Anukriti Singh

Research Scholar at IIIT-B

anukriti.singhofc@gmail.com Bengaluru, Karnataka

PROFESSIONAL EXPERIENCE

CDAC 09/2022 – 01/2025

Project Engineer Bengaluru, India

- Led the development of 20 attacks for computer vision tasks, optimizing evasion and poisoning attacks, resulting in a **23% increase** in attack performance.
- Implemented 5 Few-Shot Learning algorithms for ALS disease diagnosis using audio data, achieving a maximum accuracy of **92.38%**.
- Developed 3 AI models for malware detection through bitmap image analysis achieving accuracy of **91.5%** for 26 classes.
- Authored comprehensive Functional Requirement Specifications (FRS) and optimized product flow to ensure alignment between technical development and user needs.
- Developed an interactive dashboard showcasing analytics for ATM fraudulent transactions using React and Django.
- Contributed to new Project Proposals, Workshops & Trainings.

Cognizant Technology Solutions 01/2022 – 08/2022

Programmer Analyst Trainee

- Interned in the Data Information (full stack) domain, and gained training in data engineering tools such as Power Informatica, in SQL and in Cloud Technologies.

Varidus Asia Pacific Ventures 05/2021 – 09/2021

Lead Data Analyst (Intern)

- Led a team of Data Science interns in an experimental project focused on developing a Random Forest machine learning model to predict the success likelihood of Initial Public Offerings (IPOs).

SKILLS

Languages: — Python, C, Java

Frameworks & Libraries: — PyTorch, TensorFlow, Keras, Scikit-Learn, OpenCV

Specializations: — Adversarial Machine Learning and Few Shot Learning

Tools, Technologies & Others: — Git, Slurm, Linux

PROJECTS

Adversarial Attack Simulation Framework

PyTorch, Tensorflow, Keras, Adversarial Robustness Toolbox, Advertorch

- Associated with C-DAC in collaboration with SETS, IIT-Jammu ,Madras and Delhi

- Led the Attack-simulation Module and developed APIs for 20 Adversarial Attacks targeting computer vision models, optimized attack performance by 23% using 2 algorithms against 4 metrics.

Few Shot Learning for Bulbar Amyotrophic Lateral Sclerosis diagnosis
Easyfsl
- Designed and implemented 5 Few Shot Learning algorithms achieving a maximum accuracy of 92.38%, significantly improving diagnostic capabilities in limited data environments.

Malware Detection using Deep Learning via Bitmap Image Analysis
Deep Neural Networks, Python, PyTorch, Vision Transformers
- Developed a Vision Transformer-based model to detect malware using bitmap image analysis.
- Designed and implemented transfer learning models, including ResNet-50 and InceptionV3

CERTIFICATES

- AI Security Essentials
- Microsoft Certified: Azure AI Fundamentals (AI-900)
- Generative AI with Large Language Models

EDUCATION

MS by Research (DSAI) 01/2025 – present
IIIT Bangalore

Bachelor's in Engineering and Technology (CSE) 06/2022
Amity University
8.38 CGPA