

Ankon Mukherjee

ankon.m@somaiya.edu | [linkedin.com/in/ankon-mukherjee](https://www.linkedin.com/in/ankon-mukherjee) | github.com/AnkonM

EDUCATION

KJ Somaiya College of Engineering

B.Tech in Artificial Intelligence & Data Science, Honours in Applied Cybersecurity CGPA: 9.22/10

Mumbai, India

2023 – 2027

RESEARCH

Targeted Training-Data Poisoning of Neural Radiance Fields

Sep 2026 – Present

Independent Research | Python, PyTorch, Blender (Python API), CUDA

github.com/AnkonM/nerf-poisoning-study

- Investigating how the fraction of poisoned training views controls selective object suppression in NeRFs, and the collateral damage to non-target scene content
- Built an end-to-end pipeline: procedural Blender scene and camera rig, a scripted compositor that erases a target object from selected views, NeRF retraining, and masked vs. unmasked PSNR/SSIM/LPIPS evaluation on a frozen, checksummed held-out view set
- Proof of concept: target-region PSNR fell from 23.6 → 19.4 → 11.6 dB at 0/20/50% poisoning budgets, confirming monotonic, selective suppression
- Pre-registered the methodology and kept an append-only log of 35 design decisions and a 51-test pytest suite; caught four silent config defects (including every poisoned condition silently training on clean data) before launching an 8-condition × 3-seed sweep

EXPERIENCE

Red Team Analyst Intern

Mar 2025 – May 2025

DeepCytes

UK (Remote)

- Analyzed macOS and iOS applications for vulnerabilities using static analysis and reverse engineering in Ghidra
- Built data ingestion pipelines and backend APIs for cyber threat intelligence workflows
- Automated security analysis workflows, reducing manual effort in vulnerability assessment

Aerodynamics Lead

Sep 2023 – Sep 2026

Orion Racing India, Formula Student

Engineer, Sep 2023 – Jan 2025

- Led a cross-functional team of 10+ engineers across design, simulation and manufacturing
- Improved correlation between CFD simulations (SimScale) and on-track performance, strengthening model validation
- Drove the car to 1st place in the Skidpad event among 25+ Formula Student teams

PROJECTS

ActAudit — EU AI Act Risk Classifier

act-audit.streamlit.app

Python, Gemini API, Streamlit

github.com/AnkonM/actaudit

- Built a tool that classifies AI systems into EU AI Act risk tiers from a GitHub repository or documentation, with UNESCO and IEEE ethics flags
- Designed a two-stage extract-then-decide architecture: the LLM only fills a fixed schema of facts with quoted evidence, and an ordered, deterministic rule table assigns the tier and cites the deciding provision, so identical inputs always yield identical, auditable results
- Deployed publicly on Streamlit Cloud with 102 unit tests

LayerWise — Explainable Transfer Learning Advisor

2026

Python, PyTorch, FastAPI

github.com/AnkonM/layer-wise

- Building a rule-based advisor that recommends fine-tuning choices for image datasets, with a plain-English justification logged as a traceable evidence object for every decision
- Implemented a dataset analyzer computing per-class statistics over sampled image corpora, and a domain detector that infers dataset type (natural, medical, satellite, etc.) with confidence scores and evidence chains
- Kept the ML engine fully independent of the FastAPI layer, so all decision logic is unit-tested without a server

TECHNICAL SKILLS

Languages

Python, C++, SQL

ML & Systems

PyTorch, NumPy, CUDA environments (Linux/WSL2), Blender Python API

Backend & Tools

FastAPI, Flask, Streamlit, REST APIs, Docker, Git, Linux, pytest, AWS

Security

Ghidra, static analysis, reverse engineering

Concepts

System Design fundamentals, Data Structures & Algorithms, OOP, SDLC