

# AMITY UNIVERSITY

-----UTTAR PRADESH-----

## Amity School of Engineering and Technology

In-House Practical Training

Student Name NIRANJAN PRAVEEN  
Enrollment No A2305223087  
Programme B.Tech (Computer Science & Engineering)  
Company's Name and Address Amity University, Noida  
Amity Rd, Sector 125, Noida, Uttar Pradesh 201301  
695101

### Industry Guide

Name

Designation

Contact Number

Ph.(O) : (R) :  
Mobile :  
Fax :  
E-mail : nmishara1@amity.edu

### Project Information

1) Project Duration : (53 Days)

a) Date of Summer Internship commencement (13/05/2025)

a) Date of Summer Internship Completion (04/07/2025)

2) Topic

Interactive Web Dashboard for Visualizing Adversarial Attacks on Image Classifiers

3) Project Objective

To design and develop an interactive web-based dashboard that visualizes the effects of adversarial attacks on image classification models, highlighting their vulnerabilities through intuitive and real-time comparisons.

4) Methodology to be adopted

Methodology to be Adopted: 1. Utilize pre-trained convolutional neural network models (e.g., ResNet) for image classification tasks. 2. ? Implement gradient-based adversarial attack algorithms, such as the Fast Gradient Sign Method (FGSM). 3. ?Develop an interactive web interface using Streamlit to allow users to apply attacks, adjust parameters, and observe model predictions. 4. ?Incorporate visual tools to display original vs. perturbed images, prediction confidence levels, and perturbation metrics.

5) Brief Summery of project(to be duly certified by the industry guide)

This project focuses on creating an interactive visualization tool to demonstrate how adversarial attacks can mislead deep learning-based image classifiers. By integrating attack algorithms with a user-friendly web interface, the system will allow users to explore the impact of minimal input modifications on model predictions, thereby enhancing understanding of AI model robustness and security.

Signature  
(Student)

Close Print

Signature  
(Industry Guide)

Signature  
(Faculty Guide)