به نام ایزد یکتا

تمرین دوم درس روش پژوهش و ارائه

­­

استاد: دکتر رضا صفابخش

تهیه کننده: بردیا اردکانیان

**برسی و مهار مثال‌های خصمانه در یادگیری ماشین**

الف)

**موضوع پژوهش: برسی و مهار مثال‌های خصمانه در یادگیری ماشین**

**EXPLAINING AND HARNESSING ADVERSARIAL EXAMPLES IN MACHINE LEARNING**

**واژه‌های کلیدی:**

1. **Machine Learning**
2. **Adversarial**
3. **Adversarial Attacks**
4. **Adversarial Examples**
5. **Explaining**
6. **Harnessing**

**کلمات کلیدی ذکر‌ شده را در موتور‌های مختلف جست و جو می‌کنیم.**

1. **جست‌ و جو با Adversarial + Machine Learning**

**الف) جست و جو در Google (5 صفحه اول)**

**G01:** [**Adversarial machine learning**](https://dl.acm.org/doi/abs/10.1145/2046684.2046692)

**G02:** [**Wild patterns: Ten years after the rise of adversarial machine learning**](https://www.sciencedirect.com/science/article/abs/pii/S0031320318302565)

**G03:** [**Adversarial Machine Learning**](https://www.morganclaypool.com/doi/abs/10.2200/S00861ED1V01Y201806AIM039)

**G04:** [**Machine Learning in Adversarial Settings**](https://ieeexplore.ieee.org/abstract/document/7478523)

**G05:** [**Machine learning in adversarial environments**](https://link.springer.com/article/10.1007/s10994-010-5207-6)

**G06:** [**Machine learning uncertainties with adversarial neural networks**](https://link.springer.com/article/10.1140/epjc/s10052-018-6511-8)

**G07:** [**Adversarial Machine Learning Beyond the Image Domain**](https://ieeexplore.ieee.org/abstract/document/8806924)

**ب) جست و جو در Yahoo (2 صفحه اول)**

**Y01:** [**A Taxonomy and Terminology of 21 Adversarial Machine Learning**](https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8269-draft.pdf)

**Y02:** [**Adversarial Machine Learning Attacks and Defense Methods in the Cyber Security Domain**](https://dl.acm.org/doi/10.1145/3453158)

**Y03:** [**Adversarial machine learning for cybersecurity and computer vision: Current developments and challenges**](https://dlnext.acm.org/doi/abs/10.1002/wics.1511)

**پ) جست و جو در Bing (3 صفحه اول)**

**BO1:** [**Adversarial machine learning**](https://dl.acm.org/doi/10.1145/2046684.2046692) **(Duplicate)**

**منابع پیدا شده توسط این موتور جست و جو تکراری و یا نا مرتبط بوده‌اند.**

1. **جست و جو با Adversarial Examples + Machine Learning:**

**الف) جست و جو در Google (5 صفحه اول)**

**G08:** [**Explaining and Harnessing Adversarial Examples**](https://arxiv.org/pdf/1412.6572.pdf)

**G09:** [**Adversarial Examples: Attacks and Defenses for Deep Learning**](https://ieeexplore.ieee.org/abstract/document/8611298)

**G10:** [**Adversarial Examples Are Not Easily Detected: Bypassing Ten Detection Methods**](https://dl.acm.org/doi/abs/10.1145/3128572.3140444)

**G11:** [**Efficient Adversarial Training with Transferable Adversarial Examples**](https://openaccess.thecvf.com/content_CVPR_2020/papers/Zheng_Efficient_Adversarial_Training_With_Transferable_Adversarial_Examples_CVPR_2020_paper.pdf)

**G12:** [**Understanding Adversarial Examples From the Mutual Influence of Images and Perturbations**](https://ieeexplore.ieee.org/document/9157541)

**G13:** [**Generating Natural Adversarial Examples**](https://arxiv.org/abs/1710.11342)

**G14:** [**Adversarial Examples in Modern Machine Learning: A Review**](https://arxiv.org/abs/1911.05268)

**ب)**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **اعتبار نویسندگان** | **ضریب تاثیر** | **شاخص h** | **تعداد ارجاعات مقاله** | **ناشر** | **سال چاپ** | **کد مقاله** | **شماره** |
| **12, 59, -, 34, -** | **SJR=2.079** | **163** | **445** | **ACM** | **2011** | **G01** | **1** |
| **38, 73** | **SJR=2.079** | **163** | **30** | **ACM** | **2018** | **G02** | **2** |
| **38, 54** | **SJR=0.927** | **24** | **142** | **Morgan & Claypool** | **2018** | **G03** | **3** |
| **79, 35, 17** | **SJR=0.53** | **76** | **61** | **IEEE** | **2016** | **G04** | **4** |
| **35, 53** | **SJR=0.53** | **17** | **51** | **Springer Nature** | **2010** | **G05** | **5** |
| **10, -, 31, 66** | **SJR=0.53** | **17** | **31** | **Springer Nature** | **2019** | **G06** | **6** |
| **5, 36, 20** | **-** | **-** | **0** | **IEEE** | **2019** | **G07** | **7** |
| **79, 53, 31** | **-** | **-** | **10630** | **-** | **2015** | **G08** | **8** |
| **10, 12, 8, 81** | **SJR=2.882** | **212** | **395** | **IEEE** | **2019** | **G09** | **9** |
| **31, 95** | **SJR=2.95** | **9** | **1297** | **ACM** | **2017** | **G10** | **10** |
| **5, 2, 8, 75** | **SJR=4.658** | **406** | **39** | **IEEE** | **2020** | **G11** | **11** |
| **12, 11, 5** | **-** | **-** | **49** | **IEEE** | **2020** | **G12** | **12** |
| **6, 8, 40** | **-** | **-** | **399** | **-** | **2017** | **G13** | **13** |
| **3, 18, 4, 15** | **-** | **-** | **44** | **-** | **2019** | **G14** | **14** |
| **12** | **SJR=0.202** | **59** | **38** | **NIST** | **2019** | **Y01** | **15** |
| **10, 41, 67** | **SJR=2.079** | **163** | **13** | **ACM** | **2021** | **Y02** | **16** |
| **17** | **SJR=0.693** | **38** | **6** | **Wiley Interdisciplinary** | **2020** | **Y03** | **17** |
| **-** | **-** | **-** | **-** | **-** | **-** | **B01** | **18** |

**ج)**

**معیار‌هایی همچون سال چاپ، اعتبار نویسندگان، اعتبار ناشر، ارجاعات معتبر و ارتباط مستقیم موضوعات با موضوع پژوهشی را می‌توان اضافه کرد. در انتخاب شخصی اعتبار نویسندگاه را اضافه کرده‌ام.**

**د)**

**مقالات منتخب با اولویت به شرح ذیل می‌باشند:**

1. **G08**
2. **G01**
3. **G09**
4. **G11**
5. **Y02**
6. **Y01**