

# CITATION REPORT

List of articles citing

## Cyber security of critical infrastructures

DOI: 10.1016/j.icte.2018.02.001  
ICT Express, 2018, 4, 42-45.

**Source:** <https://exaly.com/paper-pdf/68764193/citation-report.pdf>

**Version:** 2024-04-23

This report has been generated based on the citations recorded by exaly.com for the above article. For the latest version of this publication list, visit the link given above.

The third column is the impact factor (IF) of the journal, and the fourth column is the number of citations of the article.

#	Paper	IF	Citations
98	Prototyping a Lightweight Encryption on a Field Programmable Gate Array for Securing Tele-Control Data. <b>2018</b> ,		
97	Securing WirelessHART: Monitoring, Exploring and Detecting New Vulnerabilities. <b>2018</b> ,		3
96	Industrial IoT Monitoring: Technologies and Architecture Proposal. <i>Sensors</i> , <b>2018</b> , 18,	3.8	34
95	A Novel Hierarchical Intrusion Detection System Based on Decision Tree and Rules-Based Models. <b>2019</b> ,		57
94	Securing connection between IT and OT: the Fog Intrusion Detection System prospective. <b>2019</b> ,		3
93	Deep Reinforcement Learning Algorithms in Intelligent Infrastructure. <i>Infrastructures</i> , <b>2019</b> , 4, 52	2.6	8
92	Blockchain and Random Subspace Learning-Based IDS for SDN-Enabled Industrial IoT Security. <i>Sensors</i> , <b>2019</b> , 19,	3.8	65
91	Analysis of Botnet Domain Names for IoT Cybersecurity. <i>IEEE Access</i> , <b>2019</b> , 7, 94658-94665	3.5	16
90	Cyber Security: From Regulations and Policies to Practice. <i>Springer Proceedings in Business and Economics</i> , <b>2019</b> , 763-770	0.2	6
89	Securing SCADA-based Critical Infrastructures: Challenges and Open Issues. <i>Procedia Computer Science</i> , <b>2019</b> , 155, 612-617	1.6	10
88	Trends Review of the Contemporary Security Problems in the Cyberspace. <b>2019</b> ,		1
87	Authentication and Authorization for Mobile IoT Devices Using Biofeatures: Recent Advances and Future Trends. <i>Security and Communication Networks</i> , <b>2019</b> , 2019, 1-20	1.9	32
86	Detecting stealthy attacks against industrial control systems based on residual skewness analysis. <i>Eurasip Journal on Wireless Communications and Networking</i> , <b>2019</b> , 2019,	3.2	13
85	Machine learning in cybersecurity: A review. <i>Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery</i> , <b>2019</b> , 9, e1306	6.9	27
84	Nonlinear consensus for improved resilience of distributed secondary frequency control. <b>2019</b> ,		
83	Prospective Control Systems and Cyber-Securities for Electrical Secondary Substations. <b>2019</b> ,		
82	Protecting Civilians from Cyber Warfare with Cyber Buffer Zones. <i>International Journal of Smart Security Technologies</i> , <b>2019</b> , 6, 31-48	0.3	

81	Security and Fault Detection in In-node components of IIoT Constrained Devices. <b>2019</b> ,		3
80	An Enhanced Multi-Stage Semantic Attack Against Industrial Control Systems. <i>IEEE Access</i> , <b>2019</b> , 7, 156871-156882		3.5
79	A Survey on SCADA Security and Honeypot in Industrial Control System. <i>Advances in Intelligent Systems and Computing</i> , <b>2019</b> , 598-604	0.4	1
78	Teaching the process of building an Intrusion Detection System using data from a small-scale SCADA testbed. <i>Internet Technology Letters</i> , <b>2020</b> , 3, e132	1.3	5
77	Robustness of Optimal Investment Decisions in Mixed Insurance/Investment Cyber Risk Management. <i>Risk Analysis</i> , <b>2020</b> , 40, 550-564	3.9	7
76	Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. <i>Journal of Information Security and Applications</i> , <b>2020</b> , 50, 102419	3.5	194
75	Blockchain Signaling System (BloSS): Cooperative Signaling of Distributed Denial-of-Service Attacks. <i>Journal of Network and Systems Management</i> , <b>2020</b> , 28, 953-989	2.1	6
74	On Data Integrity Attacks against Industrial Internet of Things. <b>2020</b> ,		5
73	Cyber threats for operational technologies. <i>International Journal of System of Systems Engineering</i> , <b>2020</b> , 10, 128	0.3	0
72	Assessing Risk Potential of Critical Infrastructure of NPP: Fractal Analysis and Multiple-Scale Wavelet Transform. <b>2020</b> ,		0
71	Quantitative approach to physical protection systems assessment of critical infrastructure elements: Use case in the Slovak Republic. <i>International Journal of Critical Infrastructure Protection</i> , <b>2020</b> , 30, 100376	4.1	12
70	RDTIDS: Rules and Decision Tree-Based Intrusion Detection System for Internet-of-Things Networks. <i>Future Internet</i> , <b>2020</b> , 12, 44	3.3	49
69	Injecting failure: Data center infrastructures and the imaginaries of resilience. <i>Information Society</i> , <b>2020</b> , 36, 167-176	1.9	4
68	DIVDS: Docker Image Vulnerability Diagnostic System. <i>IEEE Access</i> , <b>2020</b> , 8, 42666-42673	3.5	11
67	Cyber security for fog-based smart grid SCADA systems: Solutions and challenges. <i>Journal of Information Security and Applications</i> , <b>2020</b> , 52, 102500	3.5	22
66	Usability of the CBEST Framework for Protection of Supervisory Control and Acquisition Data Systems (SCADA) in the Energy Sector. <i>Advanced Sciences and Technologies for Security Applications</i> , <b>2021</b> , 1-20	0.6	
65	Effective Detection of Cyber Attack in a Cyber-Physical Power Grid System. <i>Advances in Intelligent Systems and Computing</i> , <b>2021</b> , 812-829	0.4	0
64	Optimal Investment in Cyber-Security under Cyber Insurance for a Multi-Branch Firm. <i>Risks</i> , <b>2021</b> , 9, 24	1.6	0

63	A Secure Decentralized Spatial Crowdsourcing Scheme for 6G-Enabled Network in Box. <i>IEEE Transactions on Industrial Informatics</i> , <b>2021</b> , 1-1	11.9	5
62	Cyber Ranges and TestBeds for Education, Training, and Research. <i>Applied Sciences (Switzerland)</i> , <b>2021</b> , 11, 1809	2.6	8
61	A Novel Multiobjective GDWCN-PSO Algorithm and Its Application to Medical Data Security. <i>ACM Transactions on Internet Technology</i> , <b>2021</b> , 21, 1-28	3.8	12
60	Some Issues of Assessing the Risk Potential of Technological Process at Nuclear Power Plants. <b>2021</b> ,		0
59	Anomaly-Based Intrusion Detection System for Cyber-Physical System Security. <b>2021</b> ,		1
58	Identifying cyber insecurities in trustworthy space and energy sector for smart grids. <i>Computers and Electrical Engineering</i> , <b>2021</b> , 93, 107204	4.3	13
57	Investigation of Cyber-Attack Methods and Measures in Smart Grids. <i>Sakarya University Journal of Science</i> ,	0.3	0
56	Newly engineered energy-based features for supervised anomaly detection in a physical model of a water supply system. <i>Ad Hoc Networks</i> , <b>2021</b> , 120, 102590	4.8	
55	The Agile Incident Response for Industrial Control Systems (AIR4ICS) framework. <i>Computers and Security</i> , <b>2021</b> , 109, 102398	4.9	1
54	System-Wide Anomaly Detection of Industrial Control Systems via Deep Learning and Correlation Analysis. <i>IFIP Advances in Information and Communication Technology</i> , <b>2021</b> , 362-373	0.5	2
53	Cyberwarfare Associated Technologies and Countermeasures. <i>Advanced Sciences and Technologies for Security Applications</i> , <b>2020</b> , 23-36	0.6	1
52	Defending Critical Infrastructure: Insights from Recommender Systems. <i>Profiles in Operations Research</i> , <b>2020</b> , 193-206	1	1
51	Deep Learning Techniques for Cyber Security Intrusion Detection : A Detailed Analysis.		12
50	Akademiklerdeki Kritik Altyapıların Güvenli Uluslararası Metim Akademisi Dergisi, 51-63	0.3	2
49	Decision Tree Based Interference Recognition for Fog Enabled IOT Architecture. <i>Journal of Trends in Computer Science and Smart Technology</i> , <b>2020</b> , 2, 15-25	3.9	14
48	A modified densenet approach with nearmiss for anomaly detection in industrial control systems. <i>Multimedia Tools and Applications</i> , 1	2.5	
47	Optimization of the Novelty Detection Model Based on LSTM Autoencoder for ICS Environment. <i>Advances in Intelligent Systems and Computing</i> , <b>2019</b> , 306-319	0.4	1
46	SEconomy: A Framework for the Economic Assessment of Cybersecurity. <i>Lecture Notes in Computer Science</i> , <b>2019</b> , 154-166	0.9	5

45	Intrusion detection system on the basis of data mining algorithms in the industrial network. <i>CEUR Workshop Proceedings</i> , <b>2019</b> , 553-565	0.2	
44	Cybersecurity of Critical Infrastructure. <i>The International Library of Ethics, Law and Technology</i> , <b>2020</b> , 157-177	0.5	2
43	Predicci3n de ciberataques en sistemas industriales SCADA a trav3s de la implementaci3n del filtro Kalman. <i>Tecno L3gicas</i> , <b>2020</b> , 23, 249-267	0.6	0
42	Towards SCADA Threat Intelligence based on Intrusion Detection Systems - A Short Review. <b>2020</b> ,		3
41	Cyber Threat Extenuation for Substation Data Communication: Evaluation of Encrypt-Authenticator Prototype for IEC 60870B Data. <b>2020</b> ,		
40	Cybersecurity Policy Compliance in Higher Education: A Theoretical Framework. <i>Journal of Applied Security Research</i> , 1-22	0.9	
39	The Cost Perspective of Password Security. <i>Advances in Information Security, Privacy, and Ethics Book Series</i> , <b>2020</b> , 319-330	0.3	1
38	Machine Learning for Network Intrusion Detection Based on SVM Binary Classification Model. <i>Advances in Science, Technology and Engineering Systems</i> , <b>2020</b> , 5, 638-644	0.3	1
37	Cyber Threats in the Healthcare Sector and Countermeasures. <i>Advances in Business Strategy and Competitive Advantage Book Series</i> , <b>2020</b> , 109-124	0.3	
36	A Short Review: Issues and Threats Pertaining the Security of SCADA Systems. <i>Communications in Computer and Information Science</i> , <b>2021</b> , 230-247	0.3	0
35	Some aspects of critical information infrastructure risk management. <b>2021</b> ,		0
34	Cryptosystem using Facial Landmark for Authentication Pairing and Key Generation in Bluetooth Security. <b>2021</b> ,		
33	Don't get stung, cover your ICS in honey: How do honeypots fit within industrial control system security. <i>Computers and Security</i> , <b>2022</b> , 114, 102598	4.9	1
32	Lightweight Testbed for Cybersecurity Experiments in SCADA-based Systems. <b>2020</b> ,		1
31	Assessment of Machine Learning Techniques for Building an Efficient IDS. <b>2020</b> ,		
30	Survey on Cyber Security for Industrial Control Systems. <b>2021</b> ,		0
29	Threats and Opportunities in Digital Transformation in SMEs from the Perspective of Sustainability: A Case Study in the Czech Republic. <i>Sustainability</i> , <b>2022</b> , 14, 3628	3.6	1
28	Emerging Cybersecurity Capability Gaps in the Industrial Internet of Things: Overview and Research Agenda IIoT Capability Gaps. <i>Digital Threats Research and Practice</i> ,	1.5	

27	A Desktop Review of Security Techniques Applicable for Optimised Water Network. <b>2021</b> ,		
26	Determinants of Assurance Management System for Critical Asset: A Literature Review. <i>International Journal of Mathematical, Engineering and Management Sciences</i> , <b>2021</b> , 6, 1667-1693	1	
25	A survey on policies, modelling and security of cyber-physical systems in smart grids. <i>Energy Conversion and Economics</i> , <b>2021</b> , 2, 197-211	0.7	2
24	Adoption and Assessment of Machine Learning Algorithms in Security Operations Centre for Critical Infrastructure. <i>Lecture Notes in Electrical Engineering</i> , <b>2022</b> , 395-407	0.2	
23	An exploratory study of organizational cyber resilience, its precursors and outcomes. <i>Journal of Organizational Computing and Electronic Commerce</i> , 1-22	1.8	1
22	Analyzing and Evaluating Critical Cyber Security Challenges Faced by Vendor Organizations in Software Development: SLR Based Approach. <i>IEEE Access</i> , <b>2022</b> , 1-1	3.5	1
21	Interpreting cyber-energy-security events: experts, social imaginaries, and policy discourses around the 2016 Ukraine blackout. <i>European Security</i> , 1-21	1.3	
20	Development and application of the Information Security Core Human Error Causes (IS-CHEC) technique. <b>2022</b> , 267-295		
19	Emerging Challenges in Cyber Security. <i>Advances in Information Security, Privacy, and Ethics Book Series</i> , <b>2022</b> , 25-34	0.3	
18	Cyber Threats in the Healthcare Sector and Countermeasures. <b>2022</b> , 1-16		
17	Configuration vulnerability in SNORT for Windows Operating Systems. <b>2022</b> ,		
16	Cybersecurity in the Automotive Industry: A Systematic Literature Review (SLR). 1-19		
15	Cyberattack Measures in Smart Cities and Grids. <b>2023</b> , 117-131		0
14	Cybersecurity anatomization and assurance of industrial control systems. <b>2022</b> ,		0
13	Role of Computational Intelligence in Cybersecurity. <b>2022</b> , 127-137		0
12	Industrial control systems cybersecurity: Back to basic cyber hygiene practices. <b>2022</b> ,		0
11	Fuzzing ICS Protocols: Modbus Fuzzer Framework. <b>2022</b> ,		0
10	Off-the-Shelf Solutions as Potential Cyber Threats to Industrial Environments and Simple-To-Implement Protection Methodology. <b>2022</b> , 10, 114735-114748		0

- 9 Categorization and Criticality Assessment of Facilities of Critical Infrastructure. **2022**, ○
- 8 Web Based Health Check Application for Water Management Systems via SNMP Protocol. **2022**, 5, 328-337 ○
- 7 Emerging Simulation Frameworks for Analyzing Smart Grid Cyberattack: A Literature Review. **2022**, ○
- 6 A cyber resilience analysis case study of an industrial operational technology environment. ○
- 5 Modelling language for cyber security incident handling for critical infrastructures. **2023**, 128, 103139 ○
- 4 Evolution of cyber-physical-human water systems: Challenges and gaps. **2023**, 191, 122540 ○
- 3 Correlation-Based Anomaly Detection in Industrial Control Systems. **2023**, 23, 1561 ○
- 2 A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions. **2023**, 12, 1333 ○
- 1 Impact, Vulnerabilities, and Mitigation Strategies for Cyber-Secure Critical Infrastructure. **2023**, 23, 4060 ○