Data-Driven Cybersecurity Incident Prediction: A Surve

IEEE Communications Surveys and Tutorials
21, 1744-1772
DOI: 10.1109/comst.2018.2885561

Citation Report

#	Article	IF	Citations
1	Predicting day-ahead solar irradiance through gated recurrent unit using weather forecasting data. Journal of Renewable and Sustainable Energy, 2019, 11, .	2.0	36
2	Optimizing rewards allocation for privacy-preserving spatial crowdsourcing. Computer Communications, 2019, 146, 85-94.	5.1	10
3	Compressed Sensing Based Selective Encryption With Data Hiding Capability. IEEE Transactions on Industrial Informatics, 2019, 15, 6560-6571.	11.3	33
4	A deep learning framework for predicting cyber attacks rates. Eurasip Journal on Information Security, 2019, 2019, .	3.1	38
5	Changes in Binocular Color Fusion Limit Caused by Different Disparities. IEEE Access, 2019, 7, 70088-70101.	4.2	5
6	A3CM: Automatic Capability Annotation for Android Malware. IEEE Access, 2019, 7, 147156-147168.	4.2	29
7	Anti-Quantum Fast Authentication and Data Transmission Scheme for Massive Devices in 5G NB-IoT System. IEEE Internet of Things Journal, 2019, 6, 9794-9805.	8.7	62
8	A Lightweight Assisted Vulnerability Discovery Method Using Deep Neural Networks. IEEE Access, 2019, 7, 80079-80092.	4.2	18
9	Predicting the Impact of Android Malicious Samples via Machine Learning. IEEE Access, 2019, 7, 66304-66316.	4.2	16
10	An innovative approach for real-time network traffic classification. Computer Networks, 2019, 158, 143-157.	5.1	76
11	Proactive Antifragility: A New Paradigm for Next-Generation Cyber Defence at the Edge. , 2019, , .		6
12	Insider Threat Identification Using the Simultaneous Neural Learning of Multi-Source Logs. IEEE Access, 2019, 7, 183162-183176.	4.2	22
13	Review of Cybersecurity Research Topics, Taxonomy and Challenges: Interdisciplinary Perspective. , 2019, , .		17
14	DeepBalance: Deep-Learning and Fuzzy Oversampling for Vulnerability Detection. IEEE Transactions on Fuzzy Systems, 2019, , 1-1.	9.8	50
15	Î¼VulDeePecker: A Deep Learning-Based System for Multiclass Vulnerability Detection. IEEE Transactions on Dependable and Secure Computing, 2019, , 1-1.	5.4	65
16	An Efficient Multi-Message and Multi-Receiver Signcryption Scheme for Heterogeneous Smart Mobile IoT. IEEE Access, 2019, 7, 180205-180217.	4.2	27
17	GUI-Squatting Attack: Automated Generation of Android Phishing Apps. IEEE Transactions on Dependable and Secure Computing, 2019, , 1-1.	5.4	20
18	Secure real-time image protection scheme with near-duplicate detection in cloud computing. Journal of Real-Time Image Processing, 2020, 17, 175-184.	3.5	12

#	Article	IF	Citations
19	Model-based evaluation of combinations of Shuffle and Diversity MTD techniques on the cloud. Future Generation Computer Systems, 2020, 111, 507-522.	7.5	14
20	Machine learning for automatic assignment of the severity of cybersecurity events. Computational and Mathematical Methods, 2020, 2, e1072.	0.8	8
21	Data-Driven Cyber Security in Perspectiveâ€"Intelligent Traffic Analysis. IEEE Transactions on Cybernetics, 2020, 50, 3081-3093.	9.5	78
22	Toward Wi-Fi Halow Signal Coverage Modeling in Collapsed Structures. IEEE Internet of Things Journal, 2020, 7, 2181-2196.	8.7	5
23	Cyber Vulnerability Intelligence for Internet of Things Binary. IEEE Transactions on Industrial Informatics, 2020, 16, 2154-2163.	11.3	34
24	Software Vulnerability Discovery via Learning Multi-Domain Knowledge Bases. IEEE Transactions on Dependable and Secure Computing, 2021, 18, 2469-2485.	5.4	52
25	Toward supervised shape-based behavioral authentication on smartphones. Journal of Information Security and Applications, 2020, 55, 102591.	2.5	6
26	Cybersecurity data science: an overview from machine learning perspective. Journal of Big Data, 2020, 7, .	11.0	246
27	Neural Model Stealing Attack to Smart Mobile Device on Intelligent Medical Platform. Wireless Communications and Mobile Computing, 2020, 2020, 1-10.	1.2	4
28	Mitigating Insider Threats Using Bio-Inspired Models. Applied Sciences (Switzerland), 2020, 10, 5046.	2.5	9
29	JSCSP: a Novel Policy-Based XSS Defense Mechanism for Browsers. IEEE Transactions on Dependable and Secure Computing, 2020, , 1-1.	5.4	3
30	Research on Behavior-Based Data Leakage Incidents for the Sustainable Growth of an Organization. Sustainability, 2020, 12, 6217.	3.2	5
31	Privacy-preserving searchable encryption in the intelligent edge computing. Computer Communications, 2020, 164, 31-41.	5.1	13
32	EncodeORE: Reducing Leakage and Preserving Practicality in Order-Revealing Encryption. IEEE Transactions on Dependable and Secure Computing, 2022, 19, 1579-1591.	5.4	15
33	Privacyâ€aware PKI model with strong forward security. International Journal of Intelligent Systems, 2022, 37, 10049-10065.	5.7	16
34	Data-Driven Security for Smart City Systems: Carving a Trail. IEEE Access, 2020, 8, 147211-147230.	4.2	19
35	Modeling cooperative behavior for resilience in cyber-physical systems using SDN and NFV. SN Applied Sciences, 2020, 2, 1.	2.9	9
36	Trustworthy blockchainâ€based medical Internet of thing for minimal invasive surgery training simulator. Concurrency Computation Practice and Experience, 2022, 34, e5816.	2.2	2

#	Article	IF	Citations
37	Cyber Resilience in Healthcare Digital Twin on Lung Cancer. IEEE Access, 2020, 8, 201900-201913.	4.2	55
38	Software Vulnerability Analysis and Discovery Using Deep Learning Techniques: A Survey. IEEE Access, 2020, 8, 197158-197172.	4.2	32
39	A Hybrid Key Agreement Scheme for Smart Homes Using the Merkle Puzzle. IEEE Internet of Things Journal, 2020, 7, 1061-1071.	8.7	12
40	IntruDTree: A Machine Learning Based Cyber Security Intrusion Detection Model. Symmetry, 2020, 12, 754.	2.2	149
41	CD-VulD: Cross-Domain Vulnerability Discovery Based on Deep Domain Adaptation. IEEE Transactions on Dependable and Secure Computing, 2022, 19, 438-451.	5.4	28
42	Software Vulnerability Detection Using Deep Neural Networks: A Survey. Proceedings of the IEEE, 2020, 108, 1825-1848.	21.3	214
43	SDCCP: Control the network using softwareâ€defined networking and endâ€toâ€end congestion control. Concurrency Computation Practice and Experience, 2020, , e5716.	2.2	0
44	Code analysis for intelligent cyber systems: A data-driven approach. Information Sciences, 2020, 524, 46-58.	6.9	25
45	Fully Homomorphic based Privacy-Preserving Distributed Expectation Maximization on Cloud. IEEE Transactions on Parallel and Distributed Systems, 2020, 31, 2668-2681.	5.6	7
46	From Coarse to Fine (FC2F): A New Scheme of Colorizing Thermal Infrared Images. IEEE Access, 2020, 8, 111159-111171.	4.2	6
47	Detection of Social Network Spam Based on Improved Extreme Learning Machine. IEEE Access, 2020, 8, 112003-112014.	4.2	29
48	HinCTI: A Cyber Threat Intelligence Modeling and Identification System Based on Heterogeneous Information Network. IEEE Transactions on Knowledge and Data Engineering, 2022, 34, 708-722.	5.7	44
49	Secure and Efficient Data Sharing in Dynamic Vehicular Networks. IEEE Internet of Things Journal, 2020, 7, 8208-8217.	8.7	13
50	Enhancing collaborative intrusion detection via disagreement-based semi-supervised learning in IoT environments. Journal of Network and Computer Applications, 2020, 161, 102631.	9.1	73
51	Predictive methods in cyber defense: Current experience and research challenges. Future Generation Computer Systems, 2021, 115, 517-530.	7.5	22
52	Fooling intrusion detection systems using adversarially autoencoder. Digital Communications and Networks, 2021, 7, 453-460.	5.0	20
53	BIoT-Based Smart Agriculture: Food and Crops Efficiency and Improvement in Supply Chain Cycle. Blockchain Technologies, 2021, , 173-189.	0.8	0
54	Combining Graph-Based Learning With Automated Data Collection for Code Vulnerability Detection. IEEE Transactions on Information Forensics and Security, 2021, 16, 1943-1958.	6.9	110

#	Article	IF	Citations
55	On Aggregation and Prediction of Cybersecurity Incident Reports. IEEE Access, 2021, 9, 102636-102648.	4.2	2
56	Platform-Dependent Computer Security Complacency: The Unrecognized Insider Threat. IEEE Transactions on Engineering Management, 2022, 69, 3814-3825.	3.5	4
57	A Real-Time Sequential Deep Extreme Learning Machine Cybersecurity Intrusion Detection System. Computers, Materials and Continua, 2021, 66, 1785-1798.	1.9	23
58	Distant Supervision for Relations Extraction via Deep Residual Learning and Multi-instance Attention in Cybersecurity. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, 2021, , 151-161.	0.3	0
59	Trustworthy and Intelligent COVID-19 Diagnostic IoMT Through XR and Deep-Learning-Based Clinic Data Access. IEEE Internet of Things Journal, 2021, 8, 15965-15976.	8.7	48
60	Using honeynet data and a time series to predict the number of cyber attacks. Computer Science and Information Systems, 2021, 18, 1197-1217.	1.0	0
61	Deep Learning Based Attack Detection for Cyber-Physical System Cybersecurity: A Survey. IEEE/CAA Journal of Automatica Sinica, 2022, 9, 377-391.	13.1	150
62	A Review of Computer Vision Methods in Network Security. IEEE Communications Surveys and Tutorials, 2021, 23, 1838-1878.	39.4	26
63	My Security: An interactive search engine for cybersecurity. , 0, , .		2
64	Encrypted Data Retrieval and Sharing Scheme in Spaceâ€“Airâ€“Ground-Integrated Vehicular Networks. IEEE Internet of Things Journal, 2022, 9, 5957-5970.	8.7	5
65	A Survey of Android Malware Detection with Deep Neural Models. ACM Computing Surveys, 2021, 53, 1-36.	23.0	156
66	An ultra light weight and secure RFID batch authentication scheme for IoMT. Computer Communications, 2021, 167, 48-54.	5.1	20
67	A Review on Role of Cyber Security in Data Science. International Journal of Advanced Research in Science, Communication and Technology, 0, , 132-140.	0.0	0
68	Deep Cybersecurity: A Comprehensive Overview from Neural Network and Deep Learning Perspective. SN Computer Science, 2021, 2, 1.	3.6	79
69	AI-Driven Cybersecurity: An Overview, Security Intelligence Modeling and Research Directions. SN Computer Science, 2021, 2, 1.	3.6	127
70	DP-QIC: A differential privacy scheme based on quasi-identifier classification for big data publication. Soft Computing, 2021, 25, 7325-7339.	3.6	8
72	Secure Collaborative Deep Learning Against GAN Attacks in the Internet of Things. IEEE Internet of Things Journal, 2021, 8, 5839-5849.	8.7	16
74	A Systematic Mapping Study on Cyber Security Indicator Data. Electronics (Switzerland), 2021, 10, 1092.	3.1	5

#	Article	IF	Citations
75	Trustworthy Image Fusion with Deep Learning for Wireless Applications. Wireless Communications and Mobile Computing, 2021, 2021, 1-9.	1.2	2
76	Data security governance in the era of big data: status, challenges, and prospects. Data Science and Management, 2021, 2, 41-44.	8.1	26
77	Network intrusion detection using machine learning approaches: Addressing data imbalance. IET Cyber-Physical Systems: Theory and Applications, 2022, 7, 30-39.	3.3	3
79	Efficient defense strategy against spam and phishing email: An evolutionary game model. Journal of Information Security and Applications, 2021, 61, 102947.	2.5	1
80	Intelligent Intraoperative Haptic-AR Navigation for COVID-19 Lung Biopsy Using Deep Hybrid Model. IEEE Transactions on Industrial Informatics, 2021, 17, 6519-6527.	11.3	11
81	Kalman prediction-based virtual network experimental platform for smart living. Computer Communications, 2021, 177, 156-165.	5.1	1
82	Survey on atrial fibrillation detection from a single-lead ECG wave for Internet of Medical Things. Computer Communications, 2021, 178, 245-258.	5.1	21
83	Machine Learningâ€“based Cyber Attacks Targeting on Controlled Information. ACM Computing Surveys, 2022, 54, 1-36.	23.0	59
84	Text Mining in Cybersecurity. ACM Computing Surveys, 2022, 54, 1-36.	23.0	21
85	Social Characteristic-Based Propagation-Efficient PBFT Protocol to Broadcast in Unstructured Overlay Networks. IEEE Transactions on Dependable and Secure Computing, 2022, 19, 3621-3639.	5.4	3
86	An Improved Dictionary Cracking Scheme Based on Multiple GPUs for Wi-Fi Network. Computers, Materials and Continua, 2021, 66, 2957-2972.	1.9	2
87	Data-Driven Android Malware Intelligence: A Survey. Lecture Notes in Computer Science, 2019, , 183-202.	1.3	14
88	Unsupervised Insider Detection Through Neural Feature Learning and Model Optimisation. Lecture Notes in Computer Science, 2019, , 18-36.	1.3	5
89	Simultaneously Advising via Differential Privacy in Cloud Servers Environment. Lecture Notes in Computer Science, 2020, , 550-563.	1.3	2
90	Lightweight and Certificateless Multi-Receiver Secure Data Transmission Protocol for Wireless Body Area Networks. IEEE Transactions on Dependable and Secure Computing, 2022, 19, 1464-1475.	5.4	21
91	A Survey of IoT Applications in Blockchain Systems. ACM Computing Surveys, 2021, 53, 1-32.	23.0	198
92	CyberSecurity Attack Prediction: A Deep Learning Approach. , 2020, , .		24
93	Data-Driven Cybersecurity Knowledge Graph Construction for Industrial Control System Security. Wireless Communications and Mobile Computing, 2020, 2020, 1-13.	1.2	18

#	Article	IF	Citations
94	Automated Expert System Knowledge Base Development Method for Information Security Risk Analysis. International Journal of Computers, Communications and Control, 2020, 14, 743.	1.8	10
95	GRU-based deep learning approach for network intrusion alert prediction. Future Generation Computer Systems, 2022, 128, 235-247.	7.5	43
96	A Visualization-Based Analysis on Classifying Android Malware. Lecture Notes in Computer Science, 2019, , 304-319.	1.3	1
97	A Logic Programming Approach to Predict Enterprise-Targeted Cyberattacks. Intelligent Systems Reference Library, 2020, , 13-32.	1.2	1
98	The Use of Runtime Verification for Identifying and Responding to Cybersecurity Threats Posed to State Actors During Cyberwarfare. , 2020, , .		0
99	Doc2vec-Based Insider Threat Detection through Behaviour Analysis of Multi-source Security Logs. , 2020, , .		4
100	NSAPs: A novel scheme for network security state assessment and attack prediction. Computers and Security, 2020, 99, 102031.	6.0	3
101	Domain adaptation for Windows advanced persistent threat detection. Computers and Security, 2022, 112, 102496.	6.0	12
102	Data Analytics of Crowdsourced Resources for Cybersecurity Intelligence. Lecture Notes in Computer Science, 2020, , 3-21.	1.3	5
103	Enhance Intrusion Detection in Computer Networks Based on Deep Extreme Learning Machine. Computers, Materials and Continua, 2020, 66, 467-480.	1.9	12
104	ANDRuspex: Leveraging Graph Representation Learning to Predict Harmful App Installations on Mobile Devices. , 2021, , .		0
105	Study and Application of Machine Learning Methods in Modern Additive Manufacturing Processes. Advances in Computational Intelligence and Robotics Book Series, 2022, , 75-95.	0.4	8
106	An Assurance-Based Risk Management Framework for Distributed Systems. , 2021, , .		5
107	A Context-Aware Neural Embedding for Function-Level Vulnerability Detection. Algorithms, 2021, 14, 335.	2.1	8
108	A Shared Cyber Threat Intelligence Solution for SMEs. Electronics (Switzerland), 2021, 10, 2913.	3.1	10
109	Image Speckle Denoising for Securing Internet of Smart Sensors. Security and Communication Networks, 2021, 2021, 1-10.	1.5	1
110	Channel-State-Based Fingerprinting Against Physical Access Attack in Industrial Field Bus Network. IEEE Internet of Things Journal, 2022, 9, 9557-9573.	8.7	7
111	Cardiac LGE MRI Segmentation With Cross-Modality Image Augmentation and Improved U-Net. IEEE Journal of Biomedical and Health Informatics, 2023, 27, 588-597.	6.3	2

#	Article	IF	Citations
112	LICALITYâ€”Likelihood and Criticality: Vulnerability Risk Prioritization Through Logical Reasoning and Deep Learning. IEEE Transactions on Network and Service Management, 2022, 19, 1746-1760.	4.9	6
114	Deep Neural Embedding for Software Vulnerability Discovery: Comparison and Optimization. Security and Communication Networks, 2022, 2022, 1-12.	1.5	13
115	An empirical evaluation of deep learningâ€based source code vulnerability detection: Representation versus models. Journal of Software: Evolution and Process, 2023, 35, .	1.6	1
116	Contemporary survey on effectiveness of machine and deep learning techniques for cyber security. , 2022, , 177-200.		9
117	DeepAG: Attack Graph Construction and Threats Prediction With Bi-Directional Deep Learning. IEEE Transactions on Dependable and Secure Computing, 2023, 20, 740-757.	5.4	16
118	Trajectory Forecasting Based on Prior-Aware Directed Graph Convolutional Neural Network. IEEE Transactions on Intelligent Transportation Systems, 2022, 23, 16773-16785.	8.0	22
119	Big Data-Driven Hierarchical Local Area Network Security Risk Event Prediction Algorithm. Scientific Programming, 2022, 2022, 1-13.	0.7	0
120	Cyber Information Retrieval Through Pragmatics Understanding and Visualization. IEEE Transactions on Dependable and Secure Computing, 2023, 20, 1186-1199.	5.4	1
122	Intelligent detection of vulnerable functions in software through neural embeddingâ€based code analysis. International Journal of Network Management, 2023, 33, .	2.2	4
123	Construction and Application of a Data-Driven Abstract Extraction Model for English Text. Scientific Programming, 2022, 2022, 1-11.	0.7	0
124	Secure medical digital twin via human-centric interaction and cyber vulnerability resilience. Connection Science, 2022, 34, 895-910.	3.0	18
125	NGS: Mitigating DDoS Attacks using SDN-based Network Gate Shield. , 2021, , .		4
126	The Empirical Analysis of Machine Learning Approaches for Enhancing the Cyber security for better Quality. , 2022, , .		2
127	A Survey on Data-driven Software Vulnerability Assessment and Prioritization. ACM Computing Surveys, 2023, 55, 1-39.	23.0	15
128	Cyber Code Intelligence for Android Malware Detection. IEEE Transactions on Cybernetics, 2023, 53, 617-627.	9.5	12
129	Defining Security Requirements With the Common Criteria: Applications, Adoptions, and Challenges. IEEE Access, 2022, 10, 44756-44777.	4.2	13
130	An Environment-Specific Prioritization Model for Information-Security Vulnerabilities Based on Risk Factor Analysis. Electronics (Switzerland), 2022, 11, 1334.	3.1	4
131	A survey on deep learning for cybersecurity: Progress, challenges, and opportunities. Computer Networks, 2022, 212, 109032.	5.1	35

#	Article	IF	Citations
132	Developing Cybersecurity Workforce: Introducing CyberSec Labs for Industry Standard Cybersecurity Training. , 2021, , .		3
134	Automation of human behaviors and its prediction using machine learning. Microsystem Technologies, 2022, 28, 1879-1887.	2.0	12
135	How Do Organizations Seek Cyber Assurance? Investigations on the Adoption of the Common Criteria and Beyond. IEEE Access, 2022, 10, 71749-71763.	4.2	7
136	Cybersecurity Threats and Their Mitigation Approaches Using Machine Learningâ€"A Review. Journal of Cybersecurity and Privacy, 2022, 2, 527-555.	3.9	23
137	An Attack Impact and Host Importance based Approach to Intrusion Response Action Selection. , 2022, , .		0
138	A Review on C3I Systemsâ€™ Security: Vulnerabilities, Attacks, and Countermeasures. ACM Computing Surveys, 2023, 55, 1-38.	23.0	3
139	Framework for Cyber Threats in Social Networks. International Journal of Engineering and Advanced Technology, 2022, 11, 128-133.	0.3	0
140	Detecting Vulnerability on IoT Device Firmware: A Survey. IEEE/CAA Journal of Automatica Sinica, 2023, 10, 25-41.	13.1	34
141	Cybers Security Analysis and Measurement Tools Using Machine Learning Approach. , 2022, , .		2
142	Impact of Artificial Intelligence on Information Security in Business. , 2022, , .		5
143	CyEvent2vec: Attributed Heterogeneous Information Network based Event Embedding Framework for Cyber Security Events Analysis. , 2022, , .		2
144	Evaluating Membership Inference Through Adversarial Robustness. Computer Journal, 2022, 65, 2969-2978.	2.4	4
145	Threats Modeling andÂAnomaly Detection inÂtheÂBehaviour ofÂaÂSystem - A Review ofÂSome Approaches. Lecture Notes in Computer Science, 2022, , 1-27.	1.3	0
146	Cybersecurity as a Digital and Economic Enabler. Advances in Information Security, Privacy, and Ethics Book Series, 2022, , 37-45.	0.5	0
147	Space-Efficient Storage Structure of Blockchain Transactions Supporting Secure Verification. IEEE Transactions on Cloud Computing, 2022, , 1-15.	4.4	0
148	Explainable machine learning in cybersecurity: A survey. International Journal of Intelligent Systems, 2022, 37, 12305-12334.	5.7	7
149	Perceived challenges and opportunities of machine learning applications in governmental organisations: an interview-based exploration in the Netherlands. , 2022, , .		1
150	SGX-Stream: A Secure Stream Analytics Framework In SGX-enabled Edge Cloud. Journal of Information Security and Applications, 2023, 72, 103403.	2.5	1

#	Article	IF	Citations
151	Threat Actorsâ€™ Tenacity to Disrupt: Examination of Major Cybersecurity Incidents. IEEE Access, 2022, 10, 134038-134051.	4.2	4
152	Cybersecurity Solutions Using AI Techniques. , 2022, , .		3
153	The application of neural network for software vulnerability detection: a review. Neural Computing and Applications, 2023, 35, 1279-1301.	5.6	2
154	Trust assessment for mobile crowdsensing via device fingerprinting. ISA Transactions, 2023, 141, 93-102.	5.7	2
155	Multiâ€aspects <scp>AI</scp>â€based modeling and adversarial learning for cybersecurity intelligence and robustness: A comprehensive overview. Security and Privacy, 2023, 6, .	2.7	4
156	A Systemic Review of the Cybersecurity Challenges in Australian Water Infrastructure Management. Water (Switzerland), 2023, 15, 168.	2.7	5
157	TINKER: A framework for Open source Cyberthreat Intelligence. , 2022, , .		2
158	Lightweight Model for Botnet Attack Detection in Software Defined Network-Orchestrated IoT. Applied Sciences (Switzerland), 2023, 13, 4699.	2.5	3
159	Implications of false alarms in dynamic games on cyber-security. Chaos, Solitons and Fractals, 2023, 169, 113322.	5.1	0
160	Detecting vulnerabilities in IoT software: New hybrid model and comprehensive data analysis. Journal of Information Security and Applications, 2023, 74, 103467.	2.5	1
161	Hybrid KD-NFT: A multi-layered NFT assisted robust Knowledge Distillation framework for Internet of Things. Journal of Information Security and Applications, 2023, 75, 103483.	2.5	0
162	Dynamic feature selection model for adaptive cross site scripting attack detection using developed multi-agent deep Q learning model. Journal of King Saud University - Computer and Information Sciences, 2023, 35, 101490.	3.9	4
163	Study ofÂanÂApproach Based onÂtheÂAnalysis ofÂComputer Program Execution Traces forÂthe Detection ofÂVulnerabilities. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, 2022, , 105-115.	0.3	0
164	Towards Generalized Deepfake Detection With Continual Learning On Limited New Data. , 2022, , .		1
165	Improving Traffic Safety through Traffic Accident Risk Assessment. Sustainability, 2023, 15, 3748.	3.2	1
166	Differentially Distributed Private Intelligence Security in Cybersecurity Infrastructures. , 2023, , .		0
167	An intelligent DDoS attack detection tree-based model using Gini index feature selection method. Microprocessors and Microsystems, 2023, 98, 104823.	2.8	13
168	Backdoor attacks against distributed swarm learning. ISA Transactions, 2023, 141, 59-72.	5.7	3

#	Article	IF	Citations
169	Deep learning for predictive alerting and cyber-attack mitigation. , 2023, , .		0
170	Privacy preserving federated learning for full heterogeneity. ISA Transactions, 2023, 141, 73-83.	5.7	1
171	SVScanner: Detecting smart contract vulnerabilities via deep semantic extraction. Journal of Information Security and Applications, 2023, 75, 103484.	2.5	2
172	Privacy preserving for AI-based 3D human pose recovery and retargeting. ISA Transactions, 2023, 141, 132-142.	5.7	0
173	Intrusion Detection using Machine Learning Techniques: An exhaustive review. , 2023, , .		0
174	Detecting contradictions from IoT protocol specification documents based on neural generated knowledge graph. ISA Transactions, 2023, 141, 10-19.	5.7	0
175	Distributed <mml:math xmlns:mml="http://www.w3.org/1998/Math/MathML" altimg="si4.svg" display="inline" id="d1e72"><mml:msub><mml:mrow><mml:mi>H</mml:mi></mml:mrow><mml:mrow><mml:mi>âˆž</mml:mi></mml:mrow></mml:ms filtering of replay attacks over sensor networks. ISA Transactions, 2023, 141, 113-120.	5.7	0
176	A Comprehensive Survey of various Cyber Attacks. , 2023, , .		0
177	An actionable maturity planning model for smart, circular cities. Cities, 2023, 140, 104403.	5.6	2
178	FCH, an incentive framework for data-owner dominated federated learning. Journal of Information Security and Applications, 2023, 76, 103521.	2.5	2
179	A Data-driven Risk Cascading Effect Evaluation for Supply and Procurement in the Construction Industry. , 2022, , .		0
180	Secure and efficient authenticated group key agreement protocol for AI-based automation systems. ISA Transactions, 2023, 141, 1-9.	5.7	2
181	Cyber Threat Intelligence Mining for Proactive Cybersecurity Defense: A Survey and New Perspectives. IEEE Communications Surveys and Tutorials, 2023, 25, 1748-1774.	39.4	15
182	Impact of Big Data Analytics and ChatGPT on Cybersecurity. , 2023, , .		15
183	GWS-Geo: A graph neural network based model for street-level IPv6 geolocation. Journal of Information Security and Applications, 2023, 75, 103511.	2.5	1
184	A graph empowered insider threat detection framework based on daily activities. ISA Transactions, 2023, 141, 84-92.	5.7	6
185	Generating synthetic clinical data that capture class imbalanced distributions with generative adversarial networks: Example using antiretroviral therapy for HIV. Journal of Biomedical Informatics, 2023, 144, 104436.	4.3	5
186	Smart contracts vulnerability detection model based on adversarial multi-task learning. Journal of Information Security and Applications, 2023, 77, 103555.	2.5	0

#	Article	IF	Citations
187	A New Wave in CyberSecurity: Democratising the Future Networking Landscape. , 2023, , .		0
188	The Role of Artificial Intelligence in Cyber Security. Advances in Information Security, Privacy, and Ethics Book Series, 2023, , 1-24.	0.5	0
189	A Survey on Threat Hunting in Enterprise Networks. IEEE Communications Surveys and Tutorials, 2023, 25, 2299-2324.	39.4	4
190	VulScan: A Vulnerability Detection Model Based on Deep Learning. , 2023, , .		0
191	PHOENI2X â€“ A European Cyber Resilience Framework With Artificial-Intelligence-Assisted Orchestration, Automation & Response Capabilities for Business Continuity and Recovery, Incident Response, and Information Exchange. , 2023, , .		2
192	Bibliometrics Study of Organizational Cybersecurity. Advances in Logistics, Operations, and Management Science Book Series, 2023, , 115-139.	0.4	0
193	CEVulDet: A Code Edge Representation Learnable Vulnerability Detector. , 2023, , .		0
194	Backdoor Attack on Deep Neural Networks in Perception Domain. , 2023, , .		0
195	High-speed anomaly traffic detection based on staged frequency domain features. Journal of Information Security and Applications, 2023, 77, 103575.	2.5	1
196	Networking Architecture and Key Supporting Technologies for Human Digital Twin in Personalized Healthcare: A Comprehensive Survey. IEEE Communications Surveys and Tutorials, 2024, 26, 706-746.	39.4	3
197	Recent developments in materials discovery and innovation: An exploration of mechanical, thermal, and tribological properties using molecular dynamics simulation. AIP Conference Proceedings, 2023, , .	0.4	0
198	Improving theÂEffectiveness ofÂCyberdefense Measures. Profiles in Operations Research, 2023, , 205-219.	0.4	0
200	Self-Organizing Computational System for Network Anomaly Exploration using Learning Algorithms. Journal of Machine and Computing, 2023, , 431-445.	0.8	0
201	Deep Graph Embedding for IoT Botnet Traffic Detection. Security and Communication Networks, 2023, 2023, 1-10.	1.5	0
202	A Survey of Data Mining and Machine Learning-Based Intrusion Detection System for Cyber Security. Advances in Information Security, Privacy, and Ethics Book Series, 2023, , 52-74.	0.5	0
203	Exploring perceptions of decision-makers and specialists in defensive machine learning cybersecurity applications: The need for a standardised approach. Computers and Security, 2024, 139, 103694.	6.0	0
204	Insider threat detection using supervised machine learning algorithms. Telecommunication Systems, 0, , .	2.5	0
205	The Credential is Not Enough: Deception withÂHoneypots andÂFake Credentials. Lecture Notes in Computer Science, 2023, , 234-254.	1.3	0

#	Article	IF	Citations
206	Modeling and management of cyber risk: a cross-disciplinary review. Annals of Actuarial Science, 0, , 1-40.	1.5	0
207	Rapid Forecasting of Cyber Events Using Machine Learning-Enabled Features. Information (Switzerland), 2024, 15, 36.	2.9	0
208	Data Sharing and Use in Cybersecurity Research. Data Science Journal, 0, 23, 3.	1.3	0
209	Hardware nanosecondâ€precision timestamping for lineâ€rate packet capture. IET Networks, 0, , .	1.8	0
210	Secure and privacy-preserving intrusion detection in wireless sensor networks: Federated learning with SCNN-Bi-LSTM for enhanced reliability. Ad Hoc Networks, 2024, 155, 103407.	5.5	2
211	Ransomware Resilience: Investigating Organizational Security Culture and Its Impact on Cybersecurity Practices against Ransomware Threats. , 2023, , .		0
212	An Assessment of Capabilities Required for Effective Cybersecurity Incident Management - A Systematic Literature Review. , 2023, , .		0
213	Deep Convolutional Neural Network for Active Intrusion Detection and Protect data from Passive Intrusion by Pascal Triangle. Wireless Personal Communications, 0, , .	2.7	0
214	Software vulnerable functions discovery based on code composite feature. Journal of Information Security and Applications, 2024, 81, 103718.	2.5	0
215	Malware Detection in Files and URLâ€™s using Machine Learning. International Journal of Scientific Research in Computer Science Engineering and Information Technology, 2024, , 79-84.	0.3	0
216	Identifying cyber security competencies and skills from online job advertisements through topic modeling. Security Journal, 0, , .	1.7	0