CptS 528 Advanced Cyber Security

Fall 2025

Team: Ye_MLAdversary

Project Deliverable 2-2

1. Architectural Design

The architectural design diagram is shown in Figure 1 in the appendix section.
Dataset Manager: Load and preprocess CIFAR-10 for train/test dataset
Model Trainer: Build CNN to train and validate the dataset
Adversarial Engine: Generate adversarial examples using pluggable attacks
Defense Module: Apply defense
Evaluator: Compute accuracy and plots
Experiment Orchestrator: Ensuring all component execute in the right sequence
Logging & Config: Centralizes configs, seeds, and metrics logging
The main pattern of the architecture design is pipeline pattern. The process is from dataset -> model -> attack -> defense -> evaluation. Plugin pattern is also used in the adversarial engine and defense module components to enable flexible addition or substitution of attack and defense algorithms without changing the pipeline structure.

2. Component-level Design

The component-level design diagram is shown in Figure 2 in the appendix section.

3. Code

Code update is committed to the GitHub repository

4. Software Documentation

Software documentation is updated to the README.md.

Before running the project, install the required Python libraries:
`pip install torch torchvision pyyaml`

How to Run:
`python main.py`
CIFAR-10 will be automatically downloaded to ./data during the first run.
Trained model weights will be saved to the path specified in save_path.

Appendix
Diagrams

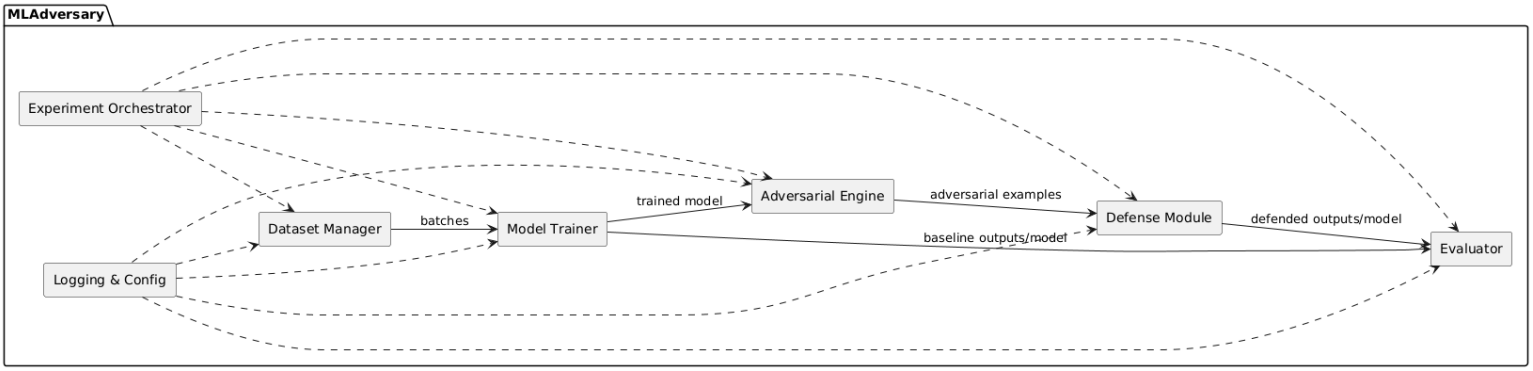

Figure 1 – Architectural Design Diagram

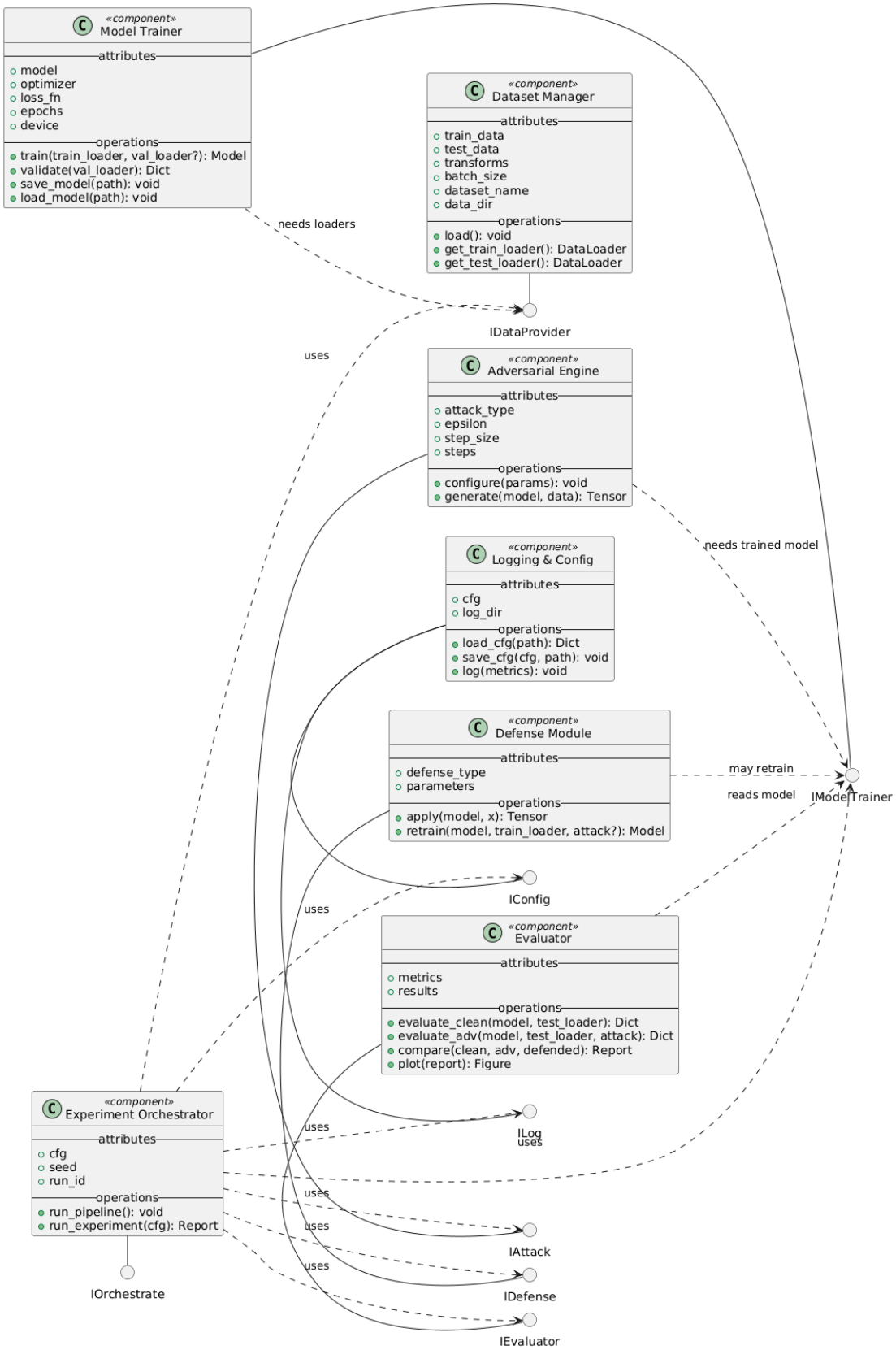

Figure 2 – Component-Level Design Diagram