# A Survey on Malware Detection Using Data Mining Tech

ACM Computing Surveys

50, 1-40

DOI: 10.1145/3073559

Citation Report

| # | Article | IF | Citations |
|---|---|---|---|
| 1 | SecureDroid. , 2017, , . | | 55 |
| 2 | A Bi-objective Hyper-Heuristic Support Vector Machines for Big Data Cyber-Security. IEEE Access, 2018, 6, 10421-10431. | 2.6 | 33 |
| 3 | A learning evasive email-based P2P-like botnet. China Communications, 2018, 15, 15-24. | 2.0 | 10 |
| 4 | Malware classification using deep learning methods. , 2018, , . | | 49 |
| 5 | Detection of malicious webmail attachments based on propagation patterns. Knowledge-Based Systems, 2018, 141, 67-79. | 4.0 | 30 |
| 6 | ICSD. , 2018, , . | | 11 |
| 7 | An Android Malware Detection Technique Using Optimized Permission and API with PCA. , 2018, , . | | 4 |
| 8 | An Open Source, Extensible Malware Analysis Platform. MATEC Web of Conferences, 2018, 188, 05009. | 0.1 | 0 |
| 9 | Malware Detection Using Machine Learning and Deep Learning. Lecture Notes in Computer Science, 2018, , 402-411. | 1.0 | 62 |
| 10 | KADetector: Automatic Identification of Key Actors in Online Hack Forums Based on Structured Heterogeneous Information Network. , 2018, , . | | 6 |
| 11 | A New Multitasking Malware Classification Model Based on Feature Fusion. , 2018, , . | | 2 |
| 12 | Common Program Similarity Metric Method for Anti-Obfuscation. IEEE Access, 2018, 6, 47557-47565. | 2.6 | 3 |
| 13 | Prediction-time Efficient Classification Using Feature Computational Dependencies. , 2018, , . | | 18 |
| 14 | Android Malware Detection: A Survey. Communications in Computer and Information Science, 2018, , 255-266. | 0.4 | 42 |
| 15 | A Survey of Machine Learning Algorithms and Their Application in Information Security. Computer Communications and Networks, 2018, , 33-55. | 0.8 | 8 |
| 16 | An investigation of a deep learning based malware detection system. , 2018, , . | | 29 |
| 17 | Scalable Detection of Server-Side Polymorphic Malware. Knowledge-Based Systems, 2018, 156, 113-128. | 4.0 | 7 |
| 18 | An Active and Dynamic Botnet Detection Approach to Track Hidden Concept Drift. Lecture Notes in Computer Science, 2018, , 646-660. | 1.0 | 3 |

| # | Article | IF | Citations |
|---|---|---|---|
| 19 | Gotcha - Sly Malware!. , 2018, , . | | 53 |
| 20 | A novel Self-Organizing Network solution towards Crypto-ransomware Mitigation. , 2018, , . | | 7 |
| 21 | Adversarial Machine Learning. Synthesis Lectures on Artificial Intelligence and Machine Learning, 2018, 12, 1-169. | 0.6 | 75 |
| 22 | An Extensive Survey on Intrusion Detection- Past, Present, Future. , 2018, , . | | 10 |
| 23 | AndrODet: An adaptive Android obfuscation detector. Future Generation Computer Systems, 2019, 90, 240-261. | 4.9 | 32 |
| 24 | A survey of challenges for runtime verification from advanced application domains (beyond) Tj ETQq1 1 0.784314 rgBT /Overlock 10 | 6.9 | 56 |
| 25 | A Novel Solutions for Malicious Code Detection and Family Clustering Based on Machine Learning. IEEE Access, 2019, 7, 148853-148860. | 2.6 | 27 |
| 26 | HSIRD: A model for characterizing dynamics of malware diffusion in heterogeneous WSNs. Journal of Network and Computer Applications, 2019, 146, 102420. | 5.8 | 29 |
| 27 | Dynamic Malware Analysis in the Modern Eraâ€"A State of the Art Survey. ACM Computing Surveys, 2020, 52, 1-48. | 16.1 | 146 |
| 28 | Malware Detection Approach Based on Artifacts in Memory Image and Dynamic Analysis. Applied Sciences (Switzerland), 2019, 9, 3680. | 1.3 | 40 |
| 29 | Towards Adversarial Malware Detection. ACM Computing Surveys, 2020, 52, 1-36. | 16.1 | 50 |
| 30 | Crypto-ransomware early detection model using novel incremental bagging with enhanced semi-random subspace selection. Future Generation Computer Systems, 2019, 101, 476-491. | 4.9 | 61 |
| 31 | A robust and secure backup system for protecting malware. , 2019, , . | | 1 |
| 32 | A multi-level deep learning system for malware detection. Expert Systems With Applications, 2019, 133, 151-162. | 4.4 | 57 |
| 33 | Application of deep learning to cybersecurity: A survey. Neurocomputing, 2019, 347, 149-176. | 3.5 | 191 |
| 34 | MalDAE: Detecting and explaining malware based on correlation and fusion of static and dynamic characteristics. Computers and Security, 2019, 83, 208-233. | 4.0 | 86 |
| 35 | Malicious code detection based on CNNs and multi-objective algorithm. Journal of Parallel and Distributed Computing, 2019, 129, 50-58. | 2.7 | 137 |
| 36 | A Deep Reinforcement Learning Malware Detection Method Based on PE Feature Distribution. , 2019, , . | | 4 |

| # | Article | IF | Citations |
|---|---|---|---|
| 37 | New Direction for Malware Detection Using System Features. , 2019, , . | | 2 |
| 38 | Detection of Malware using Artificial Neural Networks. , 2019, , . | | 2 |
| 39 | Proximity Search Method for Mining Biomedical and Genomic Information. , 2019, , . | | 0 |
| 40 | A Convolutional Transformation Network for Malware Classification. , 2019, , . | | 39 |
| 41 | Learning From Evolving Network Data for Dependable Botnet Detection. , 2019, , . | | 2 |
| 42 | Machine Learning Techniques to Detect Maliciousness of Portable Executable Files. , 2019, , . | | 9 |
| 43 | On Embedding Backdoor in Malware Detectors Using Machine Learning. , 2019, , . | | 6 |
| 44 | Discovering Future Malware Variants By Generating New Malware Samples Using Generative Adversarial Network. , 2019, , . | | 10 |
| 45 | AMVG: Adaptive Malware Variant Generation Framework Using Machine Learning. , 2019, , . | | 4 |
| 46 | Malware classification for identifying author groups. , 2019, , . | | 5 |
| 47 | Malware Detection with Malware Images using Deep Learning Techniques. , 2019, , . | | 41 |
| 48 | Review: Build a Roadmap for Stepping Into the Field of Anti-Malware Research Smoothly. IEEE Access, 2019, 7, 143573-143596. | 2.6 | 7 |
| 49 | Î±Cyber : Enhancing Robustness of Android Malware Detection System against Adversarial Attacks on Heterogeneous Graph based Model. , 2019, , . | | 17 |
| 50 | Toward Network Worm Victims Identification Based on Cascading Motif Discovery. Electronics (Switzerland), 2019, 8, 183. | 1.8 | 1 |
| 51 | Malware Detection Using Power Consumption and Network Traffic Data. , 2019, , . | | 8 |
| 52 | EIGER. , 2019, , . | | 10 |
| 53 | Windows malware detection system based on LSVC recommended hybrid features. Journal of Computer Virology and Hacking Techniques, 2019, 15, 127-146. | 1.6 | 11 |
| 54 | MalInsight: A systematic profiling based malware detection framework. Journal of Network and Computer Applications, 2019, 125, 236-250. | 5.8 | 64 |

| # | Article | IF | Citations |
|---|---|---|---|
| 55 | Survey of machine learning techniques for malware analysis. Computers and Security, 2019, 81, 123-147. | 4.0 | 294 |
| 56 | Empirical Study on Features Recommended by LSVC in Classifying Unknown Windows Malware. Advances in Intelligent Systems and Computing, 2019, , 577-590. | 0.5 | 1 |
| 57 | Wireless Sensor Networks Intrusion Detection Based on SMOTE and the Random Forest Algorithm. Sensors, 2019, 19, 203. | 2.1 | 103 |
| 58 | An opcodeâ€based technique for polymorphic Internet of Things malware detection. Concurrency Computation Practice and Experience, 2020, 32, e5173. | 1.4 | 62 |
| 59 | A Context-Aware Framework for Detecting Sensor-Based Threats on Smart Devices. IEEE Transactions on Mobile Computing, 2020, 19, 245-261. | 3.9 | 31 |
| 60 | Detecting malware evolution using support vector machines. Expert Systems With Applications, 2020, 143, 113022. | 4.4 | 52 |
| 61 | Evolution of Malware and Its DetectionÂTechniques. Advances in Intelligent Systems and Computing, 2020, , 139-150. | 0.5 | 25 |
| 62 | Detecting malware communities using socio-cultural cognitive mapping. Computational and Mathematical Organization Theory, 2020, 26, 307-319. | 1.5 | 3 |
| 63 | Malware detection in mobile environments based on Autoencoders and API-images. Journal of Parallel and Distributed Computing, 2020, 137, 26-33. | 2.7 | 76 |
| 64 | Byte2vec: Malware Representation and Feature Selection for Android. Computer Journal, 2020, 63, 1125-1138. | 1.5 | 7 |
| 65 | HIT4Mal: Hybrid image transformation for malware classification. Transactions on Emerging Telecommunications Technologies, 2020, 31, e3789. | 2.6 | 47 |
| 66 | An improved two-hidden-layer extreme learning machine for malware hunting. Computers and Security, 2020, 89, 101655. | 4.0 | 57 |
| 67 | The rise of machine learning for detection and classification of malware: Research developments, trends and challenges. Journal of Network and Computer Applications, 2020, 153, 102526. | 5.8 | 279 |
| 68 | Cyber-guided Deep Neural Network for Malicious Repository Detection in GitHub. , 2020, , . | | 7 |
| 69 | A Survey on The Accuracy of Machine Learning Techniques for Intrusion and Anomaly Detection on Public Data Sets. , 2020, , . | | 13 |
| 70 | Malware classification based on heterogeneous information network representation learning. , 2020, , . | | 0 |
| 71 | $alpha$-Satellite: An AI-Driven System and Benchmark Datasets for Dynamic COVID-19 Risk Assessment in the United States. IEEE Journal of Biomedical and Health Informatics, 2020, 24, 2755-2764. | 3.9 | 45 |
| 72 | Understanding negotiated anti-malware interruption effects on user decision quality in endpoint security. Behaviour and Information Technology, 2021, 40, 903-932. | 2.5 | 10 |

| # | Article | IF | Citations |
|---|---|---|---|
| 73 | Analysis of Malware Communities Using Multi-Modal Features. IEEE Access, 2020, 8, 77435-77448. | 2.6 | 8 |
| 74 | A Review of Android Malware Detection Approaches Based on Machine Learning. IEEE Access, 2020, 8, 124579-124607. | 2.6 | 169 |
| 75 | Robust Android Malware Detection System Against Adversarial Attacks Using Q-Learning. Information Systems Frontiers, 2021, 23, 867-882. | 4.1 | 37 |
| 76 | Protecting From Malware Obfuscation Attacks Through Adversarial Risk Analysis. Risk Analysis, 2020, 40, 2598-2609. | 1.5 | 2 |
| 77 | Hybrid Malware Classification Method Using Segmentation-Based Fractal Texture Analysis and Deep Convolution Neural Network Features. Applied Sciences (Switzerland), 2020, 10, 4966. | 1.3 | 86 |
| 78 | Automated malware recognition method based on local neighborhood binary pattern. Multimedia Tools and Applications, 2020, 79, 27815-27832. | 2.6 | 7 |
| 79 | MTHAEL: Cross-Architecture IoT Malware Detection Based on Neural Network Advanced Ensemble Learning. IEEE Transactions on Computers, 2020, 69, 1654-1667. | 2.4 | 50 |
| 80 | Malware classification for the cloud via semi-supervised transfer learning. Journal of Information Security and Applications, 2020, 55, 102661. | 1.8 | 21 |
| 81 | Semantic Feature Discovery of Trojan Malware using Vector Space Kernels. , 2020, , . | | 3 |
| 82 | Machine learning in cybersecurity: a comprehensive survey. Journal of Defense Modeling and Simulation, 2022, 19, 57-106. | 1.2 | 55 |
| 83 | Security in product lifecycle of IoT devices: A survey. Journal of Network and Computer Applications, 2020, 171, 102779. | 5.8 | 49 |
| 84 | A New Method for Ransomware Detection Based on PE Header Using Convolutional Neural Networks. , 2020, , . | | 13 |
| 85 | Threat-Event Detection for Distributed Networks Based on Spatiotemporal Markov Random Field. IEEE Transactions on Dependable and Secure Computing, 2022, 19, 1735-1752. | 3.7 | 1 |
| 86 | Building Contemporary and Efficient Static Models for Malware Detection. , 2020, , . | | 0 |
| 87 | An ensemble framework for interpretable malicious code detection. International Journal of Intelligent Systems, 2022, 37, 10100-10117. | 3.3 | 8 |
| 88 | HGM: A Novel Monte-Carlo Simulations based Model for Malware Detection. IOP Conference Series: Materials Science and Engineering, 2020, 946, 012003. | 0.3 | 4 |
| 89 | Application of MapReduce parallel association mining on IDS in cloud computing environment. Journal of Intelligent and Fuzzy Systems, 2020, 39, 1915-1923. | 0.8 | 2 |
| 90 | Detection of Anomalous Behavior in Modern Smartphones Using Software Sensor-Based Data. Sensors, 2020, 20, 2768. | 2.1 | 4 |

| # | Article | IF | Citations |
|---|---|---|---|
| 91 | Dynamic Analysis for IoT Malware Detection With Convolution Neural Network Model. IEEE Access, 2020, 8, 96899-96911. | 2.6 | 96 |
| 92 | Adversarial Deep Ensemble: Evasion Attacks and Defenses for Malware Detection. IEEE Transactions on Information Forensics and Security, 2020, 15, 3886-3900. | 4.5 | 76 |
| 93 | End-to-end malware detection for android IoT devices using deep learning. Ad Hoc Networks, 2020, 101, 102098. | 3.4 | 84 |
| 94 | A multiview learning method for malware threat hunting: windows, IoT and android as case studies. World Wide Web, 2020, 23, 1241-1260. | 2.7 | 36 |
| 95 | Detecting Cryptomining Malware: a Deep Learning Approach for Static and Dynamic Analysis. Journal of Grid Computing, 2020, 18, 293-303. | 2.5 | 63 |
| 96 | Incremental Learning for Malware Classification in Small Datasets. Security and Communication Networks, 2020, 2020, 1-12. | 1.0 | 10 |
| 97 | ConvProtoNet: Deep Prototype Induction towards Better Class Representation for Few-Shot Malware Classification. Applied Sciences (Switzerland), 2020, 10, 2847. | 1.3 | 19 |
| 98 | MalFamAware: automatic family identification and malware classification through online clustering. International Journal of Information Security, 2021, 20, 371-386. | 2.3 | 12 |
| 99 | Redundancy Coefficient Gradual Up-weighting-based Mutual Information Feature Selection technique for Crypto-ransomware early detection. Future Generation Computer Systems, 2021, 115, 641-658. | 4.9 | 29 |
| 100 | Effective detection of mobile malware behavior based on explainable deep neural network. Neurocomputing, 2021, 453, 482-492. | 3.5 | 17 |
| 101 | A Method for Windows Malware Detection Based on Deep Learning. Journal of Signal Processing Systems, 2021, 93, 265-273. | 1.4 | 48 |
| 102 | Data Mining Approach for Cyber Security. International Journal of Computer Applications Technology and Research, 2021, 10, 035-041. | 0.1 | 2 |
| 103 | Automated malware identification method using image descriptors and singular value decomposition. Multimedia Tools and Applications, 2021, 80, 10881-10900. | 2.6 | 9 |
| 104 | A Framework for Enhancing Deep Neural Networks Against Adversarial Malware. IEEE Transactions on Network Science and Engineering, 2021, 8, 736-750. | 4.1 | 29 |
| 105 | Reproducible Builds: Increasing the Integrity of Software Supply Chains. IEEE Software, 2022, 39, 62-70. | 2.1 | 18 |
| 106 | Identification of Significant Permissions for Efficient Android Malware Detection. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, 2021, , 33-52. | 0.2 | 15 |
| 107 | SIMBIoTA: Similarity-based Malware Detection on IoT Devices. , 2021, , . | | 7 |
| 108 | A Novel Method for Detecting Future Generations of Targeted and Metamorphic Malware Based on Genetic Algorithm. IEEE Access, 2021, 9, 69951-69970. | 2.6 | 22 |

| # | Article | IF | Citations |
|---|---|---|---|
| 109 | Learning to Find Usages of Library Functions in Optimized Binaries. IEEE Transactions on Software Engineering, 2022, 48, 3862-3876. | 4.3 | 4 |
| 110 | An Adaptive Behavioral-Based Incremental Batch Learning Malware Variants Detection Model Using Concept Drift Detection and Sequential Deep Learning. IEEE Access, 2021, 9, 97180-97196. | 2.6 | 33 |
| 111 | A Review of Computer Vision Methods in Network Security. IEEE Communications Surveys and Tutorials, 2021, 23, 1838-1878. | 24.8 | 26 |
| 112 | A Survey on Cross-Architectural IoT Malware Threat Hunting. IEEE Access, 2021, 9, 91686-91709. | 2.6 | 33 |
| 113 | Windows PE Malware Detection Using Ensemble Learning. Informatics, 2021, 8, 10. | 2.4 | 47 |
| 114 | Ensemble-Based Classification Using Neural Networks and Machine Learning Models for Windows PE Malware Detection. Electronics (Switzerland), 2021, 10, 485. | 1.8 | 56 |
| 115 | A survey on analysis and detection of Android ransomware. Concurrency Computation Practice and Experience, 2021, 33, e6272. | 1.4 | 21 |
| 116 | Towards Robust Android Malware Detection Models using Adversarial Learning. , 2021, , . | | 4 |
| 117 | A Review on Machine Learning Approaches for Network Malicious Behavior Detection in Emerging Technologies. Entropy, 2021, 23, 529. | 1.1 | 20 |
| 118 | Cloud Classroom Design for English Education Based on Internet of Things and Data Mining. Mobile Information Systems, 2021, 2021, 1-8. | 0.4 | 4 |
| 119 | Robust Android Malware Detection against Adversarial Example Attacks. , 2021, , . | | 11 |
| 120 | Towards A Sustainable Development Cities Through Smart Shopping Trolly: A Response to the Covid-19 Pandemic. , 2021, , . | | 4 |
| 121 | Malware detection and classification using community detection and social network analysis. Journal of Computer Virology and Hacking Techniques, 2021, 17, 333-346. | 1.6 | 5 |
| 122 | DeepMal: maliciousness-Preserving adversarial instruction learning against static malware detection. Cybersecurity, 2021, 4, . | 3.1 | 12 |
| 123 | QLLog: A log anomaly detection method based on Q-learning algorithm. Information Processing and Management, 2021, 58, 102540. | 5.4 | 21 |
| 124 | Machine Learning for Detecting Data Exfiltration. ACM Computing Surveys, 2022, 54, 1-47. | 16.1 | 21 |
| 125 | Enterprise human resource management based on big data mining technology of internet of things. Journal of Intelligent and Fuzzy Systems, 2021, , 1-7. | 0.8 | 17 |
| 126 | Malware classification and composition analysis: A survey of recent developments. Journal of Information Security and Applications, 2021, 59, 102828. | 1.8 | 28 |

| # | Article | IF | Citations |
|---|---|---|---|
| 127 | A Survey on malware detection techniques. , 2021, , . | | 16 |
| 128 | ADVERSARIALuscator: An Adversarial-DRL based Obfuscator and Metamorphic Malware Swarm Generator. , 2021, , . | | 4 |
| 129 | Robust Malware Detection Models: Learning from Adversarial Attacks and Defenses. Forensic Science International: Digital Investigation, 2021, 37, 301183. | 1.2 | 9 |
| 130 | A novel few-shot malware classification approach for unknown family recognition with multi-prototype modeling. Computers and Security, 2021, 106, 102273. | 4.0 | 21 |
| 131 | Cross-Architecture Intemet-of-Things Malware Detection Based on Graph Neural Network. , 2021, , . | | 9 |
| 132 | Identification of Adversarial Android Intents using Reinforcement Learning. , 2021, , . | | 6 |
| 133 | A New Machine Learning Approach for Malware Classification. Advances in Intelligent Systems and Computing, 2022, , 301-309. | 0.5 | 0 |
| 134 | Computation of Cyclomatic Complexity and Detection of Malware Executable Files. , 2021, , . | | 2 |
| 135 | Intelligent malware detection based on graph convolutional network. Journal of Supercomputing, 2022, 78, 4182-4198. | 2.4 | 24 |
| 136 | Data Transformation Schemes for CNN-Based Network Traffic Analysis: A Survey. Electronics (Switzerland), 2021, 10, 2042. | 1.8 | 17 |
| 137 | Heterogeneous Temporal Graph Transformer. , 2021, , . | | 18 |
| 138 | Adapting Meta Knowledge with Heterogeneous Information Network for COVID-19 Themed Malicious Repository Detection. , 2021, , . | | 5 |
| 139 | I-MAD: Interpretable malware detector using Galaxy Transformer. Computers and Security, 2021, 108, 102371. | 4.0 | 10 |
| 140 | Effective malware detection scheme based on classified behavior graph in IIoT. Ad Hoc Networks, 2021, 120, 102558. | 3.4 | 12 |
| 141 | Network Threat Detection Based on Group CNN for Privacy Protection. Wireless Communications and Mobile Computing, 2021, 2021, 1-18. | 0.8 | 3 |
| 142 | Malware detection on windows audit logs using LSTMs. Computers and Security, 2021, 109, 102389. | 4.0 | 9 |
| 143 | A Multi-Perspective malware detection approach through behavioral fusion of API call sequence. Computers and Security, 2021, 110, 102449. | 4.0 | 31 |
| 144 | Image-based malware classification using section distribution information. Computers and Security, 2021, 110, 102420. | 4.0 | 16 |

| # | Article | IF | Citations |
|---|---|---|---|
| 145 | Dynamic user-centric access control for detection of ransomware attacks. Computers and Security, 2021, 111, 102461. | 4.0 | 12 |
| 146 | Malware Variants Detection Based on Feature Fusion. Lecture Notes in Computer Science, 2021, , 67-77. | 1.0 | 1 |
| 147 | Deep Learning Applications on Cybersecurity. Lecture Notes in Computer Science, 2021, , 611-621. | 1.0 | 0 |
| 148 | Detection of Malicious Android Applications: Classical Machine Learning vs. Deep Neural Network Integrated with Clustering. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, 2021, , 109-128. | 0.2 | 12 |
| 149 | Detecting Malware Infection on Infrastructure Hosted in Iaas Cloud using Cloud Visibility and Forensics. International Journal of Advanced Computer Science and Applications, 2021, 12, . | 0.5 | 0 |
| 150 | Attacklets to Test Anomaly Detectors for Critical Infrastructure. Lecture Notes in Computer Science, 2021, , 209-227. | 1.0 | 0 |
| 151 | Context for API Calls in Malware vs Benign Programs. Communications in Computer and Information Science, 2021, , 222-234. | 0.4 | 2 |
| 152 | A survey on attack detection, estimation and control of industrial cyberâ€“physical systems. ISA Transactions, 2021, 116, 1-16. | 3.1 | 132 |
| 153 | Secure and Safe IIoT Systems via Machine and Deep Learning Approaches. , 2019, , 443-470. | | 12 |
| 154 | Timing Attacks on Machine Learning: State of the Art. Advances in Intelligent Systems and Computing, 2020, , 111-125. | 0.5 | 12 |
| 155 | Data-Driven Android Malware Intelligence: A Survey. Lecture Notes in Computer Science, 2019, , 183-202. | 1.0 | 14 |
| 156 | A Comparison Between Different Machine Learning Models for IoT Malware Detection. , 2020, , 195-202. | | 9 |
| 157 | The Fundamentals and Potential for Cybersecurity of Big Data in the Modern World. Studies in Computational Intelligence, 2021, , 51-73. | 0.7 | 4 |
| 158 | PE File-Based Malware Detection Using Machine Learning. Advances in Intelligent Systems and Computing, 2021, , 113-123. | 0.5 | 2 |
| 159 | An Ensemble of Deep Recurrent Neural Networks for Detecting IoT Cyber Attacks Using Network Traffic. IEEE Internet of Things Journal, 2020, 7, 8852-8859. | 5.5 | 113 |
| 160 | A Survey on Malware Analysis Techniques: Static, Dynamic, Hybrid and Memory Analysis. International Journal on Advanced Science, Engineering and Information Technology, 2018, 8, 1662-1671. | 0.2 | 102 |
| 161 | Social Media-Related Cybercrimes and Techniques for Their Prevention. Applied Computer Science, 2019, 24, 9-17. | 0.3 | 52 |
| 162 | Automatic Opioid User Detection from Twitter: Transductive Ensemble Built on Different Meta-graph Based Similarities over Heterogeneous Information Network. , 2018, , . | | 18 |

| # | Article | IF | Citations |
|---|---|---|---|
| 163 | Out-of-sample Node Representation Learning for Heterogeneous Graph in Real-time Android Malware Detection. , 2019, , . | | 24 |
| 164 | Zero-Day Aware Decision Fusion-Based Model for Crypto-Ransomware Early Detection. International Journal of Integrated Engineering, 2018, 10, . | 0.2 | 27 |
| 165 | Improving the Robustness of AI-Based Malware Detection Using Adversarial Machine Learning. Algorithms, 2021, 14, 297. | 1.2 | 12 |
| 166 | Evaluation of System Features Used for Malware Detection. Lecture Notes in Networks and Systems, 2022, , 46-59. | 0.5 | 0 |
| 167 | Sensors for Context-Aware Smart Healthcare: A Security Perspective. Sensors, 2021, 21, 6886. | 2.1 | 23 |
| 168 | Applications of deep learning for mobile malware detection: A systematic literature review. Neural Computing and Applications, 0, , 1. | 3.2 | 5 |
| 169 | A Review on Malware Analysis by using an Approach of Machine Learning Techniques. Ijosthe, 2018, 3, 5. | 0.0 | 0 |
| 170 | Efficient and Precise Dynamic Construction of Control Flow Graphs. , 2019, , . | | 1 |
| 171 | A Novel Image-Based Malware Classification Model Using Deep Learning. Lecture Notes in Computer Science, 2019, , 150-161. | 1.0 | 3 |
| 172 | Research on Heterogeneous Data Exchange Technology Based on Shadow Table. Advances in Intelligent Systems and Computing, 2020, , 371-377. | 0.5 | 0 |
| 173 | Malicious Code Detection Method Using LSTM Learning on the File Access Behavior. The Journal of Korean Institute of Information Technology, 2020, 18, 25-32. | 0.1 | 0 |
| 174 | Robust Android Malware Detection Based on Attributed Heterogenous Graph Embedding. Communications in Computer and Information Science, 2020, , 432-446. | 0.4 | 1 |
| 175 | Exploring the Impact of Resampling Methods for Malware Detection. , 2020, , . | | 1 |
| 176 | A survey on graph-based methods for malware detection. , 2020, , . | | 0 |
| 177 | A Dynamic Malware Detection in Cloud Platform. International Journal of Difference Equations, 2020, 15, 243-258. | 0.1 | 0 |
| 178 | Exploit Internal Structural Information for IoT Malware Detection Based on Hierarchical Transformer Model. , 2020, , . | | 5 |
| 179 | Malware Detection & Classification using Machine Learning. , 2020, , . | | 5 |
| 180 | dStyle-GAN: Generative Adversarial Network based on Writing and Photography Styles for Drug Identification in Darknet Markets. , 2020, , . | | 7 |

| # | Article | IF | Citations |
|---|---|---|---|
| 181 | A Comparative Study of Adversarial Attacks to Malware Detectors Based on Deep Learning. , 2021, , 477-511. | | 2 |
| 182 | Optimizing Multi-class Classification of Binaries Based on Static Features. , 2021, , 249-268. | | 0 |
| 183 | Machine Learning and Survey-based Predictors of InfoSec Non-Compliance. ACM Transactions on Management Information Systems, 2022, 13, 1-20. | 2.1 | 2 |
| 184 | A Scientometric Analysis of Malware Detection Research Based on CiteSpace. Lecture Notes in Computer Science, 2020, , 100-110. | 1.0 | 0 |
| 185 | An Evaluation of Image-Based Malware Classification Using Machine Learning. Communications in Computer and Information Science, 2020, , 125-138. | 0.4 | 5 |
| 186 | CAVAEva: An Engineering Platform forÂEvaluating Commercial Anti-malware Applications on Smartphones. Lecture Notes in Computer Science, 2020, , 208-224. | 1.0 | 0 |
| 187 | JavaScript Malware Detection Using Locality Sensitive Hashing. IFIP Advances in Information and Communication Technology, 2020, , 143-154. | 0.5 | 1 |
| 189 | Malware Visualization Techniques. International Journal of Applied Mathematics Electronics and Computers, 0, , 7-20. | 0.6 | 2 |
| 190 | Machine Learning Framework to Analyze IoT Malware Using ELF and Opcode Features. Digital Threats Research and Practice, 2020, 1, 1-19. | 1.7 | 30 |
| 191 | Scalable malware detection system using big data and distributed machine learning approach. Soft Computing, 2022, 26, 3987-4003. | 2.1 | 7 |
| 192 | Data Mining and Machine Learning Techniques for Malware Detection. Advances in Intelligent Systems and Computing, 2021, , 557-567. | 0.5 | 3 |
| 193 | Dictionary lookup with one genome evolution operation. Concurrency Computation Practice and Experience, 2021, 33, . | 1.4 | 1 |
| 194 | How robust are malware detection models for Android smartphones against adversarial attacks?. , 2020, , . | | 0 |
| 195 | Adversarial attacks on malware detection models for smartphones using reinforcement learning. , 2020, , . | | 1 |
| 196 | Scalable Fair Clustering Algorithm for Internet of Things Malware Classification. , 2022, , 271-287. | | 1 |
| 197 | Jadeite: A novel image-behavior-based approach for Java malware detection using deep learning. Computers and Security, 2022, 113, 102547. | 4.0 | 16 |
| 198 | KÃ¶tÃ¼cÃ¼l yazÄ±lÄ±mlarÄ±n tespitinde imza temelli ve dinamik analiz yÃ¶ntemlerinin zayÄ±flÄ±klarÄ±: Ã–rnek olay Ã§alÄ±ÅŸmasÄ±. Journal of the Faculty of Engineering and Architecture of Gazi University, 0, , . | 0.3 | 0 |
| 199 | Towards Scalable Security of Real-time Applications: A Formally Certified Approach. , 2021, , . | | 0 |

| # | Article | IF | Citations |
|---|---|---|---|
| 200 | Duplicates in the Drebin Dataset and Reduction in the Accuracy of the Malware Detection Models. , 2021, , . | | 0 |
| 201 | Hybrid Feature Selection by Combining Wrapper and Filter Methods for Malware Detection. , 2021, , . | | 1 |
| 202 | A Comprehensive Survey on Identification of Malware Types and Malware Classification Using Machine Learning Techniques. , 2021, , . | | 8 |
| 203 | Research on college English teaching based on data mining technology. Eurasip Journal on Wireless Communications and Networking, 2021, 2021, . | 1.5 | 8 |
| 204 | DEEPSEL: A novel feature selection for early identification of malware in mobile applications. Future Generation Computer Systems, 2022, 129, 54-63. | 4.9 | 9 |
| 205 | Vulnerability Recognition and Resurgence in Network based on Prediction Model and Cognitive based Elucidation. Journal of Physics: Conference Series, 2021, 2070, 012122. | 0.3 | 0 |
| 206 | A Novel Monte-Carlo Simulation-Based Model for Malware Detection (eRBCM). Electronics (Switzerland), 2021, 10, 2881. | 1.8 | 1 |
| 207 | Are CNN based Malware Detection Models Robust?. , 2021, , . | | 0 |
| 208 | Anomaly Rule Detection in Sequence Data. IEEE Transactions on Knowledge and Data Engineering, 2023, 35, 12095-12108. | 4.0 | 5 |
| 209 | Vehicle Security: A Survey of Security Issues and Vulnerabilities, Malware Attacks and Defenses. IEEE Access, 2021, 9, 162401-162437. | 2.6 | 23 |
| 210 | A study on malicious software behaviour analysis and detection techniques: Taxonomy, current trends and challenges. Future Generation Computer Systems, 2022, 130, 1-18. | 4.9 | 23 |
| 211 | Proposing a Hybrid RPL Protocol for Rank and Wormhole Attack Mitigation using Machine Learning. , 2020, , . | | 17 |
| 212 | A Comprehensive Detection Approach of Nmap: Principles, Rules and Experiments. , 2020, , . | | 9 |
| 213 | AltCC: Alternating Clustering and Classification for Batch Analysis of Malware Behavior. , 2020, , . | | 3 |
| 214 | Feature-Based Adversarial Attacks Against Machine Learnt Mobile Malware Detectors. , 2020, , . | | 0 |
| 215 | A Comparative Analysis of Machine Learning Techniques for Classification and Detection of Malware. , 2020, , . | | 8 |
| 216 | A Survey on Feature Extraction Methods of Heuristic Backdoor Detection. , 2021, , . | | 1 |
| 217 | MalDeXA - A Malware Detection system using XGBoost on Amazon Web Services. , 2021, , . | | 0 |

| # | Article | IF | Citations |
|---|---|---|---|
| 218 | Toward Efficient and Robust Deep Learning-based Malware Detection in Fog Computing. , 2021, , . | | 0 |
| 219 | A novel approach for ransomware detection based on PE header using graph embedding. Journal of Computer Virology and Hacking Techniques, 2022, 18, 285-296. | 1.6 | 14 |
| 220 | Time-interval temporal patterns can beat and explain the malware. Knowledge-Based Systems, 2022, 241, 108266. | 4.0 | 11 |
| 221 | ConRec: malware classification using convolutional recurrence. Journal of Computer Virology and Hacking Techniques, 2022, 18, 297-313. | 1.6 | 16 |
| 224 | Intelligent Malware Defenses. Lecture Notes in Computer Science, 2022, , 217-253. | 1.0 | 2 |
| 225 | Behavioral malware detection and classification using deep learning approaches. , 2022, , 29-45. | | 4 |
| 226 | A Malware Detection Approach Using Autoencoder in Deep Learning. IEEE Access, 2022, 10, 25696-25706. | 2.6 | 25 |
| 227 | A Study on the Application of Distributed System Technology-Guided Machine Learning in Malware Detection. Computational Intelligence and Neuroscience, 2022, 2022, 1-12. | 1.1 | 2 |
| 228 | Artificial intelligence empowered threat detection in the Internet of Things: A systematic review. Concurrency Computation Practice and Experience, 2022, 34, . | 1.4 | 1 |
| 229 | A New Malware Detection Method Based on VMCADR in Cloud Environments. Security and Communication Networks, 2022, 2022, 1-13. | 1.0 | 2 |
| 230 | Cybersecurity Deep: Approaches, Attacks Dataset, and Comparative Study. Applied Artificial Intelligence, 2022, 36, . | 2.0 | 8 |
| 231 | A Survey on Machine Learning-based Detection and Classification Technology of Malware. , 2021, , . | | 2 |
| 232 | Machine Learning for Static Malware Analysis. , 2022, , 1-4. | | 0 |
| 233 | A Systematic Literature Review: Usage of Logistic Regression for Malware Detection. , 2021, , . | | 4 |
| 234 | Can We Leverage Predictive Uncertainty to Detect Dataset Shift and Adversarial Examples in Android Malware Detection?. , 2021, , . | | 4 |
| 235 | Cyber Security Threats And Their Solutions Through Deep Learning: A Bibliometric Analysis. , 2021, , . | | 2 |
| 236 | Zero-day Malware Detection using Threshold-free Autoencoding Architecture. , 2021, , . | | 3 |
| 237 | A Survey of Crypto Ransomware Attack Detection Methodologies: An Evolving Outlook. Sensors, 2022, 22, 1837. | 2.1 | 29 |

| # | Article | IF | Citations |
|---|---|---|---|
| 238 | Automation Detection of Malware and Stenographical Content using Machine Learning. , 2022, , . | | 0 |
| 239 | RAPSAMS: Robust affinity propagation clustering on static android malware stream. Concurrency Computation Practice and Experience, 0, , . | 1.4 | 0 |
| 240 | Classifying Malicious Documents on the Basis of Plain-Text Features: Problem, Solution, and Experiences. Applied Sciences (Switzerland), 2022, 12, 4088. | 1.3 | 1 |
| 241 | Deep-Ensemble and Multifaceted Behavioral Malware Variant Detection Model. IEEE Access, 2022, 10, 42762-42777. | 2.6 | 7 |
| 242 | An Attribute Extraction for Automated Malware Attack Classification and Detection Using Soft Computing Techniques. Computational Intelligence and Neuroscience, 2022, 2022, 1-13. | 1.1 | 5 |
| 243 | Improving Classification Performance for Malware Detection Using Genetic Programming Feature Selection Techniques. Journal of Applied Security Research, 2023, 18, 627-647. | 0.8 | 1 |
| 244 | Scalable Malware Detection System Using Distributed Deep Learning. Cybernetics and Systems, 2023, 54, 619-647. | 1.6 | 4 |
| 245 | Network Penetration Intrusion Prediction Based on Attention Seq2seq Model. Security and Communication Networks, 2022, 2022, 1-19. | 1.0 | 0 |
| 246 | Malware Attacks: Dimensions, Impact, and Defenses. EAI/Springer Innovations in Communication and Computing, 2022, , 157-179. | 0.9 | 2 |
| 247 | Bane or Boon: Measuring the effect of evasive malware on system call classifiers. Journal of Information Security and Applications, 2022, 67, 103202. | 1.8 | 4 |
| 248 | A Survey on Heterogeneous Graph Embedding: Methods, Techniques, Applications and Sources. IEEE Transactions on Big Data, 2023, 9, 415-436. | 4.4 | 67 |
| 249 | Arms Race in Adversarial Malware Detection: A Survey. ACM Computing Surveys, 2023, 55, 1-35. | 16.1 | 12 |
| 250 | Artificial Intelligence Security: Threats and Countermeasures. ACM Computing Surveys, 2023, 55, 1-36. | 16.1 | 26 |
| 253 | Performance Evaluation of Machine Learning Classifiers in Malware Detection. , 2022, , . | | 10 |
| 254 | APMWMM: Approach to Probe Malware on Windows Machine using Machine Learning. , 2022, , . | | 2 |
| 255 | Are Malware Detection Models Adversarial Robust Against Evasion Attack?. , 2022, , . | | 0 |
| 256 | Deep Learning for Android Malware Defenses: A Systematic Literature Review. ACM Computing Surveys, 2023, 55, 1-36. | 16.1 | 24 |
| 258 | Hyper-heuristic multi-objective online optimization for cyber security in big data. International Journal of Systems Assurance Engineering and Management, 2024, 15, 314-323. | 1.5 | 0 |

| # | Article | IF | Citations |
|---|---|---|---|
| 259 | A time-interval-based active learning framework for enhanced PE malware acquisition and detection. Computers and Security, 2022, 121, 102838. | 4.0 | 2 |
| 260 | Lightweight CNN-based malware image classification for resource-constrained applications. Innovations in Systems and Software Engineering, 0, , . | 1.6 | 0 |
| 261 | Adapting novelty towards generating antigens for antivirus systems. , 2022, , . | | 2 |
| 262 | MaliCage: A packed malware family classification framework based on DNN and GAN. Journal of Information Security and Applications, 2022, 68, 103267. | 1.8 | 2 |
| 263 | Objection!: Identifying Misclassified Malicious Activities with XAI. , 2022, , . | | 0 |
| 264 | Explainability in Cyber Security using Complex Network Analysis: A Brief Methodological Overview. , 2022, , . | | 1 |
| 265 | A Review on C3I Systemsâ€™ Security: Vulnerabilities, Attacks, and Countermeasures. ACM Computing Surveys, 2023, 55, 1-38. | 16.1 | 3 |
| 266 | Malware detection for Android application using Aquila optimizer and Hybrid LSTM-SVM classifier. EAI Endorsed Transactions on Scalable Information Systems, 0, , e1. | 0.8 | 3 |
| 267 | A few-shot malware classification approach for unknown family recognition using malware feature visualization. Computers and Security, 2022, 122, 102887. | 4.0 | 11 |
| 268 | On building machine learning pipelines for Android malware detection: a procedural survey of practices, challenges and opportunities. Cybersecurity, 2022, 5, . | 3.1 | 6 |
| 269 | A Rule-Based Approach for Grey Hole Attack Prediction in Wireless Sensor Networks. Intelligent Automation and Soft Computing, 2023, 35, 3815-3827. | 1.6 | 0 |
| 270 | Adversarial Machine Learning. Synthesis Lectures on Artificial Intelligence and Machine Learning, 2018, , . | 0.6 | 33 |
| 271 | Impacto de Ofuscadores e Otimizadores de CÃ³digo na AcurÃ¡cia de Classificadores de Programas. , 2022, , . | | 0 |
| 272 | Explainable Artificial Intelligence Applications in Cyber Security: State-of-the-Art in Research. IEEE Access, 2022, 10, 93104-93139. | 2.6 | 54 |
| 273 | Malware Detection Using Automated Generation ofÂYara Rules onÂDynamic Features. Lecture Notes in Computer Science, 2022, , 315-330. | 1.0 | 3 |
| 274 | An Attention Mechanism for Combination of CNN and VAE for Image-Based Malware Classification. IEEE Access, 2022, 10, 85127-85136. | 2.6 | 4 |
| 275 | Evaluation and Survey of State of the Art Malware Detection and Classification Techniques: Analysis and Recommendation. SSRN Electronic Journal, 0, , . | 0.4 | 1 |
| 276 | A Node-Embedding Features Based Machine Learning Technique for Dynamic Malware Detection. , 2022, , . | | 1 |

| # | Article | IF | Citations |
|---|---|---|---|
| 277 | Towards AI-Enabled Hardware Security: Challenges and Opportunities. , 2022, , . | | 1 |
| 278 | Development Strategy of College Sports Information Management System Using Data Mining in Mobile Internet Environment. Journal of Environmental and Public Health, 2022, 2022, 1-10. | 0.4 | 1 |
| 279 | Teaching Practice of College Studentsâ€™ Marketing Course Based on the Background of the Internet Era. International Transactions on Electrical Energy Systems, 2022, 2022, 1-10. | 1.2 | 2 |
| 280 | An enhancement for image-based malware classification using machine learning with low dimension normalized input images. Journal of Information Security and Applications, 2022, 69, 103308. | 1.8 | 3 |
| 281 | A Malware Detection Scheme via Smart Memory Forensics for Windows Devices. Mobile Information Systems, 2022, 2022, 1-16. | 0.4 | 3 |
| 282 | Disentangled Representation Learning in Heterogeneous Information Network for Large-scale Android Malware Detection in the COVID-19 Era and Beyond. Proceedings of the AAAI Conference on Artificial Intelligence, 2021, 35, 7754-7761. | 3.6 | 5 |
| 283 | On the Resilience of Shallow Machine Learning Classification in Image-based Malware Detection. Procedia Computer Science, 2022, 207, 145-157. | 1.2 | 5 |
| 284 | CNNâ€•and GANâ€based classification of malicious code families: A code visualization approach. International Journal of Intelligent Systems, 2022, 37, 12472-12489. | 3.3 | 7 |
| 285 | Windows Malware Detection using Machine Learning and TF-IDF Enriched API Calls Information. , 2022, , . | | 1 |
| 286 | AndroMalPack: enhancing the ML-based malware classification by detection and removal of repacked apps for Android systems. Scientific Reports, 2022, 12, . | 1.6 | 3 |
| 288 | MultiEvasion: Evasion Attacks Against Multiple Malware Detectors. , 2022, , . | | 0 |
| 289 | A review of Machine Learning-based zero-day attack detection: Challenges and future directions. Computer Communications, 2023, 198, 175-185. | 3.1 | 11 |
| 290 | A Survey of Adversarial Attack and Defense Methods for Malware Classification in Cyber Security. IEEE Communications Surveys and Tutorials, 2023, 25, 467-496. | 24.8 | 10 |
| 291 | Attacking Malware Detection using Adversarial Machine Learning. , 2022, , . | | 0 |
| 292 | Mal_CNN: An Enhancement for Malicious Image Classification Based on Neural Network. Cybernetics and Systems, 0, , 1-14. | 1.6 | 1 |
| 293 | Evaluation of Machine Learning Algorithms for Malware Detection. Sensors, 2023, 23, 946. | 2.1 | 8 |
| 294 | Building Cybersecurity Ontology for Understanding and Reasoning Adversary Tactics and Techniques. , 2022, , . | | 0 |
| 295 | On the Effectiveness of Perturbations in Generating Evasive Malware Variants. IEEE Access, 2023, 11, 31062-31074. | 2.6 | 4 |

| # | Article | IF | Citations |
|---|---|---|---|
| 296 | ImageDroid: Using Deep Learning to Efficiently Detect Android Malware and Automatically Mark Malicious Features. Security and Communication Networks, 2023, 2023, 1-11. | 1.0 | 2 |
| 297 | Developing Resilient Cyber-Physical Systems: A Review of State-of-the-Art Malware Detection Approaches, Gaps, and Future Directions. Computers, 2023, 12, 79. | 2.1 | 3 |
| 298 | Adversarial attacks against Windows PE malware detection: A survey of the state-of-the-art. Computers and Security, 2023, 128, 103134. | 4.0 | 22 |
| 299 | Development of a deep stacked ensemble with process based volatile memory forensics for platform independent malware detection and classification. Expert Systems With Applications, 2023, 223, 119952. | 4.4 | 6 |
| 300 | Unsupervised Learning Approaches for Construction of Malware Families. , 2022, , . | | 0 |
| 301 | A pyramid stripe pooling-based convolutional neural network for malware detection and classification. Journal of Ambient Intelligence and Humanized Computing, 2023, 14, 2785-2796. | 3.3 | 0 |
| 302 | Beyond the Hype: An Evaluation of Commercially Available Machine Learningâ€“based Malware Detectors. Digital Threats Research and Practice, 2023, 4, 1-22. | 1.7 | 1 |
| 303 | Automated, Reliable Zero-day Malware Detection based on Autoencoding Architecture. IEEE Transactions on Network and Service Management, 2023, , 1-1. | 3.2 | 4 |
| 304 | MLP-Mixer-Autoencoder: A Lightweight Ensemble Architecture for Malware Classification. Information (Switzerland), 2023, 14, 167. | 1.7 | 1 |
| 305 | Leveraging Comment Retrieval forÂCode Summarization. Lecture Notes in Computer Science, 2023, , 439-447. | 1.0 | 0 |
| 306 | Hierarchical Classification of Android Malware Traffic. , 2022, , . | | 1 |
| 307 | A Survey on Malware Classification using Deep Learning Techniques. , 2023, , . | | 0 |
| 308 | BejaGNN: behavior-based Java malware detection via graph neural network. Journal of Supercomputing, 2023, 79, 15390-15414. | 2.4 | 1 |
| 309 | Review of Ransomware Attacks and a Data Recovery Framework using Autopsy Digital Forensics Platform. , 2023, , . | | 2 |
| 310 | The Age of Ransomware: A Survey on the Evolution, Taxonomy, and Research Directions. IEEE Access, 2023, 11, 40698-40723. | 2.6 | 9 |
| 311 | Malware Analysis and Detection. , 2022, , . | | 0 |
| 313 | Image-Based Zero-Day Malware Detection in IoMT Devices: A Hybrid AI-Enabled Method. , 2023, , . | | 1 |
| 319 | Malware Analysis Using Machine Learning Tools and Techniques in IT Industry. Advanced Technologies and Societal Change, 2023, , 195-209. | 0.8 | 2 |

| # | Article | IF | Citations |
|---|---|---|---|
| 320 | Future Trend of Network Security. , 2023, , 409-425. | | 0 |
| 322 | Machine Learning and Network Traffic to Distinguish Between Malware and Benign Applications. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, 2023, , 96-108. | 0.2 | 1 |
| 323 | Static malware detection of Ember windows-PE API call using machine learning. AIP Conference Proceedings, 2023, , . | 0.3 | 0 |
| 324 | IEWS: a Free Open Source Intelligent Early Warning System Based on Machine Learning. , 2023, , . | | 0 |
| 325 | SecBox: A Lightweight Container-based Sandbox for Dynamic Malware Analysis. , 2023, , . | | 1 |
| 327 | A Survey of Traditional and Machine Learning-based Malware Detection Techniques. , 2023, , . | | 0 |
| 329 | API2Vec: Learning Representations of API Sequences for Malware Detection. , 2023, , . | | 2 |
| 330 | Bad Snakes: Understanding and Improving Python Package Index Malware Scanning. , 2023, , . | | 0 |
| 331 | MalEfficient10%: A Novel Feature Reduction Approach forÂAndroid Malware Detection. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, 2023, , 72-92. | 0.2 | 1 |
| 333 | Malware Detection and Classification with Deep Learning Models. , 2023, , . | | 0 |
| 335 | Identification of Malware Mimicry Attacks Using Process Escalating Visualization. , 2023, , . | | 0 |
| 342 | Ransomware Taxonomy and Detection Techniques Based on Machine Learning: A Review. Communications in Computer and Information Science, 2023, , 138-160. | 0.4 | 0 |
| 343 | Machine learning aided malware detection for secure and smart manufacturing: a comprehensive analysis of the state of the art. International Journal on Interactive Design and Manufacturing, 0, , . | 1.3 | 0 |
| 346 | A feature fusion-based malicious code detection strategy. , 2023, , . | | 0 |
| 347 | Malware Analysis for IoT and Smart AI-Based Applications. Security Informatics and Law Enforcement, 2024, , 165-195. | 0.4 | 0 |
| 348 | ASParseV3: Auto-Static Parser and Customizable Visualizer. Security Informatics and Law Enforcement, 2024, , 41-61. | 0.4 | 0 |
| 350 | SDB-RGSO: Swarm-Based Data Balancing and Randomized Grid Search Optimization for IoT NetFlow Malware Detection with Ensemble Machine Learning Model. Lecture Notes in Networks and Systems, 2023, , 615-631. | 0.5 | 0 |
| 354 | IMCSCL: Image-Based Malware Classification using Self-Supervised and Contrastive Learning. , 2023, , . | | 0 |

| # | Article | IF | Citations |
|---|---|---|---|
| 358 | Performance ofÂMachine Learning Classifiers forÂMalware Detection OverÂImbalanced Data. Lecture Notes in Networks and Systems, 2024, , 496-507. | 0.5 | 0 |
| 359 | Revolutionizing Malware Detection. Advances in Medical Technologies and Clinical Practice Book Series, 2024, , 196-220. | 0.3 | 0 |
| 361 | Malware Prediction Using Tabular Deep Learning Models. Advances in Intelligent Systems and Computing, 2024, , 379-389. | 0.5 | 0 |
| 364 | An Empirical Framework for Malware Prediction Using Multi-Layer Perceptron. , 2023, , . | | 0 |
| 365 | Social Media in the Digital Age: A Comprehensive Review of Impacts, Challenges and Cybercrime. , 0, , . | | 0 |