Access provided by:
Gokaraju Ranga Raju Institute of Engineering and Technology - HYDERABAD

Sign Out

Adversarial Deep Learning Models With Multiple Adversaries

Publisher: IEEE

Cite This PDF

N. Janapriya ; K. Anuradha ; V. Srilakshmi **All Authors**

46
Full
Text Views

Alerts

Manage Content Alerts
Add to Citation Alerts

Downl
PDF

Abstract: Adversarial machine learning calculations handle adversarial instance age, producing bogus data information with the ability to fool any machine learning model. As the wo... **View more**

Metadata

Abstract:

Adversarial machine learning calculations handle adversarial instance age, producing bogus data information with the ability to fool any machine learning model. As the word implies, “foe” refers to a rival, whereas “rival” refers to a foe. In order to strengthen the machine learning models, this section discusses about the weakness of machine learning models and how effectively the misinterpretation occurs during the learning cycle. As definite as it is, existing methods such as creating adversarial models and devising powerful ML computations, frequently ignore semantics and the general skeleton including ML section. This research work develops an adversarial learning calculation by considering the coordinated portrayal by considering all the characteristics and Convolutional Neural Networks (CNN) explicitly. Figuring will most likely express minimal adjustments via data transport represented over positive and negative class markings, as well as a specific subsequent data flow misclassified by CNN. The final results recommend a certain game theory and formative figuring, which obtain incredible favored ensuring about significant learning models against the execution of shortcomings, which are reproduced as attack circumstances against various adversaries.

Published in: 2021 Third International Conference on Inventive Research in Computing Applications (ICIRCA)

Date of Conference: 02-04 September 2021

DOI: 10.1109/ICIRCA51532.2021.9544889

Date Added to IEEE *Xplore*: 01 October 2021

Publisher: IEEE

ISBN Information:

Conference Location: Coimbatore, India