Shamsul Huda

List of Publications by Year
in descending order

34	1,515	304743	395702
papers	citations	22 h-index	33 g-index

34	34	34	1653
all docs	docs citations	times ranked	citing authors

#	Article	IF	Citations
1	Human emotion recognition using deep belief network architecture. Information Fusion, 2019, 51, 10-18.	19.1	212
2	A Hybrid Feature Selection With Ensemble Classification for Imbalanced Healthcare Data: A Case Study for Brain Tumor Diagnosis. IEEE Access, 2016, 4, 9145-9154.	4.2	114
3	Hybrids of support vector machine wrapper and filter based framework for malware detection. Future Generation Computer Systems, 2016, 55, 376-390.	7.5	94
4	Increasing the Trustworthiness in the Industrial IoT Networks Through a Reliable Cyberattack Detection Model. IEEE Transactions on Industrial Informatics, 2020, 16, 6154-6162.	11.3	89
5	An Ensemble Oversampling Model for Class Imbalance Problem in Software Defect Prediction. IEEE Access, 2018, 6, 24184-24195.	4.2	83
6	Defending unknown attacks on cyber-physical systems by semi-supervised approach and available unlabeled data. Information Sciences, 2017, 379, 211-228.	6.9	77
7	Human Activity Recognition from Body Sensor Data using Deep Learning. Journal of Medical Systems, 2018, 42, 99.	3.6	77
8	Securing the operations in SCADA-IoT platform based industrial control system using ensemble of deep belief networks. Applied Soft Computing Journal, 2018, 71, 66-77.	7.2	74
9	A system call refinement-based enhanced Minimum Redundancy Maximum Relevance method for ransomware early detection. Journal of Network and Computer Applications, 2020, 167, 102753.	9.1	58
10	An approach for Ewing test selection to support the clinical assessment of cardiac autonomic neuropathy. Artificial Intelligence in Medicine, 2013, 58, 185-193.	6.5	56
11	A Framework for Software Defect Prediction and Metric Selection. IEEE Access, 2018, 6, 2844-2858.	4.2	56
12	Prostate cancer classification from ultrasound and MRI images using deep learning based Explainable Artificial Intelligence. Future Generation Computer Systems, 2022, 127, 462-472.	7.5	49
13	A malicious threat detection model for cloud assisted internet of things (CoT) based industrial control system (ICS) networks using deep belief network. Journal of Parallel and Distributed Computing, 2018, 120, 23-31.	4.1	47
14	A robust cyberattack detection approach using optimal features of SCADA power systems in smart grids. Applied Soft Computing Journal, 2020, 96, 106658.	7.2	40
15	Identifying cyber threats to mobile-IoT applications in edge computing paradigm. Future Generation Computer Systems, 2018, 89, 525-538.	7.5	38
16	A hybrid-multi filter-wrapper framework to identify run-time behaviour for fast malware detection. Future Generation Computer Systems, 2018, 83, 193-207.	7.5	36
17	Early detection of cardiovascular autonomic neuropathy: A multi-class classification model based on feature selection and deep learning feature fusion. Information Fusion, 2022, 77, 70-80.	19.1	35
18	A Robust Deep-Learning-Enabled Trust-Boundary Protection for Adversarial Industrial IoT Environment. IEEE Internet of Things Journal, 2021, 8, 9611-9621.	8.7	34

#	Article	IF	Citations
19	Avoiding Future Digital Extortion Through Robust Protection Against Ransomware Threats Using Deep Learning Based Adaptive Approaches. IEEE Access, 2020, 8, 24522-24534.	4.2	32
20	Multistage fusion approaches based on a generative model and multivariate exponentially weighted moving average for diagnosis of cardiovascular autonomic nerve dysfunction. Information Fusion, 2018, 41, 105-118.	19.1	28
21	A hybrid wrapperâ€“filter approach to detect the source(s) of out-of-control signals in multivariate manufacturing process. European Journal of Operational Research, 2014, 237, 857-870.	5.7	25
22	An adaptive framework against android privilege escalation threats using deep learning and semi-supervised approaches. Applied Soft Computing Journal, 2020, 89, 106089.	7.2	25
23	A parallel framework for software defect detection and metric selection on cloud computing. Cluster Computing, 2017, 20, 2267-2281.	5.0	20
24	A Weighted Minimum Redundancy Maximum Relevance Technique for Ransomware Early Detection in Industrial IoT. Sustainability, 2022, 14, 1231.	3.2	20
25	Automatic extraction and integration of behavioural indicators of malware for protection of cyberâ€“physical networks. Future Generation Computer Systems, 2019, 101, 1247-1258.	7.5	18
26	Exponentially weighted control charts to monitor multivariate process variability for high dimensions. International Journal of Production Research, 2017, 55, 4948-4962.	7.5	16
27	A Constraint-Based Evolutionary Learning Approach to the Expectation Maximization for Optimal Estimation of the Hidden Markov Model for Speech Signal Modeling. IEEE Transactions on Systems, Man, and Cybernetics, 2009, 39, 182-197.	5.0	14
28	Improving malicious PDF classifier with feature engineering: A data-driven approach. Future Generation Computer Systems, 2021, 115, 314-326.	7.5	14
29	A stochastic version of Expectation Maximization algorithm for better estimation of Hidden Markov Model. Pattern Recognition Letters, 2009, 30, 1301-1309.	4.2	13
30	A predictive intelligence approach to classify brainâ€“computer interface based eye state for smart living. Applied Soft Computing Journal, 2021, 108, 107453.	7.2	9
31	An Advanced Boundary Protection Control for the Smart Water Network Using Semisupervised and Deep Learning Approaches. IEEE Internet of Things Journal, 2022, 9, 7298-7310.	8.7	8
32	An Edge Tier Task Offloading to Identify Sources of Variance Shifts in Smart Grid Using a Hybrid of Wrapper and Filter Approaches. IEEE Transactions on Green Communications and Networking, 2022, 6, 329-340.	5.5	3
33	Fault Diagnostic of Variance Shifts in Clinical Monitoring Using an Artificial Neural Network Input Gain Measurement Approximation (ANNIGMA). Advances in Intelligent Systems and Computing, 2018, , 295-300.	0.6	1
34	Lightweight Authenticated Encryption for Cloud-assisted IoT Applications. Lecture Notes in Electrical Engineering, 2021, , 295-299.	0.4	0