Robust Defenses

Introduction

<1 min

The concerns associated with AI have led to a need for robust defenses. While detection is essential, there is also a need to defend both target systems and potential input data from AI.

In recent events, we've seen several ethical and legal battles focused on protecting data used by AI for training purposes. Individuals have had their likenesses stolen by organizations/users leveraging AI. And various artists/creators have alleged copyright infringement against various AI-based platforms and models. While many of these cases continue to be fought in court, it highlight the importance of robust defense against AI-based systems.

In the coming exercises, we will look at some of these defenses and how they are and can be employed.