# Project Design Phase-I Solution Architecture

|  |  |
| --- | --- |
| Date | 25 October 2023 |
| Team ID | Team-591481 |
| Project Name | Adversarial Attacks And Defenses |
| Maximum Marks | 4 Marks |

**Solution Architecture:**

This system majorly focuses on static image input and defense architecture:

* Combination of two models to effectively defend both Black box and White Box attack.
* Randomization method acts as a backup for filtration performed by auto-encoder there by increasing the robustness of the proposed model.
* Grad-CAM allows the model to predict the highlighted important region based on classification.

# Solution Architecture Diagram:

A diagram of a company

Description automatically generated