Nour Moustafa

List of Publications by Year
in descending order

Source: https://exaly.com/author-pdf/539794/publications.pdf

Version: 2024-02-01

111 papers	6,786 citations	147566 31 h-index	91712 69 g-index
118 all docs	118 docs citations	118 times ranked	3118 citing authors

#	Article	IF	Citations
1	UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network) Tj ETQq1 1 0.784314 rgBT /Ov		1,395
2	Towards the development of realistic botnet dataset in the Internet of Things for network forensic analytics: Bot-IoT dataset. Future Generation Computer Systems, 2019, 100, 779-796.	4.9	783
3	The evaluation of Network Anomaly Detection Systems: Statistical analysis of the UNSW-NB15 data set and the comparison with the KDD99 data set. Information Security Journal, 2016, 25, 18-31.	1.3	516
4	An Ensemble Intrusion Detection Technique Based on Proposed Statistical Flow Features for Protecting Network Traffic of Internet of Things. IEEE Internet of Things Journal, 2019, 6, 4815-4830.	5.5	320
5	TON_IoT Telemetry Dataset: A New Generation Dataset of IoT and IIoT for Data-Driven Intrusion Detection Systems. IEEE Access, 2020, 8, 165130-165150.	2.6	260
6	A holistic review of Network Anomaly Detection Systems: A comprehensive survey. Journal of Network and Computer Applications, 2019, 128, 33-55.	5.8	211
7	A Deep Blockchain Framework-Enabled Collaborative Intrusion Detection for Protecting IoT and Cloud Networks. IEEE Internet of Things Journal, 2021, 8, 9463-9472.	5.5	201
8	Identification of malicious activities in industrial internet of things based on deep learning models. Journal of Information Security and Applications, 2018, 41, 1-11.	1.8	184
9	A new distributed architecture for evaluating AI-based security systems at the edge: Network TON_IoT datasets. Sustainable Cities and Society, 2021, 72, 102994.	5.1	173
10	Novel Geometric Area Analysis Technique for Anomaly Detection Using Trapezoidal Area Estimation on Large-Scale Networks. IEEE Transactions on Big Data, 2019, 5, 481-494.	4.4	132
11	The Significant Features of the UNSW-NB15 and the KDD99 Data Sets for Network Intrusion Detection Systems. , 2015, , .		127
12	A Review of Intrusion Detection Systems Using Machine and Deep Learning in Internet of Things: Challenges, Solutions and Future Directions. Electronics (Switzerland), 2020, 9, 1177.	1.8	125
13	A new network forensic framework based on deep learning for Internet of Things networks: A particle deep framework. Future Generation Computer Systems, 2020, 110, 91-106.	4.9	108
14	ToN_IoT: The Role of Heterogeneity and the Need for Standardization of Features and Attack Types in IoT Network Intrusion Data Sets. IEEE Internet of Things Journal, 2022, 9, 485-496.	5.5	105
15	A Privacy-Preserving-Framework-Based Blockchain and Deep Learning for Protecting Smart Power Networks. IEEE Transactions on Industrial Informatics, 2020, 16, 5110-5118.	7.2	104
16	Novel Deep Learning-Enabled LSTM Autoencoder Architecture for Discovering Anomalous Events From Intelligent Transportation Systems. IEEE Transactions on Intelligent Transportation Systems, 2021, 22, 4507-4518.	4.7	102
17	A New Threat Intelligence Scheme for Safeguarding Industry 4.0 Systems. IEEE Access, 2018, 6, 32910-32924.	2.6	95
18	Forensics and Deep Learning Mechanisms for Botnets in Internet of Things: A Survey of Challenges and Solutions. IEEE Access, 2019, 7, 61764-61785.	2.6	87

#	Article	IF	Citations
19	NetFlow Datasets for Machine Learning-Based Network Intrusion Detection Systems. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, 2021, , 117-135.	0.2	83
20	An Integrated Framework for Privacy-Preserving Based Anomaly Detection for Cyber-Physical Systems. IEEE Transactions on Sustainable Computing, 2021, 6, 66-79.	2.2	81
21	Outlier Dirichlet Mixture Mechanism: Adversarial Statistical Learning for Anomaly Detection in the Fog. IEEE Transactions on Information Forensics and Security, 2019, 14, 1975-1987.	4.5	80
22	IoTBoT-IDS: A novel statistical learning-enabled botnet detection framework for protecting networks of smart cities. Sustainable Cities and Society, 2021, 72, 103041.	5.1	79
23	Big Data Analytics for Intrusion Detection System: Statistical Decision-Making Using Finite Dirichlet Mixture Models. Data Analytics, 2017, , 127-156.	0.8	77
24	XSRU-IoMT: Explainable simple recurrent units for threat detection in Internet of Medical Things networks. Future Generation Computer Systems, 2022, 127, 181-193.	4.9	58
25	A Review of Intrusion Detection and Blockchain Applications in the Cloud: Approaches, Challenges and Solutions. IEEE Access, 2020, 8, 104893-104917.	2.6	53
26	Supply Chain 4.0: A Survey of Cyber Security Challenges, Solutions and Future Directions. Electronics (Switzerland), 2020, 9, 1864.	1.8	52
27	A Holistic Review of Cybersecurity and Reliability Perspectives in Smart Airports. IEEE Access, 2020, 8, 209802-209834.	2.6	50
28	Deep Gaussian Mixture-Hidden Markov Model for Classification of EEG Signals. IEEE Transactions on Emerging Topics in Computational Intelligence, 2018, 2, 278-287.	3.4	49
29	Towards Developing Network Forensic Mechanism for Botnet Activities in the IoT Based on Machine Learning Techniques. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, 2018, , 30-44.	0.2	47
30	Federated Intrusion Detection in Blockchain-Based Smart Transportation Systems. IEEE Transactions on Intelligent Transportation Systems, 2022, 23, 2523-2537.	4.7	45
31	Collaborative anomaly detection framework for handling big data of cloud computing. , 2017, , .		40
32	An Enhanced Multi-Stage Deep Learning Framework for Detecting Malicious Activities From Autonomous Vehicles. IEEE Transactions on Intelligent Transportation Systems, 2022, 23, 25469-25478.	4.7	40
33	Privacy preservation intrusion detection technique for SCADA systems. , 2017, , .		35
34	Federated TON_IoT Windows Datasets for Evaluating AI-Based Security Applications. , 2020, , .		35
35	An Automated Task Scheduling Model Using Non-Dominated Sorting Genetic Algorithm II for Fog-Cloud Systems. IEEE Transactions on Cloud Computing, 2022, 10, 2294-2308.	3.1	33
36	Robustness Evaluations of Sustainable Machine Learning Models against Data Poisoning Attacks in the Internet of Things. Sustainability, 2020, 12, 6434.	1.6	32

#	Article	IF	Citations
37	AI-Driven Synthetic Biology for Non-Small Cell Lung Cancer Drug Effectiveness-Cost Analysis in Intelligent Assisted Medical Systems. IEEE Journal of Biomedical and Health Informatics, 2022, 26, 5055-5066.	3.9	32
38	Anomaly Detection System Using Beta Mixture Models and Outlier Detection. Advances in Intelligent Systems and Computing, 2018, , 125-135.	0.5	30
39	AI-Enabled Secure Microservices in Edge Computing: Opportunities and Challenges. IEEE Transactions on Services Computing, 2023, 16, 1485-1504.	3.2	29
40	Generalized Outlier Gaussian Mixture Technique Based on Automated Association Features for Simulating and Detecting Web Application Attacks. IEEE Transactions on Sustainable Computing, 2021, 6, 245-256.	2.2	27
41	Multi-Objective Task Scheduling Approach for Fog Computing. IEEE Access, 2021, 9, 126988-127009.	2.6	27
42	Data Analytics-Enabled Intrusion Detection: Evaluations of ToN_IoT Linux Datasets. , 2020, , .		27
43	Pelican: A Deep Residual Network for Network Intrusion Detection. , 2020, , .		26
44	Deep Learning-Enabled Threat Intelligence Scheme in the Internet of Things Networks. IEEE Transactions on Network Science and Engineering, 2021, 8, 2968-2981.	4.1	26
45	Privacy-Preserving Schemes for Safeguarding Heterogeneous Data Sources in Cyber-Physical Systems. IEEE Access, 2021, 9, 55077-55097.	2.6	25
46	A New Explainable Deep Learning Framework for Cyber Threat Discovery in Industrial IoT Networks. IEEE Internet of Things Journal, 2022, 9, 11604-11613.	5.5	25
47	DAD: A Distributed Anomaly Detection system using ensemble one-class statistical learning in edge networks. Future Generation Computer Systems, 2021, 118, 240-251.	4.9	24
48	Mixture Localization-Based Outliers Models for securing Data Migration in Cloud Centers. IEEE Access, 2019, 7, 114607-114618.	2.6	23
49	An Explainable Deep Learning Framework for Resilient Intrusion Detection in IoT-Enabled Transportation Networks. IEEE Transactions on Intelligent Transportation Systems, 2023, 24, 1000-1014.	4.7	22
50	A Blockchain-Enabled Privacy-Preserving Verifiable Query Framework for Securing Cloud-Assisted Industrial Internet of Things Systems. IEEE Transactions on Industrial Informatics, 2022, 18, 5007-5017.	7.2	21
51	FGMC-HADS: Fuzzy Gaussian mixture-based correntropy models for detecting zero-day attacks from linux systems. Computers and Security, 2020, 96, 101906.	4.0	19
52	Privacy-preserving big data analytics for cyber-physical systems. Wireless Networks, 2022, 28, 1241-1249.	2.0	18
53	A Blockchain-Enabled Explainable Federated Learning for Securing Internet-of-Things-Based Social Media 3.0 Networks. IEEE Transactions on Computational Social Systems, 2024, , 1-17.	3.2	17
54	Data analytics of social media 3.0: Privacy protection perspectives for integrating social media and Internet of Things (SM-IoT) systems. Ad Hoc Networks, 2022, 128, 102786.	3.4	16

#	Article	IF	Citations
55	A holistic survey on the use of emerging technologies to provision secure healthcare solutions. Computers and Electrical Engineering, 2022, 99, 107691.	3.0	15
56	A Blockchain-Based Emergency Message Transmission Protocol for Cooperative VANET. IEEE Transactions on Intelligent Transportation Systems, 2022, 23, 19624-19633.	4.7	14
57	Two-Stage Deep Learning Framework for Discrimination between COVID-19 and Community-Acquired Pneumonia from Chest CT scans. Pattern Recognition Letters, 2021, 152, 311-319.	2.6	14
58	The SAir-IIoT Cyber Testbed as a Service: A Novel Cybertwins Architecture in IIoT-Based Smart Airports. IEEE Transactions on Intelligent Transportation Systems, 2021, , 1-14.	4.7	13
59	A Security-by-Design Decision-Making Model for Risk Management in Autonomous Vehicles. IEEE Access, 2021, 9, 107657-107679.	2.6	13
60	A new Intelligent Satellite Deep Learning Network Forensic framework for smart satellite networks. Computers and Electrical Engineering, 2022, 99, 107745.	3.0	13
61	Privacy-Preserved Cyberattack Detection in Industrial Edge of Things (IEoT): A Blockchain-Orchestrated Federated Learning Approach. IEEE Transactions on Industrial Informatics, 2022, 18, 7920-7934.	7.2	13
62	A Privacy-Preserving Generative Adversarial Network Method for Securing EEG Brain Signals. , 2020, , .		12
63	Privacy-Preserving Microservices in Industrial Internet-of-Things-Driven Smart Applications. IEEE Internet of Things Journal, 2023, 10, 2821-2831.	5.5	12
64	Session Invariant EEG Signatures using Elicitation Protocol Fusion and Convolutional Neural Network. IEEE Transactions on Dependable and Secure Computing, 2022, 19, 2488-2500.	3.7	11
65	OQFL: An Optimized Quantum-Based Federated Learning Framework for Defending Against Adversarial Attacks in Intelligent Transportation Systems. IEEE Transactions on Intelligent Transportation Systems, 2023, 24, 893-903.	4.7	11
66	Blind Camcording-Resistant Video Watermarking in the DTCWT and SVD Domain. IEEE Access, 2022, 10, 15681-15698.	2.6	11
67	A Data Driven Review of Board Game Design and Interactions of Their Mechanics. IEEE Access, 2021, 9, 114051-114069.	2.6	10
68	USMD: UnSupervised Misbehaviour Detection for Multi-Sensor Data. IEEE Transactions on Dependable and Secure Computing, 2023, 20, 724-739.	3.7	10
69	Probability Risk Identification Based Intrusion Detection System for SCADA Systems. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, 2018, , 353-363.	0.2	8
70	Fair and size-scalable participant selection framework for large-scale mobile crowdsensing. Journal of Systems Architecture, 2021, 119, 102273.	2.5	8
71	Autonomous detection of malicious events using machine learning models in drone networks. , 2020, , .		8
72	A Secure and Intelligent Framework for Vehicle Health Monitoring Exploiting Big-Data Analytics. IEEE Transactions on Intelligent Transportation Systems, 2022, 23, 19727-19742.	4.7	8

#	Article	IF	Citations
73	An Ontological Graph Identification Method for Improving Localization of IP Prefix Hijacking in Network Systems. IEEE Transactions on Information Forensics and Security, 2020, 15, 1164-1174.	4.5	7
74	Streaming service provisioning in IoTâ€based healthcare: An integrated edgeâ€cloud perspective. Transactions on Emerging Telecommunications Technologies, 2020, 31, e4109.	2.6	7
75	Flow Aggregator Module for Analysing Network Traffic. Advances in Intelligent Systems and Computing, 2018, , 19-29.	0.5	7
76	A Collaborative Intrusion Detection System Using Deep Blockchain Framework for Securing Cloud Networks. Advances in Intelligent Systems and Computing, 2021, , 553-565.	0.5	7
77	A Deep Learning-based Penetration Testing Framework for Vulnerability Identification in Internet of Things Environments. , 2021, , .		7
78	A Network Forensic Scheme Using Correntropy-Variation for Attack Detection. IFIP Advances in Information and Communication Technology, 2018, , 225-239.	0.5	6
79	A digital identity stack to improve privacy in the IoT. , 2018, , .		6
80	Guest Editorial: AI-Enabled Threat Intelligence and Hunting Microservices for Distributed Industrial IoT System. IEEE Transactions on Industrial Informatics, 2022, 18, 1892-1895.	7.2	6
81	Cognitive Privacy: AI-enabled Privacy using EEG Signals in the Internet of Things. , 2020, , .		6
82	Enhancing IoT Anomaly Detection Performance for Federated Learning. , 2020, , .		6
83	Perturbation-enabled Deep Federated Learning for Preserving Internet of Things-based Social Networks. ACM Transactions on Multimedia Computing, Communications and Applications, 2022, 18, 1-19.	3.0	6
84	Towards Automation of Vulnerability and Exploitation Identification in IIoT Networks. , 2018, , .		5
85	A Novel Cognitive Computing Technique Using Convolutional Networks for Automating the Criminal Investigation Process in Policing. Advances in Intelligent Systems and Computing, 2021, , 528-539.	0.5	5
86	Privacy-Preserving Techniques for Protecting Large-Scale Data of Cyber-Physical Systems. , 2020, , .		5
87	Densely Connected Residual Network for Attack Recognition. , 2020, , .		5
88	Security and Privacy in 4G/LTE Network. , 2018, , 1-7.		4
89	An Adaptive Cuckoo Search-Based Optimization Model for Addressing Cyber-Physical Security Problems. Mathematics, 2021, 9, 1140.	1.1	4
90	Edge Intelligence-based Privacy Protection Framework for IoT-based Smart Healthcare Systems. , 2022, , .		4

#	Article	IF	Citations
91	Hierarchical Adversarial Network for Human Pose Estimation. IEEE Access, 2019, 7, 103619-103628.	2.6	3
92	Mitigating the impact of adversarial attacks in very deep networks. Applied Soft Computing Journal, 2021, 105, 107231.	4.1	3
93	A threat intelligence framework for protecting smart satellite-based healthcare networks. Neural Computing and Applications, 2024, 36, 15-35.	3.2	3
94	H2HI-Net: A Dual-Branch Network for Recognizing Human-to-Human Interactions From Channel-State Information. IEEE Internet of Things Journal, 2022, 9, 10010-10021.	5.5	3
95	Deep Learning Techniques for IoT Security and Privacy. Studies in Computational Intelligence, 2022, , .	0.7	3
96	Privacy-Encoding Models for Preserving Utility of Machine Learning Algorithms in Social Media. , 2020, , .		2
97	Oneâ€class tensor machine with randomized projection for largeâ€scale anomaly detection in highâ€dimensional and noisy data. International Journal of Intelligent Systems, 2022, 37, 4515-4536.	3.3	2
98	Rethinking maximum-margin softmax for adversarial robustness. Computers and Security, 2022, 116, 102640.	4.0	2
99	Federated Learning for Privacy-Preserving Internet of Things. Studies in Computational Intelligence, 2022, , 215-228.	0.7	2
100	Internet of Things, Preliminaries and Foundations. Studies in Computational Intelligence, 2022, , 37-65.	0.7	2
101	A Risk Assessment Model for Cyber-Physical Water and Wastewater Systems: Towards Sustainable Development. Sustainability, 2022, 14, 4480.	1.6	2
102	Designing Anomaly Detection System for Cloud Servers by Frequency Domain Features of System Call Identifiers and Machine Learning. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, 2018, , 137-149.	0.2	1
103	Toward Privacy Preserving Federated Learning in Internet of Vehicular Things: Challenges and Future Directions. IEEE Consumer Electronics Magazine, 2022, 11, 56-66.	2.3	1
104	A Tri-level Programming Framework for Modelling Attacks and Defences in Cyber-Physical Systems. Lecture Notes in Computer Science, 2020, , 94-109.	1.0	1
105	Internet of Things Security Requirements, Threats, Attacks, and Countermeasures. Studies in Computational Intelligence, 2022, , 67-112.	0.7	1
106	Hunter in the Dark: Discover Anomalous Network Activity Using Deep Ensemble Network. , 2021, , .		1
107	DeepCog: A Trustworthy Deep Learning-Based Human Cognitive Privacy Framework in Industrial Policing. IEEE Transactions on Intelligent Transportation Systems, 2023, 24, 7485-7493.	4.7	1
108	A Deep Marginal-Contrastive Defense against Adversarial Attacks on 1D Models. , 2020, , .		0

#	Article	IF	Citations
109	Digital Forensics in Internet of Things. Studies in Computational Intelligence, 2022, , 113-130.	0.7	0
110	Introduction Conceptualization of Security, Forensics, and Privacy of Internet of Things: An Artificial Intelligence Perspective. Studies in Computational Intelligence, 2022, , 1-35.	0.7	0
111	CNA-TCC: Campaign Network Attribute Based Thematic Campaign Classification. IEEE Transactions on Computational Social Systems, 2024, , 1-13.	3.2	0