Ali Dehghantanha

List of Publications by Year in Descending Order

164 papers	4,745 citations	37 h-index	64 g-index
172 ext. papers	6,471 ext. citations	3.7 avg, IF	6.98 L-index

#	Paper	IF	Citations
164	Federated IoT attack detection using decentralized edge data. *Machine Learning With Applications*, **2022**, 8, 100263	6.5	2
163	IoT Privacy, Security and Forensics Challenges: An Unmanned Aerial Vehicle (UAV) Case Study **2022**, 7-39		0
162	Big Data Analytics and Forensics: An Overview **2022**, 1-5		
161	An efficient packet parser architecture for software-defined 5G networks. *Physical Communication*, **2022**, 53, 101677	2.2	0
160	A Self-tuning Cyber-Attacks Location Identification Approach for Industrial Internet of Things. *IEEE Transactions on Industrial Informatics*, **2021**, 1-1	11.9	2
159	Editorial for the Special Issue on Sustainable Cyber Forensics and Threat Intelligence. *IEEE Transactions on Sustainable Computing*, **2021**, 6, 182-183	3.5	
158	Lower Bounds on Bandwidth Requirements of Regenerating Code Parameter Scaling in Distributed Storage Systems. *IEEE Communications Letters*, **2021**, 25, 1477-1481	3.8	
157	Enabling Drones in the Internet of Things With Decentralized Blockchain-Based Security. *IEEE Internet of Things Journal*, **2021**, 8, 6406-6415	10.7	49
156	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
155	A survey on security and privacy of federated learning. *Future Generation Computer Systems*, **2021**, 115, 619-640	7.5	165
154	A kangaroo-based intrusion detection system on software-defined networks. *Computer Networks*, **2021**, 184, 107688	5.4	12
153	A survey of machine learning techniques in adversarial image forensics. *Computers and Security*, **2021**, 100, 102092	4.9	17
152	Security aspects of Internet of Things aided smart grids: A bibliometric survey. *Internet of Things (Netherlands)*, **2021**, 14, 100111	6.9	64
151	A survey on internet of things security: Requirements, challenges, and solutions. *Internet of Things (Netherlands)*, **2021**, 14, 100129	6.9	82
150	A Recurrent Attention Model for Cyber Attack Classification **2021**, 237-250		0
149	Blockchain Applications in the Industrial Internet of Things **2021**, 41-76		1
148	A Snapshot Ensemble Deep Neural Network Model for Attack Detection in Industrial Internet of Things **2021**, 181-194		0

147	Application of Deep Learning on IoT-Enabled Smart Grid Monitoring **2021**, 77-103		0
146	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
145	Physical layer attack identification and localization in cyber–physical grid: An ensemble deep learning based approach. *Physical Communication*, **2021**, 47, 101394	2.2	6
144	Federated learning for drone authentication. *Ad Hoc Networks*, **2021**, 120, 102574	4.8	6
143	Toward Detection and Attribution of Cyber-Attacks in IoT-Enabled Cyber–Physical Systems. *IEEE Internet of Things Journal*, **2021**, 8, 13712-13722	10.7	14
142	Generative adversarial network to detect unseen Internet of Things malware. *Ad Hoc Networks*, **2021**, 122, 102591	4.8	9
141	Deep Representation Learning for Cyber-Attack Detection in Industrial IoT **2021**, 139-162		1
140	Artificial Intelligence for Threat Detection and Analysis in Industrial IoT: Applications and Challenges **2021**, 1-6		
139	Federated Learning-based Anomaly Detection for IoT Security Attacks. *IEEE Internet of Things Journal*, **2021**, 1-1	10.7	42
138	Ensemble sparse representation-based cyber threat hunting for security of smart cities. *Computers and Electrical Engineering*, **2020**, 88, 106825	4.3	8
137	An Ensemble Deep Learning-Based Cyber-Attack Detection in Industrial Control System. *IEEE Access*, **2020**, 8, 83965-83973	3.5	58
136	. *IEEE Transactions on Emerging Topics in Computational Intelligence*, **2020**, 4, 630-640	4.1	21
135	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
134	SLPoW: Secure and Low Latency Proof of Work Protocol for Blockchain in Green IoT Networks **2020** ,		14
133	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
132	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
131	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
130	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

129	Decentralized Authentication of Distributed Patients in Hospital Networks Using Blockchain. *IEEE Journal of Biomedical and Health Informatics*, **2020**, 24, 2146-2156	7.2	70
128	Detecting Cryptomining Malware: a Deep Learning Approach for Static and Dynamic Analysis. *Journal of Grid Computing*, **2020**, 18, 293-303	4.2	21
127	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
126	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
125	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
124	An Ensemble Deep Convolutional Neural Network Model for Electricity Theft Detection in Smart Grids **2020**,		7
123	**2020**,		8
122	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
121	A Bibliometric Analysis on the Application of Deep Learning in Cybersecurity **2020**, 203-221		1
120	AI and Security of Critical Infrastructure **2020**, 7-36		1
119	Big Data Application for Security of Renewable Energy Resources **2020**, 237-254		1
118	Big-Data and Cyber-Physical Systems in Healthcare: Challenges and Opportunities **2020**, 255-283		3
117	Immutable and Secure IP Address Protection Using Blockchain. *Advances in Information Security*, **2020**, 233-246	0.7	2
116	Privacy Preserving Abnormality Detection: A Deep Learning Approach **2020**, 285-303		
115	A Survey on Application of Big Data in Fin Tech Banking Security and Privacy **2020**, 319-342		3
114	RAT Hunter: Building Robust Models for Detecting Remote Access Trojans Based on Optimum Hybrid Features **2020**, 371-383		3
113	Active Spectral Botnet Detection Based on Eigenvalue Weighting **2020**, 385-397		10
112	An Empirical Evaluation of AI Deep Explainable Tools **2020**,		5

111	Big Data and Privacy: Challenges and Opportunities **2020**, 1-5		6
110	Blockchain in Cybersecurity Realm: An Overview. *Advances in Information Security*, **2020**, 1-5	0.7	3
109	Public Blockchains Scalability: An Examination of Sharding and Segregated Witness. *Advances in Information Security*, **2020**, 203-232	0.7	14
108	Secure Blockchain-Based Traffic Load Balancing Using Edge Computing and Reinforcement Learning. *Advances in Information Security*, **2020**, 99-128	0.7	2
107	Blockchain Applications in Power Systems: A Bibliometric Analysis. *Advances in Information Security*, **2020**, 129-145	0.7	3
106	Anomaly Detection in Cyber-Physical Systems Using Machine Learning **2020**, 219-235		12
105	Privacy and Security in Smart and Precision Farming: A Bibliometric Analysis **2020**, 305-318		9
104	A Hybrid Deep Generative Local Metric Learning Method for Intrusion Detection **2020**, 343-357		13
103	Malware Elimination Impact on Dynamic Analysis: An Experimental Machine Learning Approach **2020**, 359-370		4
102	Industrial Big Data Analytics: Challenges and Opportunities **2020**, 37-61		8
101	A Privacy Protection Key Agreement Protocol Based on ECC for Smart Grid **2020**, 63-76		4
100	Applications of Big Data Analytics and Machine Learning in the Internet of Things **2020**, 77-108		12
99	A Comparison of State-of-the-Art Machine Learning Models for OpCode-Based IoT Malware Detection **2020**, 109-120		5
98	Artificial Intelligence and Security of Industrial Control Systems **2020**, 121-164		5
97	Enhancing Network Security Via Machine Learning: Opportunities and Challenges **2020**, 165-189		7
96	A Comparison Between Different Machine Learning Models for IoT Malware Detection **2020**, 195-202		5
95	Learning Based Anomaly Detection in Critical Cyber-Physical Systems **2020**, 107-130		8
94	AI-Enabled Security Monitoring in Smart Cyber Physical Grids **2020**, 145-167		6

93	Application of Machine Learning in State Estimation of Smart Cyber-Physical Grid **2020**, 169-194		2
92	. *IEEE Transactions on Network Science and Engineering*, **2020**, 1-1	4.9	53
91	Threats on the horizon: understanding security threats in the era of cyber-physical systems. *Journal of Supercomputing*, **2020**, 76, 2643-2664	2.5	25
90	Sidechain technologies in blockchain networks: An examination and state-of-the-art review. *Journal of Network and Computer Applications*, **2020**, 149, 102471	7.9	72
89	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
88	An improved two-hidden-layer extreme learning machine for malware hunting. *Computers and Security*, **2020**, 89, 101655	4.9	39
87	Cryptocurrency malware hunting: A deep Recurrent Neural Network approach. *Applied Soft Computing Journal*, **2020**, 96, 106630	7.5	37
86	MVFCC: A Multi-View Fuzzy Consensus Clustering Model for Malware Threat Attribution. *IEEE Access*, **2020**, 8, 139188-139198	3.5	16
85	Real-time stability assessment in smart cyber-physical grids: a deep learning approach. *IET Smart Grid*, **2020**, 3, 454-461	2.7	8
84	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
83	An analysis of anti-forensic capabilities of B-tree file system (Btrfs). *Australian Journal of Forensic Sciences*, **2020**, 52, 371-386	1.1	7
82	An opcode-based technique for polymorphic Internet of Things malware detection. *Concurrency Computation Practice and Experience*, **2020**, 32, e5173	1.4	34
81	A systematic literature review of blockchain cyber security. *Digital Communications and Networks*, **2020**, 6, 147-156	5.9	191
80	P4-to-blockchain: A secure blockchain-enabled packet parser for software defined networking. *Computers and Security*, **2020**, 88, 101629	4.9	42
79	Non-interactive zero knowledge proofs for the authentication of IoT devices in reduced connectivity environments. *Ad Hoc Networks*, **2019**, 95, 101988	4.8	18
78	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
77	Big Data Forensics: Hadoop Distributed File Systems as a Case Study **2019**, 179-210		2
76	A systematic literature review and meta-analysis on artificial intelligence in penetration testing and vulnerability assessment. *Computers and Electrical Engineering*, **2019**, 75, 175-188	4.3	21

75	Protecting IoT and ICS Platforms Against Advanced Persistent Threat Actors: Analysis of APT1, Silent Chollima and Molerats **2019**, 225-255		8
74	A Bibliometric Analysis of Authentication and Access Control in IoT Devices **2019**, 25-51		6
73	Fuzzy pattern tree for edge malware detection and categorization in IoT. *Journal of Systems Architecture*, **2019**, 97, 1-7	5.5	99
72	Big Data and Internet of Things Security and Forensics: Challenges and Opportunities **2019**, 1-4		15
71	Evaluation and Application of Two Fuzzing Approaches for Security Testing of IoT Applications **2019**, 301-327		2
70	A Bibliometric Analysis of Botnet Detection Techniques **2019**, 345-365		3
69	Internet of Things Camera Identification Algorithm Based on Sensor Pattern Noise Using Color Filter Array and Wavelet Transform **2019**, 211-223		5
68	Security in Online Games: Current Implementations and Challenges **2019**, 367-384		3
67	A Cyber Kill Chain Based Analysis of Remote Access Trojans **2019**, 273-299		5
66	Private Cloud Storage Forensics: Seafile as a Case Study **2019**, 73-127		4
65	DRTHIS: Deep ransomware threat hunting and intelligence system at the fog layer. *Future Generation Computer Systems*, **2019**, 90, 94-104	7.5	64
64	A Cyber-Kill-Chain based taxonomy of crypto-ransomware features. *Journal of Computer Virology and Hacking Techniques*, **2019**, 15, 277-305	3	28
63	A Blockchain-based Framework for Detecting Malicious Mobile Applications in App Stores **2019**,		22
62	A Layered Intrusion Detection System for Critical Infrastructure Using Machine Learning **2019**,		21
61	Employing Composite Demand Response Model in Microgrid Energy Management **2019**,		1
60	Bibliometric Analysis on the Rise of Cloud Security **2019**, 329-344		1
59	Forensic Investigation of Cross Platform Massively Multiplayer Online Games: Minecraft as a Case Study **2019**, 153-177		
58	Data Sharing and Privacy for Patient IoT Devices Using Blockchain. *Communications in Computer and Information Science*, **2019**, 334-348	0.3	20

57	Distributed Filesystem Forensics: Ceph as a Case Study **2019**, 129-151		1
56	Analysis of APT Actors Targeting IoT and Big Data Systems: Shell_Crew, NetTraveler, ProjectSauron, CopyKittens, Volatile Cedar and Transparent Tribe as a Case Study **2019**, 257-272		2
55	**2019**,		4
54	Cyber defence triage for multimedia data intelligence: Hellsing, Desert Falcons and Lotus Blossom APT campaigns as case studies. *International Journal of Multimedia Intelligence and Security*, **2019**, 3, 221	0.4	
53	Energy Efficient Decentralized Authentication in Internet of Underwater Things Using Blockchain **2019**,		19
52	Smart Grid Cyber Attacks Detection Using Supervised Learning and Heuristic Feature Selection **2019**,		36
51	Joint State Estimation and Cyber-Attack Detection Based on Feature Grouping **2019**,		6
50	**2019**,		25
49	Analysis and Triage of Advanced Hacking Groups Targeting Western Countries Critical National Infrastructure: APT28, RED October, and Regin. *Advanced Sciences and Technologies for Security Applications*, **2019**, 221-244	0.6	5
48	Cyber intrusion detection by combined feature selection algorithm. *Journal of Information Security and Applications*, **2019**, 44, 80-88	3.5	108
47	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
46	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
45	A Model for Android and iOS Applications Risk Calculation: CVSS Analysis and Enhancement Using Case-Control Studies. *Advances in Information Security*, **2018**, 219-237	0.7	8
44	Forensics Investigation of OpenFlow-Based SDN Platforms. *Advances in Information Security*, **2018**, 281-296	0.7	5
43	BoTShark: A Deep Learning Approach for Botnet Traffic Detection. *Advances in Information Security*, **2018**, 137-153	0.7	27
42	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
41	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
40	Intelligent OS X malware threat detection with code inspection. *Journal of Computer Virology and Hacking Techniques*, **2018**, 14, 213-223	3	38

39	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
38	Leveraging Support Vector Machine for Opcode Density Based Detection of Crypto-Ransomware. *Advances in Information Security*, **2018**, 107-136	0.7	19
37	CyberPDF **2018**,		4
36	A cyber kill chain based taxonomy of banking Trojans for evolutionary computational intelligence. *Journal of Computational Science*, **2018**, 27, 394-409	3.4	45
35	CloudMe forensics: A case of big data forensic investigation. *Concurrency Computation Practice and Experience*, **2018**, 30, e4277	1.4	24
34	Application of Machine Learning Algorithms for Android Malware Detection **2018**,		8
33	On the Understanding of Gamification in Blockchain Systems **2018**,		17
32	**2018**,		3
31	Mobile Forensics: A Bibliometric Analysis. *Advances in Information Security*, **2018**, 297-310	0.7	8
30	Emerging from the Cloud: A Bibliometric Analysis of Cloud Forensics Studies. *Advances in Information Security*, **2018**, 311-331	0.7	15
29	Machine Learning Aided Static Malware Analysis: A Survey and Tutorial. *Advances in Information Security*, **2018**, 7-45	0.7	35
28	Leveraging Machine Learning Techniques for Windows Ransomware Network Traffic Detection. *Advances in Information Security*, **2018**, 93-106	0.7	44
27	Cloud storage forensics: MEGA as a case study. *Australian Journal of Forensic Sciences*, **2017**, 49, 344-357	1.1	35
26	Machine learning aided Android malware classification. *Computers and Electrical Engineering*, **2017**, 61, 266-274	4.3	161
25	Forensic Investigation of Cooperative Storage Cloud Service: Symform as a Case Study. *Journal of Forensic Sciences*, **2017**, 62, 641-654	1.8	17
24	Investigating the antecedents to the adoption of SCRM technologies by start-up companies. *Telematics and Informatics*, **2017**, 34, 655-675	8.1	29
23	Forensic investigation of P2P cloud storage services and backbone for IoT networks: BitTorrent Sync as a case study. *Computers and Electrical Engineering*, **2017**, 58, 350-363	4.3	41
22	SugarSync forensic analysis. *Australian Journal of Forensic Sciences*, **2016**, 48, 95-117	1.1	30

21	Ensemble-based multi-filter feature selection method for DDoS detection in cloud computing. *Eurasip Journal on Wireless Communications and Networking*, **2016**, 2016,	3.2	160
20	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
19	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
18	A Closer Look at Syncany Windows and Ubuntu Clients Residual Artefacts. *Lecture Notes in Computer Science*, **2016**, 342-357	0.9	5
17	Windows Instant Messaging App Forensics: Facebook and Skype as Case Studies. *PLoS ONE*, **2016**, 11, e0150300	3.7	39
16	Digital forensics: the missing piece of the Internet of Things promise. *Computer Fraud and Security*, **2016**, 2016, 5-8	2.2	57
15	Extended Kalman Filter-Based Parallel Dynamic State Estimation. *IEEE Transactions on Smart Grid*, **2015**, 6, 1539-1549	10.7	93
14	Ubuntu One investigation: Detecting evidences on client machines **2015**, 429-446		18
13	Exploit Kits: The production line of the Cybercrime economy? **2015**,		19
12	M0Droid: An Android Behavioral-Based Malware Detection Model. *Journal of Information Privacy and Security*, **2015**, 11, 141-157		46
11	An approach for forensic investigation in Firefox OS **2014**,		3
10	Mobile forensic data acquisition in Firefox OS **2014**,		3
9	Privacy-respecting digital investigation **2014**,		17
8	A Survey on Digital Forensics Trends. *International Journal of Cyber-Security and Digital Forensics*, **2014**, 3, 209-234	1.6	3
7	Towards secure model for SCADA systems **2012**,		19
6	Volatile memory acquisition using backup for forensic investigation **2012**,		12
5	**2012**,		28
4	VoIP evidence model: A new forensic method for investigating VoIP malicious attacks **2012**,		5

List of Publications

3	Investigation of bypassing malware defences and malware detections **2011**,	13
2	Towards data centric mobile security **2011**,	1
1	UPM: User-Centered Privacy Model in Pervasive Computing Systems **2009**,	4