CogniGuard Model Security Report

Error during model inspection: Weights only load failed. This file can still be loaded, to do so you have two options, [1mdo those steps only if you trust the source of the checkpoint [0m.

(1) In PyTorch 2.6, we changed the default value of the `weights_only` argument in `torch.load` from `False` to `True`. Re-running `torch.load` with `weights_only` set to `False` will likely succeed, but it can result in arbitrary code execution. Do it only if you got the file from a trusted source.

(2) Alternatively, to load with `weights_only=True` please check the recommended steps in the following error message.

WeightsUnpickler error: Unsupported global: GLOBAL __main__.SmallCNN was not an allowed global by default. Please use `torch.serialization.add_safe_globals([__main__.SmallCNN])` or the `torch.serialization.safe_globals([__main__.SmallCNN])` context manager to allowlist this global if you trust this class/function.

Check the documentation of torch.load to learn more about types accepted by default with weights_only https://pytorch.org/docs/stable/generated/torch.load.html.

Error during architecture analysis: Weights only load failed. This file can still be loaded, to do so you have two options, [1mdo those steps only if you trust the source of the checkpoint [0m.

(1) In PyTorch 2.6, we changed the default value of the `weights_only` argument in `torch.load` from `False` to `True`. Re-running `torch.load` with `weights_only` set to `False` will likely succeed, but it can result in arbitrary code execution. Do it only if you got the file from a trusted source.

(2) Alternatively, to load with `weights_only=True` please check the recommended steps in the following error message.

WeightsUnpickler error: Unsupported global: GLOBAL __main__.SmallCNN was not an allowed global by default. Please use `torch.serialization.add_safe_globals([__main__.SmallCNN])` or the `torch.serialization.safe_globals([__main__.SmallCNN])` context manager to allowlist this global if you trust this class/function.

Check the documentation of torch.load to learn more about types accepted by default with weights_only https://pytorch.org/docs/stable/generated/torch.load.html.

Error during baseline evaluation: Weights only load failed. This file can still be loaded, to do so you have two options, [1mdo those steps only if you trust the source of the checkpoint [0m.

(1) In PyTorch 2.6, we changed the default value of the `weights_only` argument in `torch.load`

from `False` to `True`. Re-running `torch.load` with `weights_only` set to `False` will likely succeed, but it can result in arbitrary code execution. Do it only if you got the file from a trusted source.

(2) Alternatively, to load with `weights_only=True` please check the recommended steps in the following error message.

WeightsUnpickler error: Unsupported global: GLOBAL __main__.SmallCNN was not an allowed global by default. Please use `torch.serialization.add_safe_globals([__main__.SmallCNN])` or the `torch.serialization.safe_globals([__main__.SmallCNN])` context manager to allowlist this global if you trust this class/function.

Check the documentation of torch.load to learn more about types accepted by default with weights_only https://pytorch.org/docs/stable/generated/torch.load.html.

Error during robustness evaluation: Weights only load failed. This file can still be loaded, to do so you have two options, [1mdo those steps only if you trust the source of the checkpoint [0m.

(1) In PyTorch 2.6, we changed the default value of the `weights_only` argument in `torch.load` from `False` to `True`. Re-running `torch.load` with `weights_only` set to `False` will likely succeed, but it can result in arbitrary code execution. Do it only if you got the file from a trusted source.

(2) Alternatively, to load with `weights_only=True` please check the recommended steps in the following error message.

WeightsUnpickler error: Unsupported global: GLOBAL __main__.SmallCNN was not an allowed global by default. Please use `torch.serialization.add_safe_globals([__main__.SmallCNN])` or the `torch.serialization.safe_globals([__main__.SmallCNN])` context manager to allowlist this global if you trust this class/function.

Check the documentation of torch.load to learn more about types accepted by default with weights_only https://pytorch.org/docs/stable/generated/torch.load.html.

Explainability analysis skipped - module not implemented yet

Trojan detection skipped - module not implemented yet