Benjamin Peter Turnbull

List of Publications by Year
in descending order

48	2,146	706676 14	536525 29
papers	citations	h-index	g-index

50	50	50	1727
all docs	docs citations	times ranked	citing authors

#	Article	IF	Citations
1	A Blockchain-Enabled Explainable Federated Learning for Securing Internet-of-Things-Based Social Media 3.0 Networks. IEEE Transactions on Computational Social Systems, 2024, , 1-17.	3.2	17
2	CNA-TCC: Campaign Network Attribute Based Thematic Campaign Classification. IEEE Transactions on Computational Social Systems, 2024, , 1-13.	3.2	0
3	OQFL: An Optimized Quantum-Based Federated Learning Framework for Defending Against Adversarial Attacks in Intelligent Transportation Systems. IEEE Transactions on Intelligent Transportation Systems, 2023, 24, 893-903.	4.7	11
4	Privacy-preserving big data analytics for cyber-physical systems. Wireless Networks, 2022, 28, 1241-1249.	2.0	18
5	A Privacy-Preserving Biometric Authentication System With Binary Classification in a Zero Knowledge Proof Protocol. IEEE Open Journal of the Computer Society, 2022, 3, 1-10.	5.2	9
6	Social media influence, trust, and conflict: An interview based study of leadership perceptions. Technology in Society, 2022, 68, 101836.	4.8	8
7	Data analytics of social media 3.0: Privacy protection perspectives for integrating social media and Internet of Things (SM-IoT) systems. Ad Hoc Networks, 2022, 128, 102786.	3.4	16
8	Perturbation-enabled Deep Federated Learning for Preserving Internet of Things-based Social Networks. ACM Transactions on Multimedia Computing, Communications and Applications, 2022, 18, 1-19.	3.0	6
9	Privacy-Preserving Schemes for Safeguarding Heterogeneous Data Sources in Cyber-Physical Systems. IEEE Access, 2021, 9, 55077-55097.	2.6	25
10	Semantically Modeling Cyber Influence Campaigns (CICs): Ontology Model and Case Studies. IEEE Access, 2021, 9, 9365-9382.	2.6	2
11	Biometrics and Privacy-Preservation: How Do They Evolve?. IEEE Open Journal of the Computer Society, 2021, 2, 179-191.	5.2	19
12	A Data Driven Review of Board Game Design and Interactions of Their Mechanics. IEEE Access, 2021, 9, 114051-114069.	2.6	10
13	A Deep Blockchain Framework-Enabled Collaborative Intrusion Detection for Protecting IoT and Cloud Networks. IEEE Internet of Things Journal, 2021, 8, 9463-9472.	5.5	201
14	A Survey on Privacy-Preserving Blockchain Systems (PPBS) and a Novel PPBS-Based Framework for Smart Agriculture. IEEE Open Journal of the Computer Society, 2021, 2, 72-84.	5.2	31
15	A Collaborative Intrusion Detection System Using Deep Blockchain Framework for Securing Cloud Networks. Advances in Intelligent Systems and Computing, 2021, , 553-565.	0.5	7
16	A Deep Learning-based Penetration Testing Framework for Vulnerability Identification in Internet of Things Environments. , 2021, , .		7
17	An Ontological Graph Identification Method for Improving Localization of IP Prefix Hijacking in Network Systems. IEEE Transactions on Information Forensics and Security, 2020, 15, 1164-1174.	4.5	7
18	A Privacy-Preserving-Framework-Based Blockchain and Deep Learning for Protecting Smart Power Networks. IEEE Transactions on Industrial Informatics, 2020, 16, 5110-5118.	7.2	104

#	Article	IF	Citations
19	Supply Chain 4.0: A Survey of Cyber Security Challenges, Solutions and Future Directions. Electronics (Switzerland), 2020, 9, 1864.	1.8	52
20	Robustness Evaluations of Sustainable Machine Learning Models against Data Poisoning Attacks in the Internet of Things. Sustainability, 2020, 12, 6434.	1.6	32
21	A Review of Intrusion Detection and Blockchain Applications in the Cloud: Approaches, Challenges and Solutions. IEEE Access, 2020, 8, 104893-104917.	2.6	53
22	Privacy-Preserving Techniques for Protecting Large-Scale Data of Cyber-Physical Systems. , 2020, , .		5
23	Privacy-Encoding Models for Preserving Utility of Machine Learning Algorithms in Social Media. , 2020, , .		2
24	Interactive 3D Visualization of Network Traffic in Time for Forensic Analysis. , 2020, , .		1
25	Experiment Design for Complex Immersive Visualisation. , 2020, , .		1
26	Mixture Localization-Based Outliers Models for securing Data Migration in Cloud Centers. IEEE Access, 2019, 7, 114607-114618.	2.6	23
27	Towards the development of realistic botnet dataset in the Internet of Things for network forensic analytics: Bot-IoT dataset. Future Generation Computer Systems, 2019, 100, 779-796.	4.9	783
28	An Ensemble Intrusion Detection Technique Based on Proposed Statistical Flow Features for Protecting Network Traffic of Internet of Things. IEEE Internet of Things Journal, 2019, 6, 4815-4830.	5.5	320
29	Towards Automation of Vulnerability and Exploitation Identification in IIoT Networks. , 2018, , .		5
30	Mission-Centric Automated Cyber Red Teaming. , 2018, , .		7
31	Volatile Memory Forensics Acquisition Efficacy. , 2018, , .		6
32	A New Threat Intelligence Scheme for Safeguarding Industry 4.0 Systems. IEEE Access, 2018, 6, 32910-32924.	2.6	95
33	Generating realistic intrusion detection system dataset based on fuzzy qualitative modeling. Journal of Network and Computer Applications, 2017, 87, 185-192.	5.8	136
34	Attrition rates and maneuver in agent-based simulation models. Journal of Defense Modeling and Simulation, 2017, 14, 257-272.	1.2	4
35	The cyber conceptual framework for developing military doctrine. Defence Studies, 2016, 16, 270-298.	0.5	8
36	System of systems cyber effects simulation ontology. , 2015, , .		4

#	Article	IF	Citations
37	Automated event and social network extraction from digital evidence sources with ontological mapping. Digital Investigation, 2015, 13, 94-106.	3.2	40
38	Visual analytics for cyber red teaming. , 2015, , .		9
39	Development of InfoVis Software for Digital Forensics. , 2012, , .		2
40	The "Explore, Investigate and Correlate' (EIC) Conceptual Framework for Digital Forensics Information Visualisation. , 2010, , .		5
41	Enhancing Computer Forensics Investigation through Visualisation and Data Exploitation. , 2009, , .		8
42	The Anatomy of Electronic Evidence – Quantitative Analysis of Police E-Crime Data. , 2009, , .		10
43	Acer Aspire One Netbooks: A Forensic Challenge. , 2009, , .		0
44	Legal and Technical Implications of Collecting Wireless Data as an Evidence Source. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, 2009, , 36-41.	0.2	3
45	Improving the Analysis of Lawfully Intercepted Network Packet Data Captured for Forensic Analysis. , 2008, , .		12
46	Wi-Fi Network Signals as a Source of Digital Evidence: Wireless Network Forensics. , 2008, , .		9
47	Wireless Forensic Analysis Tools for Use in the Electronic Evidence Collection Process. , 2007, , .		9
48	The 802.11 Technology Gap - Case Studies in Crime. , 2005, , .		3