Manodeep Ray

+91 7070598988 | manodeepray1@gmail.com | linkedin.com/in/manodeep-ray | github.com/Manodeepray | website

Core Expertise: Building real-world ML systems using NLP, Computer Vision, Deep Learning, and Generative AI. Skilled in designing and experimenting with deep learning architectures, understanding LLM inner workings, and creating AI pipelines involving RAG, fine-tuning LLMs, face recognition, and audio transcription.

Technical Skills

Languages: Python, C, SQL (MySQL), HTML/CSS
Frameworks: Gradio, FastAPI, LangChain, Streamlit, Hugging Face, LlamaIndex, RAG Pipelines, Ollama, Unsloth
Libraries: Pandas, NumPy, Matplotlib, BeautifulSoup, TensorFlow, Keras, PyTorch, PEFT , DDP, FSDP
Developer Tools: Git, GitHub, Kaggle, Jupyter, Colab, VS Code, Linux, Roboflow
Concepts: Supervised & Unsupervised Learning, CNNs, Transformers, Tokenization, Embeddings, Attention Mechanisms, AI Agents, Prompt Engineering, Vector Databases (FAISS)

Experience

Undergraduate Researcher – Project AntiDote *(Under Review)* Sep. 2024 – Present
RespAI Lab

- Focused on LLM reasoning, selective memory unlearning, and safety alignment.
- Contributed to the theoretical foundations of the paper and actively worked on implementing and debugging baseline models for evaluation.
- Developed **AntiDote**, a novel bi-level optimization framework featuring an adversary hypernetwork to make Large Language Models (LLMs) resistant to malicious fine-tuning.
- Demonstrated the framework's effectiveness against 52 red-teaming attacks, achieving a **27.4% increase in robustness** compared to existing baselines.
- Engineered a **tamper-resistant model** that preserves safety alignment while maintaining high utility, with less than **0.5% performance degradation** on key benchmarks (MMLU, HellaSwag, GSM8K).

Research Intern – Minerva: Autonomous Multi-Agent Exploit Framework May 2025 – Aug. 2025
IIT Bhilai

- Built a **3-stage autonomous XSS detection system** inspired by the **YURASCANNER** paper.
- Developed **multi-agent pipelines** (**LangGraph + Groq LLaMA 3.3 70B**) for automated web crawling, payload injection, exploit validation, and **DOM analysis** via **BeautifulSoup**.
- Integrated **LLaVA VLM** for visual exploit confirmation and a **FastAPI monitoring server** with real-time logging, automating orchestration and runtime diagnostics (**85–90% workflow success rate**).

Projects

Voice-based Active Learning Platform (Ongoing Project)

- Designing a platform that transforms lecture/audio input into structured notes linked with a **multi-level hierarchical knowledge graph**.
- Developing a **graph-based active learning system**, enabling learners to explore concepts through interactive multi-hop navigation.
- Proposing a **novel graph search algorithm** inspired by planning and reasoning techniques to enhance intelligent knowledge discovery.

AI-Powered Attendance & Notes *OpenCV, YOLOv11, Python, Flask, Groq, Hugging Face*

- Designed and deployed a scalable, **cloud-integrated server pipeline** using **Watchdog** to monitor classroom media, optimizing edge-device workflows for **real-time performance** and seamless multi-environment deployment.
- Implemented **YuNet (OpenCV)** for face detection (**95% accuracy**) and **YOLOv11** for face recognition (**90% accuracy**) to automate attendance marking and compute **student attentiveness metrics**.
- Built an audio transcription workflow using **Vosk models** with accelerated inference on **Groq**, generating **structured lecture notes** that reduced manual note-taking effort by over **80%**.

Skin Cancer Classification | *Python, TensorFlow, Keras, Kaggle*

- Built a skin lesion classification system using **Vision Transformer (ViT)** models on **ISIC2024** and **HAM10000** datasets, integrating a **token learning layer** to achieve **93% classification accuracy** while reducing training time by **40%** compared to baseline ViT.

Education

KIIT University Bhubaneshwar, Odisha
Bachelor of Technology - CGPA 9.04 - 6th sem *Jul. 2022 – Present*

D.P.S Ruby Park Kolkata, West Bengal
Higher Secondary Education - result - 90 percent *March 2020 – April 2022*