Battista Biggio

List of Publications by Year
in descending order

Source: https://exaly.com/author-pdf/1318068/publications.pdf

Version: 2024-02-01

76	4,654	279487	223531
papers	citations	23 h-index	46 g-index

78	78	78	2470
all docs	docs citations	times ranked	citing authors

#	Article	IF	Citations
1	Do gradient-based explanations tell anything about adversarial robustness to android malware?. International Journal of Machine Learning and Cybernetics, 2022, 13, 217-232.	2.3	12
2	FADER: Fast adversarial example rejection. Neurocomputing, 2022, 470, 257-268.	3.5	8
3	Domain Knowledge Alleviates Adversarial Attacks in Multi-Label Classifiers. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2022, 44, 9944-9959.	9.7	6
4	Towards learning trustworthily, automatically, and with guarantees on graphs: An overview. Neurocomputing, 2022, 493, 217-243.	3.5	11
5	secml: Secure and explainable machine learning in Python. SoftwareX, 2022, 18, 101095.	1.2	4
6	Backdoor smoothing: Demystifying backdoor attacks on deep neural networks. Computers and Security, 2022, 120, 102814.	4.0	2
7	Functionality-Preserving Black-Box Optimization of Adversarial Windows Malware. IEEE Transactions on Information Forensics and Security, 2021, 16, 3469-3478.	4.5	71
8	Poisoning Attacks on Algorithmic Fairness. Lecture Notes in Computer Science, 2021, , 162-177.	1.0	10
9	Empirical assessment of generating adversarial configurations for software product lines. Empirical Software Engineering, 2021, 26, 1.	3.0	5
10	Poisoning attacks on cyber attack detectors for industrial control systems. , 2021, , .		14
11	Adversarial Machine Learning: Attacks From Laboratories to the Real World. Computer, 2021, 54, 56-60.	1.2	8
12	The Hammer and the Nut: Is Bilevel Optimization Really Needed to Poison Linear Classifiers?. , 2021, , .		3
13	Adversarial EXEmples. ACM Transactions on Privacy and Security, 2021, 24, 1-31.	2.2	55
14	Task-Specific Automation in Deep Learning Processes. Communications in Computer and Information Science, 2021, , 159-169.	0.4	1
15	Towards Adversarial Malware Detection. ACM Computing Surveys, 2020, 52, 1-36.	16.1	50
16	Adversarial Detection of Flash Malware: Limitations and Open Issues. Computers and Security, 2020, 96, 101901.	4.0	9
17	Deep neural rejection against adversarial examples. Eurasip Journal on Information Security, 2020, 2020, .	2.4	23
18	Towards Quality Assurance of Software Product Lines with Adversarial Configurations. , 2019, , .		5

#	Article	IF	Citations
19	Optimization and deployment of CNNs at the edge. , 2019, , .		10
20	Digital Investigation of PDF Files: Unveiling Traces of Embedded Malware. IEEE Security and Privacy, 2019, 17, 63-71.	1.5	28
21	Yes, Machine Learning Can Be More Secure! A Case Study on Android Malware Detection. IEEE Transactions on Dependable and Secure Computing, 2019, 16, 711-724.	3.7	141
22	Architecture-aware design and implementation of CNN algorithms for embedded inference: the ALOHA project. , 2018, , .		1
23	Adversarial Malware Binaries: Evading Deep Learning for Malware Detection in Executables. , 2018, , .		163
24	Explaining Black-box Android Malware Detection. , 2018, , .		27
25	Wild Patterns. , 2018, , .		70
26	11th International Workshop on Artificial Intelligence and Security (AISec 2018). , 2018, , .		0
27	Manipulating Machine Learning: Poisoning Attacks and Countermeasures for Regression Learning. , 2018, , .		358
28	Wild patterns: Ten years after the rise of adversarial machine learning. Pattern Recognition, 2018, 84, 317-331.	5.1	658
29	Statistical Meta-Analysis of Presentation Attacks for Secure Multibiometric Systems. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2017, 39, 561-575.	9.7	25
30	DeltaPhish: Detecting Phishing Webpages in Compromised Websites. Lecture Notes in Computer Science, 2017, , 370-388.	1.0	44
31	10th International Workshop on Artificial Intelligence and Security (AISec 2017). , 2017, , .		1
32	Randomized Prediction Games for Adversarial Machine Learning. IEEE Transactions on Neural Networks and Learning Systems, 2017, 28, 2466-2478.	7.2	41
33	Is Deep Learning Safe for Robot Vision? Adversarial Examples Against the iCub Humanoid. , 2017, , .		37
34	Towards Poisoning of Deep Learning Algorithms with Back-gradient Optimization. , 2017, , .		234
35	Deepsquatting: Learning-Based Typosquatting Detection at Deeper Domain Levels. Lecture Notes in Computer Science, 2017, , 347-358.	1.0	5
36	Secure Kernel Machines against Evasion Attacks. , 2016, , .		43

#	Article	IF	Citations
37	Detecting Misuse of Google Cloud Messaging in Android Badware. , 2016, , .		10
38	Super-Sparse Learning in Similarity Spaces. IEEE Computational Intelligence Magazine, 2016, 11, 36-45.	3.4	4
39	Machine Learning under Attack. , 2016, , .		4
40	Adversarial Feature Selection Against Evasion Attacks. IEEE Transactions on Cybernetics, 2016, 46, 766-777.	6.2	174
41	On Security and Sparsity of Linear Classifiers for Adversarial Settings. Lecture Notes in Computer Science, 2016, , 322-332.	1.0	11
42	Support vector machines under adversarial label contamination. Neurocomputing, 2015, 160, 53-62.	3.5	152
43	Sparse support faces. , 2015, , .		4
44	Data-driven journal meta-ranking in business and management. Scientometrics, 2015, 105, 1911-1929.	1.6	14
45	Adversarial Biometric Recognition : A review on biometric system security from the adversarial machine-learning perspective. IEEE Signal Processing Magazine, 2015, 32, 31-41.	4.6	82
46	Super-Sparse Regression for Fast Age Estimation from Faces at Test Time. Lecture Notes in Computer Science, 2015, , 551-562.	1.0	5
47	One-and-a-Half-Class Multiple Classifier Systems for Secure Learning Against Evasion Attacks at Test Time. Lecture Notes in Computer Science, 2015, , 168-180.	1.0	35
48	Fast Image Classification with Reduced Multiclass Support Vector Machines. Lecture Notes in Computer Science, 2015, , 78-88.	1.0	2
49	PATTERN RECOGNITION SYSTEMS UNDER ATTACK: DESIGN ISSUES AND RESEARCH CHALLENGES. International Journal of Pattern Recognition and Artificial Intelligence, 2014, 28, 1460002.	0.7	60
50	Poisoning behavioral malware clustering. , 2014, , .		85
51	On learning and recognition of secure patterns. , 2014, , .		0
52	Security Evaluation of Pattern Classifiers under Attack. IEEE Transactions on Knowledge and Data Engineering, 2014, 26, 984-996.	4.0	268
53	Security Evaluation of Support Vector Machines in Adversarial Environments. , 2014, , 105-153.		62
54	Poisoning Complete-Linkage Hierarchical Clustering. Lecture Notes in Computer Science, 2014, , 42-52.	1.0	23

#	Article	IF	Citations
55	Anti-spoofing: Multimodal. , 2014, , 1-4.		1
56	Poisoning attacks to compromise face templates. , 2013, , .		46
57	Evasion Attacks against Machine Learning at Test Time. Lecture Notes in Computer Science, 2013, , 387-402.	1.0	678
58	Is data clustering in adversarial settings secure?. , 2013, , .		62
59	Pattern Recognition Systems under Attack. Lecture Notes in Computer Science, 2013, , 1-8.	1.0	17
60	Security evaluation of biometric authentication systems under real spoofing attacks. IET Biometrics, 2012, 1, 11.	1.6	105
61	Learning sparse kernel machines with biometric similarity functions for identity recognition. , 2012, , .		1
62	Poisoning Adaptive Biometric Systems. Lecture Notes in Computer Science, 2012, , 417-425.	1.0	34
63	Robustness of multi-modal biometric systems under realistic spoof attacks against all traits. , 2011, , .		11
64	Robustness of multi-modal biometric verification systems under realistic spoofing attacks. , 2011, , .		15
65	A survey and experimental evaluation of image spam filtering techniques. Pattern Recognition Letters, 2011, 32, 1436-1446.	2.6	84
66	Understanding the risk factors of learning in adversarial environments. , 2011, , .		11
67	Design of robust classifiers for adversarial environments. , 2011, , .		30
68	Bagging Classifiers for Fighting Poisoning Attacks in Adversarial Classification Tasks. Lecture Notes in Computer Science, 2011, , 350-359.	1.0	54
69	Multiple classifier systems for robust classifier design in adversarial environments. International Journal of Machine Learning and Cybernetics, 2010, 1, 27-41.	2.3	156
70	Multiple Classifier Systems under Attack. Lecture Notes in Computer Science, 2010, , 74-83.	1.0	37
71	Multiple Classifier Systems for Adversarial Classification Tasks. Lecture Notes in Computer Science, 2009, , 132-141.	1.0	22
72	Evade Hard Multiple Classifier Systems. Studies in Computational Intelligence, 2009, , 15-38.	0.7	14

#	Article	IF	Citations
73	Bayesian Linear Combination of Neural Networks. Studies in Computational Intelligence, 2009, , 201-230.	0.7	0
74	Adversarial Pattern Classification Using Multiple Classifiers and Randomisation. Lecture Notes in Computer Science, 2008, , 500-509.	1.0	33
75	Image Spam Filtering Using Visual Information. , 2007, , .		30
76	Bayesian Analysis of Linear Combiners. , 2007, , 292-301.		24