Transfer learning for detecting unknown network attacks

#	Paper	IF	Citations
59	An Adaptive Ensemble Machine Learning Model for Intrusion Detection. *IEEE Access*, **2019**, 7, 82512-82521.	3.5	109
58	Utilising Deep Learning Techniques for Effective Zero-Day Attack Detection. *Electronics (Switzerland)*, **2020**, 9, 1684	2.6	18
57	Learning to Learn Sequential Network Attacks Using Hidden Markov Models. *IEEE Access*, **2020**, 8, 134480-134497	3.5	9
56	Image-Based Feature Representation for Insider Threat Classification. *Applied Sciences (Switzerland)*, **2020**, 10, 4945	2.6	2
55	Deep learning methods in network intrusion detection: A survey and an objective comparison. *Journal of Network and Computer Applications*, **2020**, 169, 102767	7.9	74
54	Recognition and location of typical automotive parts based on the RGB-D camera. *Complex & Intelligent Systems*, **2020**, 7, 1759	7.1	3
53	Deep Transfer Learning for IoT Attack Detection. *IEEE Access*, **2020**, 8, 107335-107344	3.5	22
52	Deep Cybersecurity: A Comprehensive Overview from Neural Network and Deep Learning Perspective. *SN Computer Science*, **2021**, 2, 1	2	27
51	PF-TL: Payload Feature-Based Transfer Learning for Dealing with the Lack of Training Data. *Electronics (Switzerland)*, **2021**, 10, 1148	2.6	1
50	Machine learning for network application security: Empirical evaluation and optimization. *Computers and Electrical Engineering*, **2021**, 91, 107052	4.3	6
49	VSCL: Automating Vulnerability Detection in Smart Contracts with Deep Learning. **2021**,		3
48	Transfer Learning Promotes 6G Wireless Communications: Recent Advances and Future Challenges. *IEEE Transactions on Reliability*, **2021**, 70, 790-807	4.6	42
47	Deep learning-based feature extraction and optimizing pattern matching for intrusion detection using finite state machine. *Computers and Electrical Engineering*, **2021**, 92, 107094	4.3	2
46	. **2021**,		2
45	UMVD-FSL: Unseen Malware Variants Detection Using Few-Shot Learning. **2021**,		0
44	Forecasting loss of signal in optical networks with machine learning. *Journal of Optical Communications and Networking*, **2021**, 13, E109	4.1	2
43	XFinder: Detecting Unknown Anomalies in Distributed Machine Learning Scenario. *Frontiers in Computer Science*, **2021**, 3,	3.4	

42	Cyber Security Risks in MENA Region: Threats, Challenges and Countermeasures. *Advances in Intelligent Systems and Computing*, **2020**, 912-921	0.4	7
41	Anomaly Network Traffic Detection Based on Deep Transfer Learning. *Advances in Intelligent Systems and Computing*, **2021**, 384-393	0.4	1
40	Preparing Network Intrusion Detection Deep Learning Models with Minimal Data Using Adversarial Domain Adaptation. **2020**,		6
39	An Intrusion Detection Framework for IoT Using Partial Domain Adaptation. *Lecture Notes in Computer Science*, **2021**, 36-50	0.9	
38	A Survey on Data-driven Network Intrusion Detection. *ACM Computing Surveys*, **2022**, 54, 1-36	13.4	6
37	TransNet: Unseen Malware Variants Detection Using Deep Transfer Learning. *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering*, **2020**, 84-101	0.2	2
36	Unsupervised Domain Adaptation for Static Malware Detection based on Gradient Boosting Trees. **2021**,		0
35	Multimodal Biometric Authentication by Slap Swarm-Based Score Level Fusion. *Lecture Notes on Data Engineering and Communications Technologies*, **2022**, 831-842	0.4	
34	Network unknown-threat detection based on a generative adversarial network and evolutionary algorithm. *International Journal of Intelligent Systems*,	8.4	1
33	A Continuous Learning Approach for Real-Time Network Intrusion Detection. *International Journal of Neural Systems*, **2021**, 31, 2150060	6.2	0
32	Review on Deep Learning based Network Security Tools in Detecting Real-Time Vulnerabilities. *Journal of Ubiquitous Computing and Communication Technologies*, **2021**, 3, 289-302	2.5	0
31	Resilience of Smart Integrated Energy Systems. **2022**, 1-27		
30	Statistical and Signature Analysis Methods of Intrusion Detection. *Lecture Notes on Data Engineering and Communications Technologies*, **2022**, 115-131	0.4	
29	Multi-Aspect Based Approach to Attack Detection in IoT Clouds.. *Sensors*, **2022**, 22,	3.8	0
28	ATTL: An Automated Targeted Transfer Learning with Deep Neural Networks. **2021**,		0
27	Selective Targeted Transfer Learning for Malware Classification. **2021**,		
26	A novel network intrusion detection model based on two-phase detection and manually labeling. **2022**,		
25	A survey on deep learning for cybersecurity: Progress, challenges, and opportunities. *Computer Networks*, **2022**, 109032	5.4	5

24	Deep Transfer Learning for IoT Intrusion Detection. **2022**,	
23	Una revisi𝔦 del Aprendizaje profundo aplicado a la ciberseguridad. **2022**, 9, 57-65	
22	SALT: transfer learning-based threat model for attack detection in smart home. *Scientific Reports*, **2022**, 12,	4.9
21	Design of Network Intrusion Detection Model Based on TCA. *Security and Communication Networks*, **2022**, 2022, 1-6	1.9
20	DeepCAD: A Stand-alone Deep Neural Network-based Framework for Classification and Anomaly Detection in Smart Healthcare Systems. **2022**,	0
19	Transfer learning for raw network traffic detection. **2022**, 118641	1
18	Unbalanced network attack traffic detection based on feature extraction and GFDA-WGAN. **2022**, 216, 109283	0
17	Cross-domain Industrial Intrusion Detection Deep Model Trained with Imbalanced Data. **2022**, 1-1	0
16	Towards Zero-Shot Flow-Based Cyber-Security Anomaly Detection Framework. **2022**, 12, 9636	4
15	EEFED: Personalized federated learning of Execution&Evaluation dual network for CPS intrusion detection. **2022**, 1-1	0
14	A deep learning based model for detection of Android malwares using PCA over physical devices. **2022**,	0
13	Data Discretization and Decision Boundary Data Point Analysis for Unknown Attack Detection. **2022**, 10, 114008-114015	0
12	Federated Learning-Based Cyber Threat Hunting for APT Attack Detection in SDN-Enabled Networks. **2022**,	0
11	Transfer learning and fine-tuned transfer learning methodsℤeffectiveness analyse in the CNN-based deep learning models.	0
10	Unknown Attack Detection Based on Multistage One-Class SVM. **2022**,	0
9	DA-GAN: Domain Adaptation for Generative Adversarial Networks-assisted Cyber Threat Detection. **2022**,	0
8	Risk-Aware SFC Placement Method in Edge Cloud Environment. **2023**, 105-116	0
7	Image-Based Intrusion Detection in ̇Network Traffic. **2023**, 51-60	0

6	Cross-domain network attack detection enabled by heterogeneous transfer learning. **2023**, 227, 109692	0
5	Zero Day Threat Detection Using Graph and Flow Based Security Telemetry. **2022**,	0
4	Data Analytics Applications in Digital Energy System Operation. **2023**, 25-52	0
3	Zero-day attack detection: a systematic literature review.	0
2	Network Security Situation Awareness Forecasting Based on Neural Networks. **2023**, 255-270	0
1	FLAP - A Federated Learning Framework for Attribute-based Access Control Policies. **2023**,	0