Kartikeya Chitranshi

kartikeya4524@gmail.com — +49 176 61668557 — Berlin, Germany
LinkedIn: https://www.linkedin.com/in/kartikeya-chitranshi/
GitHub: https://github.com/kartikeya1234

PROFILE

Experienced Data Scientist and ML Engineer with 3+ years of expertise in developing and deploying production ML systems, specializing in cutting-edge AI technologies including Vision-Language Models, adversarial robustness, and deep learning architectures using PyTorch and Transformers. Proven track record in implementing scalable ML pipelines with Docker and Kubernetes, building end-to-end data preprocessing workflows, and translating complex AI research into robust production systems achieving 85%+ accuracy. Currently advancing multi-modal AI security research at Zuse Institute Berlin while pursuing MSc in Scientific Computing, with demonstrated ability to collaborate effectively with cross-functional teams and drive measurable business impact through innovative ML solutions and rigorous experimentation.

WORK EXPERIENCE

Student Research Assistant [Sep-2023] – [Current]
Zuse Institute Berlin - Berlin, Germany.

- Evaluated adversarial and explainability of Vision-Language Models using PyTorch and Transformers libraries on multi-GPU cluster infrastructure using SLURM.
- Implemented and tested sparse adversarial attacks on CNNs and deep neural networks.
- Analyzed transferability of adversarial examples across diverse machine learning architectures.

Machine Learning Intern [Jun-2021] – [Aug-2021]
TestAIng.com - Bangalore, India.

- Implemented multiple adversarial attack algorithms on deep neural networks using Tensorflow.
- Created clear user documentation for reproducible experiments and model robustness testing.

Data Analyst Intern [May-2020] – [Jul-2020]
Peacock Solar - Gurugram, India.

- Developed predictive ML models using Scikit-Learn, Pandas, NumPy, and A/B testing methodologies to forecast market penetration rates and revenue potential across 28 Indian states, directly enabling data-driven expansion decisions.
- Engineered comprehensive data preprocessing pipelines handling multi-dimensional datasets including regulatory frameworks, competitive landscape analysis, and regional market conditions, transforming raw market intelligence into actionable forecasting models with 85%+ accuracy for executive strategic planning.

PROJECTS

Flipkart Product Recommender System

- Developed an end-to-end product recommendation system using RAG architecture with LangChain and FAISS vector database for semantic search over product catalogs.
- Implemented document ingestion pipeline to process product descriptions, specifications, and user reviews, enabling context-aware recommendations based on natural language queries.
- Deployed scalable containerized application using Docker and orchestrated with Kubernetes on Google Cloud Platform, and monitored using Grafana.

EDUCATION

Master: MSc. in Scientific Computing [Apr-2022] – [Jul-2025]
TU Berlin - Berlin, Germany.

Main focus: Numerical Linear Algebra, Scientific Computing, Discrete Optimization and Machine Learning, Deep Learning, Machine Intelligence, Modern Algorithms for Multiagent Learning, Optimization under Uncertainty, High-Dimensional Optimization and Learning.

Bachelor: BSc. in Physical Sciences [Jul-2018] – [Jun-2021]
University of Delhi - Delhi, India.

Main focus: Numerical Methods, Calculus and Matrices, Differential Equations, Operating System, SQL, Object-Oriented Programming, Office Automation Tools, Java, System Arcitecture.

KNOWLEDGE & SKILLS

Language skills:	German (A2), English (C2), Hindi (Native).
Programming:	Python, Java.
DL Frameworks:	PyTorch, HuggingFace, LangChain, LangGraph.
Libraries:	NumPy, Pandas, Streamlit, Scikit-learn, XGBoost, Matplotlib, Seaborn.
Models:	CNNs, Vision-Language Models, Large Language Models, Multimodal AI.
Techniques:	Documentation, Prompt Engineering, Model Fine-Tuning, RAG.
Vector Databases:	FAISS, ChromaDB.
LLM APIs:	OpenAI, Ollama, Groq.
DevOps:	Docker, Git, Kubernetes.
HPC/Distributed:	SLURM, Multi-GPU Clusters.
Tools/OS:	Linux, Windows, MacOS, Microsoft Office, Latex, Vim, Jupyter.
Personal Skills:	Team Work, Communication & Presentation Skill, Collaborative & Helpful, Problem Solving & Analytical Thinking, Innovative & Self-confident, Resilience.

PUBLICATIONS

- **Training on Plausible Counterfactuals Removes Spurious Correlations,**
  Sadiku, S., Chitranshi, K., Kera, H., and Pokutta, S. (2025), *arXiv preprint, arXiv:2505.16583*.

ACADEMIC PROJECTS

Master Thesis, TU Berlin - Berlin, Germany. [Oct-2024] – [Apr-2025]
Topic: Robustness of Multi-Modal Foundation Models.

- Conducted comprehensive research on Vision-Language Model security by implementing sparse adversarial attacks for image captioning and VQA tasks, comparing CLIP model performance under different training paradigms (adversarial vs. counterfactual), and developing end-to-end robustness evaluation pipelines for multi-modal AI systems across image classification and image-text retrieval applications using PyTorch and Transformers.

Berlin, 04.April.2025