Hardik Sharma

Data Scientist — Machine Learning Engineer — AI Researcher

9877100914 | hhardikssharma@gmail.com | LinkedIn | GitHub | Kaggle | Portfolio

Technical Skills

- **Data Science**: Computer Vision, NLP, Deep Learning, DevOps
- **Libraries & Frameworks**: TensorFlow, PyTorch, Scikit-learn, Hugging Face, NLTK, spaCy, OpenCV, Keras
- **Languages & Tools**: Python, SQL, Java, Docker, AWS S3, Git, Flask, FastAPI

Experience

AI Research Intern Dec 2024 – Present
Truens AI *Remote*

- Developed real-time deepfake detection system for banking KYC video calls, achieving **73.8% F1 score** on private dataset and **70% aggregate F1 score** across multiple evaluation scenarios
- Engineered multimodal ID card verification system combining computer vision and NLP to detect both visual and textual forgeries in identification documents
- Implemented and optimized VLM architecture for fraud detection, integrating with the "TruFor" algorithm to improve detection accuracy

Research Internship July 2024 – Present
AIISC, South Carolina *Remote*

- Implemented 11 advanced jailbreak techniques from the Trees of Attack paper (EMNLP submission), evaluating vulnerability across **22 major LLMs** including GPT-4, Claude, and LLaMA models
- Discovered critical security gaps with **95.4% success rate** on LLaMA-2 70B and **89.5%** on GPT-4 using Persuasion Attack techniques, providing essential benchmarking data for AI safety research
- Developed comprehensive vulnerability matrices for 3 attack categories, enabling identification of the most resilient models

Data Science Intern May 2024 – Nov 2024
DeepAlgorithms Pvt. Ltd., Hyderabad *Remote*

- Achieved **88% authentication accuracy** with industry-leading security metrics (**FAR: 0.04, FRR: 0.08**) for behavioral biometric system, enabling reliable user identification while minimizing false rejections
- Engineered spatial attention-based deep learning model that eliminated manual feature engineering, processing raw sensor data from accelerometer, gyroscope, and magnetometer inputs
- Deployed end-to-end authentication solution using AWS S3, collaborating with app developers to implement the system in production environment

Research Internship May 2024 – Present
Indian Institute of Technology, Mandi *HP*

- Engineered spatial attention-based deep learning model that outperformed previous approaches, achieving **90.4% precision** (3% improvement) and **97.9% specificity** (0.6% improvement) on complex odor prediction tasks
- Implemented fragment-based transformer architecture for processing raw molecular data directly for more accurate classification
- Applied advanced data augmentation techniques to address severe class imbalance in dataset of **3,036 molecules** with **109 odor perception labels**

Education

Indian Institute of Technology, Madras Chennai, TN
Bachelor of Science in Data Science and Applications *CGPA: 8.0 (April 2021 – May 2025)*

Projects

Movie Sentiment Prediction | *Machine Learning, NLP* GitHub

- Implemented stacked ensemble of 5 models (Logistic Regression, Random Forest, GradientBoost, AdaBoost) with Quantile Transformation
- Secured rank **97 out of 977** participants, achieving **F1 score of 0.832** and **86% accuracy** using 5-fold cross-validation

Facial Expression Recognition | *Computer Vision, Deep Learning* Link

- Built CNN using MobileNetV2 architecture with data balancing through oversampling minority emotion classes
- Achieved **96.96%** training accuracy and **84.34%** validation accuracy using Adam optimizer with categorical crossentropy

Publications & Certifications

- **"CIRSNet: Lightweight Chemometric IR Network"**, Transactions in Instrumentations and Measurements, (review)
- **"Biomedical Fragmented Attention Spectral Transformer Network for Infrared spectra analysis"**, (submitted)
- **"Text Summarization of Publicly Available BBC News Dataset"**, Global Journal For Research Analysis, Feb 2024
- **Certifications**: Azure AI Fundamentals, Diploma in Data Science (IIT Madras), Natural Language Processing (NPTEL)