Adversarial Attacks:

Implemented for CIFAR10, but can easily be modified for any other dataset.

Custom attacks:

* Model: keras based CIFAR model (model should be trained before generating attacks)
* Two white box attacks based on technique CW0 and CW2
* Two Black box attacks Momentum based attacks and PGD
* To run code type: python Custom\_Attacks/Generate\_Adversarial.py

Generated using Cleverhans Library:

* Model: Wide ResNet using Tensorflow (Model should be trained before generating )
* Use cleverhans library to generate deepFool, PGD and FGSM based attacks.
* Important feature is batch implementation deepFool attacks, which is not straight forward like all other attacks
* To run Code type: python Cleverhans\_Attacks/GenAdv\_usingCleverhans.py