Hadis Karimipour

List of Publications by Year in Descending Order

Source: https://exaly.com/author-pdf/1412429/hadis-karimipour-publications-by-year.pdf
Version: 2024-04-19

This document has been generated based on the publications and citations recorded by exaly.com. For the latest version of this publication list, visit the link given above.
The third column is the impact factor (IF) of the journal, and the fourth column is the number of citations of the article.

133	3,904	34	59
papers	citations	h-index	g-index
139	5,375	4.2	6.87
ext. papers	ext. citations	avg, IF	L-index

#	Paper	IF	Citations
133	Federated IoT attack detection using decentralized edge data. *Machine Learning With Applications*, **2022**, 8, 100263	6.5	2
132	IoT Privacy, Security and Forensics Challenges: An Unmanned Aerial Vehicle (UAV) Case Study **2022**, 7-39		0
131	A Self-tuning Cyber-Attacks Location Identification Approach for Industrial Internet of Things. *IEEE Transactions on Industrial Informatics*, **2021**, 1-1	11.9	2
130	Assessing Insider Attacks and Privacy Leakage in Managed IoT Systems for Residential Prosumers. *Energies*, **2021**, 14, 2385	3.1	0
129	Lower Bounds on Bandwidth Requirements of Regenerating Code Parameter Scaling in Distributed Storage Systems. *IEEE Communications Letters*, **2021**, 25, 1477-1481	3.8	
128	Enabling Drones in the Internet of Things With Decentralized Blockchain-Based Security. *IEEE Internet of Things Journal*, **2021**, 8, 6406-6415	10.7	49
127	A Multikernel and Metaheuristic Feature Selection Approach for IoT Malware Threat Hunting in the Edge Layer. *IEEE Internet of Things Journal*, **2021**, 8, 4540-4547	10.7	13
126	A survey on security and privacy of federated learning. *Future Generation Computer Systems*, **2021**, 115, 619-640	7.5	165
125	A kangaroo-based intrusion detection system on software-defined networks. *Computer Networks*, **2021**, 184, 107688	5.4	12
124	Security aspects of Internet of Things aided smart grids: A bibliometric survey. *Internet of Things (Netherlands)*, **2021**, 14, 100111	6.9	64
123	A survey on internet of things security: Requirements, challenges, and solutions. *Internet of Things (Netherlands)*, **2021**, 14, 100129	6.9	82
122	A Recurrent Attention Model for Cyber Attack Classification **2021**, 237-250		0
121	Blockchain Applications in the Industrial Internet of Things **2021**, 41-76		1
120	A Snapshot Ensemble Deep Neural Network Model for Attack Detection in Industrial Internet of Things **2021**, 181-194		0
119	Application of Deep Learning on IoT-Enabled Smart Grid Monitoring **2021**, 77-103		0
118	Resilient Scheduling of Networked Microgrids Against Real-Time Failures. *IEEE Access*, **2021**, 9, 21443-21456	3.9	3
117	A Review on Security of Smart Farming and Precision Agriculture: Security Aspects, Attacks, Threats and Countermeasures. *Applied Sciences (Switzerland)*, **2021**, 11, 7518	2.6	7

116	Physical layer attack identification and localization in cyberphysical grid: An ensemble deep learning based approach. *Physical Communication*, **2021**, 47, 101394	2.2	6
115	Data Aggregation Mechanisms on the Internet of Things: A Systematic Literature Review. *Internet of Things (Netherlands)*, **2021**, 15, 100427	6.9	4
114	Federated learning for drone authentication. *Ad Hoc Networks*, **2021**, 120, 102574	4.8	6
113	Toward Detection and Attribution of Cyber-Attacks in IoT-Enabled CyberPhysical Systems. *IEEE Internet of Things Journal*, **2021**, 8, 13712-13722	10.7	14
112	A review on virtual power plant for energy management. *Sustainable Energy Technologies and Assessments*, **2021**, 47, 101370	4.7	14
111	Generative adversarial network to detect unseen Internet of Things malware. *Ad Hoc Networks*, **2021**, 122, 102591	4.8	9
110	Optimized Power Trading of Reconfigurable Microgrids in Distribution Energy Market. *IEEE Access*, **2021**, 9, 48218-48235	3.5	6
109	Deep Representation Learning for Cyber-Attack Detection in Industrial IoT **2021**, 139-162		1
108	Artificial Intelligence for Threat Detection and Analysis in Industrial IoT: Applications and Challenges **2021**, 1-6		
107	Ensemble sparse representation-based cyber threat hunting for security of smart cities. *Computers and Electrical Engineering*, **2020**, 88, 106825	4.3	8
106	An Ensemble Deep Learning-Based Cyber-Attack Detection in Industrial Control System. *IEEE Access*, **2020**, 8, 83965-83973	3.5	58
105	Relaxation-based anomaly detection in cyber-physical systems using ensemble kalman filter. *IET Cyber-Physical Systems: Theory and Applications*, **2020**, 5, 49-58	2.5	23
104	An energy-efficient artificial bee colony-based clustering in the internet of things. *Computers and Electrical Engineering*, **2020**, 86, 106733	4.3	15
103	SLPoW: Secure and Low Latency Proof of Work Protocol for Blockchain in Green IoT Networks **2020** ,		14
102	AI4SAFE-IoT: an AI-powered secure architecture for edge layer of Internet of things. *Neural Computing and Applications*, **2020**, 32, 16119-16133	4.8	32
101	A high-performance framework for a network programmable packet processor using P4 and FPGA. *Journal of Network and Computer Applications*, **2020**, 156, 102564	7.9	19
100	An Energy-Efficient SDN Controller Architecture for IoT Networks With Blockchain-Based Security. *IEEE Transactions on Services Computing*, **2020**, 13, 625-638	4.8	82
99	A multiview learning method for malware threat hunting: windows, IoT and android as case studies. *World Wide Web*, **2020**, 23, 1241-1260	2.9	24

98	Decentralized Authentication of Distributed Patients in Hospital Networks Using Blockchain. *IEEE Journal of Biomedical and Health Informatics*, **2020**, 24, 2146-2156	7.2	70
97	Detecting Cryptomining Malware: a Deep Learning Approach for Static and Dynamic Analysis. *Journal of Grid Computing*, **2020**, 18, 293-303	4.2	21
96	Machine learning based solutions for security of Internet of Things (IoT): A survey. *Journal of Network and Computer Applications*, **2020**, 161, 102630	7.9	124
95	Cost optimization of secure routing with untrusted devices in software defined networking. *Journal of Parallel and Distributed Computing*, **2020**, 143, 36-46	4.4	22
94	Artificial Bee Colony-based Routing for Mobile Agents on the Internet of Things **2020**,		1
93	An Ensemble of Deep Recurrent Neural Networks for Detecting IoT Cyber Attacks Using Network Traffic. *IEEE Internet of Things Journal*, **2020**, 7, 8852-8859	10.7	49
92	An Ensemble Deep Convolutional Neural Network Model for Electricity Theft Detection in Smart Grids **2020**,		7
91	**2020**,		8
90	**2020**,		1
89	A Multilabel Fuzzy Relevance Clustering System for Malware Attack Attribution in the Edge Layer of Cyber-Physical Networks. *ACM Transactions on Cyber-Physical Systems*, **2020**, 4, 1-22	2.3	12
88	A Bibliometric Analysis on the Application of Deep Learning in Cybersecurity **2020**, 203-221		1
87	AI and Security of Critical Infrastructure **2020**, 7-36		1
86	Big Data Application for Security of Renewable Energy Resources **2020**, 237-254		1
85	Big-Data and Cyber-Physical Systems in Healthcare: Challenges and Opportunities **2020**, 255-283		3
84	Privacy Preserving Abnormality Detection: A Deep Learning Approach **2020**, 285-303		
83	A Survey on Application of Big Data in Fin Tech Banking Security and Privacy **2020**, 319-342		3
82	RAT Hunter: Building Robust Models for Detecting Remote Access Trojans Based on Optimum Hybrid Features **2020**, 371-383		3
81	Active Spectral Botnet Detection Based on Eigenvalue Weighting **2020**, 385-397		10

(2020-2020)

80	An Empirical Evaluation of AI Deep Explainable Tools **2020**,		5
79	Big Data and Privacy: Challenges and Opportunities **2020**, 1-5		6
78	Blockchain Applications in Power Systems: A Bibliometric Analysis. *Advances in Information Security*, **2020**, 129-145	0.7	3
77	Anomaly Detection in Cyber-Physical Systems Using Machine Learning **2020**, 219-235		12
76	Privacy and Security in Smart and Precision Farming: A Bibliometric Analysis **2020**, 305-318		9
75	A Hybrid Deep Generative Local Metric Learning Method for Intrusion Detection **2020**, 343-357		13
74	Malware Elimination Impact on Dynamic Analysis: An Experimental Machine Learning Approach **2020**, 359-370		4
73	Industrial Big Data Analytics: Challenges and Opportunities **2020**, 37-61		8
72	A Privacy Protection Key Agreement Protocol Based on ECC for Smart Grid **2020**, 63-76		4
71	Applications of Big Data Analytics and Machine Learning in the Internet of Things **2020**, 77-108		12
70	A Comparison of State-of-the-Art Machine Learning Models for OpCode-Based IoT Malware Detection **2020**, 109-120		5
69	Artificial Intelligence and Security of Industrial Control Systems **2020**, 121-164		5
68	Enhancing Network Security Via Machine Learning: Opportunities and Challenges **2020**, 165-189		7
67	A Comparison Between Different Machine Learning Models for IoT Malware Detection **2020**, 195-202		5
66	Learning Based Anomaly Detection in Critical Cyber-Physical Systems **2020**, 107-130		8
65	AI-Enabled Security Monitoring in Smart Cyber Physical Grids **2020**, 145-167		6
64	Application of Machine Learning in State Estimation of Smart Cyber-Physical Grid **2020**, 169-194		2
63	. *IEEE Transactions on Network Science and Engineering*, **2020**, 1-1	4.9	53

62	Threats on the horizon: understanding security threats in the era of cyber-physical systems. *Journal of Supercomputing*, **2020**, 76, 2643-2664	2.5	25
61	An efficient route planning model for mobile agents on the internet of things using Markov decision process. *Ad Hoc Networks*, **2020**, 98, 102053	4.8	18
60	An improved two-hidden-layer extreme learning machine for malware hunting. *Computers and Security*, **2020**, 89, 101655	4.9	39
59	Cryptocurrency malware hunting: A deep Recurrent Neural Network approach. *Applied Soft Computing Journal*, **2020**, 96, 106630	7.5	37
58	MVFCC: A Multi-View Fuzzy Consensus Clustering Model for Malware Threat Attribution. *IEEE Access*, **2020**, 8, 139188-139198	3.5	16
57	Real-time stability assessment in smart cyber-physical grids: a deep learning approach. *IET Smart Grid*, **2020**, 3, 454-461	2.7	8
56	Know Abnormal, Find Evil: Frequent Pattern Mining for Ransomware Threat Hunting and Intelligence. *IEEE Transactions on Emerging Topics in Computing*, **2020**, 8, 341-351	4.1	51
55	An analysis of anti-forensic capabilities of B-tree file system (Btrfs). *Australian Journal of Forensic Sciences*, **2020**, 52, 371-386	1.1	7
54	An opcode-based technique for polymorphic Internet of Things malware detection. *Concurrency Computation Practice and Experience*, **2020**, 32, e5173	1.4	34
53	A systematic literature review of blockchain cyber security. *Digital Communications and Networks*, **2020**, 6, 147-156	5.9	191
52	PARALLEL DOMAIN-DECOMPOSITION-BASED DISTRIBUTED STATE ESTIMATION FOR LARGE-SCALE POWER SYSTEMS **2020**, 413-453		1
51	Smart Households Demand Response Management with Micro Grid **2019**,		13
50	A Deep and Scalable Unsupervised Machine Learning System for Cyber-Attack Detection in Large-Scale Smart Grids. *IEEE Access*, **2019**, 7, 80778-80788	3.5	125
49	Fuzzy pattern tree for edge malware detection and categorization in IoT. *Journal of Systems Architecture*, **2019**, 97, 1-7	5.5	99
48	DRTHIS: Deep ransomware threat hunting and intelligence system at the fog layer. *Future Generation Computer Systems*, **2019**, 90, 94-104	7.5	64
47	A hierarchical key pre-distribution scheme for fog networks. *Concurrency Computation Practice and Experience*, **2019**, 31, e4776	1.4	5
46	A Cyber-Kill-Chain based taxonomy of crypto-ransomware features. *Journal of Computer Virology and Hacking Techniques*, **2019**, 15, 277-305	3	28
45	A Blockchain-based Framework for Detecting Malicious Mobile Applications in App Stores **2019**,		22

(2018-2019)

44	A Layered Intrusion Detection System for Critical Infrastructure Using Machine Learning **2019**,		21
43	Intelligent Anomaly Detection for Large-scale Smart Grids **2019**,		12
42	Employing Composite Demand Response Model in Microgrid Energy Management **2019**,		1
41	**2019**,		4
40	**2019**,		2
39	Energy Efficient Decentralized Authentication in Internet of Underwater Things Using Blockchain **2019**,		19
38	Smart Grid Cyber Attacks Detection Using Supervised Learning and Heuristic Feature Selection **2019**,		36
37	Joint State Estimation and Cyber-Attack Detection Based on Feature Grouping **2019**,		6
36	Cyber intrusion detection by combined feature selection algorithm. *Journal of Information Security and Applications*, **2019**, 44, 80-88	3.5	108
35	Robust Malware Detection for Internet of (Battlefield) Things Devices Using Deep Eigenspace Learning. *IEEE Transactions on Sustainable Computing*, **2019**, 4, 88-95	3.5	171
34	A Two-Layer Dimension Reduction and Two-Tier Classification Model for Anomaly-Based Intrusion Detection in IoT Backbone Networks. *IEEE Transactions on Emerging Topics in Computing*, **2019**, 7, 314-323	4.1	170
33	Greening Cloud-Enabled Big Data Storage Forensics: Syncany as a Case Study. *IEEE Transactions on Sustainable Computing*, **2019**, 4, 204-216	3.5	21
32	Nonreciprocity Compensation Combined With Turbo Codes for Secret Key Generation in Vehicular Ad Hoc Social IoT Networks. *IEEE Internet of Things Journal*, **2018**, 5, 2496-2505	10.7	27
31	Robust Massively Parallel Dynamic State Estimation of Power Systems Against Cyber-Attack. *IEEE Access*, **2018**, 6, 2984-2995	3.5	72
30	A deep Recurrent Neural Network based approach for Internet of Things malware threat hunting. *Future Generation Computer Systems*, **2018**, 85, 88-96	7.5	195
29	A Systematic Review of the Availability and Efficacy of Countermeasures to Internal Threats in Healthcare Critical Infrastructure. *IEEE Access*, **2018**, 6, 25167-25177	3.5	60
28	Intelligent OS X malware threat detection with code inspection. *Journal of Computer Virology and Hacking Techniques*, **2018**, 14, 213-223	3	38
27	Detecting crypto-ransomware in IoT networks based on energy consumption footprint. *Journal of Ambient Intelligence and Humanized Computing*, **2018**, 9, 1141-1152	3.7	123

26	Leveraging Support Vector Machine for Opcode Density Based Detection of Crypto-Ransomware. *Advances in Information Security*, **2018**, 107-136	0.7	19
25	CloudMe forensics: A case of big data forensic investigation. *Concurrency Computation Practice and Experience*, **2018**, 30, e4277	1.4	24
24	Application of Machine Learning Algorithms for Android Malware Detection **2018**,		8
23	Microgrid Islanding Detection Based on Mathematical Morphology. *Energies*, **2018**, 11, 2696	3.1	21
22	Coordinated Fuzzy Controller for Dynamic Stability Improvement in Multi-Machine Power System **2018**,		2
21	Hybrid Islanding Detection for AC/DC Network Using DC-link Voltage **2018**,		2
20	On the Understanding of Gamification in Blockchain Systems **2018**,		17
19	Machine Learning Aided Static Malware Analysis: A Survey and Tutorial. *Advances in Information Security*, **2018**, 7-45	0.7	35
18	Optimal incentive-based demand response management of smart households **2018**,		13
17	Cloud storage forensics: MEGA as a case study. *Australian Journal of Forensic Sciences*, **2017**, 49, 344-357	1.1	35
16	Machine learning aided Android malware classification. *Computers and Electrical Engineering*, **2017**, 61, 266-274	4.3	161
15	Forensic Investigation of Cooperative Storage Cloud Service: Symform as a Case Study. *Journal of Forensic Sciences*, **2017**, 62, 641-654	1.8	17
14	On false data injection attack against dynamic state estimation on smart power grids **2017**,		29
13	SugarSync forensic analysis. *Australian Journal of Forensic Sciences*, **2016**, 48, 95-117	1.1	30
12	Parallel relaxation-based joint dynamic state estimation of large-scale power systems. *IET Generation, Transmission and Distribution*, **2016**, 10, 452-459	2.5	32
11	Forensic investigation of OneDrive, Box, GoogleDrive and Dropbox applications on Android and iOS devices. *Australian Journal of Forensic Sciences*, **2016**, 48, 615-642	1.1	27
10	Investigating Social Networking applications on smartphones detecting Facebook, Twitter, LinkedIn and Google+ artefacts on Android and iOS platforms. *Australian Journal of Forensic Sciences*, **2016**, 48, 469-488	1.1	49
9	Windows Instant Messaging App Forensics: Facebook and Skype as Case Studies. *PLoS ONE*, **2016**, 11, e0150300	3.7	39

8	Digital forensics: the missing piece of the Internet of Things promise. *Computer Fraud and Security*, **2016**, 2016, 5-8	2.2	57
7	Extended Kalman Filter-Based Parallel Dynamic State Estimation. *IEEE Transactions on Smart Grid*, **2015**, 6, 1539-1549	10.7	93
6	Parallel Domain-Decomposition-Based Distributed State Estimation for Large-Scale Power Systems. *IEEE Transactions on Industry Applications*, **2015**, 1-1	4.3	5
5	Exploit Kits: The production line of the Cybercrime economy? **2015**,		19
4	M0Droid: An Android Behavioral-Based Malware Detection Model. *Journal of Information Privacy and Security*, **2015**, 11, 141-157		46
3	On detailed synchronous generator modeling for massively parallel dynamic state estimation **2014**,		1
2	Accelerated parallel WLS state estimation for large-scale power systems on GPU **2013**,		13
1	A Deep Neural Network Combined with Radial Basis Function for Abnormality Classification. *Mobile Networks and Applications*,1	2.9	0