

Mohammad Sayad Haghghi

List of Publications by Year in descending order

Source: <https://exaly.com/author-pdf/7680414/publications.pdf>

Version: 2024-02-01

37
papers

1,067
citations

516215

16
h-index

454577

30
g-index

37
all docs

37
docs citations

37
times ranked

1091
citing authors

#	ARTICLE	IF	CITATIONS
1	Vulnerability Detection in IoT Applications: A Fuzzing Method on their Binaries. IEEE Transactions on Network Science and Engineering, 2022, 9, 970-979.	4.1	2
2	A Secure and Decentralized Trust Management Scheme for Smart Health Systems. IEEE Journal of Biomedical and Health Informatics, 2022, 26, 1961-1968.	3.9	17
3	Can Blockchain be Trusted in Industry 4.0? Study of a Novel Misleading Attack on Bitcoin. IEEE Transactions on Industrial Informatics, 2022, 18, 8307-8315.	7.2	6
4	Decentralized joint resource allocation and path selection in multi-hop integrated access backhaul 5G networks. Computer Networks, 2022, 207, 108837.	3.2	7
5	A Quantitative Comparative Study of Data-oriented Trust Management Schemes in Internet of Things. ACM Transactions on Management Information Systems, 2022, 13, 1-30.	2.1	6
6	High Bandwidth Green Communication With Vehicles by Decentralized Resource Optimization in Integrated Access Backhaul 5G Networks. IEEE Transactions on Green Communications and Networking, 2022, 6, 1438-1447.	3.5	5
7	Modeling of Human Cognition in Consensus Agreement on Social Media and Its Implications for Smarter Manufacturing. IEEE Transactions on Industrial Informatics, 2021, 17, 2902-2909.	7.2	3
8	Energy-Efficient Drone Trajectory Planning for the Localization of 6G-Enabled IoT Devices. IEEE Internet of Things Journal, 2021, 8, 5202-5210.	5.5	18
9	Automation of Recording in Smart Classrooms via Deep Learning and Bayesian Maximum a Posteriori Estimation of Instructor's Pose. IEEE Transactions on Industrial Informatics, 2021, 17, 2813-2820.	7.2	10
10	Detection of Anomalies in Industrial IoT Systems by Data Mining: Study of CHRIST Osmotron Water Purification System. IEEE Internet of Things Journal, 2021, 8, 10280-10287.	5.5	35
11	Anomaly Detection in Automated Vehicles Using Multistage Attention-Based Convolutional Neural Network. IEEE Transactions on Intelligent Transportation Systems, 2021, 22, 4291-4300.	4.7	111
12	Intelligent Trust-Based Public-Key Management for IoT by Linking Edge Devices in a Fog Architecture. IEEE Internet of Things Journal, 2021, 8, 12716-12723.	5.5	10
13	On the Possibility of Creating Smart Contracts on Bitcoin by MPC-based Approaches. , 2021, , .		0
14	Covert Attacks Through Adversarial Learning: Study of Lane Keeping Attacks on the Safety of Autonomous Vehicles. IEEE/ASME Transactions on Mechatronics, 2021, 26, 1350-1357.	3.7	21
15	On the Security of Networked Control Systems in Smart Vehicle and Its Adaptive Cruise Control. IEEE Transactions on Intelligent Transportation Systems, 2021, 22, 3824-3831.	4.7	28
16	Learning Influential Cognitive Links in Social Networks by a New Hybrid Model for Opinion Dynamics. IEEE Transactions on Computational Social Systems, 2021, 8, 1262-1271.	3.2	7
17	A Privacy-Preserving Homomorphic Scheme With Multiple Dimensions and Fault Tolerance for Metering Data Aggregation in Smart Grid. IEEE Transactions on Smart Grid, 2021, 12, 5212-5220.	6.2	39
18	Highly Anonymous Mobility-Tolerant Location-Based Onion Routing for VANETs. IEEE Internet of Things Journal, 2020, 7, 2582-2590.	5.5	35

#	ARTICLE	IF	CITATIONS
19	Artificial Intelligence for Detection, Estimation, and Compensation of Malicious Attacks in Nonlinear Cyber-Physical Systems and Industrial IoT. IEEE Transactions on Industrial Informatics, 2020, 16, 2716-2725.	7.2	189
20	Intelligent robust control for cyber-physical systems of rotary gantry type under denial of service attack. Journal of Supercomputing, 2020, 76, 3063-3085.	2.4	18
21	A Machine Learning-based Approach to Build Zero False-Positive IPSs for Industrial IoT and CPS with a Case Study on Power Grids Security. IEEE Transactions on Industry Applications, 2020, , 1-1.	3.3	10
22	An energy-aware drone trajectory planning scheme for terrestrial sensors localization. Computer Communications, 2020, 154, 542-550.	3.1	11
23	Discrimination-aware trust management for social internet of things. Computer Networks, 2020, 178, 107254.	3.2	41
24	Detection and Compensation of Covert Service-Degrading Intrusions in Cyber Physical Systems through Intelligent Adaptive Control. , 2019, , .		11
25	Legal framework for health cloud: A systematic review. International Journal of Medical Informatics, 2019, 132, 103953.	1.6	20
26	A mixed-integer linear programming approach for energy-constrained mobile anchor path planning in wireless sensor networks localization. Ad Hoc Networks, 2019, 87, 188-199.	3.4	14
27	Bayesian inference of private social network links using prior information and propagated data. Journal of Parallel and Distributed Computing, 2019, 125, 72-80.	2.7	8
28	A Novel Identity-Based Key Establishment Method for Advanced Metering Infrastructure in Smart Grid. IEEE Transactions on Smart Grid, 2018, 9, 2834-2842.	6.2	129
29	A conceptual trust model for the Internet of Things interactions. , 2016, , .		17
30	On the Race of Worms and Patches: Modeling the Spread of Information in Wireless Sensor Networks. IEEE Transactions on Information Forensics and Security, 2016, 11, 2854-2865.	4.5	52
31	Dynamic and verifiable multi- ϵ -secret sharing scheme based on Hermite interpolation and bilinear maps. IET Information Security, 2015, 9, 234-239.	1.1	18
32	A Sword with Two Edges: Propagation Studies on Both Positive and Negative Information in Online Social Networks. IEEE Transactions on Computers, 2015, 64, 640-653.	2.4	142
33	A Markov model of safety message broadcasting for vehicular networks. , 2013, , .		11
34	Analysis of packet loss for batch traffic arrivals in IEEE 802.15.4-based networks. , 2011, , .		1
35	Stochastic Modeling of Hello Flooding in Slotted CSMA/CA Wireless Sensor Networks. IEEE Transactions on Information Forensics and Security, 2011, 6, 1185-1199.	4.5	8
36	Overhearing Gain Analysis in Low-Traffic CDMA Wireless Sensor Networks. , 2010, , .		0

#	ARTICLE	IF	CITATIONS
37	Securing wireless sensor networks against broadcast attacks. , 2008, , .		7