George Loukas

List of Publications by Year
in descending order

Source: https://exaly.com/author-pdf/8884953/publications.pdf

Version: 2024-02-01

		393982	344852
59 papers	1,835 citations	19 h-index	36 g-index

61 all docs	61 docs citations	61 times ranked	1655 citing authors

#	Article	IF	Citations
1	Cloud-Based Cyber-Physical Intrusion Detection for Vehicles Using Deep Learning. IEEE Access, 2018, 6, 3491-3508.	2.6	183
2	A taxonomy and survey of attacks against machine learning. Computer Science Review, 2019, 34, 100199.	10.2	139
3	A self-aware approach to denial of service defence. Computer Networks, 2007, 51, 1299-1314.	3.2	137
4	Blockchain-Based Mobile Edge Computing Framework for Secure Therapy Applications. IEEE Access, 2018, 6, 72469-72478.	2.6	129
5	A Taxonomy of Attacks and a Survey of Defence Mechanisms for Semantic Social Engineering Attacks. ACM Computing Surveys, 2016, 48, 1-39.	16.1	109
6	Protection Against Denial of Service Attacks: A Survey. Computer Journal, 2010, 53, 1020-1037.	1.5	90
7	A survey of mathematical models, simulation approaches and testbeds used for research in cloud computing. Simulation Modelling Practice and Theory, 2013, 39, 92-103.	2.2	84
8	A taxonomy and survey of cyber-physical intrusion detection approaches for vehicles. Ad Hoc Networks, 2019, 84, 124-147.	3.4	81
9	A taxonomy of cyber-physical threats and impact in the smart home. Computers and Security, 2018, 78, 398-428.	4.0	70
10	Detecting semantic social engineering attacks with the weakest link: Implementation and empirical evaluation of a human-as-a-security-sensor framework. Computers and Security, 2018, 76, 101-127.	4.0	55
11	You Are Probably Not the Weakest Link: Towards Practical Prediction of Susceptibility to Semantic Social Engineering Attacks. IEEE Access, 2016, 4, 6910-6928.	2.6	54
12	Bluetooth Low Energy Based Occupancy Detection for Emergency Management. , 2016, , .		52
13	Self-Configurable Cyber-Physical Intrusion Detection for Smart Homes Using Reinforcement Learning. IEEE Transactions on Information Forensics and Security, 2021, 16, 1720-1735.	4.5	50
14	A Denial of Service Detector based on Maximum Likelihood Detection and the Random Neural Network. Computer Journal, 2007, 50, 717-727.	1.5	46
15	Decision tree-based detection of denial of service and command injection attacks on robotic vehicles. , 2015, , .		42
16	Detecting Denial of Service Attacks with Bayesian Classifiers and the Random Neural Network. IEEE International Conference on Fuzzy Systems, 2007, , .	0.0	37
17	A Review of Cyber Threats and Defence Approaches in Emergency Management. Future Internet, 2013, 5, 205-236.	2.4	30
18	Performance Evaluation of Cyber-Physical Intrusion Detection on a Robotic Vehicle. , 2015, , .		30

#	Article	IF	Citations
19	Behaviour-Based Anomaly Detection of Cyber-Physical Attacks on a Robotic Vehicle. , 2016, , .		29
20	Location-Enhanced Activity Recognition in Indoor Environments Using Off the Shelf Smart Watch Technology and BLE Beacons. Sensors, 2017, 17, 1230.	2.1	29
21	Physical-Cyber Attacks. , 2015, , 221-253.		28
22	An Autonomic Approach to Denial of Service Defence. , 0, , .		27
23	Data-Driven Decision Support for Optimizing Cyber Forensic Investigations. IEEE Transactions on Information Forensics and Security, 2021, 16, 2397-2412.	4.5	26
24	Computation offloading of a vehicleâ€™s continuous intrusion detection workload for energy efficiency and performance. Simulation Modelling Practice and Theory, 2017, 73, 83-94.	2.2	24
25	Detecting Cyber-Physical Threats in an Autonomous Robotic Vehicle Using Bayesian Networks. , 2017, , .		22
26	Dynamic decision support for resource offloading in heterogeneous Internet of Things environments. Simulation Modelling Practice and Theory, 2020, 101, 102019.	2.2	21
27	A Secure Occupational Therapy Framework for Monitoring Cancer Patientsâ€™ Quality of Life. Sensors, 2019, 19, 5258.	2.1	19
28	Physical indicators of cyber attacks against a rescue robot. , 2014, , .		17
29	Defending networks against denial-of-service attacks. , 2004, , .		14
30	Toward a Blockchain-Enabled Crowdsourcing Platform. IT Professional, 2019, 21, 18-25.	1.4	12
31	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, , .		10
32	A taxonomy of cyber attack and defence mechanisms for emergency management networks. , 2013, , .		8
33	Evaluating the reliability of users as human sensors of social media security threats. , 2016, , .		8
34	Game-Theoretic Decision Support for Cyber Forensic Investigations. Sensors, 2021, 21, 5300.	2.1	8
35	Facilitating forensic examinations of multi-user computer environments through session-to-session analysis of Internet history. Digital Investigation, 2016, 16, S124-S133.	3.2	7
36	Emotional Reactions to Cybersecurity Breach Situations: Scenario-Based Survey Study. Journal of Medical Internet Research, 2021, 23, e24879.	2.1	7

#	Article	IF	Citations
37	Activity Recognition in a Home Setting Using Off the Shelf Smart Watch Technology. , 2016, , .		6
38	Assessing the cyber-trustworthiness of human-as-a-sensor reports from mobile devices. , 2017, , .		6
39	Blockchain and IoT-based Secure Multimedia Retrieval System for a Massive Crowd. , 2019, , .		6
40	Transformer-based identification of stochastic information cascades in social networks using text and image similarity. Applied Soft Computing Journal, 2021, 108, 107413.	4.1	6
41	Spreading of computer viruses on time-varying networks. Physical Review E, 2019, 99, 050303.	0.8	5
42	Digital Deception: Cyber Fraud and Online Misinformation. IT Professional, 2020, 22, 19-20.	1.4	5
43	A Prototype Framework for Assessing Information Provenance in Decentralised Social Media: The EUNOMIA Concept. Communications in Computer and Information Science, 2020, , 196-208.	0.4	5
44	Optimizing Investments in Cyber Hygiene for Protecting Healthcare Users. Lecture Notes in Computer Science, 2020, , 268-291.	1.0	5
45	On-the-Fly Privacy for Location Histograms. IEEE Transactions on Dependable and Secure Computing, 2022, 19, 566-578.	3.7	4
46	Post quantum proxy signature scheme based on the multivariate public key cryptographic signature. International Journal of Distributed Sensor Networks, 2020, 16, 155014772091477.	1.3	4
47	Connecting trapped civilians to a wireless ad hoc network of emergency response robots. , 2008, , .		3
48	Evaluating the impact of malicious spoofing attacks on Bluetooth low energy based occupancy detection systems. , 2017, , .		3
49	Protection Against Semantic Social Engineering Attacks. Advances in Information Security, 2018, , 99-140.	0.9	3
50	A Prototype Deep Learning Paraphrase Identification Service for Discovering Information Cascades in Social Networks. , 2020, , .		3
51	On the Feasibility of Automated Semantic Attacks in the Cloud. , 2013, , 343-351.		3
52	How Secure is Home: Assessing Human Susceptibility to IoT Threats. , 2020, , .		3
53	Strengthening the security of cognitive packet networks. International Journal of Advanced Intelligence Paradigms, 2014, 6, 14.	0.2	2
54	Impact evaluation and detection of malicious spoofing attacks on BLE based occupancy detection systems. , 2017, , .		2

#	Article	IF	Citations
55	On the successful deployment of community policing services the TRILLION project case. , 2018, , .		2
56	A New Encrypted Data Switching Protocol: Bridging IBE and ABE Without Loss of Data Confidentiality. IEEE Access, 2019, 7, 50658-50668.	2.6	2
57	Information Hygiene: The Fight Against the Misinformation â€œInfodemicâ€• IT Professional, 2022, 24, 16-18.	1.4	1
58	Towards Web Usage Attribution via Graph Community Detection in Grouped Internet Connection Records. , 2017, , .		0
59	Participatory location fingerprinting through stationary crowd in a public or commercial indoor environment. , 2019, , .		0