Mirza Mujtaba Hussain

Rome,Italy

☎ +393453345547 | ✉ mujtabahussain.mirza@uniroma1.it | in linkedin.com/in/mirzamujtabahussain | 🎓 Google Scholar

Summary

As a final-year PhD student at Sapienza University in Computer Science, I come with a strong foundation from my bachelor's in Computer Science and Engineering. My previous experience as a Machine Learning Engineer has provided insights into real-world challenges and as a technical writer, I have enhanced my research skills. My current research focuses on enhancing adversarial robustness in deep learning systems, with the broader goal of making AI models fundamentally more secure and reliable across diverse architectures and applications. My goal is to make these models more practical and reliable for real-world applications, bridging the gap between academic advances and practical implementation.

Education

Sapienza University of Rome *Rome,Italy*

PhD in Computer Science *Nov 2023 - present*

- Areas of Research: Adversarial Machine Learning, AI Safety, Machine Unlearning
- Supervisor: Prof. Iacopo Masi

Sapienza University of Rome *Rome,Italy*

MSc in Computer Science *Sept 2021 - Oct 2023*

- Grade: 110/110 cum laude
- Thesis: Probing the Energy Landscape of Discriminative Classifiers with Adversarial Perturbations

University of Kashmir *Kashmir, India*

B.Tech in Computer Science and Engineering *Sept 2015 - Dec 2019*

- CGPA: 8.01/10
- Final Year Project: Integrating sentiment from Twitter and technical indicators using Machine Learning for stock price movement prediction.

Work Experience

Neptune.ai *Warsaw, Poland*

Guest writer *Dec 2021 - Present*

- Write technical articles related to Artificial Intelligence and Machine Learning
- Conduct research and analysis to ensure accuracy and relevance of the content

Jocata Financial Advisory & Technology *Hyderabad, India*

Associate Machine Learning Engineer *Dec 2020 - Dec 2021*

- Worked in the team for STAR.ai, an Anti-Money Laundering (AML) product that provides recommendations on probable suspicious transactions, by utilizing machine learning techniques
- Conducted R&D which resulted in improvement of accuracy of the ML model used in STAR.ai from 88% to 94%
- Developed expertise in Neo4j, a graphical database, by utilizing it to detect circular transactions and perform data analysis.
- Spearheaded the adoption and integration of MLflow across the organization, overseeing the implementation of this open-source platform for managing and deploying machine learning models
- Involved in supporting the client and monitoring the model

Great Learning *Bangalore, India*

Junior Research Analyst *April 2020 - Dec 2020*

- Developed and delivered technical content related to Machine Learning and Python across multiple mediums, including written articles and video productions, for Great Learning Blog and Great Learning Academy.

Publications

Shedding more light on robust classifiers under the lens of energy-based models
Mujtaba Hussain Mirza, Maria Rosaria Briglia, Senad Beadini, Iacopo Masi
European Conference on Computer Vision, 2024

Why Adversarially Train Diffusion Models?
Maria Rosaria Briglia, Mujtaba Hussain Mirza, Giuseppe Lisanti, Iacopo Masi
International Conference on Learning Representations, 2026

Understanding Adversarial Training with Energy-based Models
Mujtaba Hussain Mirza, Maria Rosaria Briglia, Filippo Bartolucci, Senad Beadini, Giuseppe Lisanti, Iacopo Masi
arXiv preprint arXiv:2505.22486 (2025). 2025

Academic Projects

Contrastive Learning on Point Clouds using Pytorch

Sapienza University of Rome *Link to Github repository*

- This project focuses on exploring the effectiveness of contrastive learning techniques, specifically the SimCLRv2 technique, for learning from non-Euclidean data such as point clouds.

Brain MRI Segmentation Using Pytorch

Sapienza University of Rome *Link to Github repository*

- This project aims to investigate and compare the performance of various deep learning architectures including U-Net, Attention U-Net, R2U-Net, Attention R2U-Net, and U-Net 3+ for brain image segmentation on MRI slices.

Information Extraction Using NLP

Sapienza University of Rome *Link to Github repository*

- In this project, I implemented various Natural Language Processing (NLP) tasks such as Named Entity Recognition, Semantic Role Labelling and Coreference Resolution.

Machine Learning Interpretability using Visual Analytics

Sapienza University of Rome *Link to Github repository*

- We design a visual analytics system designed to provide a comprehensive understanding of complex machine learning models. The goal of the project is to enable the identification and interpretation of different model strategies to gain insights into how the models work.

Face Recognition System with Spoof Detection

Sapienza University of Rome *Link to Github repository*

- This project uses a Siamese Network for feature extraction, a Deep Learning classifier to detect spoofing attacks and blink detection for liveness detection to create a robust facial recognition system that can recognize individuals accurately and reliably.

Image Classification Using Pyspark and Elephas

Sapienza University of Rome *Link to Github repository*

- This project uses technologies such as Pyspark, Elephas and Streamlit to create a web app that can classify the diseases in plants based on images of their leaves. The main aim of the project was to explore the capabilities of Pyspark on large datasets.

Time Series Analysis for Stock Price Forecasting

University of Kashmir *Link to Github repository*

- This project combines time series analysis and sentiment analysis to predict the future price movement of AAPL stock. The historical data of AAPL, NASDAQ, and S&P500 is used to train Machine Learning Models to predict future outcomes. We also tried to capture the sentiment of people regarding the stock by doing a sentiment analysis of tweets mentioning AAPL stock.

Skills

Technical Skills

- Programming Languages: Python, C/C++, HTML/CSS, JavaScript,Solidity
- Machine Learning : Pandas,Keras,PyTorch, NumPy, Scikit-learn, NLTK, OpenCV,Huggingface
- Big Data Tools: Spark (PySpark)
- Databases: Cassandra,SQL, Neo4j, PostgreSQL,Tallend
- Blockchain: Smart Contract Development
- Cloud Computing: Amazon Web Services (AWS)
- Version Control: Git
- Operating Systems: Linux, Shell
- Data Visualization: D3.js, Matplotlib, Seaborn
- Other Tools: Jupyter Notebook, Docker

Additional Skills

- Data Analysis and Interpretation
- Technical writing
- Critical Thinking
- Engaging Presentation
- Effective Communication
- Continuous Learning