

RUTTANSH BHATELIA

Toronto, Ontario | Authorized to work in Canada | No sponsorship required

Applied AI Engineer | Harness Engineering | Agentic Systems | Evaluation

rutts291@gmail.com

linkedin.com/in/ruttansh

github.com/rutts29

0xrutts.com

Summary

Applied AI engineer building production agentic systems across security, retrieval, and evaluation. At CredShields, I own harness engineering for an AI-assisted penetration-testing product and translate customer requirements into shipped system changes. Outside work, I build local-first tooling for observability, drift-resistant long-running sessions, and supply-chain security for AI-driven developer workflows.

Experience

AI Engineer

April 2025 – Present

CredShields (Contract)

US, Remote

- **Own harness engineering and the agentic systems behind CredShields One**, designing production AI-assisted penetration-testing workflows and review-ready findings.
- Partner with product and security teams to translate **customer requirements into shipped AI features and system-design changes**; modularized the AI layer for independent development and testing.
- Improve the reliability of SolidityScan's LLM-assisted findings through **retrieval grounding and second-pass validation** before analyst review.
- Built **custom OpenHands-based agent workflows using ACP** for internal engineering, wired to Slack for scan debugging, issue creation, and pull requests; also built a priority-aware CI agent with restricted production permissions.

Machine Learning Researcher

January 2025 – April 2025

Sheridan Centre for Applied AI · TELUS (Contract, part-time)

Oakville, Ontario

- Trained VAE and DDPM models to synthesize RSSI fingerprints, integrated the generated data into regression-based localization pipelines, and co-authored an **IEEE MSWiM 2025 paper** on synthetic RSSI augmentation and hybrid localization. DOI: [10.1109/MSWiM67937.2025.11309178](https://doi.org/10.1109/MSWiM67937.2025.11309178).

Full Stack Developer

September 2024 – December 2024

Sheridan Centre for Applied AI · McMaster University (Contract, part-time)

Oakville, Ontario

- Ported a research web application to Flutter for iOS and Android, with REST APIs, Strapi CMS integration, a SQL schema, and authentication and data-handling controls aligned with sensitive health-data requirements.

Machine Learning Researcher

May 2024 – August 2024

Sheridan Centre for Applied AI · Osteoporosis Canada (Co-op)

Oakville, Ontario

- Built and evaluated fracture-risk pipelines using a soft-voting ensemble of random forest, XGBoost, and logistic regression, with precision-recall, ROC-AUC, and calibration for a false-negative-sensitive clinical use case.

Selected Projects

agentlog | github.com/rutts29/agentlog | Python, TypeScript, SQLite, MCP

- Built **local-first observability and evaluation** across AI coding harnesses using read-only adapters, a provenance-aware SQLite ledger, source re-verification, a CLI, a local dashboard, and read-only MCP tools.

driftctl | github.com/rutts29/driftctl | Rust, Codex hooks

- Built an opt-in, **drift-resistant continuity layer** for long-running Codex sessions; model-proposed updates pass deterministic validation, ambiguous changes require human review, and published Hackathon MVP evaluations include negative results.

Education

Sheridan College

January 2022 – December 2025

Honours Bachelor of Science in Computer Science

Oakville, Ontario

- Specialization in Data Analytics and Machine Learning. Undergraduate thesis on smart-contract vulnerability detection using CodeBERT and graph-based models, with template-based fixes for selected vulnerability classes.

Technical Skills

Languages: Python, TypeScript, Rust, Go, SQL

Agentic Systems: harness engineering, orchestration, MCP, RAG, evaluation, observability, LangChain, Langfuse, Vercel AI SDK

ML and Delivery: model fine-tuning, PyTorch, Hugging Face, FastAPI

Infrastructure and Data: SQLite, PostgreSQL, Docker, AWS, Linux, Git