به نام ایزد یکتا

تمرین هفتم درس روش پژوهش و ارائه

استاد: دکتر رضا صفابخش

تهیه کننده: بردیا اردکانیان

برسی و مهار مثال‌های خصمانه در یادگیری ماشین

Bibliography

Vancouver

1. Tabassi E, Burns KJ, Hadjimichael M, Molina-Markham AD, Sexton JT. A taxonomy and terminology of adversarial machine learning [Internet]. 2019 Oct [cited 2022 May 27]. Available from: https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8269-draft.pdf

2. Adversarial Examples Are Not Easily Detected | Proceedings of the 10th ACM Workshop on Artificial Intelligence and Security [Internet]. [cited 2022 May 28]. Available from: https://dl.acm.org/doi/abs/10.1145/3128572.3140444

3. Wiyatno RR, Xu A, Dia O, de Berker A. Adversarial Examples in Modern Machine Learning: A Review [Internet]. arXiv; 2019 [cited 2022 May 28]. Available from: http://arxiv.org/abs/1911.05268

4. Yuan X, He P, Zhu Q, Li X. Adversarial Examples: Attacks and Defenses for Deep Learning. IEEE Transactions on Neural Networks and Learning Systems. 2019 Sep;30(9):2805–24.

5. Huang L, Joseph AD, Nelson B, Rubinstein BIP, Tygar JD. Adversarial machine learning. In: Proceedings of the 4th ACM workshop on Security and artificial intelligence [Internet]. New York, NY, USA: Association for Computing Machinery; 2011 [cited 2022 May 27]. p. 43–58. (AISec '11). Available from: https://doi.org/10.1145/2046684.2046692

6. Adversarial Machine Learning Attacks and Defense Methods in the Cyber Security Domain | ACM Computing Surveys [Internet]. [cited 2022 May 27]. Available from: https://dl.acm.org/doi/10.1145/3453158

7. Adversarial machine learning for cybersecurity and computer vision: : Current developments and challenges: WIREs Computational Statistics: Vol 12, No 5. Wiley Interdisciplinary Reviews: Computational Statistics [Internet]. [cited 2022 May 27]; Available from: https://dlnext.acm.org/doi/abs/10.1002/wics.1511

8. Zheng H, Zhang Z, Gu J, Lee H, Prakash A. Efficient Adversarial Training With Transferable Adversarial Examples. In: 2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) [Internet]. Seattle, WA, USA: IEEE; 2020 [cited 2022 May 28]. p. 1178–87. Available from: https://ieeexplore.ieee.org/document/9157681/

9. Goodfellow IJ, Shlens J, Szegedy C. Explaining and Harnessing Adversarial Examples [Internet]. arXiv; 2015 [cited 2022 May 27]. Available from: http://arxiv.org/abs/1412.6572

10. Zhao Z, Dua D, Singh S. Generating Natural Adversarial Examples [Internet]. arXiv; 2018 [cited 2022 May 28]. Available from: http://arxiv.org/abs/1710.11342

11. Zizzo G, Hankin C, Maffeis S, Jones K. INVITED: Adversarial Machine Learning Beyond the Image Domain. In: 2019 56th ACM/IEEE Design Automation Conference (DAC). 2019. p. 1–4.

12. Laskov P, Lippmann R. Machine learning in adversarial environments. Mach Learn [Internet]. 2010 Nov 1 [cited 2022 May 27];81(2):115–9. Available from: https://doi.org/10.1007/s10994-010-5207-6

13. McDaniel P, Papernot N, Celik ZB. Machine Learning in Adversarial Settings. IEEE Security Privacy. 2016 May;14(3):68–72.

14. Machine learning uncertainties with adversarial neural networks | SpringerLink [Internet]. [cited 2022 May 27]. Available from: https://link.springer.com/article/10.1140/epjc/s10052-018-6511-8

15. Brachman RJ, Stone P. Synthesis Lectures on Artificial Intelligence and Machine Learning. :169.

16. Zhang C, Benz P, Imtiaz T, Kweon IS. Understanding Adversarial Examples From the Mutual Influence of Images and Perturbations. In: 2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR). 2020. p. 14509–18.

17. Biggio B, Roli F. Wild patterns: Ten years after the rise of adversarial machine learning. Pattern Recognition [Internet]. 2018 Dec [cited 2022 May 27];84:317–31. Available from: https://linkinghub.elsevier.com/retrieve/pii/S0031320318302565