A Survey of Man In The Middle Attacks

IEEE Communications Surveys and Tutorials
18, 2027-2051
DOI: 10.1109/comst.2016.2548426

Citation Report

#	Article	IF	Citations
1	A Survey on Intelligent MAC Layer Jamming Attacks and Countermeasures in WSNs. , 2016, , .		14
2	Authentication Techniques for the Internet of Things: A Survey. , 2016, , .		46
3	Privacy-Preserving Schemes for Ad Hoc Social Networks: A Survey. IEEE Communications Surveys and Tutorials, 2017, 19, 3015-3045.	24.8	103
4	A Secure, Out-of-Band, Mechanism to Manage Internet of Things Devices. Lecture Notes in Computer Science, 2017, , 79-90.	1.0	0
5	VuRLE: Automatic Vulnerability Detection and Repair by Learning from Examples. Lecture Notes in Computer Science, 2017, , 229-246.	1.0	30
6	Capacity- and Trust-Aware BS Cooperation in Nonuniform HetNets: Spectral Efficiency and Optimal BS Density. IEEE Transactions on Vehicular Technology, 2017, 66, 11317-11329.	3.9	6
7	Keep Pies Away from Kids. , 2017, , .		3
8	Can MPTCP secure Internet communications from man-in-the-middle attacks?. , 2017, , .		5
9	Secret key generation based on private pilot under man-in-the-middle attack. Science China Information Sciences, 2017, 60, 1.	2.7	2
10	Security Smells in Android. , 2017, , .		34
11	TLSsem: A TLS Security-Enhanced Mechanism against MITM Attacks in Public WiFis. , 2017, , .		5
12	Two decades of SCADA exploitation: A brief history. , 2017, , .		41
13	Smart input: Provide mouse and keyboard input to a PC from android devices. , 2017, , .		0
14	A New Method to Analyze the Security of Protocol Implementations Based on Ideal Trace. Security and Communication Networks, 2017, 2017, 1-15.	1.0	0
15	Authentication Protocols for Internet of Things: A Comprehensive Survey. Security and Communication Networks, 2017, 2017, 1-41.	1.0	193
16	A Consensus Framework for Reliability and Mitigation of Zero-Day Attacks in IoT. Security and Communication Networks, 2017, 2017, 1-24.	1.0	22
17	Framework for Threat Analysis and Attack Modelling of Network Security Protocols. International Journal of Synthetic Emotions, 2017, 8, 62-75.	0.3	6
18	Distributed Calculation of Edge-Disjoint Spanning Trees for Robustifying Distributed Algorithms Against Man-in-the-Middle Attacks. IEEE Transactions on Control of Network Systems, 2018, 5, 1646-1656.	2.4	10

#	Article	IF	Citations
19	Anatomy of a Vulnerable Fitness Tracking System. , 2018, 2, 1-24.		41
20	Security for 5G Mobile Wireless Networks. IEEE Access, 2018, 6, 4850-4874.	2.6	200
21	A systematic review of data protection and privacy preservation schemes for smart grid communications. Sustainable Cities and Society, 2018, 38, 806-835.	5.1	73
22	Privacy-preserving wireless communications using bipartite matching in social big data. Future Generation Computer Systems, 2018, 87, 772-781.	4.9	112
23	Modeling and performance analysis of a new secure address resolution protocol. International Journal of Communication Systems, 2018, 31, e3433.	1.6	3
24	Security for 4G and 5G cellular networks: A survey of existing authentication and privacy-preserving schemes. Journal of Network and Computer Applications, 2018, 101, 55-82.	5.8	190
25	Comprehensive Assessment of Security Attack Detection Algorithms in Internet of Things. , 2018, , .		4
26	The Defense Against ARP Spoofing Attack Using Semi-Static ARP Cache Table. , 2018, , .		13
27	Key Management Using Combination of Diffieâ€“Hellman Key Exchange with AES Encryption. , 2018, , .		7
28	Personalized Shares in Visual Cryptography. Journal of Imaging, 2018, 4, 126.	1.7	1
29	Towards Security Aspects of Secret Key Transmission. , 2018, , .		1
30	A New Protocol for On-line User Authentication Based on 1 Out of n Types of Personal Data. , 2018, , .		0
31	A Botnet Detecting Infrastructure Using a Beneficial Botnet. , 2018, , .		3
32	Man-In-The-Middle Attacks in Vehicular Ad-Hoc Networks: Evaluating the Impact of Attackersâ€™ Strategies. Sensors, 2018, 18, 4040.	2.1	69
33	A Simulation Model for the Analysis of Security Attacks in Advanced Metering Infrastructure. , 2018, , .		4
34	Self-Organized Security Framework for WiGig WLAN against Attacks and Threats. , 2018, , .		0
35	Real-World Man-in-the-Middle (MITM) Attack Implementation Using Open Source Tools for Instructional Use. , 2018, , .		13
36	Man-in-the-Middle (MITM) Attack Based Hijacking of HTTP Traffic Using Open Source Tools. , 2018, , .		23

#	Article	IF	Citations
37	Walls Have Ears: Traffic-based Side-channel Attack in Video Streaming. , 2018, , .		28
38	Fog orchestration for the Internet of Everything: state-of-the-art and research challenges. Journal of Internet Services and Applications, 2018, 9, .	1.6	65
39	A Survey of Protocol-Level Challenges and Solutions for Distributed Energy Resource Cyber-Physical Security. Energies, 2018, 11, 2360.	1.6	37
40	Adding Salt to Pepper. , 2018, , .		25
41	Survey of Identity-Based Attacks Detection Techniques in Wireless Networks Using Received Signal Strength. , 2018, , .		3
42	Support Vector Machine Detection of Data Framing Attack in Smart Grid. , 2018, , .		3
43	Detection of Man In The Middle Attacks in Wi-Fi networks by IP Spoofing. , 2018, , .		0
44	Beam-Stealing. , 2018, , .		18
46	Challenges of Securing the Industrial Internet of Things Value Chain. , 2018, , .		23
47	AITSteg: An Innovative Text Steganography Technique for Hidden Transmission of Text Message via Social Media. IEEE Access, 2018, 6, 65981-65995.	2.6	40
48	A Critical Review of Practices and Challenges in Intrusion Detection Systems for IoT: Toward Universal and Resilient Systems. IEEE Communications Surveys and Tutorials, 2018, 20, 3496-3509.	24.8	143
49	Information Security in the Smart Grid: Survey and Challenges. Communications in Computer and Information Science, 2018, , 55-66.	0.4	4
51	5G Security Artifacts (DoS / DDoS and Authentication). , 2019, , .		16
52	Design and Formal Analysis of an Authentication Protocol, eWMDP on Wearable Devices. IEEE Access, 2019, 7, 97771-97783.	2.6	1
53	BUS: A Blockchain-Enabled Data Acquisition Scheme With the Assistance of UAV Swarm in Internet of Things. IEEE Access, 2019, 7, 103231-103249.	2.6	69
54	10 Years of IoT Malware: A Feature-Based Taxonomy. , 2019, , .		37
55	Toward a Hardware Man-in-the-Middle Attack on PCIe Bus for Smart Data Replay. , 2019, , .		5
56	A Model for Availability and Security Risk Evaluation for Systems With VMM Rejuvenation Enabled by VM Migration Scheduling. IEEE Access, 2019, 7, 138315-138326.	2.6	12

#	Article	IF	Citations
57	MIMIC: a Cybersecurity Threat Turns into a Fog Computing Agent for IoT Systems. , 2019, , .		1
58	HEHLKAPPE. , 2019, , .		2
59	Bibliographical review on cyber attacks from a control oriented perspective. Annual Reviews in Control, 2019, 48, 103-128.	4.4	79
60	MPTCP robustness against large-scale man-in-the-middle attacks. Computer Networks, 2019, 164, 106896.	3.2	5
61	Network Intrusion Detection for IoT Security Based on Learning Techniques. IEEE Communications Surveys and Tutorials, 2019, 21, 2671-2701.	24.8	511
62	Cyber-Physical Vulnerability Analysis of Communication-Based Train Control. IEEE Internet of Things Journal, 2019, 6, 6353-6362.	5.5	38
63	A survey on the Internet of Things security. Information and Computer Security, 2019, 27, 292-323.	1.5	36
64	TLS/PKI Challenges and Certificate Pinning Techniques for IoT and M2M Secure Communications. IEEE Communications Surveys and Tutorials, 2019, 21, 3502-3531.	24.8	29
65	Security for 5G and Beyond. IEEE Communications Surveys and Tutorials, 2019, 21, 3682-3722.	24.8	227
66	Traffic-Based Side-Channel Attack in Video Streaming. IEEE/ACM Transactions on Networking, 2019, 27, 972-985.	2.6	20
67	Fine-grained access control method for private data in android system. International Journal of Distributed Sensor Networks, 2019, 15, 155014771984023.	1.3	0
68	Intelligent Threat Hunting in Software-Defined Networking. , 2019, , .		6
69	Man-in-the-middle-attack: Understanding in simple words. International Journal of Data and Network Science, 2019, , 77-92.	3.4	38
70	IoTsafe, Decoupling Security From Applications for a Safer IoT. IEEE Access, 2019, 7, 29942-29962.	2.6	9
71	Context-Aware Intelligence in Resource-Constrained IoT Nodes: Opportunities and Challenges. IEEE Design and Test, 2019, 36, 7-40.	1.1	45
72	A Survey on malware analysis and mitigation techniques. Computer Science Review, 2019, 32, 1-23.	10.2	116
73	Assessing Architectural Patterns Trade-offs using Moment-based Pattern Taxonomies. , 2019, , .		1
74	AECC: An Enhanced Public Key Cryptosystem for User Defined Messages. , 2019, , .		1

#	Article	IF	Citations
75	Anomalous Sensor Detection Based on Nonlinear Graph Filter. , 2019, , .		0
76	Performance Analysis of Denial of Service DoS and Distributed DoS Attack of Application and Network Layer of IoT. , 2019, , .		6
77	Exploring Severity Ranking of Cyber-Attacks in Modern Power Grid. , 2019, , .		3
78	Design-for-Trust Technique for Microfluidic Biochip Layout. , 2019, , .		4
79	Simple Prevention of Advanced Stealth Man-in-The-Middle Attack in WPA2 Wi-Fi Networks. , 2019, , .		1
80	An Overview About Detection of Cyber-Attacks on Power SCADA Systems. , 2019, , .		2
81	3. Threat analysis and attack modeling for machine-to-machine communication toward Internet of things. , 2019, , 45-72.		1
82	Mitigating ARP Cache Poisoning Attack in Software-Defined Networking (SDN): A Survey. Electronics (Switzerland), 2019, 8, 1095.	1.8	10
83	The Current Research of IoT Security. , 2019, , .		15
84	ICS-SEA. , 2019, , .		4
85	Modified RAP-WOTA for Preventing Man in the Middle and Replay Attacks. , 2019, , .		1
86	Cybersecurity in the Power Electronics. IEEE Latin America Transactions, 2019, 17, 1300-1308.	1.2	3
87	A High Throughput and Secure Authentication-Encryption AES-CCM Algorithm on Asynchronous Multicore Processor. IEEE Transactions on Information Forensics and Security, 2019, 14, 1023-1036.	4.5	20
88	Vesper: Using Echo Analysis to Detect Man-in-the-Middle Attacks in LANs. IEEE Transactions on Information Forensics and Security, 2019, 14, 1638-1653.	4.5	18
89	Multilayer Data-Driven Cyber-Attack Detection System for Industrial Control Systems Based on Network, System, and Process Data. IEEE Transactions on Industrial Informatics, 2019, 15, 4362-4369.	7.2	200
90	SRASA: a Generalized Theoretical Framework for Security and Reliability Analysis in Computing Systems. Journal of Hardware and Systems Security, 2019, 3, 200-218.	0.8	0
91	Detection of malicious and low throughput data exfiltration over the DNS protocol. Computers and Security, 2019, 80, 36-53.	4.0	80
92	Securing a Network: How Effective Using Firewalls and VPNs Are?. Lecture Notes in Networks and Systems, 2020, , 1050-1068.	0.5	6

#	Article	IF	Citations
93	Hidden the true identity and dating characteristics based on quick private matching in mobile social networks. Future Generation Computer Systems, 2020, 109, 633-641.	4.9	6
94	A Secure Stop and Wait Communication Protocol for Disturbed Networks. Wireless Personal Communications, 2020, 110, 861-872.	1.8	15
95	Address Resolution Protocol Based Attacks: Prevention and Detection Schemes. Lecture Notes on Data Engineering and Communications Technologies, 2020, , 247-256.	0.5	0
96	Internet of Things: Evolution and technologies from a security perspective. Sustainable Cities and Society, 2020, 54, 101728.	5.1	90
98	Toward a hardware man-in-the-middle attack on PCIe bus. Microprocessors and Microsystems, 2020, 77, 103198.	1.8	10
99	Bloccess: Towards Fine-Grained Access Control Using Blockchain in a Distributed Untrustworthy Environment. , 2020, , .		12
100	A Privacy Preserving Model for Fog-enabled MCC systems using 5G Connection. , 2020, , .		2
101	Man-in-the-Middle Attacks to Detect and Identify Services in Encrypted Network Flows using Machine Learning. , 2020, , .		6
102	Security Vulnerabilities of Server-Centric Wireless Datacenters. , 2020, , .		3
103	A Study of Routing Protocols, Security Issues and Attacks in Network Layer of Internet of Things Framework. , 2020, , .		5
104	IoT security with Deep Learning-based Intrusion Detection Systems: A systematic literature review. , 2020, , .		24
105	EDISON: A Blockchain-based Secure and Auditable Orchestration Framework for Multi-domain Software Defined Networks. , 2020, , .		4
106	A Data-Centric Approach to Taming the Message Dissemination in the Internet of Vehicles. , 2020, , .		6
107	Fuzzy logic and Fog based Secure Architecture for Internet of Things (FLFSIoT). Journal of Ambient Intelligence and Humanized Computing, 2023, 14, 5903-5927.	3.3	16
109	Convolutional Neural Network Framework for Encrypted Image Classification in Cloud-Based ITS. IEEE Open Journal of Intelligent Transportation Systems, 2020, 1, 35-50.	2.6	16
110	Security Considerations for Internet of Things: A Survey. SN Computer Science, 2020, 1, 1.	2.3	75
111	A Localized Event-Driven Resilient Mechanism for Cooperative Microgrid Against Data Integrity Attacks. IEEE Transactions on Cybernetics, 2021, 51, 3687-3698.	6.2	27
112	Securing interim payments in construction projects through a blockchain-based framework. Automation in Construction, 2020, 118, 103284.	4.8	102

#	Article	IF	Citations
113	Universal Data Anomaly Detection via Inverse Generative Adversary Network. IEEE Signal Processing Letters, 2020, 27, 511-515.	2.1	14
114	Traffic Data Classification to Detect Man-in-the-Middle Attacks in Industrial Control System. , 2020, , .		17
115	Optimal Partial Feedback Attacks in Cyber-Physical Power Systems. IEEE Transactions on Automatic Control, 2020, 65, 3919-3926.	3.6	41
116	IoT Privacy and Security: Challenges and Solutions. Applied Sciences (Switzerland), 2020, 10, 4102.	1.3	307
117	Man-in-the-Middle Attack Detection and Localization Based on Cross-Layer Location Consistency. IEEE Access, 2020, 8, 103860-103874.	2.6	12
118	Two-Way Physical Layer Security Protocol for Gaussian Channels. IEEE Transactions on Communications, 2020, 68, 3068-3078.	4.9	10
119	Short-Range Audio Channels Security: Survey of Mechanisms, Applications, and Research Challenges. IEEE Communications Surveys and Tutorials, 2021, 23, 311-340.	24.8	6
120	KORGAN: An Efficient PKI Architecture Based on PBFT Through Dynamic Threshold Signatures. Computer Journal, 2021, 64, 564-574.	1.5	3
121	Multilayer Resilience Paradigm Against Cyber Attacks in DC Microgrids. IEEE Transactions on Power Electronics, 2021, 36, 2522-2532.	5.4	49
122	Detection, estimation, and compensation of false data injection attack for UAVs. Information Sciences, 2021, 546, 723-741.	4.0	36
123	A review on lightweight cryptography for Internet-of-Things based applications. Journal of Ambient Intelligence and Humanized Computing, 2021, 12, 8835-8857.	3.3	20
124	Context-Bound Cybersecurity Framework for Resisting Eavesdropping in Vehicle Networks. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, 2021, , 519-536.	0.2	0
125	Internet of Things Security: A Survey. Communications in Computer and Information Science, 2021, , 95-117.	0.4	23
126	On the Feasibility of DoS Attack on Smart Door Lock IoT Network. Communications in Computer and Information Science, 2021, , 123-138.	0.4	1
127	<i>Inmap-t</i>: Leveraging TTCN-3 to Test the Security Impact of Intra Network Elements. Journal of Computer and Communications, 2021, 09, 174-190.	0.6	0
128	Attacks on Formation Control for Multiagent Systems. IEEE Transactions on Cybernetics, 2022, 52, 12805-12817.	6.2	36
129	Orchestration or Automation: Authentication Flaw Detection in Android Apps. IEEE Transactions on Dependable and Secure Computing, 2022, 19, 2165-2178.	3.7	2
130	A Security Analysis of Blockchain-Based Did Services. IEEE Access, 2021, 9, 22894-22913.	2.6	15

#	Article	IF	Citations
131	Combating Adversarial Network Topology Inference by Proactive Topology Obfuscation. IEEE/ACM Transactions on Networking, 2021, 29, 2779-2792.	2.6	7
132	Secure Distributed Estimation Against Data Integrity Attacks in Internet-of-Things Systems. IEEE Transactions on Automation Science and Engineering, 2022, 19, 2552-2565.	3.4	6
133	Detecting Man-in-the-Middle Attack in Fog Computing for Social Media. Computers, Materials and Continua, 2021, 69, 1159-1181.	1.5	6
134	Consumer, Commercial, and Industrial IoT (In)Security: Attack Taxonomy and Case Studies. IEEE Internet of Things Journal, 2022, 9, 199-221.	5.5	57
135	Design-for-Trust Techniques for Digital Microfluidic Biochip Layout with Error Control Mechanism. IEEE/ACM Transactions on Computational Biology and Bioinformatics, 2021, PP, 1-1.	1.9	4
136	Control Home Appliances Through Internet of Things To Assist Elderly In Their Daily Routine. MATEC Web of Conferences, 2021, 335, 04005.	0.1	1
137	Effect Man-In the Middle on the Network Performance in Various Attack Strategies. SSRN Electronic Journal, 0, , .	0.4	1
138	DECâ€ŁADE: Dual elliptic curveâ€based lightweight authentication and data encryption scheme for resource constrained smart devices. IET Wireless Sensor Systems, 2021, 11, 91-109.	1.3	4
139	MLSNet: A Policy Complying Multilevel Security Framework for Software Defined Networking. IEEE Transactions on Network and Service Management, 2021, 18, 729-744.	3.2	9
140	A Traceable and Authenticated IoTs Trigger Event of Private Security Record Based on Blockchain. Applied Sciences (Switzerland), 2021, 11, 2843.	1.3	1
141	Secure Key Exchange by NFC for Instant Messaging. , 2021, , .		2
142	Enhancing security using digital signature in an efficient Network Coding-enabled WSN. , 2021, , .		2
143	A system dynamics, epidemiological approach for high-level cyber-resilience to zero-day vulnerabilities. Journal of Simulation, 2023, 17, 1-16.	1.0	2
144	Browser-in-the-Middle (BitM) attack. International Journal of Information Security, 2022, 21, 179-189.	2.3	7
145	Softwarized IoT Network Immunity Against Eavesdropping With Programmable Data Planes. IEEE Internet of Things Journal, 2021, 8, 6578-6590.	5.5	22
146	Contact-tracing applications: a review of technologies. BMJ Innovations, 2021, 7, 368-378.	1.0	7
147	TTAS: Trusted Token Authentication Service of Securing SCADA Network in Energy Management System for Industrial Internet of Things. Sensors, 2021, 21, 2685.	2.1	8
148	Security-Oriented Network Architecture. Security and Communication Networks, 2021, 2021, 1-16.	1.0	0

#	Article	IF	Citations
149	Security model for protecting intellectual property of state-of-the-art microfluidic biochips. Journal of Information Security and Applications, 2021, 58, 102773.	1.8	1
150	Zero Conf Protocols and their numerous Man in the Middle (MITM) Attacks. , 2021, , .		3
151	Security Measures with Enhanced Behavior Processing and Footprint Algorithm against Sybil and Bogus Attacks in Vehicular Ad Hoc Network. Sensors, 2021, 21, 3538.	2.1	8
152	LightningStrike. , 2021, , .		4
153	Machine-Learning-Enabled Intrusion Detection System for Cellular Connected UAV Networks. Electronics (Switzerland), 2021, 10, 1549.	1.8	46
154	A Survey on Machine-Learning Based Security Design for Cyber-Physical Systems. Applied Sciences (Switzerland), 2021, 11, 5458.	1.3	25
155	Cyber Security Issues and Awareness Training at Universities. BiliÅŸim Teknolojileri Dergisi, 2021, 14, 229-238.	0.2	3
156	A Profiling Based Approach To Detect ARP Poisioning Attacks. , 2021, , .		1
157	Blockchain technology and IoT-edge framework for sharing healthcare services. Soft Computing, 2021, 25, 13753-13777.	2.1	16
158	Is 5G Handover Secure and Private? A Survey. IEEE Internet of Things Journal, 2021, 8, 12855-12879.	5.5	25
159	An improved NFC device authentication protocol. PLoS ONE, 2021, 16, e0256367.	1.1	4
160	Attack Categorisation for IoT Applications in Critical Infrastructures, a Survey. Applied Sciences (Switzerland), 2021, 11, 7228.	1.3	10
161	A nationwide census on wifi security threats. , 2021, , .		6
162	Internet of Things Security: Challenges and Key Issues. Security and Communication Networks, 2021, 2021, 1-11.	1.0	34
163	The rogue access point identification: a model and classification review. Indonesian Journal of Electrical Engineering and Computer Science, 2021, 23, 1527.	0.7	1
164	A distributed communication framework for smart Grid control applications based on data distribution service. Electric Power Systems Research, 2021, 201, 107547.	2.1	3
165	Parameter tampering cyberattack and event-trigger detection in game-based interactive demand response. International Journal of Electrical Power and Energy Systems, 2022, 135, 107550.	3.3	4
166	IDrISS: Intrusion Detection for IT Systems Security : Toward a semantic modelling of side-channel signals. , 2021, , .		0

#	Article	IF	Citations
167	Hash Authentication VANETS Message (HAVM) Against Message Tampered (MITM Attack). Smart Innovation, Systems and Technologies, 2021, , 258-265.	0.5	0
168	Business Transaction Privacy and Security Issues in Near Field Communication. , 2021, , 829-847.		0
169	A Research of MITM Attacks in Wi-Fi Networks Using Single-board Computer. , 2021, , .		4
170	How to make key 5G wireless technologies environmental friendly: A review. Transactions on Emerging Telecommunications Technologies, 2018, 29, e3254.	2.6	40
171	MITM Intrusion Analysis for Advanced Metering Infrastructure Communication in a Smart Grid Environment. Communications in Computer and Information Science, 2020, , 256-267.	0.4	5
172	On the Integrity of Cross-Origin JavaScripts. IFIP Advances in Information and Communication Technology, 2018, , 385-398.	0.5	3
173	A New Method for Preventing Man-in-the-Middle Attack in IPv6 Network Mobility. Lecture Notes in Electrical Engineering, 2020, , 211-220.	0.3	3
174	Prediction-based secured handover authentication for mobile cloud computing. Wireless Networks, 2020, 26, 4657-4675.	2.0	6
175	Security on ROS: analyzing and exploiting vulnerabilities of ROS-based systems. , 2020, , .		12
176	Threats to Online Advertising and Countermeasures. Digital Threats Research and Practice, 2020, 1, 1-27.	1.7	14
177	Secure key generation and distribution scheme based on two independent local polarization scramblers. Applied Optics, 2021, 60, 147.	0.9	6
178	Business Transaction Privacy and Security Issues in Near Field Communication. Advances in Information Security, Privacy, and Ethics Book Series, 2019, , 72-90.	0.4	5
179	An Effective Lightweight Cryptographic Algorithm to Secure Internet of Things Devices. Lecture Notes in Networks and Systems, 2022, , 403-419.	0.5	2
180	Sensors for Context-Aware Smart Healthcare: A Security Perspective. Sensors, 2021, 21, 6886.	2.1	23
181	Why Hackers Love eHealth Applications. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, 2016, , 58-63.	0.2	1
182	Smart-Lock Security Re-engineered Using Cryptography and Steganography. Communications in Computer and Information Science, 2017, , 325-336.	0.4	4
183	Exploit in Smart Devices: A Case Study. Communications in Computer and Information Science, 2019, , 152-164.	0.4	0
185	Smart Cities and Open WiFis: When Android OS Permissions Cease to Protect Privacy. Lecture Notes in Computer Science, 2019, , 457-467.	1.0	0

#	Article	IF	Citations
186	A System Dynamics, Epidemiological Approach for High-Level Cyber-Resilience to Zero-Day Vulnerabilities. SSRN Electronic Journal, 0, , .	0.4	0
187	Image-Based Ciphering of Video Streams and Object Recognition for Urban and Vehicular Surveillance Services. Advances in Intelligent Systems and Computing, 2020, , 519-527.	0.5	0
188	Security and Privacy Challenges in Upcoming Intelligent Urban Micromobility Transportation Systems. , 2020, , .		6
189	ARP Spoofing Analysis and Prevention. , 2020, , .		5
190	Deep Q learning-based mitigation of man in the middle attack over secure sockets layer websites. Modern Physics Letters B, 2020, 34, 2050366.	1.0	1
191	A scalable and secure model for surveillance cameras in resource constrained IoT systems. , 2020, , .		0
192	Health Access Broker: Secure, Patient-Controlled Management of Personal Health Records in the Cloud. Advances in Intelligent Systems and Computing, 2021, , 111-121.	0.5	3
193	Transmission of Encrypted data in WSN: An Implementation of Hybridized RSA-TDES Algorithm. , 2020, , .		1
194	Applying an Energy-Aware Security Mechanism in Healthcare Internet of Things. , 2020, , .		0
195	Framework for Threat Analysis and Attack Modelling of Network Security Protocols. , 2020, , 110-124.		0
196	Technical and Behavioural Training and Awareness Solutions for Mitigating Ransomware Attacks. Advances in Intelligent Systems and Computing, 2020, , 164-176.	0.5	3
197	Security Measures in Vehicular Ad-Hoc Networks on the Example of Bogus and Sybil Attacks. Advances in Intelligent Systems and Computing, 2020, , 419-430.	0.5	1
198	Wireless Environment Security. Advances in Information Security, Privacy, and Ethics Book Series, 2020, , 65-83.	0.4	0
199	Diagnosis of Communication Security Vulnerability of Network Printer Using Wireshark. Journal of Digital Contents Society, 2020, 21, 601-607.	0.1	0
200	Threat landscape for smart grid systems. , 2020, , .		10
201	Man in the Middle Attacks: Analysis, Motivation and Prevention. International Journal of Computer Networks and Communications Security, 2020, 8, 52-58.	0.6	14
203	Situational awareness and public Wi-Fi usersâ€™ self-protective behaviors. Security Journal, 2022, 35, 154-174.	1.0	4
204	Security Threats in Wireless Network Communication-Status, Challenges, and Future Trends. , 2021, , .		15

#	Article	IF	Citations
205	Stability Investigation of DC Microgrids Under Stealth Cyber Attacks. , 2021, , .		3
206	Radio Frequency Fingerprinting for Frequency Hopping Emitter Identification. Applied Sciences (Switzerland), 2021, 11, 10812.	1.3	6
209	RealSWATT: Remote Software-based Attestation for Embedded Devices under Realtime Constraints. , 2021, , .		5
210	To track or not to track: examining perceptions of online tracking for information behavior research. Internet Research, 2022, 32, 260-279.	2.7	8
211	Pluggable Authentication Module Meets Identity-Based Identification. Communications in Computer and Information Science, 2021, , 155-175.	0.4	2
212	Secure Control of DC Microgrids for Instant Detection and Mitigation of Cyber-Attacks Based on Artificial Intelligence. IEEE Systems Journal, 2022, 16, 2580-2591.	2.9	20
213	Blockchain-Assisted Conditional Anonymity Privacy-Preserving Public Auditing Scheme With Reward Mechanism. IEEE Systems Journal, 2022, 16, 4477-4488.	2.9	12
214	Converter-Based Moving Target Defense Against Deception Attacks in DC Microgrids. IEEE Transactions on Smart Grid, 2022, 13, 3984-3996.	6.2	31
215	Development of an Intrusion Detection System Using a Botnet with the R Statistical Computing System. , 2020, , .		0
216	A Linear Regression Based Resilient Optimal Operation of AC Microgrids. , 2020, , .		1
217	Global Internet Traffic Routing and Privacy. , 2020, , .		0
218	Edge IoT-cloud Framework based on Blockchain. , 2020, , .		2
219	Foggy: A New Anonymous Communication Architecture Based on Microservices. , 2020, , .		0
220	Probabilistic Modeling and Study of Cybersecurity Attacks in Industrial Control Systems of Plants. , 2020, , .		2
221	Machine Learning-based PHY-authentication for Mobile OFDM Transceivers. , 2020, , .		0
222	A Systematic Approach Towards Compromising Remote Site HTTPS Traffic Using Open Source Tools. , 2020, , .		1
223	MitM Tool Analysis for TLS Forensics. , 2021, , .		5
224	Detection and Inference of Randomness-based Behavior for Resilient Multi-vehicle Coordinated Operations. , 2021, , .		2

#	Article	IF	Citations
225	Protection of Biometric Data Transmission and Storage in the Human State Remote Monitoring Tools. , 2021, , .		1
226	Various Threats and Challenges to Information Security via Active and Passive Attack. , 2021, , .		0
227	Man-In-The-Middle Attack Based on ARP Spoofing in IoT Educational Platform. , 2021, , .		5
228	Data Tampering Attack Design for ROS-Based Object Detection and Tracking Robotic Platform. , 2021, , .		0
230	Modern Authentication Schemes in Smartphones and IoT Devices: An Empirical Survey. IEEE Internet of Things Journal, 2022, 9, 7639-7663.	5.5	4
231	Detection of Nonrandom Sign-Based Behavior for Resilient Coordination of Robotic Swarms. IEEE Transactions on Robotics, 2022, 38, 92-109.	7.3	5
232	A Survey of Physical Layer Techniques for Secure Wireless Communications in Industry. IEEE Communications Surveys and Tutorials, 2022, 24, 810-838.	24.8	43
233	E-Banking Security Studyâ€"10 Years Later. IEEE Access, 2022, 10, 16681-16699.	2.6	3
237	A Review of Security Concerns in Smart Grid. Lecture Notes on Data Engineering and Communications Technologies, 2022, , 125-140.	0.5	4
238	Detection of Man in The Middle Attack using Machine learning. , 2022, , .		6
240	Two-party quantum private comparison based on eight-qubit entangled state. Modern Physics Letters A, 2022, 37, .	0.5	16
241	Joint Trust Management and Sharing Provisioning in IoV-Based Urban Road Network. Wireless Communications and Mobile Computing, 2022, 2022, 1-18.	0.8	7
242	An extensive vulnerability assessment and countermeasures in open network operating system software defined networking controller. Concurrency Computation Practice and Experience, 2022, 34, .	1.4	4
243	Conformity Analysis of HTTP Strict Transport Security (HSTS) Configuration and Implementation Using Bettercap Tools. , 2021, , .		0
244	Towards Security and Privacy Preservation in 5G Networks. , 2021, , .		6
245	On Robustness of the Normalized Random Block Coordinate Method for Non-Convex Optimization. , 2021, , .		0
246	A Systematic Literature Review on the Cyber Security. International Journal of Scientific Research and Management, 2021, 9, 669-710.	0.0	26
247	Blockchain-Based Community Safety Security System with IoT Secure Devices. Sustainability, 2021, 13, 13994.	1.6	2

#	Article	IF	Citations
248	BIDAC: Blockchain-enabled Identity-Based Data Access Control in IoT. , 2021, , .		3
249	Attack and defence methods in cyberâ€physical power system. IET Energy Systems Integration, 2022, 4, 159-170.	1.1	13
250	D-CEWS: DEVS-Based Cyber-Electronic Warfare M&S Framework for Enhanced Communication Effectiveness Analysis in Battlefield. Sensors, 2022, 22, 3147.	2.1	7
252	Smart Grid Security and Privacy: From Conventional to Machine Learning Issues (Threats and) Tj ETQq1 1 0.784314 rgBT /Overlock 10	2.6	16
253	D-ARP: An Efficient Scheme to Detect and Prevent ARP Spoofing. IEEE Access, 2022, 10, 49142-49153.	2.6	11
254	Software-Defined Reconfigurable Intelligent Surfaces: From Theory to End-to-End Implementation. Proceedings of the IEEE, 2022, 110, 1466-1493.	16.4	15
255	Taxonomy and Future Threat of Rogue Access Point for Wireless Network. , 2022, , .		2
256	Evaluation and Selection Models for Ensemble Intrusion Detection Systems in IoT. IoT, 2022, 3, 285-314.	2.3	4
257	What you see is not what you get. , 2022, , .		0
258	Analysis and implementation of man-in-the-middle attack on Microsoft's PPTP. , 2022, , .		0
259	E-Voting: Security, Threats and Prevention. , 2021, , .		0
260	Authentication and Key Agreement Protocol for Secure Traffic Signaling in 5G Networks. , 2021, , .		3
261	SE-Loc: Security-Enhanced Indoor Localization With Semi-Supervised Deep Learning. IEEE Transactions on Network Science and Engineering, 2023, 10, 2964-2977.	4.1	4
263	An HTTP Anomaly Detection Architecture Based on the Internet of Intelligence. IEEE Transactions on Cognitive Communications and Networking, 2022, 8, 1552-1565.	4.9	1
264	SoK: Workerounds - Categorizing Service Worker Attacks and Mitigations. , 2022, , .		1
265	Detecting IKEv1 Man-in-the-Middle Attack with Message-RTT Analysis. Wireless Communications and Mobile Computing, 2022, 2022, 1-7.	0.8	0
266	A Survey on Network Security for Cyberâ€“Physical Systems: From Threats to Resilient Design. IEEE Communications Surveys and Tutorials, 2022, 24, 1534-1573.	24.8	23
267	OTOMATISASI KARMA ATTACK. , 2021, 15, 27-33.		0

#	Article	IF	Citations
268	Fingerprinting Technique for YouTube Videos Identification in Network Traffic. IEEE Access, 2022, 10, 76731-76741.	2.6	9
269	Security Issues and Challenges in Internet of Things (IOT) System. , 2022, , .		2
270	Security and Privacy Protection Obstacles with 3D Reconstructed Models of People in Applications and the Metaverse: A Survey. , 2022, , .		14
271	Man-in-the-Middle Attacks in Mobile Ad Hoc Networks (MANETs): Analysis and Evaluation. Symmetry, 2022, 14, 1543.	1.1	23
272	IIoT Malware Detection Using Edge Computing and Deep Learning for Cybersecurity in Smart Factories. Applied Sciences (Switzerland), 2022, 12, 7679.	1.3	12
273	An Anomaly Detection Method of Time Series Data for Cyber-Physical Integrated Energy System Based on Time-Frequency Feature Prediction. Energies, 2022, 15, 5565.	1.6	6
274	Multi-Channel Man-in-the-Middle attacks against protected Wi-Fi networks: A state of the art review. Expert Systems With Applications, 2022, 210, 118401.	4.4	7
275	An Overview of Recent Advances of Resilient Consensus for Multiagent Systems under Attacks. Computational Intelligence and Neuroscience, 2022, 2022, 1-26.	1.1	2
276	Examining the Suitability of NetFlow Features in Detecting IoT Network Intrusions. Sensors, 2022, 22, 6164.	2.1	10
277	Edge computing-enabled secure and energy-efficient smart parking: A review. Microprocessors and Microsystems, 2022, 93, 104612.	1.8	6
278	A Systemic Security and Privacy Review: Attacks and Prevention Mechanisms Over IoT Layers. Studies in Big Data, 2022, , 69-89.	0.8	0
279	A Decentralised Blockchain-Based Secure Authentication Scheme for IoT Devices. Lecture Notes in Networks and Systems, 2022, , 123-144.	0.5	1
280	Cybersecurity of Smart Inverters in the Smart Grid: A Survey. IEEE Transactions on Power Electronics, 2023, 38, 2364-2383.	5.4	15
281	Detection and Mitigation of Data Tampering Attacks for Cooperative ACC Systems Based on C-V2X. , 2022, , .		1
282	A rule-based approach for detecting heartbleed cyber attacks. , 2022, , .		5
283	Machine and Deep Learning for IoT Security and Privacy: Applications, Challenges, and Future Directions. Security and Communication Networks, 2022, 2022, 1-41.	1.0	9
284	<scp>LGuard</scp> : Securing Enterprise-IoT Systems against Serial-Based Attacks via Proprietary Communication Buses. Digital Threats Research and Practice, 2023, 4, 1-26.	1.7	0
285	Digital Forensic Case Studies for In-Vehicle Infotainment Systems Using Android Auto and Apple CarPlay. Sensors, 2022, 22, 7196.	2.1	7

#	Article	IF	Citations
286	Bloccess: Enabling Fine-Grained Access Control Based on Blockchain. Journal of Network and Systems Management, 2023, 31, .	3.3	5
287	Employing Public Key Infrastructure to Encapsulate Messages During Transport Layer Security Handshake Procedure. , 2022, , .		0
288	LEMMAS: a secured and trusted Local Energy Market simulation system. , 2022, , .		1
289	Synthesis of Evidence on Existing and Emerging Social Engineering Ransomware Attack Vectors. Advances in Information Security, Privacy, and Ethics Book Series, 2022, , 234-254.	0.4	0
290	A comprehensive survey on online social networks security and privacy issues: Threats, machine learningâ€based solutions, and open challenges. Security and Privacy, 2023, 6, .	1.9	5
291	Resilient Operation of BESS in a Cooperative DC Microgrid under Data Manipulation Attacks. , 2022, , .		2
292	The Insider Threat Landscape and the FinTech Sector. Advances in Information Security, Privacy, and Ethics Book Series, 2022, , 65-90.	0.4	0
293	CovertSYS: A systematic covert communication approach for providing secure end-to-end conversation via social networks. Journal of Information Security and Applications, 2022, 71, 103368.	1.8	1
294	CTB-PKI: Clustering and Trust Enabled Blockchain Based PKI System for Efficient Communication in P2P Network. IEEE Access, 2022, 10, 124277-124290.	2.6	1
295	Private 5G networks: a survey on enabling technologies, deployment models, use cases and research directions. Telecommunication Systems, 2023, 82, 3-26.	1.6	12
296	Reinforcement Learning-Based Physical Cross-Layer Security and Privacy in 6G. IEEE Communications Surveys and Tutorials, 2023, 25, 425-466.	24.8	21
297	A Systematic Security Assessment and Review of Internet of Things in the Context of Authentication. Computers and Security, 2023, 125, 103053.	4.0	5
298	An Efficient Authenticated Group Key Agreement Protocol withÂDynamic Batch Verification forÂSecure Distributed Networks. Lecture Notes in Computer Science, 2022, , 305-318.	1.0	0
299	RokuControl-Conducting MITM Attacks on Roku. , 2022, , .		1
300	Twin-Node Neighbour Attack on AODV based Wireless Ad Hoc Network. International Journal of Computer Networks and Communications, 2022, 14, 99-113.	0.3	0
301	Identification of the Issues in IoT Devices with HSTS Not Enforced and Their Exploitation. Smart Innovation, Systems and Technologies, 2023, , 325-334.	0.5	1
302	A new method for privacy preserving association rule mining using homomorphic encryption with a secure communication protocol. Wireless Networks, 2023, 29, 1197-1212.	2.0	3
303	Information Protection in Complexes with Unmanned Aerial Vehicles Using Moving Target Technology. Inventions, 2023, 8, 18.	1.3	1

#	Article	IF	Citations
304	False Data Injection Attacks against Low Voltage Distribution Systems. , 2022, , .		3
305	Evasion-Aware Neyman-Pearson Detectors: A Game-Theoretic Approach. , 2022, , .		1
306	Security and Integrity Attacks in Named Data Networking: A Survey. IEEE Access, 2023, 11, 7984-8004.	2.6	4
307	Resilient Economical Operation of DC Microgrid Clusters with Heterogeneous Sources. , 2022, , .		1
308	Real Time Modeling, Co-Simulation and Cyber-Physical Analysis for DC Microgrid Clusters. , 2022, , .		1
309	Detection and Mitigation of IoT-Based Attacks Using SNMP and Moving Target Defense Techniques. Sensors, 2023, 23, 1708.	2.1	4
310	A survey on security and privacy issues of UAVs. Computer Networks, 2023, 224, 109626.	3.2	25
311	Combating Nationwide WiFi Security Threats. , 2023, , 191-219.		0
312	Cybersecurity Risks Mitigation in the Internet of Things. , 2022, , .		5
313	A review on cyber security. AIP Conference Proceedings, 2023, , .	0.3	1
314	Use of Machine Learning in Interactive Cybersecurity and Network Education. Sensors, 2023, 23, 2977.	2.1	0
315	A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions. Electronics (Switzerland), 2023, 12, 1333.	1.8	28
316	A Network Traffic Anomaly Detection Method Based on Gaussian Mixture Model. Electronics (Switzerland), 2023, 12, 1397.	1.8	2
317	TLS-Monitor: A Monitor for TLS Attacks. , 2023, , .		4
318	D-Shield: Enabling Processor-side Encryption and Integrity Verification for Secure NVMe Drives. , 2023, , .		0
319	Difficulties and Potential Ulnerabilities in the IOT Architecture. , 2023, , .		0
320	Impact, Vulnerabilities, and Mitigation Strategies for Cyber-Secure Critical Infrastructure. Sensors, 2023, 23, 4060.	2.1	9
321	Prioritizing the multi-criterial features based on comparative approaches for enhancing security of IoT devices. Physical Communication, 2023, 59, 102084.	1.2	6

#	Article	IF	Citations
322	SDSCCM. Advances in Information Security, Privacy, and Ethics Book Series, 2023, , 200-214.	0.4	0
326	Threat Analysis of Position, Navigation, and Timing for Highly Automated Vehicles. , 2023, , .		0
335	On the (in)Security and Weaknesses of Commonly Used Applications on Large-Scale Distributed Systems. , 2023, , .		0
340	NetLoiter: A Tool for Automated Testing of Network Applications using Fault-injection. , 2023, , .		1
346	Grid-Metaverse: The Path From Digital Twins and Prototype Tests on DC Microgrids. , 2023, , .		0
349	A New Data Communication Method Using RSA and Steganography. Algorithms for Intelligent Systems, 2024, , 203-211.	0.5	0
353	Construct New Graphs Using Information Bottleneck Against Property Inference Attacks. , 2023, , .		0
360	Evaluation of Man-in-the-Middle Attacks and Countermeasures on Autonomous Vehicles. , 2023, , .		0
361	Comprehensive Study on Smart Solar Grid with Embedded System and IoT Technology. , 2023, , .		0
363	A Comprehensive Study on Unmanned Aerial Vehicle Security Issues. , 2023, , .		0
365	Design and Implementation Using Certificate Pinning for Smart Home Power Switch System. , 2023, , .		0
372	A Holistic Review on Detection of Malicious Browser Extensions and Links using Deep Learning. , 2024, , .		0
374	Cyber security challenges and solutions in protective relaying. , 2024, , 75-103.		0