

# Hafiza Hajrah Rehman

[hafizahajra6@gmail.com](mailto:hafizahajra6@gmail.com) | [LinkedIn](#) | [GitHub Portfolio](#)

## EDUCATION

### Saarland University

*MSc in Data Science and AI*

### University of Central Punjab

*Bachelors in Computer Science*

Saarbrücken, Germany

*March 2024 – Present*

Lahore, Pakistan

*Dec 2019 – July 2023*

## EXPERIENCE

### ML/Data Analyst

*Zeeoutsourcing UK*

Remote

*Nov 2022 – Feb 2024*

- Contributed to ongoing AI research projects focused on IoT security and energy-efficient intrusion detection.
- Worked on the development of **SFlexCrypt**, a framework for detecting Sinkhole attacks in wireless sensor networks using machine learning.
- Performed data preprocessing, model training, and evaluation on the Contiki-Cooja dataset to improve detection accuracy and energy efficiency.
- Collaborated with the research team to analyze results and support publications on IoT-based security and power optimization in smart city applications.

### AI Engineering Intern

*Zeeoutsourcing UK*

Remote

*Aug 2022 – Oct 2022*

- Assisted in ML model development for IoT applications, focusing on performance tuning and evaluation
- Contributed to literature review and data preparation for energy-efficient IoT systems.
- Assisted in documentation, result visualization, and report preparation for research publications.

## TECHNICAL SKILLS

**Programming Languages:** Python, SQL, MATLAB, C++, C#, JavaScript, R, HTML/CSS

**Frameworks & Libraries:** PyTorch, Scikit-learn, XGBoost, React.js, Django, LoRA

**ML/DL Techniques:** Supervised & Unsupervised Learning, Model Evaluation, SMOTE, Grad-CAM, LIME, Contrastive Learning (SimCLR, MoCo)

**NLP & GenAI:** Hugging Face, Transformers, Masked LM, Fine-tuning LLMs, Prompt Engineering

**Data Analysis:** Pandas, NumPy, EDA, Feature Engineering, Statistical Analysis, Matplotlib, Seaborn, Tableau

**Cloud & DevOps:** AWS (SageMaker, S3, EC2), Git, Docker, Google Colab, Jupyter

**Tools:** RapidMiner, OpenCV, Scikit-learn Pipelines

**Domains:** Data Science, Trustworthy AI, Computer Vision, NLP, Generative AI, Autonomous Driving

## CERTIFICATIONS

AWS Academy Machine Learning Foundations — AWS Academy Graduate

AWS Academy Data Engineering — AWS Academy Graduate

AWS Academy Natural Language Processing — AWS Academy Graduate

Artificial Intelligence Course (SIC Cohort-II) — Samsung Innovation Campus

## PROJECTS

### Pedestrian Detection with Danger Estimation | *Python, OpenCV, PyTorch*

- Developed a deep learning model to detect pedestrians and assess accident risk in real-time from surveillance feeds.
- Integrated distance estimation and bounding box tracking to compute dynamic “danger zones.”
- Achieved third position in university FYP competition among 120+ projects.

### Membership Inference Attack on ResNet18 | *PyTorch, CIFAR-10*

- Implemented shadow model and attack classifier to determine training set membership, exposing privacy leakage in pretrained models.
- Achieved over 80% attack success rate on CIFAR-10 subset, demonstrating critical privacy risks.

### **Robust Adversarial Training for CIFAR-10** | *PyTorch, FGSM, PGD*

- Applied adversarial training with FGSM and PGD to harden ResNet18 against evasion attacks.
- Improved robust accuracy from 0% to 48% under PGD attack while maintaining 78% clean accuracy.

### **Fine-tuning Chemical LLMs with LoRA & Influence Sampling** | *Hugging Face, PyTorch*

- Compared LoRA, BitFit, and iA3 for parameter-efficient fine-tuning on chemical language datasets.
- Found LoRA most stable under influence-based sampling, improving downstream task performance.

### **Explainable AI for Medical Diagnosis** | *LIME, SHAP, Counterfactuals, PyTorch*

- Proposed interpretable AI models for healthcare diagnostics, combining LIME, SHAP, and relevance propagation.
- Enhanced diagnostic transparency and clinician trust while maintaining high predictive accuracy.

### **Conversational AI Help Desk Bot** | *Python, NLP, Dialogflow*

- Built a university help desk chatbot to handle student queries using intent recognition and dialogue management.
- Integrated FAQ and contact database, reducing manual query load by 60%.

## **ACHIEVEMENTS**

---

3rd Place — Final Year Project Competition at University of Central Punjab for “Pedestrian Detection with Danger Estimation” (2023)

Selected Project — Represented University at FICS NUST with “Intellivision: AI Content Creation and Video Lecture Generator” (2023)

Research Contribution — Collaborated with Liaqat Majeed, a professor from NUCES–FAST Lahore on research in Theory of Automata, Mathematical Computing, and Machine Learning (2022)

Research Contribution — Sinkhole Attack Detection framework (SFlexCrypt) integrated into IoT security research at Zeeoutsourcing UK (2023)

Samsung Innovation Campus — AI Cohort-II Graduate (2022)

## **VOLUNTEERING / LEADERSHIP**

---

### **Pakistan Student Association Saarland** | *President*

- Led academic, cultural, and community initiatives for Pakistani students at Saarland University.

### **LIVEX-UMT** | *ML Instructor (Volunteer)*

- Taught foundational and applied concepts in Machine Learning to undergraduate students.

### **Al-Khidmat Foundation** | *Volunteer*

- Participated in plantation and ration drives, contributing to local community welfare (2023).

### **TAAKRA'23** | *Management Head*

- Coordinated logistics and management for Pakistan's largest multi-category inter-university competition.

### **UCP Literary & Engineering Societies** | *Director Linguistics & Writer's Group*

- Mentored teams in creative and technical writing; organized inter-departmental literary workshops and competitions.

## **LANGUAGES**

---

English (Fluent), German (Intermediate), Urdu, Punjabi, Arabic