Anthony D Joseph

List of Publications by Year
in descending order

Source: https://exaly.com/author-pdf/5649624/publications.pdf

Version: 2024-02-01

39 papers	12,091 citations	687363 13 h-index	713466 21 g-index
40 all docs	40 docs citations	40 times ranked	9689 citing authors

#	Article	IF	Citations
1	A view of cloud computing. Communications of the ACM, 2010, 53, 50-58.	4.5	7,593
2	Toil enables reproducible, open source, big biomedical data analyses. Nature Biotechnology, 2017, 35, 314-316.	17.5	873
3	Adversarial machine learning. , 2011, , .		633
4	The security of machine learning. Machine Learning, 2010, 81, 121-148.	5.4	503
5	Can machine learning be secure?. , 2006, , .		470
6	Bayeux. , 2001, , .		462
7	Understanding TCP incast throughput collapse in datacenter networks. , 2009, , .		274
8	ANTIDOTE. , 2009, , .		205
9	A Markov-Based Channel Model Algorithm for Wireless Networks. Wireless Networks, 2003, 9, 189-199.	3.0	174
10	Tapestry. Computer Communication Review, 2002, 32, 81-81.	1.8	133
11	Rethinking Data-Intensive Science Using Scalable Analytics Systems. , 2015, , .		67
12	An Architecture for Secure Wide-Area Service Discovery. Wireless Networks, 2002, 8, 213-230.	3.0	64
13	A Markov-based channel model algorithm for wireless networks. , 2001, , .		61
14	Misleading Learners: Co-opting Your Spam Filter. , 2009, , 17-51.		60
15	The SAHARA Model for Service Composition across Multiple Providers. Lecture Notes in Computer Science, 2002, , 1-14.	1.3	59
16	Adversarial Active Learning. , 2014, , .		51
17	Better Malware Ground Truth. , 2015, , .		49
18	Optimizing the end-to-end performance of reliable flows over wireless links. , 1999, , .		40

#	Article	IF	Citations
19	Reviewer Integration and Performance Measurement for Malware Detection. Lecture Notes in Computer Science, 2016, , 122-141.	1.3	40
20	Approaches to adversarial drift. , 2013, , .		34
21	A Batch-Authenticated and Key Agreement Framework for P2P-Based Online Social Networks. IEEE Transactions on Vehicular Technology, 2012, 61, 1907-1924.	6.3	31
22	Optimizing the End-to-End Performance of Reliable Flows over Wireless Links. Wireless Networks, 2002, 8, 289-299.	3.0	24
23	FPGA Accelerated INDEL Realignment in the Cloud. , 2019, , .		24
24	Stealthy poisoning attacks on PCA-based anomaly detectors. Performance Evaluation Review, 2009, 37, 73-74.	0.6	23
25	Communication-Efficient Tracking of Distributed Cumulative Triggers. , 2007, , .		21
26	Determining model accuracy of network traces. Journal of Computer and System Sciences, 2006, 72, 1156-1171.	1.2	20
27	Open problems in the security of learning. , 2008, , .		19
28	Support Vector Machines, Data Reduction, and Approximate Kernel Matrices. Lecture Notes in Computer Science, 2008, , 137-153.	1.3	16
29	GPUs as an opportunity for offloading garbage collection. , 2012, , .		13
30	The case for services over cascaded networks. , 1998, , .		12
31	A Composable Framework for Secure Multi-Modal Access to Internet Services from Post-PC Devices. Mobile Networks and Applications, 2002, 7, 389-406.	3.3	10
32	Building reliable mobileâ€aware applications using the Rover toolkit. Wireless Networks, 1997, 3, 405-419.	3.0	9
33	Classifier Evasion: Models and Open Problems. Lecture Notes in Computer Science, 2011, , 92-98.	1.3	8
34	Evading Anomaly Detection through Variance Injection Attacks on PCA. Lecture Notes in Computer Science, 2008, , 394-395.	1.3	7
35	Guest Editors' Introduction: Smarter Phones. IEEE Pervasive Computing, 2009, 8, 12-13.	1.3	4
36	GPUs as an opportunity for offloading garbage collection. ACM SIGPLAN Notices, 2013, 47, 25-36.	0.2	3

#	Article	IF	Citations
37	Epitome: predicting epigenetic events in novel cell types with multi-cell deep ensemble learning. Nucleic Acids Research, 2021, 49, e110-e110.	14.5	1
38	Portable software for multiprocessor systems. Computing & Control Engineering Journal, 1992, 3, 275.	0.0	1
39	Choosing an accurate network path model. Performance Evaluation Review, 2003, 31, 314-315.	0.6	0