FÃ©lix GÃ³mez-MÃ¡rmol

List of Publications by Year
in descending order

76 papers	1,896 citations	394390 19 h-index	302107 39 g-index
81 all docs	81 docs citations	81 times ranked	1649 citing authors

#	Article	IF	Citations
1	TRIP, a trust and reputation infrastructure-based proposal for vehicular ad hoc networks. Journal of Network and Computer Applications, 2012, 35, 934-941.	9.1	240
2	Security threats scenarios in trust and reputation models for distributed systems. Computers and Security, 2009, 28, 545-556.	6.0	178
3	Do not snoop my habits: preserving privacy in the smart grid. , 2012, 50, 166-172.		135
4	Providing trust in wireless sensor networks using aÂbio-inspiredÂtechnique. Telecommunication Systems, 2011, 46, 163-180.	2.5	121
5	Towards pre-standardization of trust and reputation models for distributed and heterogeneous systems. Computer Standards and Interfaces, 2010, 32, 185-196.	5.4	117
6	Introducing Deep Learning Self-Adaptive Misuse Network Intrusion Detection Systems. IEEE Access, 2019, 7, 13546-13560.	4.2	111
7	Optimal Countermeasures Selection Against Cyber Attacks: A Comprehensive Survey on Reaction Frameworks. IEEE Communications Surveys and Tutorials, 2018, 20, 1361-1396.	39.4	85
8	Dendron : Genetic trees driven rule induction for network intrusion detection systems. Future Generation Computer Systems, 2018, 79, 558-574.	7.5	82
9	The Not Yet Exploited Goldmine of OSINT: Opportunities, Open Challenges and Future Trends. IEEE Access, 2020, 8, 10282-10304.	4.2	70
10	TRMSim-WSN, Trust and Reputation Models Simulator for Wireless Sensor Networks. , 2009, , .		67
11	TRIMS, a privacy-aware trust and reputation model for identity management systems. Computer Networks, 2010, 54, 2899-2912.	5.1	40
12	TACS, a Trust Model for P2P Networks. Wireless Personal Communications, 2009, 51, 153-164.	2.7	36
13	Shielding IoT against Cyber-Attacks: An Event-Based Approach Using SIEM. Wireless Communications and Mobile Computing, 2018, 2018, 1-18.	1.2	35
14	Trust and reputation models comparison. Internet Research, 2011, 21, 138-153.	4.9	29
15	Dynamic counter-measures for risk-based access control systems: An evolutive approach. Future Generation Computer Systems, 2016, 55, 321-335.	7.5	29
16	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.	4.9	27
17	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.	4.9	26
18	Graph-based XACML evaluation. , 2012, , .		23

#	Article	IF	Citations
19	Privacy-enhanced architecture for smart metering. International Journal of Information Security, 2013, 12, 67-82.	3.4	22
20	Dynamic and flexible selection of a reputation mechanism for heterogeneous environments. Future Generation Computer Systems, 2015, 49, 113-124.	7.5	22
21	Reporting Offensive Content in Social Networks: Toward a Reputation-Based Assessment Approach. IEEE Internet Computing, 2014, 18, 32-40.	3.3	20
22	BlockSIEM: Protecting Smart City Services through a Blockchain-based and Distributed SIEM. Sensors, 2020, 20, 4636.	3.8	20
23	Developing Secure IoT Services: A Security-Oriented Review of IoT Platforms. Symmetry, 2018, 10, 669.	2.2	15
24	Identity Management--In Privacy We Trust: Bridging the Trust Gap in eHealth Environments. IEEE Security and Privacy, 2013, 11, 34-41.	1.2	14
25	Towards the integration of reputation management in OpenID. Computer Standards and Interfaces, 2014, 36, 438-453.	5.4	14
26	Editorial: Special issue on Identity Protection and Management. Journal of Information Security and Applications, 2014, 19, 1.	2.5	14
27	Linguistic Fuzzy Logic Enhancement of a Trust Mechanism for Distributed Networks. , 2010, , .		13
28	Meta-Tacs: A Trust Model Demonstration Of Robustness Through A Genetic Algorithm. Intelligent Automation and Soft Computing, 2011, 17, 41-59.	2.1	13
29	LFTM, linguistic fuzzy trust mechanism for distributed networks. Concurrency Computation Practice and Experience, 2012, 24, 2007-2027.	2.2	13
30	Reputationâ€based Web service orchestration in cloud computing: A survey. Concurrency Computation Practice and Experience, 2015, 27, 2390-2412.	2.2	13
31	PALOT: Profiling and Authenticating Users Leveraging Internet of Things. Sensors, 2019, 19, 2832.	3.8	13
32	Screening Out Social Bots Interference: Are There Any Silver Bullets?. IEEE Communications Magazine, 2019, 57, 98-104.	6.1	13
33	COSMOS: Collaborative, Seamless and Adaptive Sentinel for the Internet of Things. Sensors, 2019, 19, 1492.	3.8	12
34	A Bio-Inspired Reaction Against Cyberattacks: AIS-Powered Optimal Countermeasures Selection. IEEE Access, 2021, 9, 60971-60996.	4.2	12
35	Managing XACML systems in distributed environments through Meta-Policies. Computers and Security, 2015, 48, 92-115.	6.0	11
36	Battling against cyberattacks: towards pre-standardization of countermeasures. Cluster Computing, 2021, 24, 57-81.	5.0	11

#	Article	IF	Citations
37	Cyberprotection in IoT environments: A dynamic rule-based solution to defend smart devices. Journal of Information Security and Applications, 2021, 60, 102878.	2.5	11
38	State of the Art in Trust and Reputation Models in P2P networks. , 2010, , 761-784.		11
39	COnVIDa: COVID-19 multidisciplinary data collection and dashboard. Journal of Biomedical Informatics, 2021, 117, 103760.	4.3	10
40	A Dynamic Continuous Authentication Framework in IoT-Enabled Environments. , 2018, , .		9
41	To Federate or Not To Federate: A Reputation-Based Mechanism to Dynamize Cooperation in Identity Management. Wireless Personal Communications, 2014, 75, 1769-1786.	2.7	8
42	Building a reputation-based bootstrapping mechanism for newcomers in collaborative alert systems. Journal of Computer and System Sciences, 2014, 80, 571-590.	1.2	8
43	Security and Privacy in Wireless and Mobile Networks. Future Internet, 2018, 10, 18.	3.8	8
44	Live digital, remember digital: State of the art and research challenges. Computers and Electrical Engineering, 2014, 40, 109-120.	4.8	7
45	C3-Sex: A Conversational Agent to Detect Online Sex Offenders. Electronics (Switzerland), 2020, 9, 1779.	3.1	7
46	Nothing to Hide? On the Security and Privacy Threats Beyond Open Data. IEEE Internet Computing, 2021, 25, 58-66.	3.3	7
47	Smart AppStore: Expanding the Frontiers of Smartphone Ecosystems. Computer, 2014, 47, 42-47.	1.1	6
48	Chasing Offensive Conduct in Social Networks. ACM Transactions on Internet Technology, 2015, 15, 1-20.	4.4	6
49	Towards Next Generation Hybrid Broadcast Broadband, Results from FP7 and HBBTV 2.0. , 2013, , .		6
50	Twitter social bots: The 2019 Spanish general election data. Data in Brief, 2020, 32, 106047.	1.0	5
51	Detecting and mitigating cyberattacks using software defined networks for integrated clinical environments. Peer-to-Peer Networking and Applications, 2021, 14, 2719-2734.	3.9	5
52	Mobility in Collaborative Alert Systems: Building Trust through Reputation. Lecture Notes in Computer Science, 2011, , 251-262.	1.3	4
53	Identity Management in Cloud Systems. , 2014, , 177-210.		4
54	Towards privacy-preserving reputation management for hybrid broadcast broadband applications. Computers and Security, 2015, 49, 220-238.	6.0	4

#	Article	IF	Citations
55	I Donâ€™t Trust ICT: Research Challenges in Cyber Security. IFIP Advances in Information and Communication Technology, 2016, , 129-136.	0.7	4
56	Resolving privacy-preserving relationships over outsourced encrypted data storages. International Journal of Information Security, 2016, 15, 195-209.	3.4	4
57	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
58	On the Power of Social Networks to Analyze Threatening Trends. IEEE Internet Computing, 2022, 26, 19-26.	3.3	4
59	Uncovering Cybercrimes in Social Media through Natural Language Processing. Complexity, 2021, 2021, 1-15.	1.6	4
60	Shall I post this now? Optimized, delay-based privacy protection in social networks. Knowledge and Information Systems, 2017, 52, 113-145.	3.2	3
61	Exploring the Affordances of Multimodal Data to Improve Cybersecurity Training with Cyber Range Environments. ColecciÃ³n Jornadas Y Congresos, 0, , .	0.0	3
62	Editorial: Developments in Security and Privacy-Preserving Mechanisms for Future Mobile Communication Networks. Mobile Networks and Applications, 2014, 19, 61-63.	3.3	2
63	Improving attack detection in self-organizing networks: A trust-based approach toward alert satisfaction. , 2015, , .		2
64	C3-Sex: a Chatbot to Chase Cyber Perverts. , 2019, , .		2
65	MalSEIRS: Forecasting Malware Spread Based on Compartmental Models in Epidemiology. Complexity, 2021, 2021, 1-19.	1.6	2
66	Enhancing OpenID through a Reputation Framework. Lecture Notes in Computer Science, 2011, , 1-18.	1.3	1
67	Introduction to advances in trust, security, and privacy for wireless networks. Eurasip Journal on Wireless Communications and Networking, 2013, 2013, .	2.4	1
68	WSANRep, WSAN Reputation-Based Selection in Open Environments. Wireless Personal Communications, 2013, 68, 921-937.	2.7	1
69	Editorial: special issue on advances in security and privacy for future mobile communications. Electronic Commerce Research, 2015, 15, 73-74.	5.0	1
70	TRIS: A Three-Rings IoT Sentinel to Protect Against Cyber-Threats. , 2018, , .		1
71	$$mathcal {B}$$ SIEM-IoT: A Blockchain-Based and Distributed SIEM for the Internet of Things. Lecture Notes in Computer Science, 2019, , 108-121.	1.3	1
72	ROMEO: ReputatiOn Model Enhancing OpenID Simulator. Lecture Notes in Computer Science, 2014, , 193-197.	1.3	1

#	Article	IF	Citations
73	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.	4.8	0
74	Editorial: special issue on advances in security and privacy for future mobile communications. Electronic Commerce Research, 2019, 19, 471-475.	5.0	0
75	AISGA: Multi-objective parameters optimization for countermeasures selection through genetic algorithm. , 2021, , .		0
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