SIMARJOT SINGH MAAN

Bhopal, Madhya Pradesh, India | simarjotsinghmaan@gmail.com | +91 97553 00773

RESEARCH

SENTINEL: Trustworthy Guardrails for Web-Agent LLM Services

Scientific AI for Development (SAID) Lab | 2026

- Co-developed an open-source, model-agnostic guardrail framework — five inference-time enforcement layers within a nine-layer reference architecture — that wraps any OpenAI-compatible LLM endpoint to block jailbreaks, prompt injection, and indirect tool-injection attacks without retraining the underlying model.
- Built and released a reproducible 226-prompt benchmark (126 adversarial, 100 benign); pre-generation layers blocked 49.2% of attacks at a 5.0% benign false-positive rate — more than double a keyword-matching baseline (19.0%).
- End-to-end evaluation on Llama 3.1 8B raised the attack-block rate from 80.2% to 90.5% and cut true attack-success rate from 19.8% to 9.5%; open-sourced the full benchmark and codebase at github.com/saidlaboratory/SENTINEL.

PROJECTS

Algorithmic Trading System Development *Independent Research | 2024–2025*

Designed, implemented, and backtested algorithmic trading systems for crypto futures and prediction markets in Python, building signal-generation modules and backtesting frameworks to evaluate strategy P&L. Applied risk-management principles (position sizing, drawdown controls, exposure limits) and independently researched market microstructure and statistical arbitrage.

Custom LLM Development via Dataset Training *Independent Research | 2024–2025*

Fine-tuned large language models through custom dataset-training pipelines, studying training dynamics, distribution shift, and failure modes; built end-to-end research infrastructure using Python and the broader ML tooling ecosystem.

AI-Powered B2B SaaS *Founder & Full-Stack Developer | 2024–2025*

Independently architected, built, and deployed a full-stack AI product end-to-end as sole developer, writing all code by hand with zero no-code tools, and owning product design, feature prioritization, and the deployment pipeline.

EXPERIENCE

Equity Research Intern

Millennium Money Finance (Remote) | May–Jun 2026

- Completed a hands-on equity research internship at a BSE/NSE-registered firm; gained practical exposure to demat account workflows, DuPont analysis, and technical analysis of listed equities.

Human Resource Intern

Simtrak Solutions · ADORE (Remote) | May 2025–Present

- Selected for a structured mentorship program; manage daily reporting and task workflows and coordinate cross-team efforts across a distributed team.

HONORS & LEADERSHIP

- **INFOSPARK 2526 Hackathon** | 1st Place — time-constrained technical build challenge, DPS Kolar Road, Bhopal (2025)
- **Mount Carmel Declamation** | 1st Place — Mount Carmel Literary Fest 2025–26
- **Harvard MUN India 2025** | Debate Club Leader — represented a nation in committee, Bangalore
- **Founder, Chess Club**, Billabong High International School — built the club from scratch; volunteered 100+ hours coaching Grade 5–6 students in chess and accompanying them to tournaments
- **ThinkStartup Program**, IIT Delhi (RNI Park) — certified by TIDES Business Incubator, IIT Roorkee (May 2026)

EDUCATION

Billabong High International School, Bhopal

ICSE, Science + Computer Applications | 2025–2026

- Coursework: Physics, Chemistry, Biology, Computer Science

SKILLS

Languages: Python, Java, HTML / CSS / JS

AI / ML: PyTorch ecosystem, Hugging Face Transformers, LLM fine-tuning & evaluation, adversarial robustness, NLP

Quantitative Finance: Algorithmic trading, backtesting, statistical arbitrage, risk management, equity research (DuPont & technical analysis)