Hadis Karimipour

List of Publications by Year
in descending order

137	7,089	76196	71532
papers	citations	40 h-index	76 g-index

139	139	139	4260
all docs	docs citations	times ranked	citing authors

#	Article	IF	Citations
1	A survey on security and privacy of federated learning. Future Generation Computer Systems, 2021, 115, 619-640.	4.9	534
2	A systematic literature review of blockchain cyber security. Digital Communications and Networks, 2020, 6, 147-156.	2.7	373
3	A deep Recurrent Neural Network based approach for Internet of Things malware threat hunting. Future Generation Computer Systems, 2018, 85, 88-96.	4.9	302
4	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.	3.2	285
5	Machine learning based solutions for security of Internet of Things (IoT): A survey. Journal of Network and Computer Applications, 2020, 161, 102630.	5.8	266
6	Robust Malware Detection for Internet of (Battlefield) Things Devices Using Deep Eigenspace Learning. IEEE Transactions on Sustainable Computing, 2019, 4, 88-95.	2.2	252
7	Machine learning aided Android malware classification. Computers and Electrical Engineering, 2017, 61, 266-274.	3.0	245
8	A Deep and Scalable Unsupervised Machine Learning System for Cyber-Attack Detection in Large-Scale Smart Grids. IEEE Access, 2019, 7, 80778-80788.	2.6	224
9	Cyber intrusion detection by combined feature selection algorithm. Journal of Information Security and Applications, 2019, 44, 80-88.	1.8	192
10	Detecting crypto-ransomware in IoT networks based on energy consumption footprint. Journal of Ambient Intelligence and Humanized Computing, 2018, 9, 1141-1152.	3.3	190
11	An Energy-Efficient SDN Controller Architecture for IoT Networks With Blockchain-Based Security. IEEE Transactions on Services Computing, 2020, 13, 625-638.	3.2	168
12	A survey on internet of things security: Requirements, challenges, and solutions. Internet of Things (Netherlands), 2021, 14, 100129.	4.9	167
13	Fuzzy pattern tree for edge malware detection and categorization in IoT. Journal of Systems Architecture, 2019, 97, 1-7.	2.5	155
14	An Ensemble Deep Learning-Based Cyber-Attack Detection in Industrial Control System. IEEE Access, 2020, 8, 83965-83973.	2.6	139
15	Decentralized Authentication of Distributed Patients in Hospital Networks Using Blockchain. IEEE Journal of Biomedical and Health Informatics, 2020, 24, 2146-2156.	3.9	137
16	Extended Kalman Filter-Based Parallel Dynamic State Estimation. IEEE Transactions on Smart Grid, 2015, 6, 1539-1549.	6.2	127
17	Enabling Drones in the Internet of Things With Decentralized Blockchain-Based Security. IEEE Internet of Things Journal, 2021, 8, 6406-6415.	5.5	113
18	An Ensemble of Deep Recurrent Neural Networks for Detecting IoT Cyber Attacks Using Network Traffic. IEEE Internet of Things Journal, 2020, 7, 8852-8859.	5.5	113

#	Article	IF	Citations
19	Security aspects of Internet of Things aided smart grids: A bibliometric survey. Internet of Things (Netherlands), 2021, 14, 100111.	4.9	108
20	Robust Massively Parallel Dynamic State Estimation of Power Systems Against Cyber-Attack. IEEE Access, 2018, 6, 2984-2995.	2.6	106
21	DRTHIS: Deep ransomware threat hunting and intelligence system at the fog layer. Future Generation Computer Systems, 2019, 90, 94-104.	4.9	102
22	Know Abnormal, Find Evil: Frequent Pattern Mining for Ransomware Threat Hunting and Intelligence. IEEE Transactions on Emerging Topics in Computing, 2020, 8, 341-351.	3.2	93
23	A Systematic Review of the Availability and Efficacy of Countermeasures to Internal Threats in Healthcare Critical Infrastructure. IEEE Access, 2018, 6, 25167-25177.	2.6	87
24	Blockchain-Enabled Authentication Handover With Efficient Privacy Protection in SDN-Based 5G Networks. IEEE Transactions on Network Science and Engineering, 2021, 8, 1120-1132.	4.1	87
25	Cryptocurrency malware hunting: A deep Recurrent Neural Network approach. Applied Soft Computing Journal, 2020, 96, 106630.	4.1	78
26	Smart Grid Cyber Attacks Detection Using Supervised Learning and Heuristic Feature Selection. , 2019, , .		76
27	Digital forensics: the missing piece of the Internet of Things promise. Computer Fraud and Security, 2016, 2016, 5-8.	1.3	73
28	M0Droid: An Android Behavioral-Based Malware Detection Model. Journal of Information Privacy and Security, 2015, 11, 141-157.	0.4	66
29	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.	0.7	65
30	A Cyber-Kill-Chain based taxonomy of crypto-ransomware features. Journal of Computer Virology and Hacking Techniques, 2019, 15, 277-305.	1.6	64
31	Detecting Cryptomining Malware: a Deep Learning Approach for Static and Dynamic Analysis. Journal of Grid Computing, 2020, 18, 293-303.	2.5	63
32	Windows Instant Messaging App Forensics: Facebook and Skype as Case Studies. PLoS ONE, 2016, 11, e0150300.	1.1	62
33	An opcodeâ€based technique for polymorphic Internet of Things malware detection. Concurrency Computation Practice and Experience, 2020, 32, e5173.	1.4	62
34	Machine Learning Aided Static Malware Analysis: A Survey and Tutorial. Advances in Information Security, 2018, , 7-45.	0.9	61
35	An improved two-hidden-layer extreme learning machine for malware hunting. Computers and Security, 2020, 89, 101655.	4.0	57
36	AI4SAFE-IoT: an AI-powered secure architecture for edge layer of Internet of things. Neural Computing and Applications, 2020, 32, 16119-16133.	3.2	55

#	Article	IF	Citations
37	Toward Detection and Attribution of Cyber-Attacks in IoT-Enabled Cyberâ€“Physical Systems. IEEE Internet of Things Journal, 2021, 8, 13712-13722.	5.5	55
38	Intelligent OS X malware threat detection with code inspection. Journal of Computer Virology and Hacking Techniques, 2018, 14, 213-223.	1.6	49
39	Threats on the horizon: understanding security threats in the era of cyber-physical systems. Journal of Supercomputing, 2020, 76, 2643-2664.	2.4	45
40	A Layered Intrusion Detection System for Critical Infrastructure Using Machine Learning. , 2019, , .		44
41	On false data injection attack against dynamic state estimation on smart power grids. , 2017, , .		43
42	A review on virtual power plant for energy management. Sustainable Energy Technologies and Assessments, 2021, 47, 101370.	1.7	43
43	Cloud storage forensics: MEGA as a case study. Australian Journal of Forensic Sciences, 2017, 49, 344-357.	0.7	42
44	Federated learning for drone authentication. Ad Hoc Networks, 2021, 120, 102574.	3.4	42
45	Parallel relaxationâ€based joint dynamic state estimation of largeâ€scale power systems. IET Generation, Transmission and Distribution, 2016, 10, 452-459.	1.4	38
46	Forensic investigation of OneDrive, Box, GoogleDrive and Dropbox applications on Android and iOS devices. Australian Journal of Forensic Sciences, 2016, 48, 615-642.	0.7	38
47	SugarSync forensic analysis. Australian Journal of Forensic Sciences, 2016, 48, 95-117.	0.7	38
48	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.	5.5	37
49	Cost optimization of secure routing with untrusted devices in software defined networking. Journal of Parallel and Distributed Computing, 2020, 143, 36-46.	2.7	37
50	A multiview learning method for malware threat hunting: windows, IoT and android as case studies. World Wide Web, 2020, 23, 1241-1260.	2.7	36
51	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.	5.5	35
52	A kangaroo-based intrusion detection system on software-defined networks. Computer Networks, 2021, 184, 107688.	3.2	35
53	Relaxationâ€based anomaly detection in cyberâ€physical systems using ensemble kalman filter. IET Cyber-Physical Systems: Theory and Applications, 2020, 5, 49-58.	1.9	34
54	Leveraging Support Vector Machine for Opcode Density Based Detection of Crypto-Ransomware. Advances in Information Security, 2018, , 107-136.	0.9	33

#	Article	IF	Citations
55	A Review on Security of Smart Farming and Precision Agriculture: Security Aspects, Attacks, Threats and Countermeasures. Applied Sciences (Switzerland), 2021, 11, 7518.	1.3	33
56	A Blockchain-based Framework for Detecting Malicious Mobile Applications in App Stores. , 2019, , .		31
57	Energy Efficient Decentralized Authentication in Internet of Underwater Things Using Blockchain. , 2019, , .		31
58	CloudMe forensics: A case of big data forensic investigation. Concurrency Computation Practice and Experience, 2018, 30, e4277.	1.4	30
59	An energy-efficient artificial bee colony-based clustering in the internet of things. Computers and Electrical Engineering, 2020, 86, 106733.	3.0	30
60	Intelligent Anomaly Detection for Large-scale Smart Grids. , 2019, , .		29
61	Generative adversarial network to detect unseen Internet of Things malware. Ad Hoc Networks, 2021, 122, 102591.	3.4	29
62	On the Understanding of Gamification in Blockchain Systems. , 2018, , .		26
63	Greening Cloud-Enabled Big Data Storage Forensics: Syncany as a Case Study. IEEE Transactions on Sustainable Computing, 2019, 4, 204-216.	2.2	26
64	An efficient route planning model for mobile agents on the internet of things using Markov decision process. Ad Hoc Networks, 2020, 98, 102053.	3.4	26
65	A high-performance framework for a network programmable packet processor using P4 and FPGA. Journal of Network and Computer Applications, 2020, 156, 102564.	5.8	26
66	Exploit Kits: The production line of the Cybercrime economy?. , 2015, , .		25
67	SLPoW: Secure and Low Latency Proof of Work Protocol for Blockchain in Green IoT Networks. , 2020, , .		25
68	Microgrid Islanding Detection Based on Mathematical Morphology. Energies, 2018, 11, 2696.	1.6	24
69	Smart Households Demand Response Management with Micro Grid. , 2019, , .		24
70	MVFCC: A Multi-View Fuzzy Consensus Clustering Model for Malware Threat Attribution. IEEE Access, 2020, 8, 139188-139198.	2.6	23
71	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.	1.9	22
72	Parallel Domain Decomposition Based Distributed State Estimation for Large-scale Power Systems. IEEE Transactions on Industry Applications, 2015, , 1-1.	3.3	21

#	Article	IF	Citations
73	Forensic Investigation of Cooperative Storage Cloud Service: Symform as a Case Study. Journal of Forensic Sciences, 2017, 62, 641-654.	0.9	19
74	Realâ€time stability assessment in smart cyberâ€physical grids: a deep learning approach. IET Smart Grid, 2020, 3, 454-461.	1.5	19
75	Data Aggregation Mechanisms on the Internet of Things: A Systematic Literature Review. Internet of Things (Netherlands), 2021, 15, 100427.	4.9	19
76	Anomaly Detection in Cyber-Physical Systems Using Machine Learning. , 2020, , 219-235.		19
77	Ensemble sparse representation-based cyber threat hunting for security of smart cities. Computers and Electrical Engineering, 2020, 88, 106825.	3.0	18
78	An Ensemble Deep Convolutional Neural Network Model for Electricity Theft Detection in Smart Grids. , 2020, , .		18
79	An Empirical Evaluation of AI Deep Explainable Tools. , 2020, , .		18
80	Optimal incentive-based demand response management of smart households. , 2018, , .		17
81	Physical layer attack identification and localization in cyberâ€“physical grid: An ensemble deep learning based approach. Physical Communication, 2021, 47, 101394.	1.2	17
82	A Hybrid Deep Generative Local Metric Learning Method for Intrusion Detection. , 2020, , 343-357.		17
83	Unsupervised Stacked Autoencoders for Anomaly Detection on Smart Cyber-physical Grids. , 2020, , .		17
84	Accelerated parallel WLS state estimation for large-scale power systems on GPU. , 2013, , .		16
85	Optimized Power Trading of Reconfigurable Microgrids in Distribution Energy Market. IEEE Access, 2021, 9, 48218-48235.	2.6	16
86	Applications of Big Data Analytics and Machine Learning in the Internet of Things. , 2020, , 77-108.		16
87	Industrial Big Data Analytics: Challenges and Opportunities. , 2020, , 37-61.		14
88	Learning Based Anomaly Detection in Critical Cyber-Physical Systems. , 2020, , 107-130.		14
89	Application of Machine Learning Algorithms for Android Malware Detection. , 2018, , .		13
90	Making Sense of Blockchain for AI Deepfakes Technology. , 2020, , .		13

#	Article	IF	Citations
91	A hierarchical key preâ€distribution scheme for fog networks. Concurrency Computation Practice and Experience, 2019, 31, e4776.	1.4	12
92	Enhancing Network Security Via Machine Learning: Opportunities and Challenges. , 2020, , 165-189.		12
93	Federated IoT attack detection using decentralized edge data. Machine Learning With Applications, 2022, 8, 100263.	3.0	12
94	Privacy and Security in Smart and Precision Farming: A Bibliometric Analysis. , 2020, , 305-318.		11
95	An analysis of anti-forensic capabilities of B-tree file system (Btrfs). Australian Journal of Forensic Sciences, 2020, 52, 371-386.	0.7	10
96	Active Spectral Botnet Detection Based on Eigenvalue Weighting. , 2020, , 385-397.		10
97	A Comparison Between Different Machine Learning Models for IoT Malware Detection. , 2020, , 195-202.		9
98	Joint State Estimation and Cyber-Attack Detection Based on Feature Grouping. , 2019, , .		8
99	Big Data and Privacy: Challenges and Opportunities. , 2020, , 1-5.		8
100	A Self-Tuning Cyber-Attacksâ€™ Location Identification Approach for Critical Infrastructures. IEEE Transactions on Industrial Informatics, 2022, 18, 5018-5027.	7.2	8
101	Resilient Scheduling of Networked Microgrids Against Real-Time Failures. IEEE Access, 2021, 9, 21443-21456.	2.6	7
102	Blockchain Applications in Power Systems: A Bibliometric Analysis. Advances in Information Security, 2020, , 129-145.	0.9	7
103	A Comparison of State-of-the-Art Machine Learning Models for OpCode-Based IoT Malware Detection. , 2020, , 109-120.		7
104	AI-Enabled Security Monitoring in Smart Cyber Physical Grids. , 2020, , 145-167.		7
105	A Machine Learning-based SDN Controller Framework for Drone Management. , 2021, , .		7
106	Coordinated Fuzzy Controller for Dynamic Stability Improvement in Multi-Machine Power System. , 2018, , .		6
107	Hybrid Islanding Detection for AC/DC Network Using DC-link Voltage. , 2018, , .		6
108	AI and Security of Critical Infrastructure. , 2020, , 7-36.		6

#	Article	IF	Citations
109	Deep Federated Learning-Based Cyber-Attack Detection in Industrial Control Systems. , 2021, , .		6
110	Power System Dynamic State Estimation Using Smooth Variable Structure Filter. , 2019, , .		5
111	Malware Elimination Impact on Dynamic Analysis: An Experimental Machine Learning Approach. , 2020, , 359-370.		5
112	Artificial Intelligence and Security of Industrial Control Systems. , 2020, , 121-164.		5
113	Artificial Bee Colony-based Routing for Mobile Agents on the Internet of Things. , 2020, , .		5
114	A Hybrid RSA Algorithm in Support of IoT Greenhouse Applications. , 2019, , .		4
115	A Privacy Protection Key Agreement Protocol Based on ECC for Smart Grid. , 2020, , 63-76.		4
116	Application of Machine Learning in State Estimation of Smart Cyber-Physical Grid. , 2020, , 169-194.		4
117	Big-Data and Cyber-Physical Systems in Healthcare: Challenges and Opportunities. , 2020, , 255-283.		4
118	A Survey on Application of Big Data in Fin Tech Banking Security and Privacy. , 2020, , 319-342.		4
119	Secure AI and Blockchain-enabled Framework in Smart Vehicular Networks. , 2021, , .		4
120	SteelEye: An Application-Layer Attack Detection and Attribution Model in Industrial Control Systems using Semi-Deep Learning. , 2021, , .		4
121	Blockchain Applications in the Industrial Internet of Things. , 2021, , 41-76.		3
122	RAT Hunter: Building Robust Models for Detecting Remote Access Trojans Based on Optimum Hybrid Features. , 2020, , 371-383.		3
123	IoT Privacy, Security and Forensics Challenges: An Unmanned Aerial Vehicle (UAV) Case Study. , 2022, , 7-39.		3
124	Instability Prediction in Smart Cyber-physical Grids Using Feedforward Neural Networks. , 2020, , .		3
125	On detailed synchronous generator modeling for massively parallel dynamic state estimation. , 2014, , .		2
126	A Snapshot Ensemble Deep Neural Network Model for Attack Detection in Industrial Internet of Things. , 2021, , 181-194.		2

#	Article	IF	Citations
127	Assessing Insider Attacks and Privacy Leakage in Managed IoT Systems for Residential Prosumers. Energies, 2021, 14, 2385.	1.6	2
128	A Deep Neural Network Combined with Radial Basis Function for Abnormality Classification. Mobile Networks and Applications, 2021, 26, 2318-2328.	2.2	2
129	A Hybrid Deep Learning-Based Power System State Forecasting. , 2020, , .		2
130	A Bibliometric Analysis on the Application of Deep Learning in Cybersecurity. , 2020, , 203-221.		2
131	Employing Composite Demand Response Model in Microgrid Energy Management. , 2019, , .		1
132	Application of Deep Learning on IoT-Enabled Smart Grid Monitoring. , 2021, , 77-103.		1
133	Deep Representation Learning for Cyber-Attack Detection in Industrial IoT. , 2021, , 139-162.		1
134	Big Data Application for Security of Renewable Energy Resources. , 2020, , 237-254.		1
135	Lower Bounds on Bandwidth Requirements of Regenerating Code Parameter Scaling in Distributed Storage Systems. IEEE Communications Letters, 2021, 25, 1477-1481.	2.5	0
136	Artificial Intelligence for Threat Detection and Analysis in Industrial IoT: Applications and Challenges. , 2021, , 1-6.		0
137	Privacy Preserving Abnormality Detection: A Deep Learning Approach. , 2020, , 285-303.		0