Hayretdin Bahsi

List of Publications by Year
in descending order

Source: https://exaly.com/author-pdf/1860250/publications.pdf

Version: 2024-02-01

25 papers	307 citations	1874746 5 h-index	1526636 10 g-index
27 all docs	27 docs citations	27 times ranked	233 citing authors

#	Article	IF	Citations
1	Using MedBIoT Dataset toÂBuild Effective Machine Learning-Based IoT Botnet Detection Systems. Communications in Computer and Information Science, 2022, , 222-243.	0.4	0
2	Concept drift and cross-device behavior: Challenges and implications for effective android malware detection. Computers and Security, 2022, 120, 102757.	4.0	11
3	On the relativity of time: Implications and challenges of data drift on long-term effective android malware detection. Computers and Security, 2022, 122, 102835.	4.0	6
4	A machine learning-based forensic tool for image classification - A design science approach. Forensic Science International: Digital Investigation, 2021, 38, 301265.	1.2	3
5	KronoDroid: Time-based Hybrid-featured Dataset for Effective Android Malware Detection and Characterization. Computers and Security, 2021, 110, 102399.	4.0	37
6	MedBIoT: Generation of an IoT Botnet Dataset in a Medium-sized IoT Network. , 2020, , .		54
7	Model-Based Analysis of Secure and Patient-Dependent Pacemaker Monitoring System. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, 2020, , 77-91.	0.2	0
8	Mapping the Information Flows for the Architecture of a Nationwide Situation Awareness System : (Poster). , 2019, , .		0
9	The cyber-insurance market in Norway. Information and Computer Security, 2019, 28, 54-67.	1.5	14
10	Towards the Integration of a Post-Hoc Interpretation Step into the Machine Learning Workflow for IoT Botnet Detection. , 2019, , .		9
11	Expert Knowledge Elicitation for Skill Level Categorization of Attack Paths. , 2019, , .		0
12	Hybrid Feature Selection Models for Machine Learning Based Botnet Detection in IoT Networks. , 2019, , .		28
13	Time-frame Analysis of System Calls Behavior in Machine Learning-Based Mobile Malware Detection. , 2019, , .		2
14	Differences in Android Behavior Between Real Device and Emulator: A Malware Detection Perspective. , 2019, , .		5
15	In-depth Feature Selection and Ranking for Automated Detection of Mobile Malware. , 2019, , .		5
16	Unsupervised Anomaly Based Botnet Detection in IoT Networks. , 2018, , .		53
17	Dimensionality Reduction for Machine Learning Based IoT Botnet Detection. , 2018, , .		45
18	A case study about the use and evaluation of cyber deceptive methods against highly targeted attacks. , 2017, , .		3

#	Article	IF	Citations
19	Impact assessment of cyber attacks: A quantification study on power generation systems. , 2016, , .		7
20	A Conceptual Nationwide Cyber Situational Awareness Framework for Critical Infrastructures. Lecture Notes in Computer Science, 2015, , 3-10.	1.0	4
21	Securityâ€level classification for confidential documents by using adaptive neuroâ€fuzzy inference systems. Expert Systems, 2013, 30, 233-242.	2.9	1
22	Classification of confidential documents by using adaptive neurofuzzy inference systems. Procedia Computer Science, 2011, 3, 1412-1417.	1.2	9
23	Data Collection Framework for Energy Efficient Privacy Preservation in Wireless Sensor Networks Having Many-to-Many Structures. Sensors, 2010, 10, 8375-8397.	2.1	2
24	Security Level Classification of Confidential Documents Written in Turkish. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, 2010, , 329-334.	0.2	2
25	Energy Efficient Privacy Preserved Data Gathering in Wireless Sensor Networks Having Multiple Sinks. , 2009, , .		4