A Deep and Scalable Unsupervised Machine Learning System for Cyber-Attack Detection in Large-Scale Smart Grids

DOI: 10.1109/access.2019.2920326
IEEE Access, 2019, 7, 80778-80788.

#	Paper	IF	Citations
163	A Layered Intrusion Detection System for Critical Infrastructure Using Machine Learning. **2019**,		21
162	Employing Composite Demand Response Model in Microgrid Energy Management. **2019**,		1
161	Can Active Learning Benefit the Smart Grid? A Perspective on Overcoming the Data Scarcity. **2019**,		0
160	Transformation of Smart Grid using Machine Learning. **2019**,		4
159	Joint State Estimation and Cyber-Attack Detection Based on Feature Grouping. **2019**,		6
158	Preventing False Tripping Cyberattacks Against Distance Relays: A Deep Learning Approach. **2019**,		3
157	Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. **2020**, 50, 102419		194
156	An efficient route planning model for mobile agents on the internet of things using Markov decision process. **2020**, 98, 102053		18
155	An improved two-hidden-layer extreme learning machine for malware hunting. **2020**, 89, 101655		39
154	Integrated cyberattack detection and resilient control strategies using Lyapunov-based economic model predictive control. **2020**, 66, e17084		4
153	MQTTset, a New Dataset for Machine Learning Techniques on MQTT. **2020**, 20,		27
152	Security of Cyber-Physical Systems. **2020**,		5
151	MVFCC: A Multi-View Fuzzy Consensus Clustering Model for Malware Threat Attribution. *IEEE Access*, **2020**, 8, 139188-139198	3.5	16
150	IoT Architecture for Cyber-Physical System State Estimation Using Unscented Kalman Filter. **2020**,		
149	. *IEEE Access*, **2020**, 8, 156053-156066	3.5	22
148	Real-time stability assessment in smart cyber-physical grids: a deep learning approach. **2020**, 3, 454-461		8
147	Machine learning driven smart electric power systems: Current trends and new perspectives. **2020**, 272, 115237		62

146	Relaxation-based anomaly detection in cyber-physical systems using ensemble kalman filter. **2020**, 5, 49-58		23
145	Applications of Artificial Intelligence and Machine learning in smart cities. **2020**, 154, 313-323		152
144	Research and application of artificial intelligence service platform for the power field. **2020**, 3, 175-185		8
143	Blockchain Cybersecurity, Trust and Privacy. **2020**,		4
142	Machine learning based solutions for security of Internet of Things (IoT): A survey. **2020**, 161, 102630		124
141	On the Resiliency of Power and Gas Integration Resources Against Cyber Attacks. *IEEE Transactions on Industrial Informatics*, **2021**, 17, 3099-3110	11.9	6
140	A survey on security and privacy of federated learning. **2021**, 115, 619-640		165
139	A review of machine learning applications in IoT-integrated modern power systems. **2021**, 34, 106879		17
138	A Learning-Based Framework for Detecting Cyber-Attacks Against Line Current Differential Relays. **2021**, 36, 2274-2286		6
137	Security aspects of Internet of Things aided smart grids: A bibliometric survey. **2021**, 14, 100111		64
136	. **2021**, 1-15		1
135	Support Vector Machine-Based Dynamic Cyber-Attack Detection in AGC System. *Lecture Notes in Electrical Engineering*, **2021**, 343-355	0.2	0
134	A Secure Control Design for Networked Control Systems with Linear Dynamics under a Time-Delay Switch Attack. *Electronics (Switzerland)*, **2021**, 10, 322	2.6	4
133	Deep Learning in Smart Grid Technology: A Review of Recent Advancements and Future Prospects. *IEEE Access*, **2021**, 9, 54558-54578	3.5	21
132	A Review of Cyber-Physical Security for Photovoltaic Systems. **2021**, 1-1		7
131	A Recurrent Attention Model for Cyber Attack Classification. **2021**, 237-250		0
130	Privacy Preserving Federated Learning Solution for Security of Industrial Cyber Physical Systems. **2021**, 195-211		
129	CPS Attacks Mitigation Approaches on Power Electronic Systems With Security Challenges for Smart Grid Applications: A Review. *IEEE Access*, **2021**, 9, 38571-38601	3.5	5

128	Cyber Security of Smart Manufacturing Execution Systems: A Bibliometric Analysis. **2021**, 105-119		1
127	Exploiting Internet of Things Protocols for Malicious Data Exfiltration Activities. *IEEE Access*, **2021**, 9, 104261-104280	3.5	5
126	Machine learning-based energy efficient technologies for smart grid. **2021**, 31, e12744		2
125	A Multi-Stage Machine Learning Model for Security Analysis in Industrial Control System. **2021**, 213-236		1
124	Application of Deep Learning on IoT-Enabled Smart Grid Monitoring. **2021**, 77-103		0
123	Security Risk Modeling in Smart Grid Critical Infrastructures in the Era of Big Data and Artificial Intelligence. **2021**, 13, 3196		12
122	Detecting and locating cyber and physical stresses in smart grids using the k-nearest neighbour analysis of instantaneous correlation of states. **2021**, 4, 307-320		2
121	Prediction of burning performance and emissions indexes of a turboprop motor with artificial neural network. **2021**, 93, 394-409		0
120	. **2021**, 7, 35-60		8
119	Artificial Intelligence Techniques in Smart Grid: A Survey. **2021**, 4, 548-568		25
118	A Survey of Machine Learning-based Cyber-physical Attack Generation, Detection, and Mitigation in Smart-Grid. **2021**,		3
117	Intrusion Detection System for IOT Botnet Attacks Using Deep Learning. **2021**, 2, 1		5
116	Reliability Evaluation of Smart Microgrids Considering Cyber Failures and Disturbances under Various Cyber Network Topologies and Distributed Generation□s Scenarios. **2021**, 13, 5695		4
115	A Deep Learning-Based Cyberattack Detection System for Transmission Protective Relays. **2021**, 12, 2554-2565		7
114	Handling of stealthy sensor and actuator cyberattacks on evolving nonlinear process systems. **2021** , 3,		0
113	A Survey on Machine-Learning Based Security Design for Cyber-Physical Systems. **2021**, 11, 5458		6
112	Detection of false data cyber-attacks for the assessment of security in smart grid using deep learning. **2021**, 93, 107211		16
111	. **2021**, 12, 3624-3636		1

(2020-2021)

110	On the Pivotal Role of Artificial Intelligence Toward the Evolution of Smart Grids. **2021**, 359-420		2
109	Physical layer attack identification and localization in cyber-physical grid: An ensemble deep learning based approach. **2021**, 47, 101394		6
108	SDN-Based Resilient Smart Grid: The SDN-microSENSE Architecture. **2021**, 1, 173-187		4
107	Cybersecurity in Power Grids: Challenges and Opportunities. **2021**, 21,		5
106	Machine learning on sustainable energy: A review and outlook on renewable energy systems, catalysis, smart grid and energy storage. **2021**, 174, 414-441		20
105	Generative adversarial network to detect unseen Internet of Things malware. **2021**, 122, 102591		9
104	A Hybrid Deep Random Neural Network for Cyberattack Detection in the Industrial Internet of Things. *IEEE Access*, **2021**, 9, 55595-55605	3.5	20
103	Deep Representation Learning for Cyber-Attack Detection in Industrial IoT. **2021**, 139-162		1
102	The Role of Machine Learning in IIoT Through FPGAs. **2021**, 121-137		
101	Artificial Intelligence for Threat Detection and Analysis in Industrial IoT: Applications and Challenges. **2021**, 1-6		
100	Complementing IIoT Services Through AI: Feasibility and Suitability. **2021**, 7-19		2
99	Blockchain Applications in Power Systems: A Bibliometric Analysis. **2020**, 129-145		3
98	Anomaly Detection in Cyber-Physical Systems Using Machine Learning. **2020**, 219-235		12
97	Privacy and Security in Smart and Precision Farming: A Bibliometric Analysis. **2020**, 305-318		9
96	A Hybrid Deep Generative Local Metric Learning Method for Intrusion Detection. **2020**, 343-357		13
95	Industrial Big Data Analytics: Challenges and Opportunities. **2020**, 37-61		8
94	A Privacy Protection Key Agreement Protocol Based on ECC for Smart Grid. **2020**, 63-76		4
93	Applications of Big Data Analytics and Machine Learning in the Internet of Things. **2020**, 77-108		12

92	A Comparison of State-of-the-Art Machine Learning Models for OpCode-Based IoT Malware Detection. **2020**, 109-120	5
91	Artificial Intelligence and Security of Industrial Control Systems. **2020**, 121-164	5
90	Enhancing Network Security Via Machine Learning: Opportunities and Challenges. **2020**, 165-189	7
89	A Comparison Between Different Machine Learning Models for IoT Malware Detection. **2020**, 195-202	5
88	The Risk of Botnets in Cyber Physical Systems. **2020**, 81-106	5
87	Learning Based Anomaly Detection in Critical Cyber-Physical Systems. **2020**, 107-130	8
86	AI-Enabled Security Monitoring in Smart Cyber Physical Grids. **2020**, 145-167	6
85	Application of Machine Learning in State Estimation of Smart Cyber-Physical Grid. **2020**, 169-194	2
84	An Ensemble of Deep Recurrent Neural Networks for Detecting IoT Cyber Attacks Using Network Traffic. **2020**, 7, 8852-8859	49
83	An Ensemble Deep Convolutional Neural Network Model for Electricity Theft Detection in Smart Grids. **2020**,	7
82	. **2020**,	8
81	Introduction and Literature Review of Power System Challenges and Issues. **2021**, 19-43	1
80	. **2021**,	2
79	Deep Learning in IoT Intrusion Detection. **2022**, 30, 1	11
78	An Approach of Security Model to Mitigate Risk of Cyberattacks on Public Institutions in Ecuador. **2020**,	
77	The Spatial Analysis of the Malicious Uniform Resource Locators (URLs): 2016 Dataset Case Study. **2021**, 12, 2	1
76	False Data Injection Attacks in Smart Grid Using Gaussian Mixture Model. **2020**,	
75	Big Data and Privacy: Challenges and Opportunities. **2020**, 1-5	6

(2022-2020)

74	AI and Security of Critical Infrastructure. **2020**, 7-36		1
73	Big Data Application for Security of Renewable Energy Resources. **2020**, 237-254		1
72	Big-Data and Cyber-Physical Systems in Healthcare: Challenges and Opportunities. **2020**, 255-283		3
71	Design and Operation Framework for Industrial Control System Security Exercise. **2020**, 25-51		1
70	Privacy Preserving Abnormality Detection: A Deep Learning Approach. **2020**, 285-303		
69	A Survey on Application of Big Data in Fin Tech Banking Security and Privacy. **2020**, 319-342		3
68	Securing SCADA Systems against Cyber-Attacks using Artificial Intelligence. **2021**,		1
67	A Survey on Energy Efficiency in Smart Homes and Smart Grids. *Energies*, **2021**, 14, 7273	3.1	5
66	. *IEEE Access*, **2021**, 9, 152379-152396	3.5	4
65	Joint Adversarial Example and False Data Injection Attacks for State Estimation in Power Systems. **2021**, PP,		2
64	Adaptive Neural Trees for Attack Detection in Cyber Physical Systems. **2022**, 89-104		
63	Fuzzy Bayesian Learning for Cyber Threat Hunting in Industrial Control Systems. **2022**, 117-130		
62	Security of Industrial Cyberspace: Fair Clustering with Linear Time Approximation. **2022**, 75-88		
61	Scalable Fair Clustering Algorithm for Internet of Things Malware Classification. **2022**, 271-287		0
60	Cyber-Attack Detection in Cyber-Physical Systems Using Supervised Machine Learning. **2022**, 131-140		1
59	Evaluation of Scalable Fair Clustering Machine Learning Methods for Threat Hunting in Cyber-Physical Systems. **2022**, 141-158		
58	Time Series Anomaly Detection for Smart Grids: A Survey. **2021**,		1
57	Intrusion Resilience Analysis of Smart Meters. *Lecture Notes in Electrical Engineering*, **2022**, 377-391	0.2	

56	A Self-tuning Cyber-Attacks Location Identification Approach for Industrial Internet of Things. *IEEE Transactions on Industrial Informatics*, **2021**, 1-1	11.9	2
55	MQTT Attack Detection Using AI and ML Algorithm. *Lecture Notes in Networks and Systems*, **2022**, 13-22	0.5	
54	Optimized cyber-attack detection method of power systems using sliding mode observer. *Electric Power Systems Research*, **2022**, 205, 107745	3.5	1
53	Instability Prediction in Smart Cyber-physical Grids Using Feedforward Neural Networks. **2020**,		
52	Cyber-Attack Identification of Synchrophasor Data Via VMD and Multi-fusion SVM. *IEEE Transactions on Industry Applications*, **2022**, 1-1	4.3	0
51	A comprehensive survey on machine learning approaches for malware detection in IoT-based enterprise information system. *Enterprise Information Systems*, 1-25	3.5	15
50	Data-Driven Detection of Stealthy False Data Injection Attack Against Power System State Estimation. *IEEE Transactions on Industrial Informatics*, **2022**, 1-1	11.9	4
49	Salp Swarm-Artificial Neural Network Based Cyber-Attack Detection in Smart Grid. *Neural Processing Letters*,	2.4	0
48	LSTM based Deep Learning Technique to Forecast Internet of Things Attacks in MQTT Protocol. **2022**,		1
47	Data Integrity Attack in Dynamic State Estimation of Smart Grid: Attack Model and Countermeasures. *IEEE Transactions on Automation Science and Engineering*, **2022**, 1-14	4.9	0
46	Challenges and opportunities for the energy management of sustainable data centers in smart grids. *IOP Conference Series: Earth and Environmental Science*, **2022**, 984, 012005	0.3	
45	A Review on Conceptual Model of Cyber Attack Detection and Mitigation Using Deep Ensemble Model. *International Journal of Applied Engineering and Management Letters*, 149-159		
44	Novel SHP-ECC Mechanism Architecture for Attack Node Mitigation and to Predict Future Community Intrusions. *International Journal of Applied Engineering and Management Letters*, 176-183		1
43	Detection of false data injection attacks leading to line congestions using Neural Networks. *Sustainable Cities and Society*, **2022**, 103861	10.1	0
42	Data analytics for cybersecurity enhancement of transformer protection. **2021**, 1, 12-19		0
41	A Synoptic Review on Feature Selection and Machine Learning models used for Detecting Cyber Attacks in IoT. **2021**,		
40	Neural Networks-Based Detection of Cyber-Physical Attacks Leading to Blackouts in Smart Grids. **2021**,		
39	SteelEye: An Application-Layer Attack Detection and Attribution Model in Industrial Control Systems using Semi-Deep Learning. **2021**,		0

38	Intraday Optimization Control of IES with Hydrogen Injection under Attack Scenarios. **2021**,		
37	Deep Federated Learning-Based Cyber-Attack Detection in Industrial Control Systems. **2021**,		0
36	Adequacy and Limitations of the Information Technology Act in Addressing Cyber-Security Issues of Indian Power Systems. **2021**,		
35	Identification of the best model to predict optical properties of water. *Environment, Development and Sustainability*, 1	4.5	1
34	Smart Grid Security and Privacy: From Conventional to Machine Learning Issues (Threats and Countermeasures). *IEEE Access*, **2022**, 1-1	3.5	0
33	Recent review of Distributed Denial of Service Attacks in the Internet of Things. **2022**,		0
32	Anomaly Detection in Multi-Host Environment Based on Federated Hypersphere Classifier. *Electronics (Switzerland)*, **2022**, 11, 1529	2.6	
31	Monitoring and Controlling of Smart Grid Based on Cyber-Physical System. *Lecture Notes in Electrical Engineering*, **2022**, 637-654	0.2	0
30	Anomaly Detection in Smart Grids: A Survey From Cybersecurity Perspective*. **2022**,		1
29	Intrusion Detection Method Based on SMOTE Transformation for Smart Grid Cybersecurity. **2022**,		0
28	Heuristic Intrusion Detection Based on Traffic Flow Statistical Analysis. *Energies*, **2022**, 15, 3951	3.1	0
27	A Synoptic Review on Feature Selection and Machine Learning models used for Detecting Cyber Attacks in IoT. **2021**,		
26	A Review of Unsupervised Machine Learning Frameworks for Anomaly Detection in Industrial Applications. *Lecture Notes in Networks and Systems*, **2022**, 158-189	0.5	
25	A Survey on Network Security for Cyber-Physical Systems: From Threats to Resilient Design. *IEEE Communications Surveys and Tutorials*, **2022**, 1-1	37.1	3
24	Machine learning for cybersecurity in smart grids: A comprehensive review-based study on methods, solutions, and prospects. *International Journal of Critical Infrastructure Protection*, **2022**, 38, 100547	4.1	1
23	Facilitating DoS Attack Detection using Unsupervised Anomaly Detection. **2022**,		
22	Intelligent Intrusion Detection Scheme for Smart Power-Grid Using Optimized Ensemble Learning on Selected Features. **2022**, 39, 100567		0
21	Improving the Stability of Intrusion Detection with Causal Deep Learning. **2022**, 1-1		0

20	Leveraging the Influence of Power Grid Links in Renewable Energy Power Generation. **2022**, 10, 100234-100246	0
19	Digital Modeling System for Dynamic Nonlinear Systems of Power Equipment in Digital Grids and 5G. **2022**, 2022, 1-11	1
18	Accurate threat hunting in industrial internet of things edge devices. **2022**,	0
17	A systematic review of machine learning techniques related to local energy communities. **2022**, 170, 112651	0
16	Smart Grid Cyber Security Enhancement: Challenges and SolutionsA Review. **2022**, 14, 14226	2
15	Recurrent nonsymmetric deep auto encoder approach for network intrusion detection system. **2022**, 24, 100527	0
14	An ensemble deep federated learning cyber-threat hunting model for Industrial Internet of Things. **2022**,	1
13	A comprehensive review of cyber-attacks and defense mechanisms for improving security in smart grid energy systems: Past, present and future. **2023**, 215, 108975	9
12	Evaluating Synthetic Datasets for Training Machine Learning Models to Detect Malicious Commands. **2022**,	0
11	An innovative deep anomaly detection of building energy consumption using energy time-series images. **2023**, 119, 105775	0
10	A Comparative Analysis of Supervised and Unsupervised Models for Detecting Attacks on the Intrusion Detection Systems. **2023**, 14, 103	2
9	A Supervised Early Attack Detection Mechanism for Smart Grid Networks. **2023**,	0
8	A Survey of Explainable Artificial Intelligence for Smart Cities. **2023**, 12, 1020	2
7	Hybrid ML-Based Technique to Classify Malicious Activity Using Log Data of Systems. **2023**, 13, 2707	0
6	Data-Driven Apprehension of Cyber and Physical Anomalies in Distribution System. **2022**,	0
5	A Review of Data-Driven Approaches with Emphasis on Machine Learning Base Intrusion Detection Algorithms. **2022**,	0
4	An Artificial Intelligence Enabled Self Replication System Against Cyber Attacks. **2023**,	0
3	A Review on Cyber Security and Anomaly Detection Perspectives of Smart Grid. **2023**,	0

2	Artificial Intelligence Techniques: Smart Way to Smart Grid. **2023**,	0
1	Encrypted Cost Based Load Forecasting With Attack Regression Capacity for CPS Model Based Anomaly Detection in Smart Grid Security. **2023**,	0