PRABINDER SINGH

Mohali, India · +91 6239712653 · prabindersinghh@gmail.com · prabindersinghh.com · github.com/prabindersinghh · HuggingFace: prabindersinghh

SUMMARY

AI Engineer & founder building production-grade ML systems at the intersection of open-source infrastructure, agentic AI, and manufacturing intelligence. Merged contributor to **CNCF Kubeflow SDK** & **kubernetes-sigs/headlamp**; active across MLflow (Linux Foundation), Metaflow (Netflix) & OpenMined Syft. Founded **Leorit.ai** — AI execution layer for Indian manufacturing; **leorit.xyz** shipped as production B2B SaaS with 3,000+ real orders decoded to build proprietary execution intelligence. Research: multi-modal learning (ViT, Wav2Vec2, diffusion forensics), RAG, spatial transcriptomics — paper under review IEEE ICAIB 2025; three 3rd-place international hackathon finishes.

EDUCATION

Thapar Institute of Engineering & Technology — B.Tech, CS with Business Systems · JEE Mains 2024: 94.2 Percentile *Aug 2024 – Aug 2028*
Relevant coursework: Machine Learning, Cloud & Microservices, Computational Finance & Modeling, Database Management Systems, Operations Research, Data Structures & Algorithms

TECHNICAL SKILLS

ML/AI: Multi-Modal Learning, Vision Transformers (ViT), LLMs (LLaMA3, Qwen2.5, Gemini), RAG pipelines, Agentic AI, OpenTelemetry instrumentation, Audio Forensics (Wav2Vec2, ECAPA-TDNN), Deep Learning, FAISS vector search, Diffusion model analysis
Systems & Infra: FastAPI, Microservices, Kubernetes, Docker, ML Pipelines, Model Deployment, CNCF Ecosystem, OpenTelemetry SDK, Protobuf, CI/CD (GitHub Actions), Linux, Bash
Languages & Data: Python (pytest, SDK dev, pipelines), TypeScript, SQL, Feature Engineering, Analytics (PostHog, Sentry), n8n workflow automation
Frontend & Tools: React 18, Vite, shadcn/ui, Three.js, Tailwind CSS, Framer Motion · **Databases:** Supabase, PostgreSQL, Redis (Upstash) · **Cloud:** AWS, GCP, HuggingFace Spaces
Open Source: Kubeflow SDK (CNCF · 2 merged PRs) · kubernetes-sigs/headlamp (merged PR) · MLflow (Linux Foundation AI) · Metaflow (Netflix) · OpenMined Syft · npm: opensec-intelligence (v3.0.1)

OPEN SOURCE CONTRIBUTIONS

Kubeflow SDK (CNCF — ML Infrastructure) *2026*
- **PR #402 MERGED** by lead maintainer @andreyvelich — polling_interval validation across all 3 backends (TrainingClient, PipelineClient, StorageClient); zero breaking changes
- PR #401: centralized **telemetry.py** module with OpenTelemetry instrumentation, 15 unit tests, 0 regressions (under review) · PR #341: cluster-scoped runtime fallback, /ok-to-test granted by @astefanutti

kubernetes-sigs/headlamp (CNCF — Kubernetes UI) *2026*
- **PR #5558 MERGED** by @illume — ReleaseNotesModal GitHub Flavored Markdown rendering fix; production impact across all Headlamp users
- PR #5371: token expiry warning banner + auto-logout; backend /me endpoint extended to expose tokenExpiry · active review — Copilot comments resolved, OIDC behavior documented

MLflow (Linux Foundation AI) · **Metaflow** (Netflix) · **OpenMined Syft** *2025–26*
- MLflow: entity-level validation + protobuf serialization; union-type validation, tracing tests, backward compatibility · Metaflow: PR #3018 + working Nomad executor backend · Syft: persistent-mode dataset discovery bug + idempotency fix

PROFESSIONAL EXPERIENCE

Leorit.ai — Founder & CEO *May 2025 – Present*
- Building the AI execution layer for Indian manufacturing — WhatsApp-native, Hindi-first agents (Inquiry Handler, Production Tracker, QC & Dispatch) replacing ₹20,000/month coordinator salaries; targets 4M+ factories running on WhatsApp chaos
- **leorit.xyz** (Leorit OS): fully shipped B2B SaaS for garment manufacturers across Ludhiana, Tirupur & Ahmedabad; 3,000+ orders personally executed pre-launch to decode real manufacturing workflows; React 18 + TypeScript + Supabase + Three.js 3D mockup engine; 32-migration schema; 10-stage production tracking
- Proprietary data moat: pricing patterns, defect rates, QC outcomes, timeline adherence captured per order — structural AI training advantage no Indian startup can replicate without years on factory floors

RemoteStar — Business Development & Data Systems Intern *Jul – Sep 2025*
- Built automation enabling one-click prospect calling; reduced manual work by 70%; engineered engagement data models to surface high-conversion patterns and optimize follow-up sequencing

SyntX by OrangeCat — Product & Growth Strategist (Part-Time) *Sep – Oct 2025*
- Built n8n + Google Sheets automated conversion tracking pipeline; aligned behavioral analytics with feature prioritization; data-backed product decisions for retention strategy

SELECTED PROJECTS & RESEARCH

opensec-intelligence — Local-First Multi-Agent AI Security Engine · github.com/prabindersinghh/opensec-intelligence *2026*
- Published **npm package v3.0.1** (TypeScript); 4-agent pipeline: Scanner → Analyst → Consensus → Fixer; cross-modal analysis (code, Docker, k8s, Terraform, CI/CD, secrets); 0.7+ consensus threshold; 20 built-in tools; MCP server; OWASP Top 10 + 200+ secret-pattern skills injected per agent
- Daemon/watch mode; RAG codebase indexing; session persistence + undo; VS Code ready; reshared on launch by senior OSS contributor; ~8k Reddit views on r/ollama

Kubeflow OTel PoC — OpenTelemetry SDK Instrumentation · github.com/prabindersinghh/kubeflow-otel-poc *2026*
- Centralized telemetry.py; per-iteration child spans with max_traced_iterations cap; verified OTel JSON span output; direct pre-work for GSoC 2026 Project #7 (Hard, 350hrs)

TruthShield Pro — Multi-Modal AI Forensics · **CyberSentinel** — Hybrid Agentic IDS *2025*
- TruthShield: ViT visual forensics + Wav2Vec2/ECAPA-TDNN voice clone detection + LLaMA3 text analysis + diffusion artifact fingerprinting; Cross-Modal Consistency Engine + FAISS provenance graphs with full explainability layer
- CyberSentinel: hybrid IDS (rule-based + ML anomaly detection, **92%+ accuracy**); NLP phishing engine; UEBA behavioral drift analysis; Raspberry Pi edge gateway achieving sub-2s IoT/Wi-Fi threat blocking — 3rd Place, Univ. of Ulster UK

RAG-ST — Retrieval-Augmented Deep Learning for Spatial Transcriptomics *2025*
- 9-stage pipeline: EfficientNet patch encoder + FAISS retrieval + MLP gene expression prediction; PCA/t-SNE/UMAP interpretability stack; bridging computer vision and genomics · **Paper under review: IEEE ICAIB 2025**

HACKATHONS & AWARDS

3rd Place + Innovation Award — AI for Sustainability Hackathon 2026, Canadian University Dubai (CIVITAS-INTEL) · **3rd Place** — Agentic AI Hackathon 2025, University of Ulster UK (CyberSentinel) · **3rd Place** — BIOS Hackathon 2025, IEEE × CSED Thapar (TruthShield Pro)
Top 12 National Finalist — Secure Bharat AI & Cybersecurity Summit 2026, ISB Mohali, Punjab Police × CyberPeace Foundation · **Finalist** — PNB Cybersecurity Hackathon 2026, Live Jury VC Session (QuantumSight) · **Finalist** — Sabka AI 2026, TIET-UQ (FairHire360)

LEADERSHIP & ENTREPRENEURSHIP

CollabSphere (Founder): 72-member student ecosystem; ₹90,000 in real client projects delivered in week 1 · **Google Gemini Student Ambassador:** cloud adoption, developer workshops, campus AI engagement · **McKinsey Forward Program:** global cohort, leadership & analytical decision-making · **Innovation Mission Punjab Campus Ambassador** · Languages: English, Hindi, Punjabi