

Rafal Kozik

List of Publications by Citations

Source: <https://exaly.com/author-pdf/1015793/rafal-kozik-publications-by-citations.pdf>

Version: 2024-04-25

This document has been generated based on the publications and citations recorded by exaly.com. For the latest version of this publication list, visit the link given above.

The third column is the impact factor (IF) of the journal, and the fourth column is the number of citations of the article.

128
papers

743
citations

12
h-index

20
g-index

137
ext. papers

1,036
ext. citations

1.4
avg, IF

5.03
L-index

#	Paper	IF	Citations
128	A scalable distributed machine learning approach for attack detection in edge computing environments. <i>Journal of Parallel and Distributed Computing</i> , 2018 , 119, 18-26	4.4	65
127	Contactless palmprint and knuckle biometrics for mobile devices. <i>Pattern Analysis and Applications</i> , 2012 , 15, 73-85	2.3	49
126	Defending network intrusion detection systems against adversarial evasion attacks. <i>Future Generation Computer Systems</i> , 2020 , 110, 148-154	7.5	34
125	Simulation platform for cyber-security and vulnerability analysis of critical infrastructures. <i>Journal of Computational Science</i> , 2017 , 22, 179-186	3.4	28
124	Machine learning techniques applied to detect cyber attacks on web applications. <i>Logic Journal of the IGPL</i> , 2015 , 23, 45-56	1	25
123	A Deep Learning Ensemble for Network Anomaly and Cyber-Attack Detection. <i>Sensors</i> , 2020 , 20,	3.8	24
122	Advanced services for critical infrastructures protection. <i>Journal of Ambient Intelligence and Humanized Computing</i> , 2015 , 6, 783-795	3.7	16
121	Distributing extreme learning machines with Apache Spark for NetFlow-based malware activity detection. <i>Pattern Recognition Letters</i> , 2018 , 101, 14-20	4.7	16
120	Sentiment Analysis for Fake News Detection by Means of Neural Networks. <i>Lecture Notes in Computer Science</i> , 2020 , 653-666	0.9	15
119	Network Traffic Prediction and Anomaly Detection Based on ARFIMA Model. <i>Advances in Intelligent Systems and Computing</i> , 2014 , 545-554	0.4	14
118	Q-Rapids Tool Prototype: Supporting Decision-Makers in Managing Quality in Rapid Software Development. <i>Lecture Notes in Business Information Processing</i> , 2018 , 200-208	0.6	13
117	Correlation Approach for SQL Injection Attacks Detection. <i>Advances in Intelligent Systems and Computing</i> , 2013 , 177-185	0.4	13
116	SocialTruth Project Approach to Online Disinformation (Fake News) Detection and Mitigation 2019 ,		11
115	Hybrid Model for Improving the Classification Effectiveness of Network Intrusion Detection. <i>Advances in Intelligent Systems and Computing</i> , 2021 , 405-414	0.4	11
114	Comprehensive Approach to Increase Cyber Security and Resilience 2015 ,		10
113	Data-driven and tool-supported elicitation of quality requirements in agile companies. <i>Software Quality Journal</i> , 2020 , 28, 931-963	1.2	10
112	Machine Learning Methods for Fake News Classification. <i>Lecture Notes in Computer Science</i> , 2019 , 332-339		10

111	Machine Learning [The Results Are Not the only Thing that Matters! What About Security, Explainability and Fairness?]. <i>Lecture Notes in Computer Science</i> , 2020 , 615-628	0.9	10
110	A Practical Framework and Guidelines to Enhance Cyber Security and Privacy. <i>Advances in Intelligent Systems and Computing</i> , 2015 , 485-495	0.4	10
109	A Proposal of Algorithm for Web Applications Cyber Attack Detection. <i>Lecture Notes in Computer Science</i> , 2014 , 680-687	0.9	10
108	Achieving Explainability of Intrusion Detection System by Hybrid Oracle-Explainer Approach 2020 ,		10
107	Knuckle Biometrics Based on Texture Features 2010 ,		9
106	Fake News Detection from Data Streams 2020 ,		9
105	Pattern Recognition Solutions for Fake News Detection. <i>Lecture Notes in Computer Science</i> , 2018 , 130-139	0.9	9
104	Current cyber security threats and challenges in critical infrastructures protection 2013 ,		8
103	Ontology Applied in Decision Support System for Critical Infrastructures Protection. <i>Lecture Notes in Computer Science</i> , 2010 , 671-680	0.9	8
102	Modelling HTTP Requests with Regular Expressions for Detection of Cyber Attacks Targeted at Web Applications. <i>Advances in Intelligent Systems and Computing</i> , 2014 , 527-535	0.4	8
101	Lightweight Verification Schema for Image-Based Palmprint Biometric Systems. <i>Mobile Information Systems</i> , 2019 , 2019, 1-9	1.4	7
100	DWT-based anomaly detection method for cyber security of wireless sensor networks. <i>Security and Communication Networks</i> , 2016 , 9, 2911-2922	1.9	7
99	Packets tokenization methods for web layer cyber security. <i>Logic Journal of the IGPL</i> , 2017 , 25, 103-113	1	7
98	Adapting an Ensemble of One-Class Classifiers for a Web-Layer Anomaly Detection System 2015 ,		7
97	The overview of trends and challenges in mobile biometrics. <i>Journal of Applied Mathematics and Computational Mechanics</i> , 2017 , 16, 173-185	2.1	7
96	Data-Driven Elicitation of Quality Requirements in Agile Companies. <i>Communications in Computer and Information Science</i> , 2019 , 49-63	0.3	7
95	Decision Aid Tool and Ontology-Based Reasoning for Critical Infrastructure Vulnerabilities and Threats Analysis. <i>Lecture Notes in Computer Science</i> , 2010 , 98-110	0.9	7
94	Network Events Correlation for Federated Networks Protection System. <i>Lecture Notes in Computer Science</i> , 2011 , 100-111	0.9	7

93	A new method of hybrid time window embedding with transformer-based traffic data classification in IoT-networked environment. <i>Pattern Analysis and Applications</i> , 2021 , 24, 1441	2.3	7
92	Patterns Extraction Method for Anomaly Detection in HTTP Traffic. <i>Advances in Intelligent Systems and Computing</i> , 2015 , 227-236	0.4	6
91	Pattern Extraction Algorithm for NetFlow-Based Botnet Activities Detection. <i>Security and Communication Networks</i> , 2017 , 2017, 1-10	1.9	6
90	Extreme Learning Machines for Web Layer Anomaly Detection. <i>Advances in Intelligent Systems and Computing</i> , 2017 , 226-233	0.4	6
89	New explainability method for BERT-based model in fake news detection. <i>Scientific Reports</i> , 2021 , 11, 23705	4.9	6
88	Solution to Data Imbalance Problem in Application Layer Anomaly Detection Systems. <i>Lecture Notes in Computer Science</i> , 2016 , 441-450	0.9	6
87	Practical Employment of Granular Computing to Complex Application Layer Cyberattack Detection. <i>Complexity</i> , 2019 , 2019, 1-9	1.6	5
86	Measuring and Improving Agile Processes in a Small-Size Software Development Company. <i>IEEE Access</i> , 2020 , 8, 78452-78466	3.5	5
85	The HTTP Content Segmentation Method Combined with AdaBoost Classifier for Web-Layer Anomaly Detection System. <i>Advances in Intelligent Systems and Computing</i> , 2017 , 555-563	0.4	5
84	Ontology-Based Decision Support for Security Management in Heterogeneous Networks. <i>Lecture Notes in Computer Science</i> , 2009 , 920-927	0.9	5
83	Evaluation of guard channel admission control schemes for IEEE 802.16 with integrated nb-LDPC codes 2009 ,		5
82	Software Development Metrics Prediction Using Time Series Methods. <i>Lecture Notes in Computer Science</i> , 2019 , 311-323	0.9	5
81	The Feasibility of Deep Learning Use for Adversarial Model Extraction in the Cybersecurity Domain. <i>Lecture Notes in Computer Science</i> , 2019 , 353-360	0.9	5
80	Application of the BERT-Based Architecture in Fake News Detection. <i>Advances in Intelligent Systems and Computing</i> , 2021 , 239-249	0.4	5
79	Cyber Threats Impacting Critical Infrastructures. <i>Studies in Systems, Decision and Control</i> , 2016 , 139-161	0.8	5
78	Evolutionary-based packets classification for anomaly detection in web layer. <i>Security and Communication Networks</i> , 2016 , 9, 2901-2910	1.9	5
77	Increasing product owners recognition and decision-making capabilities by data analysis approach. <i>Cognition, Technology and Work</i> , 2019 , 21, 191-200	2.9	5
76	Q-Rapids framework for advanced data analysis to improve rapid software development. <i>Journal of Ambient Intelligence and Humanized Computing</i> , 2019 , 10, 1927-1936	3.7	5

75	Cost-Sensitive Distributed Machine Learning for NetFlow-Based Botnet Activity Detection. <i>Security and Communication Networks</i> , 2018 , 2018, 1-8	1.9	5
74	Platform for Software Quality and Dependability Data Analysis. <i>Advances in Intelligent Systems and Computing</i> , 2019 , 306-315	0.4	4
73	Machine Learning Techniques for Cyber Attacks Detection. <i>Advances in Intelligent Systems and Computing</i> , 2014 , 391-398	0.4	4
72	On the Impact of Network Data Balancing in Cybersecurity Applications. <i>Lecture Notes in Computer Science</i> , 2020 , 196-210	0.9	4
71	Semi-unsupervised Machine Learning for Anomaly Detection in HTTP Traffic. <i>Advances in Intelligent Systems and Computing</i> , 2016 , 767-775	0.4	4
70	Cyber Security of the Application Layer of Mission Critical Industrial Systems. <i>Lecture Notes in Computer Science</i> , 2016 , 342-351	0.9	4
69	The Concept of Applying Lifelong Learning Paradigm to Cybersecurity. <i>Lecture Notes in Computer Science</i> , 2017 , 663-671	0.9	4
68	SMAS - Stereovision Mobility Aid System for People with a Vision Impairment. <i>Advances in Intelligent and Soft Computing</i> , 2010 , 315-322		4
67	Network Event Correlation and Semantic Reasoning for Federated Networks Protection System. <i>Communications in Computer and Information Science</i> , 2011 , 48-54	0.3	4
66	A \$10 million question and other cybersecurity-related ethical dilemmas amid the COVID-19 pandemic. <i>Business Horizons</i> , 2021 , 64, 729-734	10.1	4
65	First broad and systematic horizon scanning campaign and study to detect societal and ethical dilemmas and emerging issues spanning over cybersecurity solutions. <i>Personal and Ubiquitous Computing</i> , 1	2.1	4
64	Machine Learning Techniques for Threat Modeling and Detection 2018 , 179-192		3
63	Evaluation of the Pre-processing Methods in Image-Based Palmprint Biometrics. <i>Advances in Intelligent Systems and Computing</i> , 2018 , 43-48	0.4	3
62	Proposal and comparison of network anomaly detection based on long-memory statistical models. <i>Logic Journal of the IGPL</i> , 2016 , 24, 944-956	1	3
61	Emerging Cyber Security: Bio-inspired Techniques and MITM Detection in IoT. <i>Advanced Sciences and Technologies for Security Applications</i> , 2016 , 193-207	0.6	3
60	Are We Doing All the Right Things to Counter Cybercrime?. <i>Advanced Sciences and Technologies for Security Applications</i> , 2016 , 279-294	0.6	3
59	Palmprint Recognition Enhanced by the Shape Features 2008 ,		3
58	Recognizing Faults in Software Related Difficult Data. <i>Lecture Notes in Computer Science</i> , 2019 , 263-272	0.9	3

57	Fusion of Bayesian and Ontology Approach Applied to Decision Support System for Critical Infrastructures Protection. <i>Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering</i> , 2010 , 451-463	0.2	3
56	Stereovision System for Visually Impaired. <i>Advances in Intelligent and Soft Computing</i> , 2011 , 459-468		3
55	Protecting the application layer in the public domain with machine learning methods. <i>Logic Journal of the IGPL</i> , 2019 , 27, 149-159	1	3
54	Technical solution to counter potential crime: Text analysis to detect fake news and disinformation. <i>Journal of Computational Science</i> , 2022 , 60, 101576	3-4	3
53	Data analysis tool supporting software development process 2017 ,		2
52	Knuckle Recognition for Human Identification. <i>Advances in Intelligent and Soft Computing</i> , 2011 , 61-70		2
51	Performance comparison of guard channel admission control schemes for IEEE 802.16 system with various turbo code FEC schemes 2009 ,		2
50	An Empirical Investigation into Industrial Use of Software Metrics Programs. <i>Lecture Notes in Computer Science</i> , 2020 , 419-433	0.9	2
49	Stegomalware detection through structural analysis of media files 2020 ,		2
48	The Identification and Creation of Ontologies for the Use in Law Enforcement AI Solutions □ MAGNETO Platform Use Case. <i>Lecture Notes in Computer Science</i> , 2019 , 335-345	0.9	2
47	Evaluation of Various Techniques for SQL Injection Attack Detection. <i>Advances in Intelligent Systems and Computing</i> , 2013 , 753-762	0.4	2
46	Improving Depth Map Quality with Markov Random Fields. <i>Advances in Intelligent and Soft Computing</i> , 2011 , 149-156		2
45	Fast Feature Extractors for Palmprint Biometrics. <i>Communications in Computer and Information Science</i> , 2011 , 121-127	0.3	2
44	Real-Time Analysis of Non-stationary and Complex Network Related Data for Injection Attempts Detection. <i>Advances in Intelligent Systems and Computing</i> , 2014 , 257-264	0.4	2
43	Common Representational Model and Ontologies for Effective Law Enforcement Solutions. <i>Vietnam Journal of Computer Science</i> , 2020 , 07, 1-18	0.8	2
42	New solutions for exposing clustered applications deployed in the cloud. <i>Cluster Computing</i> , 2019 , 22, 829-838	2.1	2
41	Multimedia analysis platform for crime prevention and investigation. <i>Multimedia Tools and Applications</i> , 2021 , 80, 23681	2.5	2
40	Implementation of the BERT-derived architectures to tackle disinformation challenges. <i>Neural Computing and Applications</i> , 2021 , 1-13	4.8	2

39	A Systematic Review of Recommender Systems and Their Applications in Cybersecurity. <i>Sensors</i> , 2021 , 21,	3.8	2
38	Hardening Web Applications against SQL Injection Attacks Using Anomaly Detection Approach. <i>Advances in Intelligent Systems and Computing</i> , 2015 , 285-292	0.4	1
37	Artificial Neural Network Hyperparameter Optimisation for Network Intrusion Detection. <i>Lecture Notes in Computer Science</i> , 2019 , 749-760	0.9	1
36	Distributed System for Botnet Traffic Analysis and Anomaly Detection 2017 ,		1
35	WiMAX Cell Level Simulation Platform Based on ns-2 and DSP Integration. <i>International Journal of Electronics and Telecommunications</i> , 2010 , 56, 169-176		1
34	A Novel Shape-Texture Approach to Palmprint Detection and Identification 2008 ,		1
33	Actionable Software Metrics 2020 ,		1
32	Switching Network Protocols to Improve Communication Performance in Public Clouds. <i>Advances in Intelligent Systems and Computing</i> , 2019 , 224-236	0.4	1
31	Proposition of Innovative and Scalable Information System for Call Detail Records Analysis and Visualisation. <i>Advances in Intelligent Systems and Computing</i> , 2021 , 174-183	0.4	1
30	Online Social Networks: Emerging Security and Safety Applications. <i>Advances in Intelligent Systems and Computing</i> , 2013 , 291-302	0.4	1
29	Information Exchange Mechanism between Federated Domains: P2P Approach. <i>Advances in Intelligent Systems and Computing</i> , 2013 , 187-196	0.4	1
28	Feature Extraction Method for Contactless Palmprint Biometrics. <i>Communications in Computer and Information Science</i> , 2010 , 435-442	0.3	1
27	Rapid Threat Detection for Stereovision Mobility Aid System. <i>Advances in Intelligent and Soft Computing</i> , 2011 , 115-123		1
26	Computer Vision Method for Detecting Adult-Oriented Content in Images. <i>Advances in Intelligent Systems and Computing</i> , 2013 , 19-24	0.4	1
25	Intelligent operator: Machine learning based decision support and explainer for human operators and service providers in the fog, cloud and edge networks. <i>Journal of Information Security and Applications</i> , 2021 , 56, 102685	3.5	1
24	Hybrid Feature Extraction for Palmprint-Based User Authentication 2018 ,		1
23	Recent Granular Computing Implementations and its Feasibility in Cybersecurity Domain 2018 ,		1
22	Why Do Law Enforcement Agencies Need AI for Analyzing Big Data?. <i>Lecture Notes in Computer Science</i> , 2021 , 331-342	0.9	1

21	How Machine Learning May Prevent the Breakdown of Democracy by Contributing to Fake News Detection. <i>IT Professional</i> , 2022 , 24, 25-31	1.9	1
20	Transformer Based Models in Fake News Detection. <i>Lecture Notes in Computer Science</i> , 2021 , 28-38	0.9	0
19	Finger Knuckle Print Identification with Hierarchical Model of Local Gradient Features. <i>Studies in Computational Intelligence</i> , 2015 , 73-80	0.8	
18	Knuckle Biometrics for Human Identification. <i>Advances in Intelligent and Soft Computing</i> , 2010 , 91-98		
17	Gated Recurrent Units for Intrusion Detection. <i>Advances in Intelligent Systems and Computing</i> , 2020 , 142-148		
16	Towards Mobile Palmprint Biometric System with the New Palmprint Database. <i>Advances in Intelligent Systems and Computing</i> , 2020 , 149-157	0.4	
15	Distributed Architecture for Fake News Detection. <i>Advances in Intelligent Systems and Computing</i> , 2021 , 208-217	0.4	
14	Local Statistic Embedding for Malware Behaviour Modelling. <i>Advances in Intelligent Systems and Computing</i> , 2016 , 267-273	0.4	
13	Netflow-Based Malware Detection and Data Visualisation System. <i>Lecture Notes in Computer Science</i> , 2017 , 652-660	0.9	
12	Recent Advances in Image Pre-processing Methods for Palmprint Biometrics. <i>Advances in Intelligent Systems and Computing</i> , 2018 , 268-275	0.4	
11	Running Sports Decision Aid Tool Based on Reinforcement Learning Approach. <i>Advances in Intelligent Systems and Computing</i> , 2018 , 160-169	0.4	
10	Head Rotation Estimation Algorithm for Hand-Free Computer Interaction. <i>Advances in Intelligent and Soft Computing</i> , 2009 , 535-541		
9	Recognizing Anomalies/Intrusions in Heterogeneous Networks. <i>Advances in Intelligent and Soft Computing</i> , 2009 , 577-584		
8	Image Recognition Techniques Applied to Automated and Objective QoE Assessment of Mobile WWW Services. <i>Lecture Notes in Computer Science</i> , 2010 , 275-282	0.9	
7	Innovative Man Machine Interfaces and Solutions to Support Totally Blind People. <i>Advances in Intelligent and Soft Computing</i> , 2011 , 437-444		
6	A Simplified Visual Cortex Model for Efficient Image Coding and Object Recognition. <i>Advances in Intelligent Systems and Computing</i> , 2014 , 271-278	0.4	
5	Fault-Prone Software Classes Recognition via Artificial Neural Network with Granular Dataset Balancing. <i>Advances in Intelligent Systems and Computing</i> , 2020 , 130-140	0.4	
4	Towards AI-Based Reaction and Mitigation for e-Commerce - the ENSURESEC Engine. <i>Lecture Notes in Computer Science</i> , 2021 , 24-31	0.9	

- 3 The Proposition of Balanced and Explainable Surrogate Method for Network Intrusion Detection in Streamed Real Difficult Data. *Communications in Computer and Information Science*, **2021**, 241-252 0.3
- 2 Extending Machine Learning-Based Intrusion Detection with the Imputation Method. *Lecture Notes in Networks and Systems*, **2022**, 284-292 0.5
- 1 Cyber-Attack Detection from IoT Benchmark Considered as Data Streams. *Lecture Notes in Networks and Systems*, **2022**, 230-239 0.5