Stage 1: Data Preparation (Correct & Adversarial Examples) Fullyconnected **Attack Generation** MaxPooling Flatten Convolution Layer Layer (3 x3) Kernel size 3 x3) pool size valid padding Example **Example** Correct **PGD BIM FGSM** Deepfool **Examples** Aversarial **Examples Generate Adversarial Examples UMAP Visualization Train CNN Model**





