

# Devesh Jinwala

## List of Publications by Year in descending order

Source: <https://exaly.com/author-pdf/9493739/publications.pdf>

Version: 2024-02-01

39  
papers

288  
citations

840776

11  
h-index

940533

16  
g-index

39  
all docs

39  
docs citations

39  
times ranked

224  
citing authors

#	ARTICLE	IF	CITATIONS
1	Multi-Keyword Searchable Encryption for E-Health System With Multiple Data Writers and Readers. <i>Advances in Wireless Technologies and Telecommunication Book Series</i> , 2022, , 107-131.	0.4	0
2	Simple index based symmetric searchable encryption with result verifiability. <i>Frontiers of Computer Science</i> , 2021, 15, 1.	2.4	2
3	Multi-writer multi-reader conjunctive keyword searchable encryption. <i>International Journal of Information and Computer Security</i> , 2021, 15, 141.	0.2	2
4	Privacy preserving secure expansive aggregation with malicious node identification in linear wireless sensor networks. <i>Frontiers of Computer Science</i> , 2021, 15, 1.	2.4	16
5	A Trust-Integrated RPL Protocol to Detect Blackhole Attack in Internet of Things. <i>International Journal of Information Security and Privacy</i> , 2021, 15, 1-17.	0.8	2
6	6MID:Mircochain based Intrusion Detection for 6LoWPAN based IoT networks. <i>Procedia Computer Science</i> , 2021, 184, 929-934.	2.0	1
7	R-OO-KASE: Revocable Online/Offline Key Aggregate Searchable Encryption. <i>Data Science and Engineering</i> , 2020, 5, 391-418.	6.4	9
8	Multi-writer Multi-reader Boolean Keyword Searchable Encryption. <i>Arabian Journal for Science and Engineering</i> , 2020, 45, 10709-10729.	3.0	3
9	Constructing a Knowledge-Based Quality Attributes Relationship Matrix to Identify Conflicts in Non-Functional Requirements. <i>Journal of Computational and Theoretical Nanoscience</i> , 2020, 17, 122-129.	0.4	2
10	A Semi-automated Approach to Generate an Adaptive Quality Attribute Relationship Matrix. <i>Lecture Notes in Computer Science</i> , 2020, , 239-256.	1.3	0
11	Decentralized Context Aware Access Control Model for Internet of Things. <i>Journal of Computational and Theoretical Nanoscience</i> , 2020, 17, 162-171.	0.4	1
12	P <sup>2</sup> KASE A <sup>2</sup> –privacy-preserving key aggregate searchable encryption supporting authentication and access control on multi-delegation. <i>IET Information Security</i> , 2020, 14, 704-723.	1.7	2
13	MULKASE: a novel approach for key-aggregate searchable encryption for multi-owner data. <i>Frontiers of Information Technology and Electronic Engineering</i> , 2019, 20, 1717-1748.	2.6	10
14	An Ontological Approach to Specify Conflicts among Non-Functional Requirements. , 2019, , .		0
15	Novel Approach of Key Predistribution for Grid Based Sensor Networks. <i>Wireless Personal Communications</i> , 2019, 108, 939-955.	2.7	4
16	BMMI-tree: A Peer-to-Peer m-ary tree using 1-m node splitting for an efficient multidimensional complex query search. <i>Journal of Parallel and Distributed Computing</i> , 2019, 125, 1-17.	4.1	5
17	BTG-RKASE: Privacy Preserving Revocable Key Aggregate Searchable Encryption with Fine-grained Multi-delegation & Break-The-Glass Access Control. , 2019, , .		5
18	Privacy Preserving, Verifiable and Resilient Data Aggregation in Grid-Based Networks. <i>Computer Journal</i> , 2018, 61, 614-628.	2.4	18

#	ARTICLE	IF	CITATIONS
19	Novel Approach for Pre-distributing Keys in WSNs for Linear Infrastructure. <i>Wireless Personal Communications</i> , 2017, 95, 3905-3921.	2.7	11
20	Multiuser Searchable Encryption with Token Freshness Verification. <i>Security and Communication Networks</i> , 2017, 2017, 1-16.	1.5	9
21	A novel approach for privacy homomorphism using attribute-based encryption. <i>Security and Communication Networks</i> , 2016, 9, 4451-4467.	1.5	1
22	Malleability Resilient Concealed Data Aggregation in Wireless Sensor Networks. <i>Wireless Personal Communications</i> , 2016, 87, 971-993.	2.7	19
23	A novel privacy-preserving scheme for collaborative frequent itemset mining across vertically partitioned data. <i>Security and Communication Networks</i> , 2015, 8, 4407-4420.	1.5	14
24	Functional Encryption in IoT E-Health Care System. <i>Lecture Notes in Computer Science</i> , 2015, , 345-363.	1.3	12
25	A Novel Approach for Searchable CP-ABE with Hidden Ciphertext-Policy. <i>Lecture Notes in Computer Science</i> , 2014, , 167-184.	1.3	11
26	Fully secure ciphertext policy attribute-based encryption with constant length ciphertext and faster decryption. <i>Security and Communication Networks</i> , 2014, 7, 1988-2002.	1.5	30
27	AB-OR: Improving the Efficiency in Onion Routing Using Attribute Based Cryptography. <i>Lecture Notes in Electrical Engineering</i> , 2013, , 425-432.	0.4	1
28	Privacy Preserving Distributed K-Means Clustering in Malicious Model Using Zero Knowledge Proof. <i>Lecture Notes in Computer Science</i> , 2013, , 420-431.	1.3	17
29	Privacy Preservation for Global Cyclic Associations in Distributed Databases. <i>Procedia Technology</i> , 2012, 6, 962-969.	1.1	7
30	Hidden Access Structure Ciphertext Policy Attribute Based Encryption with Constant Length Ciphertext. <i>Lecture Notes in Computer Science</i> , 2012, , 515-523.	1.3	19
31	Anonymity in Attribute-Based Group Signatures. <i>Lecture Notes in Computer Science</i> , 2012, , 495-504.	1.3	3
32	An Efficient Approach for Privacy Preserving Distributed K-Means Clustering Based on Shamir's Secret Sharing Scheme. <i>International Federation for Information Processing</i> , 2012, , 129-141.	0.4	15
33	A Sensitive Attribute Based Clustering Method for k-Anonymization. <i>Lecture Notes in Computer Science</i> , 2012, , 163-170.	1.3	1
34	A Novel Approach for Web Services Discovery Using Rough Sets. <i>Advances in Intelligent and Soft Computing</i> , 2012, , 759-771.	0.2	0
35	ID-based secure key generation protocol. , 2011, , .		0
36	Constant ciphertext length in multi-authority Ciphertext Policy Attribute Based Encryption. , 2011, , .		13

#	ARTICLE	IF	CITATIONS
37	Exploring Homomorphic Encryption in Wireless Sensor Networks. Communications in Computer and Information Science, 2011, , 400-408.	0.5	4
38	Replay Protection at the Link Layer Security in Wireless Sensor Networks. , 2009, , .		5
39	Optimizing the Block Cipher and Modes of Operations Overhead at the Link Layer Security Framework in the Wireless Sensor Networks. Lecture Notes in Computer Science, 2008, , 258-272.	1.3	14