

Thaier Hayajneh, Ph D, Smieeee

List of Publications by Year in descending order

Source: <https://exaly.com/author-pdf/6679264/publications.pdf>

Version: 2024-02-01

75
papers

2,701
citations

304368

22
h-index

301761

39
g-index

76
all docs

76
docs citations

76
times ranked

2545
citing authors

#	ARTICLE	IF	CITATIONS
1	AntiConcealer: Reliable Detection of Adversary Concealed Behaviors in EdgeAI-Assisted IoT. IEEE Internet of Things Journal, 2022, 9, 22184-22193.	5.5	16
2	Run-Time Monitoring and Validation Using Reverse Function (RMVRF) for Hardware Trojans Detection. IEEE Transactions on Dependable and Secure Computing, 2021, 18, 2689-2704.	3.7	3
3	Hardware Trojan detection for lightweight ciphers implemented on field-programmable gate arrays using the replay algorithm. International Journal of Circuit Theory and Applications, 2021, 49, 3607.	1.3	1
4	Event Detection Through Differential Pattern Mining in Cyber-Physical Systems. IEEE Transactions on Big Data, 2020, 6, 652-665.	4.4	14
5	TrustData: Trustworthy and Secured Data Collection for Event Detection in Industrial Cyber-Physical System. IEEE Transactions on Industrial Informatics, 2020, 16, 3311-3321.	7.2	60
6	Preserving Balance Between Privacy and Data Integrity in Edge-Assisted Internet of Things. IEEE Internet of Things Journal, 2020, 7, 2679-2689.	5.5	89
7	A Survey of Defensive Measures for Digital Persecution in the Global South. Future Internet, 2020, 12, 166.	2.4	1
8	Erratum to "An Energy-Efficient and Security Aware Route Selection Protocol for Wireless Sensor Networks" Security and Communication Networks, 2020, 2020, 1-1.	1.0	0
9	Secured Data Collection With Hardware-Based Ciphers for IoT-Based Healthcare. IEEE Internet of Things Journal, 2019, 6, 410-420.	5.5	135
10	Hardware Security in IoT Devices with Emphasis on Hardware Trojans. Journal of Sensor and Actuator Networks, 2019, 8, 42.	2.3	56
11	Power-Aware Adaptive Encryption. , 2019, , .		4
12	Smartphone and Smartwatch-Based Biometrics Using Activities of Daily Living. IEEE Access, 2019, 7, 133190-133202.	2.6	218
13	Cyber Security in Social Media: Challenges and the Way Forward. IT Professional, 2019, 21, 41-49.	1.4	32
14	Secure and efficient data delivery for fog-assisted wireless body area networks. Peer-to-Peer Networking and Applications, 2019, 12, 1289-1307.	2.6	16
15	Hardware design and modeling of lightweight block ciphers for secure communications. Future Generation Computer Systems, 2018, 83, 510-521.	4.9	38
16	A Framework to Identify Security and Privacy Issues of Smart Home Devices. , 2018, , .		4
17	Exploring Problems with Virtualization in Cloud Computing. , 2018, , .		2
18	A Comprehensive Attack Flow Model and Security Analysis for Wi-Fi and WPA3. Electronics (Switzerland), 2018, 7, 284.	1.8	30

#	ARTICLE	IF	CITATIONS
19	Biometric Authentication and Verification for Medical Cyber Physical Systems. Electronics (Switzerland), 2018, 7, 436.	1.8	16
20	Security Vulnerabilities in Bluetooth Technology as Used in IoT. Journal of Sensor and Actuator Networks, 2018, 7, 28.	2.3	103
21	A Review of Facial Biometrics Security for Smart Devices. Computers, 2018, 7, 37.	2.1	23
22	Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring. Journal of Medical Systems, 2018, 42, 130.	2.2	623
23	Lightweight Block Ciphers for IoT: Energy Optimization and Survivability Techniques. IEEE Access, 2018, 6, 35966-35978.	2.6	72
24	Security and Privacy Issues with IoT in Healthcare. EAI Endorsed Transactions on Pervasive Health and Technology, 2018, .	0.7	57
25	An Enhanced WLAN Security System With FPGA Implementation for Multimedia Applications. IEEE Systems Journal, 2017, 11, 2536-2545.	2.9	26
26	Next generation wireless-LAN: Security issues and performance analysis. , 2017, , .		2
27	An investigation of Bluetooth security vulnerabilities. , 2017, , .		27
28	Maintaining the Balance between Privacy and Data Integrity in Internet of Things. , 2017, , .		13
29	Heartbleed attacks implementation and vulnerability. , 2017, , .		5
30	Detection and prevention of crypto-ransomware. , 2017, , .		30
31	A Framework for Preventing the Exploitation of IoT Smart Toys for Reconnaissance and Exfiltration. Lecture Notes in Computer Science, 2017, , 581-592.	1.0	10
32	CAre: Certificate Authority Rescue Engine for Proactive Security. , 2017, , .		0
33	Security and privacy issues affecting cloud-based IP camera. , 2017, , .		11
34	Security and Attack Vector Analysis of IoT Devices. Lecture Notes in Computer Science, 2017, , 593-606.	1.0	19
35	A Framework for Zero Day Exploit Detection and Containment. , 2017, , .		7
36	Security issues with certificate authorities. , 2017, , .		10

#	ARTICLE	IF	CITATIONS
37	Reevaluating the effectiveness of visual cues for website security. , 2017, , .		0
38	KeyStroke logs: Are strong passwords enough?. , 2017, , .		1
39	Extrinsic Calibration of Camera and 2D Laser Sensors without Overlap. Sensors, 2017, 17, 2346.	2.1	15
40	Electromagnetic Warfare and the Cybersecurity Threat. , 2017, , .		0
41	Secure Authentication for Remote Patient Monitoring with Wireless Medical Sensor Networks. Sensors, 2016, 16, 424.	2.1	65
42	A comparative study of steganography designs based on multiple FPGA platforms. International Journal of Electronic Security and Digital Forensics, 2016, 8, 164.	0.1	9
43	Reverse TCP and Social Engineering Attacks in the Era of Big Data. , 2016, , .		8
44	Message from the Program Chairs of HPSC 2016. , 2016, , .		0
45	Modeling and optimization of the lightweight HIGHT block cipher design with FPGA implementation. Security and Communication Networks, 2016, 9, 2200-2216.	1.0	42
46	Penetration testing: Concepts, attack methods, and defense strategies. , 2016, , .		81
47	Optimization and modeling of FPGA implementation of the Katan Cipher. , 2015, , .		8
48	A Green Approach for Selfish Misbehavior Detection in 802.11-Based Wireless Networks. Mobile Networks and Applications, 2015, 20, 623-635.	2.2	20
49	Security Issues in WSNs with Cooperative Communication. , 2015, , .		0
50	A survey on lightweight block ciphers for low-resource devices: Comparative study and open issues. Journal of Network and Computer Applications, 2015, 58, 73-93.	5.8	144
51	ANALYSIS AND EVALUATION OF RANDOM PLACEMENT STRATEGIES IN WIRELESS SENSOR NETWORKS. Journal of Circuits, Systems and Computers, 2014, 23, 1450138.	1.0	5
52	ANALYSIS AND MODELING OF FPGA IMPLEMENTATIONS OF SPATIAL STEGANOGRAPHY METHODS. Journal of Circuits, Systems and Computers, 2014, 23, 1450018.	1.0	16
53	An energyâ€efficient and security aware route selection protocol for wireless sensor networks. Security and Communication Networks, 2014, 7, 2015-2038.	1.0	33
54	Multimedia traffic over WLANs: QoS support and performance evaluation. , 2014, , .		3

#	ARTICLE	IF	CITATIONS
55	A cloud-based interference-aware remote health monitoring system for non-hospitalized patients. , 2014, , .		16
56	QoS-Aware Health Monitoring System Using Cloud-Based WBANs. Journal of Medical Systems, 2014, 38, 121.	2.2	57
57	A survey of wireless technologies coexistence in WBAN: analysis and open research issues. Wireless Networks, 2014, 20, 2165-2199.	2.0	152
58	Public-Key Authentication for Cloud-based WBANs. , 2014, , .		3
59	Hierarchical steganography using novel optimum quantization technique. Signal, Image and Video Processing, 2013, 7, 1029-1040.	1.7	6
60	Wavelet-transform steganography: algorithm and hardware implementation. International Journal of Electronic Security and Digital Forensics, 2013, 5, 241.	0.1	17
61	Performance and Information Security Evaluation with Firewalls. International Journal of Security and Its Applications, 2013, 7, 355-372.	0.5	27
62	Classification of Ischemic Optic Neuropathy Using Custom Image Processing Algorithm-Statistical Based Analysis. International Journal of Digital Content Technology and Its Applications, 2013, 7, 95-106.	0.1	0
63	FPGA hardware of the LSB steganography method. , 2012, , .		18
64	Secure Neighborhood Creation in Wireless Ad Hoc Networks using Hop Count Discrepancies. Mobile Networks and Applications, 2012, 17, 415-430.	2.2	26
65	Sourceâ€™destination obfuscation in wireless <i>ad hoc</i> networks. Security and Communication Networks, 2011, 4, 888-901.	1.0	14
66	Random variation in coverage of sensor networks. Communications in Computer and Information Science, 2011, , 31-41.	0.4	0
67	On limited-range strategic/random jamming attacks in wireless ad hoc networks. , 2009, , .		22
68	Detecting Malicious Packet Dropping in the Presence of Collisions and Channel Errors in Wireless Ad Hoc Networks. , 2009, , .		32
69	A graph-coloring-based navigational algorithm for personnel safety in nuclear applications. , 2009, , .		0
70	DeWorm: A Simple Protocol to Detect Wormhole Attacks in Wireless Ad Hoc Networks. , 2009, , .		37
71	SECLUD: Source and Destination Seclusion Using Clouds for wireless ad hoc networks. , 2009, , .		17
72	SECUND: A protocol for SECURE neighborhood creation in wireless ad hoc networks. , 2009, , .		3

#	ARTICLE	IF	CITATIONS
73	A biometric-secure e-voting system for election processes. , 2008, , .		28
74	A secure novel sensor fusion architecture for nuclear applications. , 2008, , .		3
75	A modified optical network for interactive video-on-demand services. , 0, , .		0