Georgios Theodorakopoulos

List of Publications by Year
in descending order

Source: https://exaly.com/author-pdf/8474683/publications.pdf

Version: 2024-02-01

42 papers	1,949 citations	1039880 9 h-index	752573 20 g-index
43 all docs	43 docs citations	43 times ranked	1491 citing authors

#	Article	IF	Citations
1	On-the-Fly Privacy for Location Histograms. IEEE Transactions on Dependable and Secure Computing, 2022, 19, 566-578.	3.7	4
2	Joint obfuscation of location and its semantic information for privacy protection. Computers and Security, 2021, 107, 102310.	4.0	9
3	Location histogram privacy by Sensitive Location Hiding and Target Histogram Avoidance/Resemblance. Knowledge and Information Systems, 2020, 62, 2613-2651.	2.1	0
4	BLATTA: Early Exploit Detection on Network Traffic with Recurrent Neural Networks. Security and Communication Networks, 2020, 2020, 1-15.	1.0	6
5	Password Managersâ€"Itâ€™s All about Trust and Transparency. Future Internet, 2020, 12, 189.	2.4	6
6	A flexible <i>n</i>/2 adversary node resistant and halting recoverable blockchain sharding protocol. Concurrency Computation Practice and Experience, 2020, 32, e5773.	1.4	3
7	GDPR Compliance Verification in Internet of Things. IEEE Access, 2020, 8, 119697-119709.	2.6	30
8	Joint Obfuscation for Privacy Protection in Location-Based Social Networks. Lecture Notes in Computer Science, 2020, , 111-127.	1.0	0
9	Automating GDPR Compliance Verification for Cloud-hosted Services. , 2020, , .		1
10	Detecting IoT User Behavior and Sensitive Information in Encrypted IoT-App Traffic. Sensors, 2019, 19, 4777.	2.1	23
11	Privacy-Aware Cloud Ecosystems and GDPR Compliance. , 2019, , .		12
12	Secure Data Sharing and Analysis in Cloud-Based Energy Management Systems. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, 2018, , 228-242.	0.2	6
13	Unsupervised Approach for Detecting Low Rate Attacks on Network Traffic with Autoencoder. , 2018, , .		15
14	Ensuring Compliance of IoT Devices with Their Privacy Policy Agreement. , 2018, , .		18
15	EclipseIoT: A secure and adaptive hub for the Internet of Things. Computers and Security, 2018, 78, 477-490.	4.0	24
16	An open framework for flexible plug-in privacy mechanisms in crowdsensing applications. , 2017, , .		1
17	Privacy Games Along Location Traces. ACM Transactions on Privacy and Security, 2017, 19, 1-31.	2.2	45
18	Private and Secure Distribution of Targeted Advertisements to Mobile Phones. Future Internet, 2017, 9, 16.	2.4	2

#	Article	IF	Citations
19	Behavioural Verification: Preventing Report Fraud in Decentralized Advert Distribution Systems. Future Internet, 2017, 9, 88.	2.4	5
20	On the Inference of User Paths from Anonymized Mobility Data. , 2016, , .		8
21	The Same-Origin Attack against Location Privacy. , 2015, , .		10
22	Prolonging the Hide-and-Seek Game. , 2014, , .		49
23	Cognitive Structure of Collective Awareness Platforms. , 2014, , .		10
24	A BROKER BASED CONSUMPTION MECHANISM FOR SOCIAL CLOUDS. Services Transactions on Cloud Computing, 2014, 2, 31-43.	0.1	1
25	Broker Emergence in Social Clouds. , 2013, , .		4
26	Selfish Response to Epidemic Propagation. IEEE Transactions on Automatic Control, 2013, 58, 363-376.	3.6	36
27	Protecting location privacy. , 2012, , .		263
28	Traps and pitfalls of using contact traces in performance studies of opportunistic networks. , 2012, , .		23
29	Collaborative Location Privacy. , 2011, , .		32
30	Quantifying Location Privacy. , 2011, , .		462
31	Selfish response to epidemic propagation. , 2011, , .		3
32	Quantifying Location Privacy: The Case of Sporadic Location Exposure. Lecture Notes in Computer Science, 2011, , 57-76.	1.0	63
33	Path Problems in Networks. Synthesis Lectures on Communication Networks, 2010, 3, 1-77.	6.3	26
34	Preserving privacy in collaborative filtering through distributed aggregation of offline profiles. , 2009, , .		69
35	Adaptive message authentication for vehicular networks. , 2009, , .		5
36	Game Theoretic Modeling of Malicious Users in Collaborative Networks. IEEE Journal on Selected Areas in Communications, 2008, 26, 1317-1327.	9.7	63

#	Article	IF	Citations
37	Dynamic network security deployment under partial information. , 2008, , .		7
38	Intrusion Detection System Resiliency to Byzantine Attacks: The Case Study of Wormholes in OLSR. , 2007, , .		19
39	Enhancing Benign User Cooperation in the Presence of Malicious Adversaries in Ad Hoc Networks. , 2006, , .		3
40	NIS02-6: A Game for Ad Hoc Network Connectivity in the Presence of Malicious Users. IEEE Global Telecommunications Conference (GLOBECOM), 2006, , .	0.0	2
41	On trust models and trust evaluation metrics for ad hoc networks. IEEE Journal on Selected Areas in Communications, 2006, 24, 318-328.	9.7	403
42	Trust evaluation in ad-hoc networks. , 2004, , .		175