AI VERIFY

AI GOVERNANCE TESTING FRAMEWORK AND TOOLKIT

Quick Start Guide

Installation (via Dockerfile)

To build and run from source code, check out the User Manual.

1 Requirements

System

- OS Ubuntu 22.04
- CPU > 4 cores
- Memory > 16GB
- Free Space > 10GB

Software

- Docker

2 Build

Download `compose.yaml` file to setup docker build.

```
wget https://raw.githubusercontent.com/aiverify-foundation/aiverify/refs/heads/main/deployment/docker-compose/compose.yaml
```

Ensure this file is in the same folder where you install and start services.

3 Install and Start Services

1 For Manual Test Execution and upload, use

```
docker-compose --profile portal up -d
```

2 For Automated Test Execution via Portal, use

```
docker-compose --profile portal --profile automated-tests-venv up -d
```

3 Open http://localhost:3000

Prepare Input Files

The AI Verify Toolkit supports technical tests for these models & datasets:

Binary Classification

Scikit-Learn 1.2.2
- Logistic Regression
- Decision Tree
- Gradient Boosting Classifier
- Random Forest
- Bagging Classifier
- Perceptron

Tensorflow 2.12.0
- Keras Sequential

XGBoost 1.7.5
- XGB Classifier
- XGB Booster

LightGBM 3.3.5
- LGBM Classifier

Pytorch
- torch.nn.Module

Multiclass Classification

Scikit-Learn-1.2.2
- Logistic Regression
- Decision Tree
- Gradient Boosting Classifier
- Random Forest
- Bagging Classifier
- Perceptron

Tensorflow 2.12.0
- Keras Sequential

XGBoost 1.7.5
- XGB Classifier

Pytorch
- torch.nn.Module

Regression

Scikit-Learn 1.2.2
- Linear Regression
- Decision Tree
- Gradient Boosting Classifier
- Random Forest Regression

Tensorflow 2.12.0
- Keras Sequential

XGBoost 1.7.5
- XGB Regressor

Pytorch
- torch.nn.Module

Dataset Formats Supported
Tabular: Pandas, Delimiter-separated Values (comma, tab, semicolon, pipe, space, colon)
Image: .jpeg, .jpg, .png

You will need the following files:

AI Model or Pipeline
The prediction model to be tested. You can include any data pre-processing as part of a pipeline. (only scikit-learn pipelines are supported)

Testing Dataset
Any dataset to be used for Testing

Ground Truth Dataset*
A dataset that contains the ground truth. For image datasets, this is the annotated ground truth file and should contain the image file names and ground truth.

Background Dataset*
A dataset that is representative of the dataset's population.

* The Testing Dataset can be used if it fulfils the requirements.

Running Tests

Running Tests via Command Line

1 Install the Algorithm

```
pip install aiverify-accumulated-local-effect
```

2 Run the Test

```
#!/bin/bash
root_path="<PATH_TO_FOLDER>/aiverify/stock-plugins/user_defined_files"
python -m aiverify_accumulated_local_effect \
    --data_path  $root_path/data/sample_bc_credit_data.sav \
    --model_path $root_path/model/sample_bc_credit_sklearn_linear.LogisticRegression.sav
    --ground_truth_path $root_path/data/sample_bc_credit_data.sav \
    --ground_truth default \
    --model_type CLASSIFICATION
```

Replace <PATH_TO_FOLDER> with the actual path to your files.

3 Check output

Output folder will contain results.json and other artefacts (images).

4 Upload results

Zip the entire output folder and upload to portal for further analysis and reporting.

Running Tests via AI Verify Portal

Prerequisites

Ensure the following services are running:
- *Test Engine Worker: At least one worker must be active.*
- *Valkey service: Required for task queue*

1 Upload the Model

Navigate to **Homepage > Manage > Models > Upload Model**.
Follow on-screen instructions to upload model file to be tested.

2 Upload the Dataset

Navigate to **Homepage > Manage > Data > Upload Dataset**
Follow on-screen instructions to upload test and ground truth datasets to be tested.

3 Run the Test

Navigate to **Homepage > Manage > Test Results > Run New Tests**
Configure test parameters and initiate the test.

4 View results

Upon successful completion, results will be uploaded to the portal.

Completing AI Verify Process Checklist & Fairness Tree

To complete AI Verify Process Checklist

1 Access the Checklist Section

Navigate to **Homepage > Manage > User Inputs > AI Verify Process Checklists**

2 Create or Update Checklist

To create a New Checklist: Select **"Add Checklists".**
To update an existing checklist, select an existing checklist to update it.

3 Fill in the Checklist

- Click on each checklist item to provide the required information.
- Use the **sidebar on the left** to track your progress.

4 Export or Import Checklists (Optional)

- Export to Excel: Export the AI Verify checklists to an Excel file for offline editing.
- Import from Excel: Import an updated checklist from an Excel file.

To select the Fairness Tree Using Fairness Metrics

1 Access the Fairness Tree Section

Navigate to **Homepage > Manage > User Inputs > Fairness Tree**.
Follow on-screen instructions to upload model file to be tested.

2 Select Fairness Metrics

Follow the on-screen instructions to select the appropriate fairness metrics.
Ensure the test is a **"fairness classification test"**, as this feature is only applicable for Classification models.

Generating the AI Verify Report

1 Create a New Project

Navigate to **Homepage > Create New Project**
Enter the **Project Name, Description, Title** and **Name**.
Select the template "**AI Verify Summary Report Template for Classification Models**".

2 Configure User Inputs

- Navigate to Homepage > Manage > User Inputs, select:
  - AI Model to test
  - Test Results uploaded to the portal.
  - AI Verify Process Checklists
  - Fairness Tree records (if applicable).
- Click the **Next** button to proceed.

3 View and Download the Report

- The web report will be generated and displayed.
- Use the **Print** button to download the report in your preferred format.