

Hyun Kwon

List of Publications by Year in descending order

Source: <https://exaly.com/author-pdf/7740971/publications.pdf>

Version: 2024-02-01

45
papers

491
citations

687363

13
h-index

794594

19
g-index

48
all docs

48
docs citations

48
times ranked

340
citing authors

#	ARTICLE	IF	CITATIONS
1	AdvGuard: Fortifying Deep Neural Networks Against Optimized Adversarial Example Attack. IEEE Access, 2024, 12, 5345-5356.	4.2	14
2	Friend-Guard Textfooler Attack on Text Classification System. IEEE Access, 2024, , 1-1.	4.2	9
3	Defending Deep Neural Networks against Backdoor Attack by Using De-trigger Autoencoder. IEEE Access, 2024, , 1-1.	4.2	15
4	Dual-Targeted Textfooler Attack on Text Classification Systems. IEEE Access, 2023, 11, 15164-15173.	4.2	2
5	Optimized Adversarial Example With Classification Score Pattern Vulnerability Removed. IEEE Access, 2022, 10, 35804-35813.	4.2	2
6	Compliance-Driven Cybersecurity Planning Based on Formalized Attack Patterns for Instrumentation and Control Systems of Nuclear Power Plants. Security and Communication Networks, 2022, 2022, 1-13.	1.5	0
7	BlindNet backdoor: Attack on deep neural network using blind watermark. Multimedia Tools and Applications, 2022, 81, 6217-6234.	3.9	27
8	Multi-Model Selective Backdoor Attack with Different Trigger Positions. IEICE Transactions on Information and Systems, 2022, E105.D, 170-174.	0.7	7
9	Ensemble transfer attack targeting text classification systems. Computers and Security, 2022, 117, 102695.	6.0	13
10	Textual Adversarial Training of Machine Learning Model for Resistance to Adversarial Examples. Security and Communication Networks, 2022, 2022, 1-12.	1.5	3
11	Automatic Measurements of Garment Sizes Using Computer Vision Deep Learning Models and Point Cloud Data. Applied Sciences (Switzerland), 2022, 12, 5286.	2.5	3
12	AdvU-Net: Generating Adversarial Example Based on Medical Image and Targeting U-Net Model. Journal of Sensors, 2022, 2022, 1-13.	1.1	5
13	Restricted-Area Adversarial Example Attack for Image Captioning Model. Wireless Communications and Mobile Computing, 2022, 2022, 1-9.	1.2	3
14	Classification score approach for detecting adversarial example in deep neural network. Multimedia Tools and Applications, 2021, 80, 10339-10360.	3.9	21
15	Diversity Adversarial Training against Adversarial Attack on Deep Neural Networks. Symmetry, 2021, 13, 428.	2.2	10
16	MedicalGuard: U-Net Model Robust against Adversarially Perturbed Images. Security and Communication Networks, 2021, 2021, 1-8.	1.5	10
17	SqueezeFace: Integrative Face Recognition Methods with LiDAR Sensors. Journal of Sensors, 2021, 2021, 1-8.	1.1	9
18	Data Correction For Enhancing Classification Accuracy By Unknown Deep Neural Network Classifiers. KSII Transactions on Internet and Information Systems, 2021, 15, .	0.3	0

#	ARTICLE	IF	CITATIONS
19	Adv-Plate Attack: Adversarially Perturbed Plate for License Plate Recognition System. Journal of Sensors, 2021, 2021, 1-10.	1.1	5
20	Textual Backdoor Attack for the Text Classification System. Security and Communication Networks, 2021, 2021, 1-11.	1.5	7
21	Selective Audio Adversarial Example in Evasion Attack on Speech Recognition System. IEEE Transactions on Information Forensics and Security, 2020, 15, 526-538.	6.9	40
22	Acoustic-decoy: Detection of adversarial examples through audio modification on speech recognition system. Neurocomputing, 2020, 417, 357-370.	5.9	26
23	Detecting Backdoor Attacks via Class Difference in Deep Neural Networks. IEEE Access, 2020, 8, 191049-191056.	4.2	15
24	CAPTCHA Image Generation: Two-Step Style-Transfer Learning in Deep Neural Networks. Sensors, 2020, 20, 1495.	3.8	6
25	Robust CAPTCHA Image Generation Enhanced with Adversarial Example Methods. IEICE Transactions on Information and Systems, 2020, E103.D, 879-882.	0.7	12
26	CAPTCHA Image Generation Using Style Transfer Learning in Deep Neural Network. Lecture Notes in Computer Science, 2020, , 234-246.	1.3	3
27	Multi-Targeted Backdoor: Identifying Backdoor Attack for Multiple Deep Neural Networks. IEICE Transactions on Information and Systems, 2020, E103.D, 883-887.	0.7	19
28	FriendNet Backdoor. , 2020, , .		3
29	TargetNet Backdoor. , 2020, , .		4
30	Restricted Evasion Attack: Generation of Restricted-Area Adversarial Example. IEEE Access, 2019, , 1-1.	4.2	12
31	Selective Poisoning Attack on Deep Neural Networks. Symmetry, 2019, 11, 892.	2.2	13
32	Selective Untargeted Evasion Attack: An Adversarial Example That Will Not Be Classified as Certain Avoided Classes. IEEE Access, 2019, 7, 73493-73503.	4.2	3
33	Face Friend-Safe Adversarial Example on Face Recognition System. , 2019, , .		4
34	Selective Poisoning Attack on Deep Neural Network to Induce Fine-Grained Recognition Error. , 2019, , .		3
35	Priority Adversarial Example in Evasion Attack on Multiple Deep Neural Networks. , 2019, , .		2
36	Rootkit inside GPU Kernel Execution. IEICE Transactions on Information and Systems, 2019, E102.D, 2261-2264.	0.7	0

#	ARTICLE	IF	CITATIONS
37	Instruction2vec: Efficient Preprocessor of Assembly Code to Detect Software Weakness with CNN. Applied Sciences (Switzerland), 2019, 9, 4086.	2.5	23
38	Friend-Safe Adversarial Examples in an Evasion Attack on a Deep Neural Network. Lecture Notes in Computer Science, 2018, , 351-367.	1.3	0
39	Random Untargeted Adversarial Example on Deep Neural Network. Symmetry, 2018, 10, 738.	2.2	16
40	Fooling a Neural Network in Military Environments: Random Untargeted Adversarial Example. , 2018, , .		5
41	Advanced Ensemble Adversarial Example on Unknown Deep Neural Network Classifiers. IEICE Transactions on Information and Systems, 2018, E101.D, 2485-2500.	0.7	14
42	CAPTCHA Image Generation Systems Using Generative Adversarial Networks. IEICE Transactions on Information and Systems, 2018, E101.D, 543-546.	0.7	18
43	Friend-safe evasion attack: An adversarial example that is correctly recognized by a friendly classifier. Computers and Security, 2018, 78, 380-397.	6.0	19
44	Multi-Targeted Adversarial Example in Evasion Attack on Deep Neural Network. IEEE Access, 2018, 6, 46084-46096.	4.2	31
45	Optimal Cluster Expansion-Based Intrusion Tolerant System to Prevent Denial of Service Attacks. Applied Sciences (Switzerland), 2017, 7, 1186.	2.5	11