An Ensemble of Deep Recurrent Neural Networks for D
Network Traffic

IEEE Internet of Things Journal

7, 8852-8859

DOI: 10.1109/jiot.2020.2996425

Citation Report

#	Article	IF	Citations
1	Quantifying the need for supervised machine learning in conducting live forensic analysis of emergent configurations (ECO) in IoT environments. Forensic Science International: Reports, 2020, 2, 100122.	0.4	23
2	Deep-IFS: Intrusion Detection Approach for Industrial Internet of Things Traffic in Fog Environment. IEEE Transactions on Industrial Informatics, 2021, 17, 7704-7715.	7.2	54
3	Boosting-Based DDoS Detection in Internet of Things Systems. IEEE Internet of Things Journal, 2022, 9, 2109-2123.	5.5	75
4	Hybrid Statistical-Machine Learning for Real-Time Anomaly Detection in Industrial Cyberâ€“Physical Systems. IEEE Transactions on Automation Science and Engineering, 2023, 20, 32-46.	3.4	27
5	A Hybrid DL-Based Detection Mechanism for Cyber Threats in Secure Networks. IEEE Access, 2021, 9, 73938-73947.	2.6	9
6	Intrusion Detection for Secure Social Internet of Things Based on Collaborative Edge Computing: A Generative Adversarial Network-Based Approach. IEEE Transactions on Computational Social Systems, 2022, 9, 134-145.	3.2	56
7	Machine learning research towards combating COVID-19: Virus detection, spread prevention, and medical assistance. Journal of Biomedical Informatics, 2021, 117, 103751.	2.5	47
8	A Unified Deep Learning Anomaly Detection and Classification Approach for Smart Grid Environments. IEEE Transactions on Network and Service Management, 2021, 18, 1137-1151.	3.2	93
9	A Hybrid Deep Learning-Driven SDN Enabled Mechanism for Secure Communication in Internet of Things (IoT). Sensors, 2021, 21, 4884.	2.1	42
10	Internet Traffic Classification Using an Ensemble of Deep Convolutional Neural Networks. , 2021, , .		6
11	Compacting Deep Neural Networks for Internet of Things: Methods and Applications. IEEE Internet of Things Journal, 2021, 8, 11935-11959.	5.5	27
12	Semi-Supervised Spatiotemporal Deep Learning for Intrusions Detection in IoT Networks. IEEE Internet of Things Journal, 2021, 8, 12251-12265.	5.5	50
13	XAI-Based Microarchitectural Side-Channel Analysis for Website Fingerprinting Attacks and Defenses. IEEE Transactions on Dependable and Secure Computing, 2022, 19, 4039-4051.	3.7	6
14	A Hybrid Deep Random Neural Network for Cyberattack Detection in the Industrial Internet of Things. IEEE Access, 2021, 9, 55595-55605.	2.6	52
15	Artificial Intelligence for Threat Detection and Analysis in Industrial IoT: Applications and Challenges. , 2021, , 1-6.		0
16	Federated-Learning-Based Anomaly Detection for IoT Security Attacks. IEEE Internet of Things Journal, 2022, 9, 2545-2554.	5.5	213
17	An Empirical Evaluation of AI Deep Explainable Tools. , 2020, , .		18
18	The Role of Artificial Intelligence and Machine Learning in Covid-19 led Pandemic. , 2021, , .		0

#	Article	IF	Citations
19	Detection of Enumeration Attacks in Cloud Environments Using Infrastructure Log Data. , 2022, , 41-52.		1
20	Cyber Threat Attribution with Multi-View Heuristic Analysis. , 2022, , 53-73.		4
21	Machine Learning for OSX Malware Detection. , 2022, , 209-222.		1
22	Big Data Analytics and Forensics: An Overview. , 2022, , 1-5.		1
23	Evaluating Performance of Scalable Fair Clustering Machine Learning Techniques in Detecting Cyber Attacks in Industrial Control Systems. , 2022, , 105-116.		4
24	Scalable Fair Clustering Algorithm for Internet of Things Malware Classification. , 2022, , 271-287.		1
25	Evaluation of Supervised and Unsupervised Machine Learning Classifiers for Mac OS Malware Detection. , 2022, , 159-175.		2
26	Cyber-Attack Detection in Cyber-Physical Systems Using Supervised Machine Learning. , 2022, , 131-140.		4
27	Mapping CKC Model Through NLP Modelling for APT Groups Reports. , 2022, , 239-252.		1
28	Mac OS X Malware Detection with Supervised Machine Learning Algorithms. , 2022, , 193-208.		3
29	Evaluation of Scalable Fair Clustering Machine Learning Methods for Threat Hunting in Cyber-Physical Systems. , 2022, , 141-158.		0
30	Secure IIoT-Enabled Industry 4.0. Sustainability, 2021, 13, 12384.	1.6	11
31	Intrusion Detection Framework for the Internet of Things Using a Dense Random Neural Network. IEEE Transactions on Industrial Informatics, 2022, 18, 6435-6444.	7.2	33
32	Detecting Cybersecurity Attacks in Internet of Things Using Artificial Intelligence Methods: A Systematic Literature Review. Electronics (Switzerland), 2022, 11, 198.	1.8	90
33	Privacy-Preserved Generative Network for Trustworthy Anomaly Detection in Smart Grids: A Federated Semisupervised Approach. IEEE Transactions on Industrial Informatics, 2023, 19, 995-1005.	7.2	7
34	An Exploration Into Secure IoT Networks Using Deep Learning Methodologies. , 2022, , .		1
35	Predicting Cyber-Attacks on IoT Networks Using Deep-Learning and Different Variants of SMOTE. Lecture Notes in Networks and Systems, 2022, , 243-255.	0.5	2
36	A Hybrid Intelligent Framework to Combat Sophisticated Threats in Secure Industries. Sensors, 2022, 22, 1582.	2.1	26

#	Article	IF	Citations
37	A Review on Conceptual Model of Cyber Attack Detection and Mitigation Using Deep Ensemble Model. International Journal of Applied Engineering and Management Letters, 0, , 149-159.	0.0	1
38	A Synoptic Review on Feature Selection and Machine Learning models used for Detecting Cyber Attacks in IoT. , 2021, , .		0
39	A Novel Trust Model In Detecting Final-Phase Attacks in Substations. , 2021, , .		3
40	Learning-Based Methods for Cyber Attacks Detection in IoT Systems: A Survey on Methods, Analysis, and Future Prospects. Electronics (Switzerland), 2022, 11, 1502.	1.8	54
41	A Synoptic Review on Feature Selection and Machine Learning models used for Detecting Cyber Attacks in IoT. , 2021, , .		0
42	Internet of Things use case applications for COVID-19. , 2022, , 377-412.		1
43	Fog computing based ultrasound nerve segmentation system using deep learning for mIoT. Journal of Discrete Mathematical Sciences and Cryptography, 2022, 25, 649-659.	0.5	0
44	Industrial IoT Intrusion Detection via Evolutionary Cost-Sensitive Learning and Fog Computing. IEEE Internet of Things Journal, 2022, 9, 23260-23271.	5.5	17
45	Identification of Intrusion Events Based on Distributed Optical Fiber Sensing in Complex Environment. IEEE Internet of Things Journal, 2022, 9, 24212-24220.	5.5	9
47	Predicting future community intrusions using a novel type and encryption mechanism architecture for attack node mitigation. , 2022, 49, 174-182.		0
48	A Trust-Influenced Smart Grid: A Survey and a Proposal. Journal of Sensor and Actuator Networks, 2022, 11, 34.	2.3	6
49	Internet of Things Intrusion Detection System based on Transfer Learning. , 2022, , .		0
50	Internet of Things Remote Piano Information Teaching System and Its Control Method. Journal of Sensors, 2022, 2022, 1-6.	0.6	3
51	A Proposal forÂFPGA-Accelerated Deep Learning Ensembles inÂMPSoC Platforms Applied toÂMalware Detection. Communications in Computer and Information Science, 2022, , 239-249.	0.4	0
52	Predicting Future Community Intrusions Using a Novel Type and Encryption Mechanism Architecture for Attack Node Mitigation. SSRN Electronic Journal, 0, , .	0.4	0
53	Recurrent and Deep Learning Neural Network Models for DDoS Attack Detection. Journal of Sensors, 2022, 2022, 1-21.	0.6	3
54	Accurate threat hunting in industrial internet of things edge devices. Digital Communications and Networks, 2023, 9, 1123-1130.	2.7	14
55	Secure Smart Communication Efficiency in Federated Learning: Achievements and Challenges. Applied Sciences (Switzerland), 2022, 12, 8980.	1.3	15

#	Article	IF	Citations
56	An ensemble deep learning model for cyber threat hunting in industrial internet of things. Digital Communications and Networks, 2023, 9, 101-110.	2.7	29
57	A Survey of Computational Intelligence Techniques Used for Cyber-Attack Detection. Smart Innovation, Systems and Technologies, 2023, , 515-527.	0.5	0
58	Hybrid Deep Learning Model and Fuzzy C Means Clustering Method for Pulmonary Nodule Detection in CT Images. IETE Journal of Research, 2023, 69, 7993-8005.	1.8	2
59	DEMD-IoT: a deep ensemble model for IoT malware detection using CNNs and network traffic. Evolving Systems, 2023, 14, 461-477.	2.4	5
60	An Abnormal Traffic Detection Method for IoT Devices Based on Federated Learning and Depthwise Separable Convolutional Neural Networks. , 2022, , .		5
61	Anomaly detection in Internet of medical Things with Blockchain from the perspective of deep neural network. Information Sciences, 2022, 617, 133-149.	4.0	14
62	Explainable AI Over the Internet of Things (IoT): Overview, State-of-the-Art and Future Directions. IEEE Open Journal of the Communications Society, 2022, 3, 2106-2136.	4.4	18
63	Evolution and Trends in Artificial Intelligence of Things Security: When Good Enough is Not Good Enough!. IEEE Internet of Things Magazine, 2022, 5, 62-66.	2.0	1
64	Adversarial Malicious Encrypted Traffic Detection Based on Refined Session Analysis. Symmetry, 2022, 14, 2329.	1.1	1
65	Detection and mitigation of field flooding attacks on oil and gas critical infrastructure communication. Computers and Security, 2023, 124, 103007.	4.0	7
66	Forecasting the <scp>IoT</scp>â€based cyber threats using the hybrid forage dependent ensemble classifier. Concurrency Computation Practice and Experience, 2023, 35, .	1.4	1
67	IoT Attack Detection and Mitigation with Optimized Deep Learning Techniques. Cybernetics and Systems, 0, , 1-27.	1.6	1
68	Cyber Forensic Investigation in IoT Using Deep Learning Based Feature Fusion in Big Data. International Journal of Wireless Information Networks, 0, , .	1.8	1
69	An accurate attack detection framework based on exponential polynomial kernelâ€centered deep neural networks in the wireless sensor network. Transactions on Emerging Telecommunications Technologies, 2023, 34, .	2.6	4
70	Blockchain Mechanism-Based Attack Detection in IoT with Hybrid Classification and Proposed Feature Selection. Cybernetics and Systems, 0, , 1-26.	1.6	0
71	A Comprehensive Review on Cyber-Attack Detection and Control of Microgrid Systems. Power Systems, 2023, , 1-45.	0.3	2
72	OPTIMIST: Lightweight and Transparent IDS With Optimum Placement Strategy to Mitigate Mixed-Rate DDoS Attacks in IoT Networks. IEEE Internet of Things Journal, 2023, 10, 8357-8370.	5.5	10
73	DeepAK-IoT: An effective deep learning model for cyberattack detection in IoT networks. Information Sciences, 2023, 634, 157-171.	4.0	7

#	Article	IF	Citations
74	A Cyber-Attack Detection System Using Late Fusion Aggregation Enabled Cyber-Net. Intelligent Automation and Soft Computing, 2023, 36, 3101-3119.	1.6	0
75	Investigating the Security Issues of Multi-layer IoT Attacks Using Machine Learning Techniques. , 2022, , .		0
76	Implementation of a RADIUS server for access control through authentication in wireless networks. International Journal of Advanced and Applied Sciences, 2023, 10, 183-188.	0.2	0
77	Heart Disease Prediction Analysis Using Hybrid Machine Learning Approach. , 2023, , .		0
78	A Novel Hybrid Deep Learning Model for Botnet Attacks Detection in a Secure IoMT Environment *. , 2023, , .		2
79	Time Series-Based IDS for Detecting Botnet Attacks in IoT and Embedded Devices. Lecture Notes in Electrical Engineering, 2023, , 351-361.	0.3	0
84	Malware Detection and Classification Using Ensemble of BiLSTMs with Huffman Feature Optimization. Lecture Notes on Data Engineering and Communications Technologies, 2023, , 427-445.	0.5	0
93	SSS-EC: Cryptographic based Single-Factor Authentication for Fingerprint Data with Machine Learning Technique. , 2023, , .		1
95	Federated Learning Support for Cybersecurity: Fundamentals, Applications, and Opportunities. , 2023, , .		1
97	Analyze and Forecast the Cyber Attack Detection Process using Machine Learning Techniques. , 2023, , .		0
100	A CNN Deep Learning Technique for Botnet Attack Detection for IoT Application. , 2023, , .		0
102	A comprehensive analysis of hybrid machine learning algorithms for securing IoT data. AIP Conference Proceedings, 2023, , .	0.3	0
105	An Optimized Deep Learning Algorithm for Cyber-Attack Detection. Smart Innovation, Systems and Technologies, 2023, , 465-472.	0.5	0
106	RSM: A Real-time Security Monitoring Platform for IoT Networks. , 2023, , .		0
111	Multimodal Sensor Data Fusion Based Cyberattack Detection in Industrial Internet of Things Environment. , 2023, , .		0