Srinjoy Roy

6297431381 | srinjoy.roy.work365@gmail.com | LinkedIn | GitHub | Portfolio

Professional Summary

Results-driven AI-ML Engineer who designed and built a Transformer-based AI Web Application Firewall from scratch – spanning data generation, model training, and low-latency inference deployment. National hackathon winner and active open-source contributor to large-scale MLOps platforms. Specialized in NLP, LLMs, and applied deep learning, with a strong foundation in MLOps, security engineering, and scalable system design.

Technical Skills

Programming: Python, SQL, C/C++, Java, JavaScript, Bash, R
Machine Learning: Scikit-learn, XGBoost, LightGBM, TensorFlow, PyTorch, Keras
Deep Learning & CV: OpenCV, YOLOv5, CNNs, Vision Transformers (ViT), Transfer Learning
NLP & GenAI: Transformers, Tokenization, Embeddings, HuggingFace, BERT, GPT, LLMs, RAG, LangChain
GenAI Systems: Vector Databases, Semantic Search, Retrieval Pipelines, AI Agents, Tool Calling, ONNX, LoRA/PEFT
MLOps & Security: Docker, Kubernetes, MLflow, Airflow, CI/CD, GitHub Actions, WAF, File Integrity Monitoring
Data & Analytics: Pandas, NumPy, Spark, PowerBI, Tableau, Matplotlib
Databases: MySQL, PostgreSQL, MongoDB, Redis, Elasticsearch
Cloud: AWS (EC2, S3, SageMaker), GCP, Azure ML
Core CS: DSA, DBMS, OOP, System Design, REST APIs
Certifications: View Credentials

Experience

Cybersecurity Intern *June 2026 – Present*
Cybernara – WPShield Security Dashboard [Project]

- **AI-Powered WAF (built from scratch):** Designed and built a Transformer-based anomaly-detection firewall – a 5-stage pipeline (log ingestion, parser/normalizer, custom BPE tokenizer, 6-layer DistilBERT-scale encoder ∼66M params, FastAPI + ONNX inference sidecar) that flags requests deviating from learned-benign traffic
- Generated a 500K+ entry labelled training corpus by deploying 9 intentionally vulnerable web apps across 7 tech stacks (DVWA, Juice Shop, WebGoat, Mutillidae, crAPI, DVGA, VAmPI) with Locust-based traffic simulation
- Architected non-blocking sidecar inference via an Nginx/Lua hook and async worker pool, plus a LoRA-based continuous retraining pipeline for zero-downtime model hot-swaps
- Built the platform's authentication system (login, signup, MFA) and core security/admin modules: IP blocking, geo-blocking, and maintenance ("away") mode

Open Source Contributor *May 2026*
MLflow – Open Source AI/ML Platform (26k+ GitHub stars) [Pull Request #23601]

- Diagnosed and fixed a Clipboard API bug causing UI crashes on Copy actions across MLflow's prompt, tracing, and evaluation modules in non-HTTPS deployments
- Designed a shared `copyToClipboard()` utility with Clipboard API and `execCommand` fallback, refactoring 5 frontend components with full unit-test coverage

Achievements & Leadership

Smart India Hackathon 2025 – National Winner & Team Leader *December 2025*
[Winner Post] [TV Interview]

- Architected an AI-powered legal metrology compliance engine using an OCR + LLM pipeline (Tesseract, Gemini 2.5 Flash, LangChain) with real-time trust-score generation and pre-upload compliance validation
- Led end-to-end system integration with forensic hardware (ToF, MPU6050, UV+IR); owned model logic, system design, leadership, and final deployment
- Recognized with national television coverage for innovation and hackathon achievement

HackHeritage 2024 – Team Code Nirvana (1st Place) *September 2024*
[Winner Post] [GitHub]

- Led ML pipeline design for anomaly detection in drug inventory supply chains and built scalable backend services with CI/CD, Docker, and cloud deployment

Selected Projects

Phishing Website Detection (MLOps) [GitHub]

- Built end-to-end ML pipeline with automated training, evaluation, and deployment; CI/CD via Docker and GitHub Actions with AWS-based inference
- Designed monitoring and alerting for model drift and performance degradation

Education

Heritage Institute of Technology, Kolkata *2023 – 2027*
B.Tech in Information Technology — CGPA: 6.97

Burdwan Municipal High School *2020 – 2022*
Higher Secondary (Science) — 89.7%

Target Roles

Data Scientist • Machine Learning Engineer • Applied GenAI Engineer • ML / Security Intern