NGI EXPLORERS

# CHALLENGE #22
# USC-AML-01

## Adversarial Machine Learning

Meet the expectations of this US Node through the technology challenge described below


## GOALS

The project involves several challenging problems in the context of adversarial machine learning (https://softsys4ai.github.io/athena/):

- Probabilistic ATHENA: Bayesian Neural Networks as WDs. Bayesian ensemble.
- Hybrid ATHENA: An ensemble on hybrid DL models.
- Ensemble-based on the distribution of transformations. In which, instead of a single transformation variant, each WD will be trained on the distribution of transformations.
- Automated construction of ATHENA (multi-objective optimization problem), Synthesized ATHENA (Synthena), a framework for automatically constructing, adapting, and maintaining a dynamic ensemble.

## DETAILS

The goal is to outperform the original adversarial defense, ATHENA (https://github.com/csce585-mlsystems/project-athena)

## SKILLS REQUIRED

Machine learning knowledge, good programming skills and relevant theory.

FUNDED BY NGI

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 825183