Abdul-Sobur Ayinde

ML Systems Engineer

abdulsobur245@gmail.com · github.com/Croesus245/My-POrt · linkedin.com/in/abdulsobur-ayinde · croesusml.vercel.app

SUMMARY

ML engineer focused on production systems that survive real-world conditions. Experience building fraud detection pipelines, secure LLM applications, and ML evaluation infrastructure. Every project ships with CI-gated evals, drift monitoring, and documented failure modes.

TECHNICAL PROJECTS

FraudShield — Real-time Fraud Detection System

github.com/Croesus245/My-POrt/fraudshield

- Built streaming fraud scoring API achieving ~1.2K TPS per instance with <50ms p95 latency
- Designed delayed-label reconciliation pipeline handling 30-day label lag via proxy labels + periodic reconciliation
- Implemented automated drift detection with PSI monitoring, retraining triggers, and CI-gated model promotion
- Created slice-based evaluation harness testing model performance across transaction types, amounts, and demographics
- Documented complete incident simulation with staged outage, response timeline, and postmortem analysis

SecureRAG — Defense-in-Depth RAG System

github.com/Croesus245/My-POrt/securerag

- Built multi-tenant document Q&A system with layered security: input validation, permission filtering, tool sandboxing
- Developed attack test suite with 1,400+ adversarial cases (prompt injection, jailbreak, data exfiltration, tool abuse)
- Achieved 100% block rate on data exfiltration attempts, 95.9% overall attack mitigation
- Implemented faithfulness scoring to detect hallucinations and unsupported claims in LLM responses

ShiftBench — Distribution Shift Benchmark

github.com/Croesus245/My-POrt/shiftbench

- Created skin lesion classification benchmark with explicit temporal (2015–2018 → 2019–2022) and demographic splits
- Documented negative results: models overfit to temporal artifacts, calibration degraded under shift
- Built reproducible evaluation pipeline with slice metrics, calibration curves, and uncertainty quantification
- Published dataset datasheet, model card, and reproduction guide following ML documentation best practices

TECHNICAL SKILLS

ML Frameworks:	PyTorch, scikit-learn, XGBoost, LightGBM, Hugging Face	**MLOps:**	MLflow, DVC, Weights & Biases, GitHub Actions, Docker
Data:	PostgreSQL, Redis, Kafka, Pandas, NumPy, Polars	**Infrastructure:**	FastAPI, AWS (S3, Lambda, SageMaker), Kubernetes, Terraform
LLM/GenAI:	LangChain, OpenAI API, RAG architectures, prompt engineering	**Languages:**	Python, SQL, Bash, JavaScript

WHAT I SHIP WITH EVERY PROJECT

- **CI-Gated Evals:** Automated slice metrics, regression tests, and quality gates before any model ships
- **Drift Monitoring:** PSI tracking, alert thresholds, and documented response runbooks
- **Cost Reports:** Latency benchmarks, infrastructure costs, and scaling projections
- **Model Cards:** Intended use, limitations, ethical considerations, and failure modes
- **Postmortems:** Real or simulated incidents with root cause analysis and corrective actions

EDUCATION & TRAINING

AI/ML Training Program — Robotics and Artificial Intelligence Nigeria (RAIN)

2024 · Intensive training in machine learning fundamentals, deep learning, and AI systems development

Self-Directed ML Systems Education

Continuous learning through building production-grade systems, open-source contributions, and technical writing

Portfolio: croesusml.vercel.app · Updated December 2025