Qi Shi

List of Publications by Year
in descending order

Source: https://exaly.com/author-pdf/4199395/publications.pdf

Version: 2024-02-01

87 papers	2,208 citations	643344 15 h-index	286692 43 g-index
89 all docs	89 docs citations	89 times ranked	2523 citing authors

#	Article	IF	Citations
1	SC-TRUST: A Dynamic Model for Trustworthy Service Composition in the Internet of Things. IEEE Internet of Things Journal, 2022, 9, 3298-3312.	5.5	11
2	A Centralized Win-Win Cooperative Framework for Wi-Fi and 5G Radio Access Networks. Wireless Communications and Mobile Computing, 2021, 2021, 1-11.	0.8	2
3	Per-Flow Radio Resource Management to Mitigate Interference in Dense IEEE 802.11 Wireless LANs. IEEE Transactions on Mobile Computing, 2020, 19, 1170-1183.	3.9	9
4	The Internet of Things: Challenges and Considerations for Cybercrime Investigations and Digital Forensics. International Journal of Digital Crime and Forensics, 2020, 12, 1-13.	0.5	11
5	Strengthen user authentication on mobile devices by using userâ€™s touch dynamics pattern. Journal of Ambient Intelligence and Humanized Computing, 2020, 11, 4019-4039.	3.3	24
6	A dynamic access point allocation algorithm for dense wireless LANs using potential game. Computer Networks, 2020, 167, 106991.	3.2	15
7	Efficient Non-Linear Covert Channel Detection in TCP Data Streams. IEEE Access, 2020, 8, 1680-1690.	2.6	8
8	Deep COLA: A Deep COmpetitive Learning Algorithm for Future Home Energy Management Systems. IEEE Transactions on Emerging Topics in Computational Intelligence, 2020, , 1-11.	3.4	2
9	Intrusion Detection Using Extremely Limited Data Based on SDN. , 2020, , .		4
10	A GPS-Less Localization and Mobility Modelling (LMM) System for Wildlife Tracking. IEEE Access, 2020, 8, 102709-102732.	2.6	15
11	Adjusted Location Privacy Scheme for VANET Safety Applications. , 2020, , .		4
12	Realizing Physical Layer Security in Large Wireless Networks using Spectrum Programmability. , 2020, , .		3
13	Machine Learning Based Trust Computational Model for IoT Services. IEEE Transactions on Sustainable Computing, 2019, 4, 39-52.	2.2	147
14	Securing Things in the Healthcare Internet of Things. , 2019, , .		15
15	Radio resource management framework for energyâ€efficient communications in the Internet of Things. Transactions on Emerging Telecommunications Technologies, 2019, 30, e3766.	2.6	5
16	Survey on Revocation in Ciphertext-Policy Attribute-Based Encryption. Sensors, 2019, 19, 1695.	2.1	46
17	Toward secure trading of unlicensed spectrum in cyber-physical systems. , 2019, , .		7
18	CTRUST: A Dynamic Trust Model for Collaborative Applications in the Internet of Things. IEEE Internet of Things Journal, 2019, 6, 5432-5445.	5.5	72

#	Article	IF	Citations
19	Behaviour-aware Malware Classification: Dynamic Feature Selection. , 2019, , .		6
20	A Fresh Look at Combining Logs and Network Data to Detect Anomalous Activity. , 2019, , .		2
21	Efficient, Secure, and Privacy-Preserving PMIPv6 Protocol for V2G Networks. IEEE Transactions on Vehicular Technology, 2019, 68, 19-33.	3.9	20
22	Iot Forensics: Challenges for the Ioa Era. , 2018, , .		56
23	A Deep Learning Approach to Network Intrusion Detection. IEEE Transactions on Emerging Topics in Computational Intelligence, 2018, 2, 41-50.	3.4	944
24	A Novel Physical Layer Secure Key Generation and Refreshment Scheme for Wireless Sensor Networks. IEEE Access, 2018, 6, 11374-11387.	2.6	51
25	Measuring web service security in the era of Internet of Things. Computers and Electrical Engineering, 2018, 66, 305-315.	3.0	7
26	Access Privilege Elevation and Revocation in Collusion-Resistant Cloud Access Control. , 2018, , .		1
27	Revocable, Decentralized Multi-Authority Access Control System. , 2018, , .		2
28	Wi-5: A Programming Architecture for Unlicensed Frequency Bands. IEEE Communications Magazine, 2018, 56, 178-185.	4.9	20
29	A low-power and high-speed True Random Number Generator using generated RTN. , 2018, , .		22
30	A 3-D Security Modeling Platform for Social IoT Environments. IEEE Transactions on Computational Social Systems, 2018, 5, 1174-1188.	3.2	11
31	Security policy monitoring of BPMNâ€based service compositions. Journal of Software: Evolution and Process, 2018, 30, e1944.	1.2	16
32	AP selection algorithm based on a potential game for large IEEE 802.11 WLANs. , 2018, , .		9
33	Quality of Service Oriented Access Point Selection Framework for Large Wi-Fi Networks. IEEE Transactions on Network and Service Management, 2017, 14, 441-455.	3.2	42
34	Fine-Grained Radio Resource Management to Control Interference in Dense Wi-Fi Networks. , 2017, , .		12
35	Modelling, validating, and ranking of secure service compositions. Software - Practice and Experience, 2017, 47, 1923-1943.	2.5	8
36	Intrusion Prediction Systems. Studies in Computational Intelligence, 2017, , 155-174.	0.7	14

#	Article	IF	Citations
37	Towards a Framework for the Extension and Visualisation of Cyber Security Requirements in Modelling Languages. , 2017, , .		1
38	Deep learning combined with de-noising data for network intrusion detection. , 2017, , .		7
39	A Survey on Quantitative Evaluation of Web Service Security. , 2016, , .		6
40	A centralised Wi-Fi management framework for D2D communications in dense Wi-Fi networks. , 2016, , .		8
41	Adding a Third Dimension to BPMN as a Means of Representing Cyber Security Requirements. , 2016, , .		12
42	Secure and Privacy-Aware Cloud-Assisted Video Reporting Service in 5G-Enabled Vehicular Networks. IEEE Transactions on Vehicular Technology, 2016, 65, 7868-7881.	3.9	102
43	A System for Intrusion Prediction in Cloud Computing. , 2016, , .		6
44	SDN-based channel assignment algorithm for interference management in dense Wi-Fi networks. , 2016, , .		21
45	Secure and privacy-aware proxy mobile IPv6 protocol for vehicle-to-grid networks. , 2016, , .		6
46	A Selective Regression Testing Approach for Composite Web Services. , 2015, , .		0
47	Detecting Intrusions in Federated Cloud Environments Using Security as a Service. , 2015, , .		1
48	Digital Memories Based Mobile User Authentication for IoT. , 2015, , .		14
49	Fair signature exchange via delegation on ubiquitous networks. Journal of Computer and System Sciences, 2015, 81, 615-631.	0.9	6
50	Situation-Aware QoS Routing Algorithm for Vehicular Ad Hoc Networks. IEEE Transactions on Vehicular Technology, 2015, 64, 5520-5535.	3.9	79
51	Security Policy Monitoring of Composite Services. Lecture Notes in Computer Science, 2014, , 192-202.	1.0	1
52	The Aniketos Service Composition Framework. Lecture Notes in Computer Science, 2014, , 121-135.	1.0	2
53	Towards Efficient Collaborative Behavioural Monitoring in a System-of-Systems. , 2013, , .		0
54	Resource-efficient authentic key establishment in heterogeneous wireless sensor networks. Journal of Parallel and Distributed Computing, 2013, 73, 235-249.	2.7	11

#	ARTICLE	IF	CITATIONS
55	Component-based security system (COMSEC) with QoS for wireless sensor networks. Security and Communication Networks, 2013, 6, 461-472.	1.0	9
56	Prototype for design-time secure and trustworthy service composition. , 2013, , .		1
57	Event Driven Monitoring of Composite Services. , 2013, , .		6
58	Efficient autonomous signature exchange on ubiquitous networks. Journal of Network and Computer Applications, 2012, 35, 1793-1806.	5.8	4
59	Pypette. International Journal of Digital Crime and Forensics, 2012, 4, 31-46.	0.5	2
60	Identity management in System-of-Systems Crisis Management situation. , 2011, , .		4
61	Achieving autonomous fair exchange in ubiquitous network settings. Journal of Network and Computer Applications, 2011, 34, 653-667.	5.8	4
62	Fair exchange of valuable information: A generalised framework. Journal of Computer and System Sciences, 2011, 77, 348-371.	0.9	7
63	ContextRank. , 2011, , 275-297.		1
64	Data Mishandling and Profile Building in Ubiquitous Environments. , 2010, , .		5
65	System-of-systems boundary check in a public event scenario. , 2010, , .		12
66	A Novel Intrusion Detection System for Smart Space. Advances in Digital Crime, Forensics, and Cyber Terrorism, 2010, , 307-333.	0.4	0
67	Balancing intrusion detection resources in ubiquitous computing networks. Computer Communications, 2008, 31, 3643-3653.	3.1	8
68	Practical and efficient fair document exchange over networks. Journal of Network and Computer Applications, 2006, 29, 46-61.	5.8	13
69	Statistical Signatures for Early Detection of Flooding Denial-of-Service Attacks. IFIP Advances in Information and Communication Technology, 2005, , 327-341.	0.5	5
70	Efficient fair digital-signature exchange based on misbehaviour penalisation. IET Communications, 2005, 152, 257.	1.0	5
71	Revocation of privacy-enhanced public-key certificates. Journal of Systems and Software, 2005, 75, 205-214.	3.3	0
72	Buffer overrun prevention through component composition analysis. , 2005, , .		0

#	Article	IF	Citations
73	Early detection and prevention of denial-of-service attacks: a novel mechanism with propagated traced-back attack blocking. IEEE Journal on Selected Areas in Communications, 2005, 23, 1994-2002.	9.7	16
74	Autonomous mobile agent based fair exchange. Computer Networks, 2004, 46, 751-770.	3.2	5
75	A unified approach to a fair document exchange system. Journal of Systems and Software, 2004, 72, 83-96.	3.3	7
76	Signature-based approach to fair document exchange. IET Communications, 2003, 150, 21.	1.0	9
77	MNPA: A basis for privacy-enhanced QoS in mobile networks. Microprocessors and Microsystems, 2003, 27, 93-100.	1.8	0
78	An efficient protocol for anonymous and fair document exchange. Computer Networks, 2003, 41, 19-28.	3.2	15
79	MNPA: a mobile network privacy architecture. Computer Communications, 2000, 23, 1777-1788.	3.1	5
80	Anonymous public-key certificates for anonymous and fair document exchange. IET Communications, 2000, 147, 345.	1.0	15
81	An effective model for composition of secure systems. Journal of Systems and Software, 1998, 43, 233-244.	3.3	16
82	Achieving Non-repudiation of Receipt. Computer Journal, 1996, 39, 844-853.	1.5	43
83	Achieving user privacy in mobile networks. , 0, , .		23
84	Applying noninterference to composition of systems: a more practical approach. , 0, , .		6
85	Secure component composition for networked appliances. , 0, , .		6
86	A security framework for executables in a ubiquitous computing environment. , 0, , .		4
87	DiDDeM: a system for early detection of TCP SYN flood attacks. , 0, , .		21