Raza Imam

(+971) 523 308 676 raza.imam@mbzuai.ac.ae Linkedin Github Website

Education

Mohamed Bin Zayed University of Artificial Intelligence, Abu Dhabi, UAE **August 2022 – June 2024**
Master of Science in Machine Learning *GPA: 3.63/4*
Coursework: Probabilistic Machine Learning, Trustworthy AI, Medical Imaging
Thesis (on-going): Test time prompt tuning for zero-shot generalization

Aligarh Muslim University, Aligarh, India **August 2019 – July 2022**
Bachelor of Science in Computer Science *GPA: 8.93/10*
Dissertation: Attribute Based Encryption in Cloud Based Health Services

Research Interests

Trustworthy AI, Vision-Language Models, Healthcare Security, Sustainability, Explainable AI

Experience

Sprint AI Lab **September 2022 – Present**
Research Student *MBZUAI, UAE*
- Working on improving zero shot classification of CLIP using Test time prompting to learn adaptive prompts on the fly
- Developed an adversarial detection method for ViT that uses attention on the fly to classify attack and clean samples
- Introduced Generic prompts for robust vision-language models that increases accuracy without fixed template prompts

Fujairah Research Center **June 2023 – September 2023**
Visiting Researcher *Fujairah, UAE*
- Combined the foundational models SAM & GroundingDINO for automated annotation of raw CCTV/video dataset
- Introduced zero-shot fine tune distillation which distills knowledge from large GroundingDINO to lightweight YOLOv8
- Evaluated SOTA object detection algorithms like YOLO models for enhancing physical security in camel farm settings

Aligarh Muslim University **March 2021 – July 2022**
Research Assistant *Aligarh, India*
- Developed XRSA, an enhanced version of RSA public key encryption algorithm that is based on xor-operations
- Worked on a fast variant of RSA algorithm by parallelizing the RSA algorithm using C's OpenMp & GMP libraries
- Developed a Attribute Based Encryption (CPABE) & Blockchain based framework for secure EHR sharing across Cloud

National University of Malaysia (UKM) **September 2021 – December 2021**
Research Intern *Bangi, Malaysia*
- Conducted a Systematic Literature Review on cyberbully detection on social media using CNNs

Computer Science Society **June 2021 – August 2021**
Research Intern *AMU, India*
- Analyzed Ramganga River's heavy metal levels pre and post-Covid19 with XGBoost and LightGBM leading in accuracy
- Investigated potato disease classification and quality prediction using Transfer Learning via FastAI in Deep Learning
- Developed a CNN model for art quality classification, trained on our CSS team's poster competition dataset

Indian Institute of Information Technology **May 2021 – August 2021**
Research Intern *Allahabad, India*
- Evaluated DNS-PKI options with-&-without central authority using Blockchain, for distributed and P2P frameworks
- Researched Ethereum blockchain consensus algorithms, smart contracts, and DApps
- Explored Blockchain use cases in IoT for data storage, privacy, authentication, and access control

Projects

Attack agnostic Adversarial Detection using XAI in Medical Imaging | *Git* **September 20203 – Present**
- Introduced a adversarial detection method that uses attentions on the fly to differentiate among clean/attack samples
- In ViT-B/16, offline/proxy mean attentions are introduced to distinct the test samples using several similarity metrics

On enhancing the robustness of Vision Transformers: Defensive Diffusion | *Git* **February – June 2023**
- Introduced Diffusion to the ViT as an adversarial purifier to eliminate adversarial noise introduced in the input image
- Utilized the reverse diffusion process to denoise the attack sample, resulting in clean sample, which is then fed into ViT

Enhancement of Ensembling ViTs for Chest XRay Classification | *Git* **Januray – August 2023**
- Enhanced Ensembling ViTs by replacing MLP blocks with CNN along with Adversarial Training and Distillation
- Resulting architecture shows computational efficiency with $70x$ times lighter model and enhanced robustness of +9%

Generic Prompts for Robust Vision Language Models | *Git* **Januray – June 2023**
- Explored CLIP with automated class-specific prompts instead of manual fixed templates, achieving competitive results
- Introduced a set of prompts that includes class labels to differentiate more between the classes during inference

Transfer Learning Approach for Imbalance Classification of Brain Tumor MRI | *Git* **August – December 2022**
- Employed 8 transfer learning models integrated with CNNs to increase the classification accuracy on 4 cancer types
- Applied Focal loss, Cross Entropy, Data Augmentation, SMOTE, and ADASYN to solve imbalance problems

Publications

- Raza Imam, I. Almakky, S. Alrashdi, B. Alrashdi, M. Yaqub, **SEDA: Self-Ensembling ViT with Defensive Distillation and Adversarial Training for robust Chest X-rays Classification,** *DART Workshop, 26th MICCAI, Vancouver, Canada, 2023* | *Publication link*
- Raza Imam, M. Huzaifa, MEA. Azz, **On enhancing the robustness of Vision Transformers: Defensive Diffusion,** *27th Conference on MIUA 2023, Scotland, 2023* | *Publication link*
- Raza Imam, MT. Alam, **Optimizing Brain Tumor Classification,** *Epistemic AI Workshop, 39th UAI Conference, Pittsburgh, USA, 2023.* | *Publication link*
- QM. Areeb, M. Nadeem, SS. Sohail, Raza Imam, F. Doctor, et al., **Filter bubbles in recommender systems: Fact or fallacy—A systematic review,** *Wiley Reviews: Data Mining & Knowledge Discovery, 2023* | *Publication link*
- Raza Imam, F. Anwer, **Practically adaptable CPABE based Health-Records sharing framework,** *Under Review, 2023* | *Publication link*
- Raza Imam, F. Anwer, Mohammad Nadeem, **An Effective and Enhanced RSA based Public Key Encryption Scheme (XRSA),** *International Journal of Information Technology, 2022* | *Publication link*
- N. Fatima, Raza Imam, M. Belal, P. Verma, G. Ullah, **A Computer Vision-Based Quality Analysis of Potatoes,** *Sustainability and Resilience Conference, Bahrain, 2022* | *Publication link*
- N. Fatima, Raza Imam, M. Belal, AM. Siddiqui, R. Sarah, **Toxicity Assessment of River Ramganga,** *Sustainability and Resilience Conference, Bahrain, 2022* | *Publication link*
- Raza Imam, K. Kumar, SM. Raza, R. Sadaf, F. Anwer, et al., **A systematic literature review of attribute based encryption in health services,** *Journal of King Saud University, 2022* | *Publication link*
- Raza Imam, F. Anwer, **An Empirical Study of Secure and Complex Variants of RSA Scheme,** *International Conference on Cyber Security, Privacy and Networking, Thailand, 2021* | *Publication link*
- M Anas, Raza Imam, F. Anwer, **Elliptic curve cryptography in cloud security: a survey,** *12th International Conference on Cloud Computing, Data Science & Engineering, India, 2022* | *Publication link*
- Raza Imam, QM Areeb, A. Alturki, F. Anwer, **Systematic and critical review of RSA based public key cryptographic schemes: Past and present status,** *IEEE Access, 2021* | *Publication link*
- QM. Areeb, Raza Imam, N. Fatima, M. Nadeem, **AI art critic: Artistic classification of poster images using neural networks,** *International Conference on Data Analytics for Business and Industry, Bahrain, 2021* | *Publication link*

Skills

Technical: PyTorch, Tensorflow, Keras, Git, Data Structures, AWS, SLURM
Programming Languaes: Python, C/C++, JAVA, C#
Languages: English (IELTS - 8.0), Hindi, Urdu

Achievements

- Selected for **Spotlight Presentation**, at DART Workshop, 26th MICCAI, Vancouver, Canada **2023**
- **Nominated for Best Paper** Award, under Abstract Category, at 27th Conference on MIUA, Scotland **2023**
- Secured **Fully Funded Scholarship** for Graduate School at MBZUAI for MS program in Machine Learning **2022**
- Achieved **2nd place and Cash prize** at the Ideathon, AMU, for presenting blockchain solution in medical records **2021**
- Secured **92 Percentile** in JEE Mains examination among more than a million of applicants **2019**
- Received **Merit-Cum Means Scholarship**, 2018 for attending bachelor's program by Indian government **2018**
- Secured **3rd place** among all district schools in the National Mathematics Olympiad, TIFR **2013**

Positions

- Acting as **Ambassador** at Graduate Students Council, MBZUAI **2023 – Present**
- Acted as **Sports Vice President** at Graduate Students Council, MBZUAI **2023 – 2023**
- Acted as **Cybersecurity Lead** at Google Developer Student Club, Aligarh Muslim University **2021 – 2022**
- Acted as a **Member** at Computer Science Society at Department of Computer Science, AMU **2019 – 2022**
- Acted as a **Member** at UAV-ZHCET, Aligarh Muslim University **2020 – 2021**
- Acted as **Sports Captain** at Senior School, represented at State-level Multi-Sports Competition **2017 – 2018**

Certifications / MOOCs

- Generative AI with Large Language Models, DeepLearning.AI **2023**
- Finetuning Large Language Models, DeepLearning.AI **2023**
- Neural Networks and Deep Learning, DeepLearning.AI **2022**
- Improving Deep Neural Networks: Hyperparameter Tuning, Regularization and Optimization, DeepLearning.AI **2022**
- Cryptography, Stanford University, USA **2021**
- Machine Learning Essentials, Amazon Web Services **2021**
- Information Security & Blockchain Workshop, National Institute of Technology, Hamirpur **2021**
- Virtual Experience in Cyber Security, Goldman Sachs **2021**

References

References are available upon request