

George Loukas

List of Publications by Citations

Source: <https://exaly.com/author-pdf/8884953/george-loukas-publications-by-citations.pdf>

Version: 2024-04-26

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.

57
papers

1,100
citations

18
h-index

32
g-index

61
ext. papers

1,450
ext. citations

3.6
avg, IF

5
L-index

#	Paper	IF	Citations
57	Cloud-Based Cyber-Physical Intrusion Detection for Vehicles Using Deep Learning. <i>IEEE Access</i> , 2018 , 6, 3491-3508	3.5	105
56	A self-aware approach to denial of service defence. <i>Computer Networks</i> , 2007 , 51, 1299-1314	5.4	101
55	Blockchain-Based Mobile Edge Computing Framework for Secure Therapy Applications. <i>IEEE Access</i> , 2018 , 6, 72469-72478	3.5	90
54	A Taxonomy of Attacks and a Survey of Defence Mechanisms for Semantic Social Engineering Attacks. <i>ACM Computing Surveys</i> , 2016 , 48, 1-39	13.4	65
53	Protection Against Denial of Service Attacks: A Survey. <i>Computer Journal</i> , 2010 , 53, 1020-1037	1.3	65
52	A survey of mathematical models, simulation approaches and testbeds used for research in cloud computing. <i>Simulation Modelling Practice and Theory</i> , 2013 , 39, 92-103	3.9	57
51	A taxonomy and survey of attacks against machine learning. <i>Computer Science Review</i> , 2019 , 34, 100199	8.3	51
50	A taxonomy and survey of cyber-physical intrusion detection approaches for vehicles. <i>Ad Hoc Networks</i> , 2019 , 84, 124-147	4.8	44
49	. <i>IEEE Access</i> , 2016 , 4, 6910-6928	3.5	42
48	A Denial of Service Detector based on Maximum Likelihood Detection and the Random Neural Network. <i>Computer Journal</i> , 2007 , 50, 717-727	1.3	40
47	A taxonomy of cyber-physical threats and impact in the smart home. <i>Computers and Security</i> , 2018 , 78, 398-428	4.9	38
46	Detecting semantic social engineering attacks with the weakest link: Implementation and empirical evaluation of a human-as-a-security-sensor framework. <i>Computers and Security</i> , 2018 , 76, 101-127	4.9	36
45	Detecting Denial of Service Attacks with Bayesian Classifiers and the Random Neural Network. <i>IEEE International Conference on Fuzzy Systems</i> , 2007 ,		28
44	Decision tree-based detection of denial of service and command injection attacks on robotic vehicles 2015 ,		26
43	A Review of Cyber Threats and Defence Approaches in Emergency Management. <i>Future Internet</i> , 2013 , 5, 205-236	3.3	23
42	2015 ,		21
41	2016 ,		21

40	Location-Enhanced Activity Recognition in Indoor Environments Using Off the Shelf Smart Watch Technology and BLE Beacons. <i>Sensors</i> , 2017 , 17,	3.8	18
39	Bluetooth Low Energy Based Occupancy Detection for Emergency Management 2016 ,		18
38	Physical-Cyber Attacks 2015 , 221-253		17
37	An autonomic approach to denial of service defence		17
36	Detecting Cyber-Physical Threats in an Autonomous Robotic Vehicle Using Bayesian Networks 2017 ,		14
35	Physical indicators of cyber attacks against a rescue robot 2014 ,		13
34	Computation offloading of a vehicle's continuous intrusion detection workload for energy efficiency and performance. <i>Simulation Modelling Practice and Theory</i> , 2017 , 73, 83-94	3.9	13
33	. <i>IEEE Transactions on Information Forensics and Security</i> , 2021 , 16, 1720-1735	8	13
32	A Secure Occupational Therapy Framework for Monitoring Cancer Patients' Quality of Life. <i>Sensors</i> , 2019 , 19,	3.8	12
31	Dynamic decision support for resource offloading in heterogeneous Internet of Things environments. <i>Simulation Modelling Practice and Theory</i> , 2020 , 101, 102019	3.9	11
30	. <i>IT Professional</i> , 2019 , 21, 18-25	1.9	10
29	Data-Driven Decision Support for Optimizing Cyber Forensic Investigations. <i>IEEE Transactions on Information Forensics and Security</i> , 2021 , 16, 2397-2412	8	10
28	Occupancy Detection for Building Emergency Management Using BLE Beacons. <i>Communications in Computer and Information Science</i> , 2016 , 233-240	0.3	9
27	An eye for deception: A case study in utilizing the human-as-a-security-sensor paradigm to detect zero-day semantic social engineering attacks 2017 ,		8
26	Defending networks against denial-of-service attacks 2004 ,		8
25	Assessing the cyber-trustworthiness of human-as-a-sensor reports from mobile devices 2017 ,		5
24	Evaluating the reliability of users as human sensors of social media security threats 2016 ,		5
23	Activity Recognition in a Home Setting Using Off the Shelf Smart Watch Technology 2016 ,		5

22	Blockchain and IoT-based Secure Multimedia Retrieval System for a Massive Crowd 2019 ,		4
21	A taxonomy of cyber attack and defence mechanisms for emergency management networks 2013 ,		4
20	A Prototype Framework for Assessing Information Provenance in Decentralised Social Media: The EUNOMIA Concept. <i>Communications in Computer and Information Science</i> , 2020 , 196-208	0.3	3
19	Facilitating forensic examinations of multi-user computer environments through session-to-session analysis of Internet history. <i>Digital Investigation</i> , 2016 , 16, S124-S133	3.3	3
18	On the Feasibility of Automated Semantic Attacks in the Cloud 2013 , 343-351		3
17	Spreading of computer viruses on time-varying networks. <i>Physical Review E</i> , 2019 , 99, 050303	2.4	2
16	. <i>IEEE Access</i> , 2019 , 7, 50658-50668	3.5	2
15	Digital Deception: Cyber Fraud and Online Misinformation. <i>IT Professional</i> , 2020 , 22, 19-20	1.9	2
14	Impact evaluation and detection of malicious spoofing attacks on BLE based occupancy detection systems 2017 ,		2
13	Evaluating the impact of malicious spoofing attacks on Bluetooth low energy based occupancy detection systems 2017 ,		2
12	Connecting trapped civilians to a wireless ad hoc network of emergency response robots 2008 ,		2
11	Optimizing Investments in Cyber Hygiene for Protecting Healthcare Users. <i>Lecture Notes in Computer Science</i> , 2020 , 268-291	0.9	2
10	Protection Against Semantic Social Engineering Attacks. <i>Advances in Information Security</i> , 2018 , 99-140	0.7	2
9	Transformer-based identification of stochastic information cascades in social networks using text and image similarity. <i>Applied Soft Computing Journal</i> , 2021 , 108, 107413	7.5	2
8	On the successful deployment of community policing services the TRILLION project case 2018 ,		1
7	Strengthening the security of cognitive packet networks. <i>International Journal of Advanced Intelligence Paradigms</i> , 2014 , 6, 14	0.5	1
6	How Secure is Home: Assessing Human Susceptibility to IoT Threats 2020 ,		1
5	A Prototype Deep Learning Paraphrase Identification Service for Discovering Information Cascades in Social Networks 2020 ,		1

4	Emotional Reactions to Cybersecurity Breach Situations: Scenario-Based Survey Study. <i>Journal of Medical Internet Research</i> , 2021 , 23, e24879	7.6	1
3	On-the-fly Privacy for Location Histograms. <i>IEEE Transactions on Dependable and Secure Computing</i> , 2020 , 1-1	3.9	0
2	Post quantum proxy signature scheme based on the multivariate public key cryptographic signature. <i>International Journal of Distributed Sensor Networks</i> , 2020 , 16, 155014772091477	1.7	0
1	Information Hygiene: The Fight Against the Misinformation Infodemic <i>IT Professional</i> , 2022 , 24, 16-18	1.9	