 calls vs. $1.36 for Opus after a cost/quality comparison
- Built a Go aggregator on Cloud Run that matches equivalent Kalshi and Polymarket contracts at 1.00 precision on 95 human-confirmed labels and back-tested 208,064 cross-venue pairs, with 29/29 payout verdicts agreeing
- Also shipped a Monte Carlo pricer on AWS Lambda (1M paths in 0.58 s), Solana markets in Rust and an LA zoning engine

**Handshake AI, micro1, Mercor**
*AI Training & Evaluation Engineer (Contract)* — *November 2025 – Present*

- Built LTspice, ngspice, KiCad and Qucs simulation environments that generate circuit-design LLM training data (Handshake AI)
- Built automated tooling and test frameworks that programmatically verify enterprise AI models' API behavior (Mercor)
- Designed prompts and execution environments to test AI-generated code for correctness and edge cases (micro1)

**SkyTerra Group**
*AI & Data Analyst* — *April 2025 – November 2025*

- Trained ML models to detect cardiac abnormalities from ECG data on a HIPAA/GDPR-compliant edge-to-cloud stack
- Led field integration of an off-grid hybrid microgrid: battery systems, inverters, generators and remote telemetry

**Fundare Finance**
*Co-Founder & Engineer* — *May 2024 – December 2024*

- Led development of a Python and SQL dashboard that tracks revenue growth for small businesses

## PROJECTS AND RESEARCH

**Company Agent Layer:** indexes API, event and DB contracts across repos and flags breaking PRs to the affected teams; 45/58 scenarios on a 14-repo simulated company, ~14 s to PR comment

**AI Agent Red Team Engine + AuditLens** — github.com/paawandesai/redteam-engine
*Adversarial security research (open source)* — *April 2026*

- Built an engine that runs RAG-injection, tool-misuse and multi-turn attacks on LangGraph agents and grades the tools each agent actually called; 6 of 10 chains broke all 4 frontier models tested; hardening cut RAG exploits from 14/71 to 6/71
- Mapped 113 prompts to OWASP LLM Top 10, MITRE ATLAS and CWE; AuditLens maps findings to the EU AI Act

**Hardware Accelerator for Post-Quantum Cryptography (ML-DSA)**
*Senior design project* — *September 2024 – May 2025*

- Led a Verilog ML-DSA accelerator, designing the NTT and random-bit-generator modules and its C driver

**Energy AI Hackathon – 1st Place**
*Predictive energy modeling* — *January 2025*

- Forecast grid, diesel and CNG use for fracking with XGBoost/Random Forest and uncertainty modeling ($R^2$ 0.99/0.98/0.97)

## SKILLS

**Languages:** Python, TypeScript, Go, Rust, C/C++, C#, SQL, Verilog
**AI & LLM:** Claude/OpenAI APIs, LangGraph, RAG (pgvector, ChromaDB), LoRA, vLLM, Hugging Face, LLM-as-judge evals
**Infrastructure:** AWS (Lambda, CDK, Terraform), GCP Cloud Run, Azure, Modal, Docker, Postgres, Kafka, GitLab CI
**ML & Hardware:** PyTorch, TensorFlow, XGBoost, scikit-learn, time-series forecasting, Edge AI, LTspice, KiCad, microgrids
**Honors:** AIME Qualifier; Top 2.5% AMC; 3rd Place Nationally, ARML; Captain, Punjabbawockeez