Mohammad Wazid

List of Publications by Year
in descending order

Source: https://exaly.com/author-pdf/2345733/publications.pdf

Version: 2024-02-01

97	5,630	87888	91884
papers	citations	38 h-index	69 g-index

97	97	97	3445
all docs	docs citations	times ranked	citing authors

#	Article	IF	Citations
1	MADP-IIME: malware attack detection protocol in IoT-enabled industrial multimedia environment using machine learning approach. Multimedia Systems, 2023, 29, 1785-1797.	4.7	5
2	Design and Testbed Experiments of User Authentication and Key Establishment Mechanism for Smart Healthcare Cyber Physical Systems. IEEE Transactions on Network Science and Engineering, 2023, 10, 2697-2709.	6.4	12
3	BACKM-EHA: A Novel Blockchain-enabled Security Solution for IoMT-based E-healthcare Applications. ACM Transactions on Internet Technology, 2023, 23, 1-28.	4.4	17
4	On the design of an AI-driven secure communication scheme for internet of medical things environment. Digital Communications and Networks, 2023, 9, 1080-1089.	5.0	6
5	SCS-WoT: Secure Communication Scheme for Web of Things Deployment. IEEE Internet of Things Journal, 2022, 9, 10411-10423.	8.7	14
6	BUAKA-CS: Blockchain-enabled user authentication and key agreement scheme for crowdsourcing system. Journal of Systems Architecture, 2022, 123, 102370.	4.3	14
7	An efficient node placement scheme to mitigate routing attacks in Internet of Battlefield Things. Computers and Electrical Engineering, 2022, 97, 107623.	4.8	4
8	Blockchainâ€enabled secure communication mechanism for IoTâ€driven personal health records. Transactions on Emerging Telecommunications Technologies, 2022, 33, .	3.9	6
9	ACM-SH: An Efficient Access Control and Key Establishment Mechanism for Sustainable Smart Healthcare. Sustainability, 2022, 14, 4661.	3.2	5
10	Uniting cyber security and machine learning: Advantages, challenges and future research. ICT Express, 2022, 8, 313-321.	4.8	32
11	Security in <scp>IoMT</scp>â€driven smart healthcare: A comprehensive review and open challenges. Security and Privacy, 2022, 5, .	2.7	10
12	ASCP-IoMT: AI-Enabled Lightweight Secure Communication Protocol for Internet of Medical Things. IEEE Access, 2022, 10, 57990-58004.	4.2	24
13	TACAS-IoT: Trust Aggregation Certificate-Based Authentication Scheme for Edge-Enabled IoT Systems. IEEE Internet of Things Journal, 2022, 9, 22643-22656.	8.7	10
14	BDESF-ITS: Blockchain-Based Secure Data Exchange and Storage Framework for Intelligent Transportation System. , 2022, , .		2
15	Machine learning security attacks and defense approaches for emerging cyber physical applications: A comprehensive survey. Computer Communications, 2022, 192, 316-331.	5.1	10
16	Designing Secure User Authentication Protocol for Big Data Collection in IoT-Based Intelligent Transportation System. IEEE Internet of Things Journal, 2021, 8, 7727-7744.	8.7	58
17	Designing Authenticated Key Management Scheme in 6G-Enabled Network in a Box Deployed for Industrial Applications. IEEE Transactions on Industrial Informatics, 2021, 17, 7174-7184.	11.3	25
18	On the Design of Mutual Authentication and Key Agreement Protocol in Internet of Vehicles-Enabled Intelligent Transportation System. IEEE Transactions on Vehicular Technology, 2021, 70, 1736-1751.	6.3	59

#	Article	IF	Citations
19	A blockchain based secure communication framework for community interaction. Journal of Information Security and Applications, 2021, 58, 102790.	2.5	5
20	SPCS-IoTEH: Secure Privacy-Preserving Communication Scheme for IoT-Enabled e-Health Applications. , 2021, , .		7
21	iGCACS-IoD: An Improved Certificate-Enabled Generic Access Control Scheme for Internet of Drones Deployment. IEEE Access, 2021, 9, 87024-87048.	4.2	15
22	Security in 5G-Enabled Internet of Things Communication: Issues, Challenges, and Future Research Roadmap. IEEE Access, 2021, 9, 4466-4489.	4.2	40
23	On the Security of a Secure and Lightweight Authentication Scheme for Next Generation IoT Infrastructure. IEEE Access, 2021, 9, 71856-71867.	4.2	13
24	Blockchain-Envisioned Secure Authentication Approach in AIoT: Applications, Challenges, and Future Research. Wireless Communications and Mobile Computing, 2021, 2021, 1-19.	1.2	11
25	ANN-Based Multi-class Malware Detection Scheme for IoT Environment. Smart Innovation, Systems and Technologies, 2021, , 269-277.	0.6	2
26	Securing Internet of Drones Networks Using AI-Envisioned Smart-Contract-Based Blockchain. IEEE Internet of Things Magazine, 2021, 4, 68-73.	2.6	5
27	Secure Remote User Authenticated Key Establishment Protocol for Smart Home Environment. IEEE Transactions on Dependable and Secure Computing, 2020, 17, 391-406.	5.4	230
28	Anonymous Lightweight Chaotic Map-Based Authenticated Key Agreement Protocol for Industrial Internet of Things. IEEE Transactions on Dependable and Secure Computing, 2020, 17, 1133-1146.	5.4	126
29	Intrusion Detection Protocols in Wireless Sensor Networks Integrated to Internet of Things Deployment: Survey and Future Challenges. IEEE Access, 2020, 8, 3343-3363.	4.2	103
30	LAM-CIoT: Lightweight authentication mechanism in cloud-based IoT environment. Journal of Network and Computer Applications, 2020, 150, 102496.	9.1	169
31	On the Design of Secure Communication Framework for Blockchain-Based Internet of Intelligent Battlefield Things Environment. , 2020, , .		10
32	A Tutorial and Future Research for Building a Blockchain-Based Secure Communication Scheme for Internet of Intelligent Things. IEEE Access, 2020, 8, 88700-88716.	4.2	41
33	Authentication Protocols in Internet of Vehicles: Taxonomy, Analysis, and Challenges. IEEE Access, 2020, 8, 54314-54344.	4.2	73
34	Designing Efficient Sinkhole Attack Detection Mechanism in Edge-Based IoT Deployment. Sensors, 2020, 20, 1300.	3.8	30
35	LAKS-NVT: Provably Secure and Lightweight Authentication and Key Agreement Scheme Without Verification Table in Medical Internet of Things. IEEE Access, 2020, 8, 119387-119404.	4.2	49
36	BAKMP-IoMT: Design of Blockchain Enabled Authenticated Key Management Protocol for Internet of Medical Things Deployment. IEEE Access, 2020, 8, 95956-95977.	4.2	138

#	Article	IF	Citations
37	Private blockchain-envisioned security framework for AI-enabled IoT-based drone-aided healthcare services. , 2020, , .		44
38	SAC-FIIoT: Secure Access Control Scheme for Fog-Based Industrial Internet of Things. , 2020, , .		11
39	RADâ€EI: A routing attack detection scheme for edgeâ€based Internet of Things environment. International Journal of Communication Systems, 2019, 32, e4024.	2.5	28
40	AKM-IoV: Authenticated Key Management Protocol in Fog Computing-Based Internet of Vehicles Deployment. IEEE Internet of Things Journal, 2019, 6, 8804-8817.	8.7	161
41	Provably Secure ECC-Based Device Access Control and Key Agreement Protocol for IoT Environment. IEEE Access, 2019, 7, 55382-55397.	4.2	121
42	Mobile Banking: Evolution and Threats: Malware Threats and Security Solutions. IEEE Consumer Electronics Magazine, 2019, 8, 56-60.	2.3	47
43	User authentication in a tactile internet based remote surgery environment: Security issues, challenges, and future research directions. Pervasive and Mobile Computing, 2019, 54, 71-85.	3.3	19
44	IoMT Malware Detection Approaches: Analysis and Research Challenges. IEEE Access, 2019, 7, 182459-182476.	4.2	95
45	LDAKM-EIoT: Lightweight Device Authentication and Key Management Mechanism for Edge-Based IoT Deployment. Sensors, 2019, 19, 5539.	3.8	48
46	Authentication in cloud-driven IoT-based big data environment: Survey and outlook. Journal of Systems Architecture, 2019, 97, 185-196.	4.3	120
47	Design and Analysis of Secure Lightweight Remote User Authentication and Key Agreement Scheme in Internet of Drones Deployment. IEEE Internet of Things Journal, 2019, 6, 3572-3584.	8.7	218
48	Design of secure key management and user authentication scheme for fog computing services. Future Generation Computer Systems, 2019, 91, 475-492.	7.5	170
49	Design of Secure User Authenticated Key Management Protocol for Generic IoT Networks. IEEE Internet of Things Journal, 2018, 5, 269-282.	8.7	298
50	Authentication Protocols for Implantable Medical Devices: Taxonomy, Analysis and Future Directions. IEEE Consumer Electronics Magazine, 2018, 7, 57-65.	2.3	34
51	A secure enhanced privacy-preserving key agreement protocol for wireless mobile networks. Telecommunication Systems, 2018, 69, 431-445.	2.5	8
52	A Novel Authentication and Key Agreement Scheme for Implantable Medical Devices Deployment. IEEE Journal of Biomedical and Health Informatics, 2018, 22, 1299-1309.	6.3	119
53	Design of Secure and Lightweight Authentication Protocol for Wearable Devices Environment. IEEE Journal of Biomedical and Health Informatics, 2018, 22, 1310-1322.	6.3	145
54	Biometrics-Based Privacy-Preserving User Authentication Scheme for Cloud-Based Industrial Internet of Things Deployment. IEEE Internet of Things Journal, 2018, 5, 4900-4913.	8.7	159

#	Article	IF	Citations
55	Authenticated key management protocol for cloud-assisted body area sensor networks. Journal of Network and Computer Applications, 2018, 123, 112-126.	9.1	69
56	Secure Signature-Based Authenticated Key Establishment Scheme for Future IoT Applications. IEEE Access, 2017, 5, 3028-3043.	4.2	330
57	Secure Authentication Scheme for Medicine Anti-Counterfeiting System in IoT Environment. IEEE Internet of Things Journal, 2017, 4, 1634-1646.	8.7	85
58	Lightweight authentication protocols for wearable devices. Computers and Electrical Engineering, 2017, 63, 196-208.	4.8	32
59	An efficient authentication and key agreement scheme for multi-gateway wireless sensor networks in IoT deployment. Journal of Network and Computer Applications, 2017, 89, 72-85.	9.1	141
60	Secure Three-Factor User Authentication Scheme for Renewable-Energy-Based Smart Grid Environment. IEEE Transactions on Industrial Informatics, 2017, 13, 3144-3153.	11.3	116
61	Design of Lightweight Authentication and Key Agreement Protocol for Vehicular Ad Hoc Networks. IEEE Access, 2017, 5, 14966-14980.	4.2	90
62	On the design of a secure user authentication and key agreement scheme for wireless sensor networks. Concurrency Computation Practice and Experience, 2017, 29, e3930.	2.2	32
63	A Secure Group-Based Blackhole Node Detection Scheme for Hierarchical Wireless Sensor Networks. Wireless Personal Communications, 2017, 94, 1165-1191.	2.7	41
64	Provably secure authenticated key agreement scheme for distributed mobile cloud computing services. Future Generation Computer Systems, 2017, 68, 74-88.	7.5	97
65	Design of an efficient and provably secure anonymity preserving threeâ€factor user authentication and key agreement scheme for TMIS. Security and Communication Networks, 2016, 9, 1983-2001.	1.5	74
66	An efficient multiâ€gatewayâ€based threeâ€factor user authentication and key agreement scheme in hierarchical wireless sensor networks. Security and Communication Networks, 2016, 9, 2070-2092.	1.5	82
67	Provably secure biometricâ€based user authentication and key agreement scheme in cloud computing. Security and Communication Networks, 2016, 9, 4103-4119.	1.5	39
68	Provably Secure Authenticated Key Agreement Scheme for Smart Grid. IEEE Transactions on Smart Grid, 2016, , 1-1.	9.0	158
69	Secure anonymity-preserving password-based user authentication and session key agreement scheme for telecare medicine information systems. Computer Methods and Programs in Biomedicine, 2016, 135, 167-185.	4.7	43
70	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
71	Analysis of Security Protocols for Mobile Healthcare. Journal of Medical Systems, 2016, 40, 229.	3.6	27
72	Secure anonymous mutual authentication for star two-tier wireless body area networks. Computer Methods and Programs in Biomedicine, 2016, 135, 37-50.	4.7	106

#	Article	IF	Citations
73	Design of sinkhole node detection mechanism for hierarchical wireless sensor networks. Security and Communication Networks, 2016, 9, 4596-4614.	1.5	50
74	An Efficient Hybrid Anomaly Detection Scheme Using K-Means Clustering for Wireless Sensor Networks. Wireless Personal Communications, 2016, 90, 1971-2000.	2.7	64
75	An Efficient Cryptographic Scheme for Text Message Protection Against Brute Force and Cryptanalytic Attacks. Procedia Computer Science, 2015, 48, 360-366.	2.0	16
76	Forensics of Random-UDP Flooding Attacks. Journal of Networks, 2015, 10, .	0.4	18
77	Efficient Protocol Prediction Algorithm for MANET Multimedia Transmission Under JF Periodic Dropping Attack. Advances in Intelligent Systems and Computing, 2014, , 419-428.	0.6	0
78	Hacktivism trends, digital forensic tools and challenges: A survey. , 2013, , .		20
79	Data recovery with energy efficient task allocation in Wireless Sensor Networks. , 2013, , .		2
80	Implementation and Embellishment of Prevention of Keylogger Spyware Attacks. Communications in Computer and Information Science, 2013, , 262-271.	0.5	4
81	Misdirection attack in WSN: Topological analysis and an algorithm for delay and throughput prediction. , 2013, , .		7
82	Coverage life time improvement in Wireless Sensor Networks by novel deployment technique. , 2013, , .		1
83	Big data: Issues, challenges, tools and Good practices. , 2013, , .		496
84	Effective Clustering Technique for Selecting Cluster Heads and Super Cluster Head in MANET. , 2013, , .		2
85	A cluster based detection and prevention mechanism against novel datagram chunk dropping attack in MANET multimedia transmission. , 2013, , .		9
86	Hiding the Sink Location from the Passive Attack in WSN. Procedia Engineering, 2013, 64, 16-25.	1.2	3
87	Authentication and authorization: Domain specific Role Based Access Control using Ontology. , 2013, , .		1
88	Detection and prevention mechanism for Blackhole attack in Wireless Sensor Network. , 2013, , .		40
89	A cluster based intrusion detection and prevention technique for misdirection attack inside WSN. , 2013, , .		8
90	A framework for detection and prevention of novel keylogger spyware attacks. , 2013, , .		21

#	Article	IF	Citations
91	E-TCP for efficient performance of MANET under JF delay variance attack. , 2013, , .		11
92	TBESP algorithm for Wireless Sensor Network under Blackhole attack. , 2013, , .		1
93	Performance of a LAN under different ethernet wiring standards. , 2012, , .		1
94	Cluster and super cluster based intrusion detection and prevention techniques for JellyFish Reorder Attack. , 2012, , .		8
95	Comparative performance analysis of routing protocols in mobile ad hoc networks under JellyFish attack. , 2012, , .		7
96	Performance Evaluation of a LAN under Different Ethernet Wiring Standards with Different Frame Size. International Journal of Computer Applications, 2012, 43, 7-12.	0.2	3
97	Authentication protocols for the internet of drones: taxonomy, analysis and future directions. Journal of Ambient Intelligence and Humanized Computing, 0, , 1.	4.9	43