

Taeshik Shon

List of Publications by Year in descending order

Source: <https://exaly.com/author-pdf/7744588/publications.pdf>

Version: 2024-02-01

96
papers

1,419
citations

430442

18
h-index

360668

35
g-index

96
all docs

96
docs citations

96
times ranked

1325
citing authors

#	ARTICLE	IF	CITATIONS
1	AI-enabled device digital forensics for smart cities. Journal of Supercomputing, 2022, 78, 3029-3044.	2.4	13
2	Industrial network-based behavioral anomaly detection in AI-enabled smart manufacturing. Journal of Supercomputing, 2022, 78, 13554-13563.	2.4	10
3	Digital Forensic Analysis to Improve User Privacy on Android. Sensors, 2022, 22, 3971.	2.1	4
4	Automatic whitelist generation system for ethernet based in-vehicle network. Computers in Industry, 2022, 142, 103735.	5.7	6
5	Unknown Payload Anomaly Detection Based on Format and Field Semantics Inference in Cyber-Physical Infrastructure Systems. IEEE Access, 2021, 9, 75542-75552.	2.6	7
6	In-Vehicle Networking/Autonomous Vehicle Security for Internet of Things/Vehicles. Electronics (Switzerland), 2021, 10, 637.	1.8	10
7	Ext4 and XFS File System Forensic Framework Based on TSK. Electronics (Switzerland), 2021, 10, 2310.	1.8	4
8	MitM Tool Analysis for TLS Forensics. , 2021, , .		5
9	Security Analysis of Smart Watch and Band Devices. , 2021, , .		0
10	Data Deletion and Recovery of Androd Plaforms. , 2021, , .		0
11	Adversarial attack-based security vulnerability verification using deep learning library for multimedia video surveillance. Multimedia Tools and Applications, 2020, 79, 16077-16091.	2.6	16
12	ExtSFR: scalable file recovery framework based on an Ext file system. Multimedia Tools and Applications, 2020, 79, 16093-16111.	2.6	12
13	APAD: Autoencoder-based Payload Anomaly Detection for industrial IoE. Applied Soft Computing Journal, 2020, 88, 106017.	4.1	50
14	Certificate Injection-Based Encrypted Traffic Forensics in AI Speaker Ecosystem. Forensic Science International: Digital Investigation, 2020, 33, 301010.	1.2	14
15	Packet Preprocessing in CNN-Based Network Intrusion Detection System. Electronics (Switzerland), 2020, 9, 1151.	1.8	33
16	IEEE 1815.1-Based Power System Security With Bidirectional RNN-Based Network Anomalous Attack Detection for Cyber-Physical System. IEEE Access, 2020, 8, 77572-77586.	2.6	46
17	Smart seed selection-based effective black box fuzzing for IIoT protocol. Journal of Supercomputing, 2020, 76, 10140-10154.	2.4	4
18	Correcting design flaws: An improved and cloud assisted key agreement scheme in cyber physical systems. Computer Communications, 2020, 153, 527-537.	3.1	66

#	ARTICLE	IF	CITATIONS
19	Digital Forensic Practices and Methodologies for AI Speaker Ecosystems. Digital Investigation, 2019, 29, S80-S93.	3.2	34
20	Digital Forensic Analysis using Android Application Cache Data. , 2019, , .		2
21	Digital Forensic Readiness for Financial Network. , 2019, , .		5
22	RNN-based Anomaly Detection in DNP3 Transport Layer. , 2019, , .		8
23	An Security Analysis of Ext Filesystem metadata. , 2019, , .		0
24	Visualization for internet of things: power system and financial network cases. Multimedia Tools and Applications, 2019, 78, 3241-3265.	2.6	8
25	An improved anonymous authentication scheme for distributed mobile cloud computing services. Cluster Computing, 2019, 22, 1595-1609.	3.5	49
26	An improved and robust biometrics-based three factor authentication scheme for multiserver environments. Journal of Supercomputing, 2018, 74, 3504-3520.	2.4	39
27	Design and implementation of cybersecurity testbed for industrial IoT systems. Journal of Supercomputing, 2018, 74, 4506-4520.	2.4	32
28	Field classification-based novel fuzzing case generation for ICS protocols. Journal of Supercomputing, 2018, 74, 4434-4450.	2.4	10
29	Digital forensic science approach by file recovery research. Journal of Supercomputing, 2018, 74, 3704-3725.	2.4	3
30	Game theory-based Security Vulnerability Quantification for Social Internet of Things. Future Generation Computer Systems, 2018, 82, 752-760.	4.9	25
31	Backtracking and Visualization Techniques for Financial Network Security. , 2018, , .		1
32	Toward Security Enhanced Provisioning in Industrial IoT Systems. Sensors, 2018, 18, 4372.	2.1	12
33	A Robust and Efficient Privacy Aware Handover Authentication Scheme for Wireless Networks. Wireless Personal Communications, 2017, 93, 311-335.	1.8	26
34	Two Tier Search Scheme Using Micro UAV Swarm. Wireless Personal Communications, 2017, 93, 349-363.	1.8	8
35	Design and Implementation of Fuzzing Framework Based on IoT Applications. Wireless Personal Communications, 2017, 93, 365-382.	1.8	5
36	A privacy preserving authentication scheme for roaming in ubiquitous networks. Cluster Computing, 2017, 20, 1223-1236.	3.5	20

#	ARTICLE	IF	CITATIONS
37	Recovery Measure against Disabling Reassembly Attack to DNP3 Communication. IEICE Transactions on Information and Systems, 2017, E100.D, 1790-1797.	0.4	2
38	Velocity Obstacle Based 3D Collision Avoidance Scheme for Low-Cost Micro UAVs. Sustainability, 2017, 9, 1174.	1.6	16
39	Data Aggregation Gateway Framework for CoAP Group Communications. Symmetry, 2016, 8, 138.	1.1	4
40	Towards a novel quantification approach based on smart grid network vulnerability score. International Journal of Energy Research, 2016, 40, 298-312.	2.2	7
41	Case Studies for Analyzing DLMS/COSEM-Based Smart Meter Vulnerabilities in Korea. , 2016, , .		1
42	Digital forensic consideration for financial IT security. , 2016, , .		2
43	Digital forensic approach for file recovery in Unix systems: Research of data recovery on Unix file system. , 2016, , .		3
44	A novel vulnerability analysis approach to generate fuzzing test case in industrial control systems. , 2016, , .		12
45	A Multiserver Biometric Authentication Scheme for TMIS using Elliptic Curve Cryptography. Journal of Medical Systems, 2016, 40, 230.	2.2	35
46	Exploring an area by groups of UAVs in the presence of a refueling base. Journal of Supercomputing, 2016, 72, 3409-3427.	2.4	1
47	A novel security architecture of electronic vehicle system for smart grid communication. Journal of Supercomputing, 2016, 72, 214-231.	2.4	1
48	User privacy-enhanced security architecture for home area network of Smartgrid. Multimedia Tools and Applications, 2016, 75, 12749-12764.	2.6	16
49	Challenges and research directions for heterogeneous cyber-physical system based on IEC 61850: Vulnerabilities, security requirements, and security architecture. Future Generation Computer Systems, 2016, 61, 128-136.	4.9	63
50	Neighbor stability-based VANET clustering for urban vehicular environments. Journal of Supercomputing, 2016, 72, 161-176.	2.4	19
51	Network protocol fuzz testing for information systems and applications: a survey and taxonomy. Multimedia Tools and Applications, 2016, 75, 14745-14757.	2.6	16
52	Data investigation based on XFS file system metadata. Multimedia Tools and Applications, 2016, 75, 14721-14743.	2.6	4
53	Packet Diversity-Based Anomaly Detection System with OCSVM and Representative Model. , 2016, , .		3
54	Logical Architecture of HAN-Centric Smartgrid Model. , 2015, , .		3

#	ARTICLE	IF	CITATIONS
55	Reliability Enhanced Communication Guidance for Electric Utilities Based on Regulatory Standard. , 2015, , .		0
56	A Phase of Deleted File Recovery for Digital Forensics Research in Tizen. , 2015, , .		1
57	A study on memory dump analysis based on digital forensic tools. Peer-to-Peer Networking and Applications, 2015, 8, 694-703.	2.6	8
58	Authentication of mobile applications through various local distributors. Multimedia Tools and Applications, 2015, 74, 1541-1555.	2.6	2
59	An interactive pervasive whiteboard based on MVC architecture for ubiquitous collaboration. Multimedia Tools and Applications, 2015, 74, 1557-1576.	2.6	3
60	Novel Approach for Detecting Network Anomalies for Substation Automation based on IEC 61850. Multimedia Tools and Applications, 2015, 74, 303-318.	2.6	44
61	Multi-hop-based opportunistic concurrent directional transmission in 60 GHz WPANs. Multimedia Tools and Applications, 2015, 74, 1627-1644.	2.6	5
62	AVQS: Attack Route-Based Vulnerability Quantification Scheme for Smart Grid. Scientific World Journal, The, 2014, 2014, 1-6.	0.8	1
63	Software Authority Transition through Multiple Distributors. Scientific World Journal, The, 2014, 2014, 1-6.	0.8	3
64	Scenario-Based Attack Route on Industrial Control System. , 2014, , .		1
65	Study on Analysis of Security Vulnerabilities and Countermeasures in ISO/IEC 15118 Based Electric Vehicle Charging Technology. , 2014, , .		16
66	Merkle tree-based wormhole attack avoidance mechanism in low power and lossy network based networks. Security and Communication Networks, 2014, 7, 1292-1309.	1.0	12
67	Applying Digital Forensics in Various Application Fields: Required Elements for Having Legal Force. , 2014, , .		0
68	Survey on security techniques for AMI metering system. , 2014, , .		1
69	An effective authentication mechanism for ubiquitous collaboration in heterogeneous computing environment. Peer-to-Peer Networking and Applications, 2014, 7, 612-619.	2.6	6
70	Improved deleted file recovery technique for Ext2/3 filesystem. Journal of Supercomputing, 2014, 70, 20-30.	2.4	15
71	Physical Memory Collection and Analysis in Smart Grid Embedded System. Mobile Networks and Applications, 2014, 19, 382-391.	2.2	2
72	Toward Advanced Mobile Cloud Computing for the Internet of Things: Current Issues and Future Direction. Mobile Networks and Applications, 2014, 19, 404-413.	2.2	39

#	ARTICLE	IF	CITATIONS
73	Secure and reliable electronic record management system using digital forensic technologies. Journal of Supercomputing, 2014, 70, 149-165.	2.4	8
74	An Obstacle Avoidance Scheme Maintaining Connectivity for Micro-Unmanned Aerial Vehicles. International Journal of Distributed Sensor Networks, 2014, 10, 920534.	1.3	5
75	Adaptive anomaly control for alleviating the exclusive channel occupation in wireless networks. International Journal of Communication Systems, 2013, 26, 720-731.	1.6	1
76	Design and implementation of a wireless sensor network architecture using smart mobile devices. Telecommunication Systems, 2013, 52, 2311-2320.	1.6	11
77	Information delivery scheme of micro UAVs having limited communication range during tracking the moving target. Journal of Supercomputing, 2013, 66, 950-972.	2.4	9
78	Editorial of special section on advanced in high performance, algorithm, and framework for future computing. Journal of Supercomputing, 2013, 65, 483-483.	2.4	0
79	Asynchronous inter-network interference avoidance for wireless body area networks. Journal of Supercomputing, 2013, 65, 562-579.	2.4	30
80	Dynamic learning model update of hybrid-classifiers for intrusion detection. Journal of Supercomputing, 2013, 64, 522-526.	2.4	7
81	A novel secure key paring protocol for RF4CE ubiquitous smart home systems. Personal and Ubiquitous Computing, 2013, 17, 945-949.	1.9	30
82	Security Architecture Model for Smart Grid Communication Systems. , 2013, , .		9
83	A Novel Approach to Analyzing for Detecting Malicious Network Activity Using a Cloud Computing Testbed. Mobile Networks and Applications, 2013, 18, 122-128.	2.2	12
84	Editorial for Special Issue on "New Technologies and Applications for Wireless Communications & Mobile Cloud Computing". Mobile Networks and Applications, 2013, 18, 98-102.	2.2	0
85	A Novel Network Modeling and Evaluation Approach for Security Vulnerability Quantification in Substation Automation Systems. IEICE Transactions on Information and Systems, 2013, E96.D, 2021-2025.	0.4	4
86	An Efficient and Secure Service Discovery Protocol for Ubiquitous Computing Environments. IEICE Transactions on Information and Systems, 2012, E95-D, 117-125.	0.4	1
87	Monitoring Agent for Detecting Malicious Packet Drops for Wireless Sensor Networks in the Microgrid and Grid-Enabled Vehicles. International Journal of Advanced Robotic Systems, 2012, 9, 31.	1.3	4
88	An Adaptive Allocation Algorithm Using Directional CSMA/CA over mmWave Wireless Personal Area Networks. International Journal of Advanced Robotic Systems, 2012, 9, 17.	1.3	3
89	A scalable and privacy-preserving child-care and safety service in a ubiquitous computing environment. Mathematical and Computer Modelling, 2012, 55, 45-57.	2.0	7
90	An efficient and scalable re-authentication protocol over wireless sensor network. IEEE Transactions on Consumer Electronics, 2011, 57, 516-522.	3.0	12

#	ARTICLE	IF	CITATIONS
91	Enhancing Credibility of Location Based Service Using Multiple Sensing Technologies. IEICE Transactions on Information and Systems, 2011, E94-D, 1181-1184.	0.4	2
92	Providing security vertical handoff in SARAH for heterogeneous networks. Journal of Network and Computer Applications, 2011, 34, 1903-1907.	5.8	1
93	Editorial: Special Issue on "Advanced Technologies and Practices in Recent Wireless Sensor Networks". Wireless Personal Communications, 2011, 60, 385-388.	1.8	0
94	Design and Implementation of One-Way Key Agreement Model for Enhancing VoIP Internet Phone Security. IEICE Transactions on Communications, 2011, E94-B, 2235-2238.	0.4	0
95	Location-Aware and Privacy-Preserving Approach for Child Safety in Ubiquitous Computing Environment. IEICE Transactions on Communications, 2011, E94-B, 686-689.	0.4	1
96	A hybrid machine learning approach to network anomaly detection. Information Sciences, 2007, 177, 3799-3821.	4.0	308