

Dheerendra Mishra

List of Publications by Year in descending order

Source: <https://exaly.com/author-pdf/1492735/publications.pdf>

Version: 2024-02-01

74
papers

1,504
citations

361413

20
h-index

345221

36
g-index

77
all docs

77
docs citations

77
times ranked

935
citing authors

#	ARTICLE	IF	CITATIONS
1	A secure user anonymity-preserving biometric-based multi-server authenticated key agreement scheme using smart cards. <i>Expert Systems With Applications</i> , 2014, 41, 8129-8143.	7.6	208
2	Secure and efficient user authentication scheme for multi-gateway wireless sensor networks. <i>Ad Hoc Networks</i> , 2017, 54, 147-169.	5.5	122
3	Cryptanalysis and Improvement of Yan et al.'s Biometric-Based Authentication Scheme for Telecare Medicine Information Systems. <i>Journal of Medical Systems</i> , 2014, 38, 24.	3.6	73
4	A secure and efficient ECC-based user anonymity-preserving session initiation authentication protocol using smart card. <i>Peer-to-Peer Networking and Applications</i> , 2016, 9, 171-192.	3.9	73
5	Security Enhancement of a Biometric based Authentication Scheme for Telecare Medicine Information Systems with Nonce. <i>Journal of Medical Systems</i> , 2014, 38, 41.	3.6	70
6	Efficient authentication protocol for secure multimedia communications in IoT-enabled wireless sensor networks. <i>Multimedia Tools and Applications</i> , 2018, 77, 18295-18325.	3.9	69
7	A Secure and Efficient Chaotic Map-Based Authenticated Key Agreement Scheme for Telecare Medicine Information Systems. <i>Journal of Medical Systems</i> , 2014, 38, 120.	3.6	58
8	A Mutual Authentication Framework for Wireless Medical Sensor Networks. <i>Journal of Medical Systems</i> , 2017, 41, 80.	3.6	57
9	PALK: Password-based anonymous lightweight key agreement framework for smart grid. <i>International Journal of Electrical Power and Energy Systems</i> , 2020, 121, 106121.	5.5	56
10	RSEAP: RFID based secure and efficient authentication protocol for vehicular cloud computing. <i>Vehicular Communications</i> , 2020, 22, 100213.	4.0	49
11	A secure password-based authentication and key agreement scheme using smart cards. <i>Journal of Information Security and Applications</i> , 2015, 23, 28-43.	2.5	36
12	On the Security Flaws in ID-based Password Authentication Schemes for Telecare Medical Information Systems. <i>Journal of Medical Systems</i> , 2015, 39, 154.	3.6	32
13	Construction of RSA-Based Authentication Scheme in Authorized Access to Healthcare Services. <i>Journal of Medical Systems</i> , 2020, 44, 6.	3.6	31
14	Design and Analysis of a Provably Secure Multi-server Authentication Scheme. <i>Wireless Personal Communications</i> , 2016, 86, 1095-1119.	2.7	26
15	An anonymous and secure biometric-based enterprise digital rights management system for mobile environment. <i>Security and Communication Networks</i> , 2015, 8, 3383-3404.	1.5	25
16	An anonymous biometric-based remote user authenticated key agreement scheme for multimedia systems. <i>International Journal of Communication Systems</i> , 2017, 30, e2946.	2.5	23
17	Efficient and Secure Attribute Based Access Control Architecture for Smart Healthcare. <i>Journal of Medical Systems</i> , 2020, 44, 97.	3.6	23
18	Improved Biometric-Based Three-factor Remote User Authentication Scheme with Key Agreement Using Smart Card. <i>Lecture Notes in Computer Science</i> , 2013, , 63-77.	1.3	22

#	ARTICLE	IF	CITATIONS
19	Provably secure biometric based authentication and key agreement protocol for wireless sensor networks. Journal of Ambient Intelligence and Humanized Computing, 2018, 9, 875-895.	4.9	22
20	A provably secure dynamic ID-based authenticated key agreement framework for mobile edge computing without a trusted party. Journal of Information Security and Applications, 2020, 55, 102648.	2.5	22
21	A privacy preserving biometric-based three-factor remote user authenticated key agreement scheme. Journal of Information Security and Applications, 2017, 32, 15-26.	2.5	21
22	Understanding Security Failures of Two Authentication and Key Agreement Schemes for Telecare Medicine Information Systems. Journal of Medical Systems, 2015, 39, 19.	3.6	20
23	Design of a lightweight two-factor authentication scheme with smart card revocation. Journal of Information Security and Applications, 2015, 23, 44-53.	2.5	20
24	LCPPA: Lattice-based conditional privacy preserving authentication in vehicular communication. Transactions on Emerging Telecommunications Technologies, 2020, 31, e3810.	3.9	20
25	Design of a secure smart card-based multi-server authentication scheme. Journal of Information Security and Applications, 2016, 30, 64-80.	2.5	18
26	A Pairing-Free Identity Based Authentication Framework for Cloud Computing. Lecture Notes in Computer Science, 2013, , 721-727.	1.3	17
27	SFVCC: Chaotic map-based security framework for vehicular cloud computing. IET Intelligent Transport Systems, 2020, 14, 241-249.	3.0	14
28	A Self-Verifiable Password Based Authentication Scheme for Multi-Server Architecture Using Smart Card. Wireless Personal Communications, 2017, 96, 6273-6297.	2.7	13
29	Efficient and secure two-factor dynamic ID-based password authentication scheme with provable security. Cryptologia, 2018, 42, 146-175.	0.5	13
30	Efficient design of an authenticated key agreement protocol for dew-assisted IoT systems. Journal of Supercomputing, 2022, 78, 3696-3714.	3.6	13
31	An enhanced dynamic ID-based authentication scheme for telecare medical information systems. Journal of King Saud University - Computer and Information Sciences, 2017, 29, 54-62.	3.9	12
32	Lattice-based key agreement protocol under ring-LWE problem for IoT-enabled smart devices. Sadhana - Academy Proceedings in Engineering Sciences, 2021, 46, 1.	1.3	12
33	A password based authentication scheme for wireless multimedia systems. Multimedia Tools and Applications, 2017, 76, 25893-25918.	3.9	11
34	Secure and ubiquitous authenticated content distribution framework for IoT enabled DRM system. Multimedia Tools and Applications, 2020, 79, 20319-20341.	3.9	10
35	Post-quantum digital signature scheme based on multivariate cubic problem. Journal of Information Security and Applications, 2020, 53, 102512.	2.5	9
36	Cryptanalysis of Yang et al.'s Digital Rights Management Authentication Scheme Based on Smart Card. Communications in Computer and Information Science, 2014, , 288-297.	0.5	9

#	ARTICLE	IF	CITATIONS
37	Vector Space Access Structure and ID Based Distributed DRM Key Management. Communications in Computer and Information Science, 2011, , 223-232.	0.5	8
38	PSSCC: Provably secure communication framework for crowdsourced industrial Internet of Things environments. Software - Practice and Experience, 2022, 52, 744-755.	3.6	8
39	Computational Efficient Authenticated Digital Content Distribution Frameworks for DRM Systems: Review and Outlook. IEEE Systems Journal, 2021, 15, 1586-1593.	4.6	8
40	An authenticated access control framework for digital right management system. Multimedia Tools and Applications, 2021, 80, 25255.	3.9	8
41	Privacy rights management in multiparty multilevel DRM system. , 2012, , .		7
42	A Secure and Robust Smartcard-Based Authentication Scheme for Session Initiation Protocol Using Elliptic Curve Cryptography. Wireless Personal Communications, 2016, 91, 1361-1391.	2.7	7
43	Improving Security of Lightweight Authentication Technique for Heterogeneous Wireless Sensor Networks. Wireless Personal Communications, 2017, 95, 3141-3166.	2.7	7
44	Privacy Preserving Password-Based Multi-server Authenticated Key Agreement Protocol Using Smart Card. Wireless Personal Communications, 2018, 99, 1-21.	2.7	7
45	An improved biometric-based remote user authentication scheme for connected healthcare. International Journal of Ad Hoc and Ubiquitous Computing, 2015, 18, 75.	0.5	6
46	Chaos-Based Content Distribution Framework for Digital Rights Management System. IEEE Systems Journal, 2021, 15, 570-576.	4.6	6
47	SFECC: Provably Secure Signcryption-Based Big Data Security Framework for Energy-Efficient Computing Environment. IEEE Systems Journal, 2021, 15, 598-606.	4.6	6
48	Construction of a Chaotic Map-Based Authentication Protocol for TMIS. Journal of Medical Systems, 2021, 45, 77.	3.6	6
49	On the security enhancement of integrated electronic patient records information systems. Computer Science and Information Systems, 2015, 12, 857-872.	1.0	6
50	Construction of lightweight authentication scheme for network applicants using smart cards. Sadhana - Academy Proceedings in Engineering Sciences, 2020, 45, 1.	1.3	5
51	Privacy-Preserving Key Agreement Protocol for Fog Computing Supported Internet of Things Environment. Wireless Personal Communications, 2021, 119, 727-747.	2.7	5
52	A provably secure content distribution framework for portable DRM systems. Journal of Information Security and Applications, 2021, 61, 102928.	2.5	5
53	An Authentication Framework for Roaming Service in Global Mobility Networks. Information Technology and Control, 2019, 48, .	2.1	5
54	A secure authentication framework for WSN-based safety monitoring in coal mines. Sadhana - Academy Proceedings in Engineering Sciences, 2020, 45, 1.	1.3	4

#	ARTICLE	IF	CITATIONS
55	A Certificateless Authenticated Key Agreement Protocol for Digital Rights Management System. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, 2013, , 568-577.	0.3	4
56	Construction of elliptic curve cryptographyâ€based authentication protocol for internet of things. Security and Privacy, 2022, 5, .	2.7	4
57	Secure Lightweight User Authentication and Key Agreement Scheme for Wireless Sensor Networks Tailored for the Internet of Things Environment. Lecture Notes in Computer Science, 2016, , 45-65.	1.3	3
58	Understanding signcryption security in standard model. Security and Privacy, 2020, 3, e105.	2.7	3
59	Towards a Secure, Transparent and Privacy-Preserving DRM System. Communications in Computer and Information Science, 2012, , 304-313.	0.5	3
60	Design of a password-based authenticated key exchange protocol for SIP. Multimedia Tools and Applications, 2016, 75, 16017-16038.	3.9	2
61	PSMECS: A provably secure IDâ€based communication in mobile edge computing. International Journal of Communication Systems, 2023, 36, e4116.	2.5	2
62	Authenticated content distribution framework for digital rights management systems with smart card revocation. International Journal of Communication Systems, 2020, 33, e4388.	2.5	2
63	Secure Content Delivery in DRM System with Consumer Privacy. Lecture Notes in Computer Science, 2013, , 321-335.	1.3	2
64	Computationally Efficient and Secure Session Key Agreement Techniques for Vehicular Cloud Computing. Lecture Notes in Electrical Engineering, 2021, , 453-467.	0.4	2
65	Privacy Preserving Location-based Content Distribution Framework for Digital Rights Management Systems. , 2021, , .		2
66	Construction of Lightweight Content key Distribution Framework for DRM systems. , 2021, , .		2
67	Privacy preserving hierarchical content distribution in multiparty multilevel DRM. , 2012, , .		1
68	A privacy enabling content distribution framework for digital rights management. International Journal of Trust Management in Computing and Communications, 2014, 2, 22.	0.1	1
69	1-out-of-2: post-quantum oblivious transfer protocols based on multivariate public key cryptography. Sadhana - Academy Proceedings in Engineering Sciences, 2020, 45, 1.	1.3	1
70	Cryptanalysis and improvement of biometric based content distribution framework for digital rights management systems. Security and Privacy, 2021, 4, e133.	2.7	1
71	Blockchain-based multimedia content distribution with the assured system update mechanism. Multimedia Tools and Applications, 2021, 80, 29423-29436.	3.9	1
72	Reply to comment on â€SFVCC: Chaotic mapâ€based security framework for vehicular cloud computingâ€™. IET Intelligent Transport Systems, 2020, 14, 1724-1724.	3.0	1

#	ARTICLE	IF	CITATIONS
73	Construction of Identity Based Signcrypton Using Learning with Rounding. Communications in Computer and Information Science, 2020, , 612-626.	0.5	1
74	Cryptanalysis of Two Authentication Scheme for DRM System. Communications in Computer and Information Science, 2014, , 184-191.	0.5	0