

Research outputs

Listing of Research outputs

Pierazzi F, Pendlebury F, Cortellazzi J, Cavallaro L. **Intriguing Properties of Adversarial ML Attacks in the Problem Space.** 2020 IEEE Symposium on Security and Privacy. 2020 May 18;1332-1349. <https://doi.org/10.1109/SP40000.2020.00073>

The above report is produced using the following setup

Ordered by: null