Zubair A Baig

List of Publications by Year
in descending order

60 papers	2,077 citations	236925 25 h-index	276875 41 g-index
64 all docs	64 docs citations	64 times ranked	2042 citing authors

#	Article	IF	Citations
1	Zero Trust Architecture (ZTA): A Comprehensive Survey. IEEE Access, 2022, 10, 57143-57179.	4.2	40
2	Unsupervised Machine Learning for Drone Forensics through Flight Path Analysis. , 2022, , .		0
3	Securing the Smart City Airspace: Drone Cyber Attack Detection through Machine Learning. Future Internet, 2022, 14, 205.	3.8	8
4	Towards a deep learning-driven intrusion detection approach for Internet of Things. Computer Networks, 2021, 186, 107784.	5.1	87
5	ICME: an informed consent management engine for conformance in smart building environments. , 2021, , .		2
6	Averaged dependence estimators for DoS attack detection in IoT networks. Future Generation Computer Systems, 2020, 102, 198-209.	7.5	73
7	Machine learning and data analytics for the IoT. Neural Computing and Applications, 2020, 32, 16205-16233.	5.6	144
8	Denial of service attack detection through machine learning for the IoT. Journal of Information and Telecommunication, 2020, 4, 482-503.	2.8	44
9	Harnessing Artificial Intelligence Capabilities to Improve Cybersecurity. IEEE Access, 2020, 8, 23817-23837.	4.2	108
10	An informed consent model for managing the privacy paradox in smart buildings. , 2020, , .		9
11	Digital Forensics for Drones: A Study of Tools and Techniques. Communications in Computer and Information Science, 2020, , 29-41.	0.5	6
12	SeArch: A Collaborative and Intelligent NIDS Architecture for SDN-Based Cloud IoT Networks. IEEE Access, 2019, 7, 107678-107694.	4.2	87
13	Physical Layer Security for the Smart Grid: Vulnerabilities, Threats, and Countermeasures. IEEE Transactions on Industrial Informatics, 2019, 15, 6522-6530.	11.3	83
14	On Secure Wireless Sensor Networks With Cooperative Energy Harvesting Relaying. IEEE Access, 2019, 7, 139212-139225.	4.2	11
15	25 Years of Bluetooth Technology. Future Internet, 2019, 11, 194.	3.8	40
16	Editorial: Sustainable Mobile Networks and its Applications. Mobile Networks and Applications, 2019, 24, 295-297.	3.3	2
17	Smart healthcare. PSU Research Review, 2019, 4, 149-168.	2.4	75
18	Deep Learning-Based Intrusion Detection for IoT Networks. , 2019, , .		106

#	Article	IF	Citations
19	Healthcare Data Breaches: Implications for Digital Forensic Readiness. Journal of Medical Systems, 2019, 43, 7.	3.6	67
20	Digital Forensics for Drone Data â€" Intelligent Clustering Using Self Organising Maps. Communications in Computer and Information Science, 2019, , 172-189.	0.5	11
21	Internet of Things (IoT): Research, Simulators, and Testbeds. IEEE Internet of Things Journal, 2018, 5, 1637-1647.	8.7	194
22	Ransomware behavioural analysis on windows platforms. Journal of Information Security and Applications, 2018, 40, 44-51.	2.5	60
23	Performance Analysis of DF/AF Cooperative MISO Wireless Sensor Networks With NOMA and SWIPT Over Nakagami-<inline-formula> <tex-math notation="LaTeX">m </tex-math> </inline-formula> Fading. IEEE Access, 2018, 6, 56142-56161.	4.2	27
24	Preparing for Secure Wireless Medical Environment in 2050: A Vision. IEEE Access, 2018, 6, 25666-25674.	4.2	5
25	Secrecy Outage Performance Analysis for Energy Harvesting Sensor Networks With a Jammer Using Relay Selection Strategy. IEEE Access, 2018, 6, 23406-23419.	4.2	45
26	Internet of Things Forensics: The Need, Process Models, and Open Issues. IT Professional, 2018, 20, 40-49.	1.5	38
27	Stealthy Denial of Service (DoS) attack modelling and detection for HTTP/2 services. Journal of Network and Computer Applications, 2017, 91, 1-13.	9.1	31
28	Future challenges for smart cities: Cyber-security and digital forensics. Digital Investigation, 2017, 22, 3-13.	3.2	176
29	Modelling and Evaluation of Malicious Attacks against the IoT MQTT Protocol. , 2017, , .		53
30	Mobile Forensics: Advances, Challenges, and Research Opportunities. IEEE Security and Privacy, 2017, 15, 42-51.	1.2	31
31	Security Attacks and Solutions in Electronic Health (E-health) Systems. Journal of Medical Systems, 2016, 40, 263.	3.6	45
32	An Experimental Evaluation of the EDoS-Shield Mitigation Technique for Securing the Cloud. Arabian Journal for Science and Engineering, 2016, 41, 5037-5047.	1.1	11
33	Controlled Android Application Execution for the IoT Infrastructure. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, 2016, , 16-26.	0.3	0
34	Distributed denial-of-service attacks against HTTP/2 services. Cluster Computing, 2016, 19, 79-86.	5.0	22
35	Controlled access to cloud resources for mitigating Economic Denial of Sustainability (EDoS) attacks. Computer Networks, 2016, 97, 31-47.	5.1	40
36	Detection of compromised smart meters in the Advanced Metering Infrastructure. , 2015, , .		4

#	ARTICLE	IF	CITATIONS
37	Low-Rate Denial-of-Service Attacks against HTTP/2 Services. , 2015, , .		18
38	Real-Time QoS-Aware Video Streaming: A Comparative and Experimental Study. Advances in Multimedia, 2014, 2014, 1-11.	0.4	19
39	A Novel Mobility-Aware Data Transfer Service (MADTS) Based on DDS Standards. Arabian Journal for Science and Engineering, 2014, 39, 2843-2856.	1.1	1
40	Controlled Virtual Resource Access to Mitigate Economic Denial of Sustainability (EDoS) Attacks against Cloud Infrastructures. , 2013, , .		16
41	GMDH-based networks for intelligent intrusion detection. Engineering Applications of Artificial Intelligence, 2013, 26, 1731-1740.	8.1	41
42	An Analysis of Smart Grid Attacks and Countermeasures. Journal of Communications, 2013, 8, 473-479.	1.6	53
43	Rapid anomaly detection for smart grid infrastructures through hierarchical pattern matching. International Journal of Security and Networks, 2012, 7, 83.	0.2	10
44	Multi-agent systems for protecting critical infrastructures: A survey. Journal of Network and Computer Applications, 2012, 35, 1151-1161.	9.1	26
45	Videoâ€on†Demand (VoD) deployment over hospitality networks. International Journal of Network Management, 2012, 22, 65-80.	2.2	2
46	Abductive Neural Network Modeling for Hand Recognition Using Geometric Features. Lecture Notes in Computer Science, 2012, , 593-602.	1.3	5
47	A trust-based mechanism for protecting IPv6 networks against stateless address auto-configuration attacks. , 2011, , .		8
48	On the use of pattern matching for rapid anomaly detection in smart grid infrastructures. , 2011, , .		12
49	A selective parameter-based evolutionary technique for network intrusion detection. , 2011, , .		0
50	An AODE-based intrusion detection system for computer networks. , 2011, , .		6
51	Pattern recognition for detecting distributed node exhaustion attacks in wireless sensor networks. Computer Communications, 2011, 34, 468-484.	5.1	36
52	An Entropy and Volume-Based Approach for Identifying Malicious Activities in Honeynet Traffic. , 2011, , .		4
53	Discovering last-matching rules in popular open-source and commercial firewalls. International Journal of Internet Protocol Technology, 2010, 5, 23.	0.2	2
54	Multi-Agent pattern recognition mechanism for detecting distributed denial of service attacks. IET Information Security, 2010, 4, 333.	1.7	10

#	Article	IF	Citations
55	On the use of Unified And-Or fuzzy operator for distributed node exhaustion attack decision-making in wireless sensor networks. , 2010, , .		4
56	Resiliency of open-source firewalls against remote discovery of last-matching rules. , 2009, , .		2
57	A Fault-Tolerant Scheme for Detection of DDoS Attack Patterns in Cluster-Based Wireless Sensor Networks. Lecture Notes in Electrical Engineering, 2008, , 277-296.	0.4	4
58	A Simulated Evolution-Tabu search hybrid metaheuristic for routing in computer networks. , 2007, , .		3
59	SGSIA-in-Network Data Preprocessing for Secure Grid-Sensor Integration. , 2006, , .		2
60	Cyber-security risk assessment framework for critical infrastructures. Intelligent Automation and Soft Computing, 0, , -1--1.	2.1	5