

The vulnerability of machine learning systems to adversarial attacks questions their usage in many applications. In this paper, we propose a randomized diversification