**Instructions to Run Poisoning Attack**

### ****Step 1: Activate the Environment****

Run the following command to activate the virtual environment:

# Replace 'your\_env' with the actual environment name

source your\_env/bin/activate # For Linux/macOS

your\_env\Scripts\activate # For Windows (Command Prompt)

### ****Step 2: Deploy the Model on the Server****

Execute the deployment script:

python deploy.py

### ****Step 3: Open Jupyter Notebook****

Start Jupyter Lab:

jupyter lab

Then, navigate to the **"False Data Injection"** and **"Adversarial Poisoning"** notebooks and execute the cells one by one.

### ****Step 4: Analyze the Results****

Compare the model’s performance before and after the poisoning attack to observe its impact.