FÃ©lix GÃ³mez-MÃ¡rmol

List of Publications by Year
in descending order

Source: https://exaly.com/author-pdf/5470220/publications.pdf

Version: 2024-02-01

76 papers	1,896 citations	394286 19 h-index	302012 39 g-index
81 all docs	81 docs citations	81 times ranked	1649 citing authors

#	Article	IF	Citations
1	On the Power of Social Networks to Analyze Threatening Trends. IEEE Internet Computing, 2022, 26, 19-26.	3.2	4
2	Battling against cyberattacks: towards pre-standardization of countermeasures. Cluster Computing, 2021, 24, 57-81.	3.5	11
3	A Bio-Inspired Reaction Against Cyberattacks: AIS-Powered Optimal Countermeasures Selection. IEEE Access, 2021, 9, 60971-60996.	2.6	12
4	Detecting and mitigating cyberattacks using software defined networks for integrated clinical environments. Peer-to-Peer Networking and Applications, 2021, 14, 2719-2734.	2.6	5
5	COnVIDa: COVID-19 multidisciplinary data collection and dashboard. Journal of Biomedical Informatics, 2021, 117, 103760.	2.5	10
6	Nothing to Hide? On the Security and Privacy Threats Beyond Open Data. IEEE Internet Computing, 2021, 25, 58-66.	3.2	7
7	AISGA: Multi-objective parameters optimization for countermeasures selection through genetic algorithm. , 2021, , .		0
8	Cyberprotection in IoT environments: A dynamic rule-based solution to defend smart devices. Journal of Information Security and Applications, 2021, 60, 102878.	1.8	11
9	MalSEIRS: Forecasting Malware Spread Based on Compartmental Models in Epidemiology. Complexity, 2021, 2021, 1-19.	0.9	2
10	Uncovering Cybercrimes in Social Media through Natural Language Processing. Complexity, 2021, 2021, 1-15.	0.9	4
11	Twitter social bots: The 2019 Spanish general election data. Data in Brief, 2020, 32, 106047.	0.5	5
12	C3-Sex: A Conversational Agent to Detect Online Sex Offenders. Electronics (Switzerland), 2020, 9, 1779.	1.8	7
13	BlockSIEM: Protecting Smart City Services through a Blockchain-based and Distributed SIEM. Sensors, 2020, 20, 4636.	2.1	20
14	Spotting Political Social Bots in Twitter: A Use Case of the 2019 Spanish General Election. IEEE Transactions on Network and Service Management, 2020, 17, 2156-2170.	3.2	26
15	The Not Yet Exploited Goldmine of OSINT: Opportunities, Open Challenges and Future Trends. IEEE Access, 2020, 8, 10282-10304.	2.6	70
16	$$mathcal {B}$$ SIEM-IoT: A Blockchain-Based and Distributed SIEM for the Internet of Things. Lecture Notes in Computer Science, 2019, , 108-121.	1.0	1
17	Editorial: special issue on advances in security and privacy for future mobile communications. Electronic Commerce Research, 2019, 19, 471-475.	3.0	0
18	COSMOS: Collaborative, Seamless and Adaptive Sentinel for the Internet of Things. Sensors, 2019, 19, 1492.	2.1	12

#	Article	IF	Citations
19	PALOT: Profiling and Authenticating Users Leveraging Internet of Things. Sensors, 2019, 19, 2832.	2.1	13
20	Screening Out Social Bots Interference: Are There Any Silver Bullets?. IEEE Communications Magazine, 2019, 57, 98-104.	4.9	13
21	Introducing Deep Learning Self-Adaptive Misuse Network Intrusion Detection Systems. IEEE Access, 2019, 7, 13546-13560.	2.6	111
22	C3-Sex: a Chatbot to Chase Cyber Perverts. , 2019, , .		2
23	Optimal Countermeasures Selection Against Cyber Attacks: A Comprehensive Survey on Reaction Frameworks. IEEE Communications Surveys and Tutorials, 2018, 20, 1361-1396.	24.8	85
24	Dendron : Genetic trees driven rule induction for network intrusion detection systems. Future Generation Computer Systems, 2018, 79, 558-574.	4.9	82
25	Developing Secure IoT Services: A Security-Oriented Review of IoT Platforms. Symmetry, 2018, 10, 669.	1.1	15
26	A Dynamic Continuous Authentication Framework in IoT-Enabled Environments. , 2018, , .		9
27	TRIS: A Three-Rings IoT Sentinel to Protect Against Cyber-Threats. , 2018, , .		1
28	Shielding IoT against Cyber-Attacks: An Event-Based Approach Using SIEM. Wireless Communications and Mobile Computing, 2018, 2018, 1-18.	0.8	35
29	Security and Privacy in Wireless and Mobile Networks. Future Internet, 2018, 10, 18.	2.4	8
30	Shall I post this now? Optimized, delay-based privacy protection in social networks. Knowledge and Information Systems, 2017, 52, 113-145.	2.1	3
31	I Donâ€™t Trust ICT: Research Challenges in Cyber Security. IFIP Advances in Information and Communication Technology, 2016, , 129-136.	0.5	4
32	Dynamic counter-measures for risk-based access control systems: An evolutive approach. Future Generation Computer Systems, 2016, 55, 321-335.	4.9	29
33	Resolving privacy-preserving relationships over outsourced encrypted data storages. International Journal of Information Security, 2016, 15, 195-209.	2.3	4
34	Reputationâ€based Web service orchestration in cloud computing: A survey. Concurrency Computation Practice and Experience, 2015, 27, 2390-2412.	1.4	13
35	Chasing Offensive Conduct in Social Networks. ACM Transactions on Internet Technology, 2015, 15, 1-20.	3.0	6
36	Editorial: special issue on advances in security and privacy for future mobile communications. Electronic Commerce Research, 2015, 15, 73-74.	3.0	1

#	Article	IF	Citations
37	Improving attack detection in self-organizing networks: A trust-based approach toward alert satisfaction. , 2015, , .		2
38	Managing XACML systems in distributed environments through Meta-Policies. Computers and Security, 2015, 48, 92-115.	4.0	11
39	Towards privacy-preserving reputation management for hybrid broadcast broadband applications. Computers and Security, 2015, 49, 220-238.	4.0	4
40	Dynamic and flexible selection of a reputation mechanism for heterogeneous environments. Future Generation Computer Systems, 2015, 49, 113-124.	4.9	22
41	Identity Management in Cloud Systems. , 2014, , 177-210.		4
42	Editorial: Developments in Security and Privacy-Preserving Mechanisms for Future Mobile Communication Networks. Mobile Networks and Applications, 2014, 19, 61-63.	2.2	2
43	To Federate or Not To Federate: A Reputation-Based Mechanism to Dynamize Cooperation in Identity Management. Wireless Personal Communications, 2014, 75, 1769-1786.	1.8	8
44	Reporting Offensive Content in Social Networks: Toward a Reputation-Based Assessment Approach. IEEE Internet Computing, 2014, 18, 32-40.	3.2	20
45	Towards the integration of reputation management in OpenID. Computer Standards and Interfaces, 2014, 36, 438-453.	3.8	14
46	Editorial: Special issue on Identity Protection and Management. Journal of Information Security and Applications, 2014, 19, 1.	1.8	14
47	Introduction to the special issue on Recent advances in security and privacy in distributed communications (third edition). Computers and Electrical Engineering, 2014, 40, 1903-1905.	3.0	0
48	Smart AppStore: Expanding the Frontiers of Smartphone Ecosystems. Computer, 2014, 47, 42-47.	1.2	6
49	Building a reputation-based bootstrapping mechanism for newcomers in collaborative alert systems. Journal of Computer and System Sciences, 2014, 80, 571-590.	0.9	8
50	Live digital, remember digital: State of the art and research challenges. Computers and Electrical Engineering, 2014, 40, 109-120.	3.0	7
51	ROMEO: ReputatiOn Model Enhancing OpenID Simulator. Lecture Notes in Computer Science, 2014, , 193-197.	1.0	1
52	Introduction to advances in trust, security, and privacy for wireless networks. Eurasip Journal on Wireless Communications and Networking, 2013, 2013, .	1.5	1
53	RepCIDN: A Reputation-based Collaborative Intrusion Detection Network to Lessen the Impact of Malicious Alarms. Journal of Network and Systems Management, 2013, 21, 128-167.	3.3	27
54	WSANRep, WSAN Reputation-Based Selection in Open Environments. Wireless Personal Communications, 2013, 68, 921-937.	1.8	1

#	Article	IF	Citations
55	Privacy-enhanced architecture for smart metering. International Journal of Information Security, 2013, 12, 67-82.	2.3	22
56	Identity Management--In Privacy We Trust: Bridging the Trust Gap in eHealth Environments. IEEE Security and Privacy, 2013, 11, 34-41.	1.5	14
57	Towards Next Generation Hybrid Broadcast Broadband, Results from FP7 and HBBTV 2.0. , 2013, , .		6
58	Do not snoop my habits: preserving privacy in the smart grid. , 2012, 50, 166-172.		135
59	Graph-based XACML evaluation. , 2012, , .		23
60	LFTM, linguistic fuzzy trust mechanism for distributed networks. Concurrency Computation Practice and Experience, 2012, 24, 2007-2027.	1.4	13
61	TRIP, a trust and reputation infrastructure-based proposal for vehicular ad hoc networks. Journal of Network and Computer Applications, 2012, 35, 934-941.	5.8	240
62	Meta-Tacs: A Trust Model Demonstration Of Robustness Through A Genetic Algorithm. Intelligent Automation and Soft Computing, 2011, 17, 41-59.	1.6	13
63	Trust and reputation models comparison. Internet Research, 2011, 21, 138-153.	2.7	29
64	Providing trust in wireless sensor networks using aÂbio-inspiredÂtechnique. Telecommunication Systems, 2011, 46, 163-180.	1.6	121
65	Enhancing OpenID through a Reputation Framework. Lecture Notes in Computer Science, 2011, , 1-18.	1.0	1
66	Mobility in Collaborative Alert Systems: Building Trust through Reputation. Lecture Notes in Computer Science, 2011, , 251-262.	1.0	4
67	Towards pre-standardization of trust and reputation models for distributed and heterogeneous systems. Computer Standards and Interfaces, 2010, 32, 185-196.	3.8	117
68	TRIMS, a privacy-aware trust and reputation model for identity management systems. Computer Networks, 2010, 54, 2899-2912.	3.2	40
69	Linguistic Fuzzy Logic Enhancement of a Trust Mechanism for Distributed Networks. , 2010, , .		13
70	State of the Art in Trust and Reputation Models in P2P networks. , 2010, , 761-784.		11
71	TACS, a Trust Model for P2P Networks. Wireless Personal Communications, 2009, 51, 153-164.	1.8	36
72	Security threats scenarios in trust and reputation models for distributed systems. Computers and Security, 2009, 28, 545-556.	4.0	178

#	Article	IF	Citations
73	TRMSim-WSN, Trust and Reputation Models Simulator for Wireless Sensor Networks. , 2009, , .		67
74	Exploring the Affordances of Multimodal Data to Improve Cybersecurity Training with Cyber Range Environments. ColecciÃ³n Jornadas Y Congresos, 0, , .	0.0	3
75	A Review of Spotting political social bots in Twitter: A use case of the 2019 Spanish general election. ColecciÃ³n Jornadas Y Congresos, 0, , .	0.0	4
76	COBRA: Cibermaniobras adaptativas y personalizables de simulaciÃ³n hiperrealista de APTs y entrenamiento en ciberdefensa usando gamificaciÃ³n. ColecciÃ³n Jornadas Y Congresos, 0, , .	0.0	0