# Robust Malware Detection for Internet of (Battlefield) T Eigenspace Learning

IEEE Transactions on Sustainable Computing

4, 88-95

DOI: 10.1109/tsusc.2018.2809665

Citation Report

| # | Article | IF | Citations |
|---|---|---|---|
| 1 | Recent Advancements in Intrusion Detection Systems for the Internet of Things. Security and Communication Networks, 2019, 2019, 1-19. | 1.0 | 25 |
| 2 | A Detailed Investigation and Analysis of Deep Learning Architectures and Visualization Techniques forÂMalware Family Identification. Advanced Sciences and Technologies for Security Applications, 2019, , 241-286. | 0.4 | 7 |
| 3 | Towards a rooted subgraph classifier for IoT botnet detection. , 2019, , . | | 7 |
| 4 | Application Specific Internet of Things (ASIoTs): Taxonomy, Applications, Use Case and Future Directions. IEEE Access, 2019, 7, 56577-56590. | 2.6 | 66 |
| 5 | Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations. IEEE Communications Surveys and Tutorials, 2019, 21, 2702-2733. | 24.8 | 468 |
| 6 | New Multiparametric Similarity Measure and Distance Measure for Interval Neutrosophic Set With IoT Industry Evaluation. IEEE Access, 2019, 7, 28258-28280. | 2.6 | 23 |
| 7 | Protecting IoT and ICS Platforms Against Advanced Persistent Threat Actors: Analysis of APT1, Silent Chollima and Molerats. , 2019, , 225-255. | | 12 |
| 8 | A Bibliometric Analysis of Authentication and Access Control in IoT Devices. , 2019, , 25-51. | | 7 |
| 9 | Evaluation and Application of Two Fuzzing Approaches for Security Testing of IoT Applications. , 2019, , 301-327. | | 5 |
| 12 | Malware Analytics: Review of Data Mining, Machine Learning and Big Data Perspectives. , 2019, , . | | 9 |
| 13 | Adversarial Learning Attacks on Graph-based IoT Malware Detection Systems. , 2019, , . | | 44 |
| 14 | DLâ€ÌDS: a deep learningâ€“based intrusion detection framework for securing IoT. Transactions on Emerging Telecommunications Technologies, 2022, 33, e3803. | 2.6 | 109 |
| 15 | IoMT Malware Detection Approaches: Analysis and Research Challenges. IEEE Access, 2019, 7, 182459-182476. | 2.6 | 95 |
| 16 | Analysis and Triage of Advanced Hacking Groups Targeting Western Countries Critical National Infrastructure: APT28, RED October, and Regin. Advanced Sciences and Technologies for Security Applications, 2019, , 221-244. | 0.4 | 8 |
| 17 | An Ensemble Intrusion Detection Technique Based on Proposed Statistical Flow Features for Protecting Network Traffic of Internet of Things. IEEE Internet of Things Journal, 2019, 6, 4815-4830. | 5.5 | 320 |
| 18 | A novel graph-based approach for IoT botnet detection. International Journal of Information Security, 2020, 19, 567-577. | 2.3 | 71 |
| 19 | Intrusion Detection Protocols in Wireless Sensor Networks Integrated to Internet of Things Deployment: Survey and Future Challenges. IEEE Access, 2020, 8, 3343-3363. | 2.6 | 103 |
| 20 | Deep learning and big data technologies for IoT security. Computer Communications, 2020, 151, 495-517. | 3.1 | 209 |

| # | Article | IF | Citations |
|---|---|---|---|
| 21 | Performance Analysis of Decision Tree C4.5 as a Classification Technique to Conduct Network Forensics for Botnet Activities in Internet of Things. , 2020, , . | | 7 |
| 22 | Medium Access Control Protocols for the Internet of Things Based on Unmanned Aerial Vehicles: A Comparative Survey. Sensors, 2020, 20, 5586. | 2.1 | 11 |
| 23 | Cryptocurrency malware hunting: A deep Recurrent Neural Network approach. Applied Soft Computing Journal, 2020, 96, 106630. | 4.1 | 78 |
| 24 | IoT Botnet Attack Detection Based on Optimized Extreme Gradient Boosting and Feature Selection. Sensors, 2020, 20, 6336. | 2.1 | 38 |
| 25 | SOMDROID: android malware detection by artificial neural network trained using unsupervised learning. Evolutionary Intelligence, 2022, 15, 407-437. | 2.3 | 17 |
| 26 | Cognitive and Scalable Technique for Securing IoT Networks Against Malware Epidemics. IEEE Access, 2020, 8, 138508-138528. | 2.6 | 21 |
| 27 | MTHAEL: Cross-Architecture IoT Malware Detection Based on Neural Network Advanced Ensemble Learning. IEEE Transactions on Computers, 2020, 69, 1654-1667. | 2.4 | 50 |
| 28 | V-Sandbox for Dynamic Analysis IoT Botnet. IEEE Access, 2020, 8, 145768-145786. | 2.6 | 20 |
| 29 | Malicious Code Detection Based on Code Semantic Features. IEEE Access, 2020, 8, 176728-176737. | 2.6 | 11 |
| 30 | Real time Application of Malware Patching on Decentralized IoT Systems Through Disease Spread Analysis. , 2020, , . | | 0 |
| 31 | IoT Vulnerability Assessment for Sustainable Computing: Threats, Current Solutions, and Open Challenges. IEEE Access, 2020, 8, 168825-168853. | 2.6 | 74 |
| 32 | IoT-Malware Detection Based on Byte Sequences of Executable Files. , 2020, , . | | 11 |
| 33 | Research on Artificial Intelligence Enhancing Internet of Things Security: A Survey. IEEE Access, 2020, 8, 153826-153848. | 2.6 | 89 |
| 34 | Efficient Detection and Classification of Internet-of-Things Malware Based on Byte Sequences from Executable Files. IEEE Open Journal of the Computer Society, 2020, 1, 262-275. | 5.2 | 20 |
| 35 | The Performance of IoT Malware Detection Technique Using Feature Selection and Feature Reduction in Fog Layer. IOP Conference Series: Materials Science and Engineering, 2020, 928, 022047. | 0.3 | 3 |
| 36 | On securing IoT from Deep Learning perspective. , 2020, , . | | 8 |
| 38 | An Enhanced Stacked LSTM Method With No Random Initialization for Malware Threat Hunting in Safety and Time-Critical Systems. IEEE Transactions on Emerging Topics in Computational Intelligence, 2020, 4, 630-640. | 3.4 | 50 |
| 39 | A Systematic Literature Review of Android Malware Detection Using Static Analysis. IEEE Access, 2020, 8, 116363-116379. | 2.6 | 80 |

| # | Article | IF | Citations |
|---|---|---|---|
| 40 | Intrusion Detection in IoT Networks Using Deep Learning Algorithm. Information (Switzerland), 2020, 11, 279. | 1.7 | 90 |
| 42 | Rider Optimization based Optimized Deep-CNN towards Attack Detection in IoT. , 2020, , . | | 1 |
| 43 | 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 |
| 44 | A Machine Learning Based Intrusion Detection System for Mobile Internet of Things. Sensors, 2020, 20, 461. | 2.1 | 65 |
| 45 | A novel approach to detect IoT malware by system calls using Deep learning techniques. , 2020, , . | | 19 |
| 46 | Machine Learning in IoT Security: Current Solutions and Future Challenges. IEEE Communications Surveys and Tutorials, 2020, 22, 1686-1721. | 24.8 | 409 |
| 47 | A new network forensic framework based on deep learning for Internet of Things networks: A particle deep framework. Future Generation Computer Systems, 2020, 110, 91-106. | 4.9 | 108 |
| 48 | NB-IoT Security: A Survey. Wireless Personal Communications, 2020, 113, 2661-2708. | 1.8 | 35 |
| 49 | An internet of things malware classification method based on mixture of experts neural network. Transactions on Emerging Telecommunications Technologies, 2021, 32, e3920. | 2.6 | 1 |
| 50 | ANGUISH: Security attack in narrowbandâ€Internet of Things (NBâ€IoT) using game theory and hardware analysis. Transactions on Emerging Telecommunications Technologies, 2021, 32, e3987. | 2.6 | 4 |
| 51 | A Multikernel and Metaheuristic Feature Selection Approach for IoT Malware Threat Hunting in the Edge Layer. IEEE Internet of Things Journal, 2021, 8, 4540-4547. | 5.5 | 35 |
| 52 | Resilient Machine Learning for Networked Cyber Physical Systems: A Survey for Machine Learning Security to Securing Machine Learning for CPS. IEEE Communications Surveys and Tutorials, 2021, 23, 524-552. | 24.8 | 97 |
| 53 | Industrial Internet-of-Things Security Enhanced With Deep Learning Approaches for Smart Cities. IEEE Internet of Things Journal, 2021, 8, 6393-6405. | 5.5 | 41 |
| 54 | An invisible warfare with the internet of battlefield things: A literature review. Human Behavior and Emerging Technologies, 2021, 3, 255-260. | 2.5 | 13 |
| 55 | An Efficient Algorithm to Extract Control Flow-Based Features for IoT Malware Detection. Computer Journal, 2021, 64, 599-609. | 1.5 | 7 |
| 56 | Diversity-By-Design for Dependable and Secure Cyber-Physical Systems: A Survey. IEEE Transactions on Network and Service Management, 2021, , 1-1. | 3.2 | 0 |
| 57 | Detection of malware on the internet of things and its applications depends on long short-term memory network. Journal of Ambient Intelligence and Humanized Computing, 0, , 1. | 3.3 | 12 |
| 58 | DADEM. International Journal of Ambient Computing and Intelligence, 2021, 12, 114-139. | 0.8 | 11 |

| # | Article | IF | Citations |
|---|---|---|---|
| 59 | Hierarchical Bidirectional RNN for Safety-Enhanced B5G Heterogeneous Networks. IEEE Transactions on Network Science and Engineering, 2021, 8, 2946-2957. | 4.1 | 39 |
| 60 | Application of Machine Learning for Ransomware Detection in IoT Devices. Studies in Computational Intelligence, 2021, , 393-420. | 0.7 | 12 |
| 61 | Parallel machine learning and deep learning approaches for internet of medical things (IoMT). , 2021, , 89-103. | | 2 |
| 62 | Security Threats and Artificial Intelligence Based Countermeasures for Internet of Things Networks: A Comprehensive Survey. IEEE Access, 2021, 9, 94668-94690. | 2.6 | 50 |
| 63 | A Survey on Cross-Architectural IoT Malware Threat Hunting. IEEE Access, 2021, 9, 91686-91709. | 2.6 | 33 |
| 64 | FSDroid:- A feature selection technique to detect malware from Android using Machine Learning Techniques. Multimedia Tools and Applications, 2021, 80, 13271-13323. | 2.6 | 43 |
| 65 | CNN-Based Malware Variants Detection Method for Internet of Things. IEEE Internet of Things Journal, 2021, 8, 16946-16962. | 5.5 | 24 |
| 66 | How Good Are Classification Models inÂHandling Dynamic Intrusion Attacks inÂIoT?. Lecture Notes in Networks and Systems, 2021, , 81-94. | 0.5 | 0 |
| 67 | A hybrid attack detection strategy for cybersecurity using moth elephant herding optimisationâ€based stacked autoencoder. IET Circuits, Devices and Systems, 2021, 15, 224-236. | 0.9 | 4 |
| 68 | Convolutional Neural Network-Based Cryptography Ransomware Detection for Low-End Embedded Processors. Mathematics, 2021, 9, 705. | 1.1 | 8 |
| 69 | Backbones for Internet of Battlefield Things. , 2021, , . | | 6 |
| 70 | Deep Learning for Network Traffic Monitoring and Analysis (NTMA): A Survey. Computer Communications, 2021, 170, 19-41. | 3.1 | 147 |
| 71 | CRIDS: Correlation and Regression-Based Network Intrusion Detection System for IoT. SN Computer Science, 2021, 2, 1. | 2.3 | 3 |
| 72 | A hybrid DL-driven intelligent SDN-enabled malware detection framework for Internet of Medical Things (IoMT). Computer Communications, 2021, 170, 209-216. | 3.1 | 43 |
| 73 | DDoS detection in 5G-enabled IoT networks using deep Kalman backpropagation neural network. International Journal of Machine Learning and Cybernetics, 2021, 12, 3337-3349. | 2.3 | 22 |
| 74 | Design and Implementation of Intelligent English Electronic Dictionary System Based on Internet of Things. Wireless Communications and Mobile Computing, 2021, 2021, 1-11. | 0.8 | 4 |
| 75 | Intelligent Mirai Malware Detection in IoT Devices. , 2021, , . | | 7 |
| 76 | Intelligent Mirai Malware Detection for IoT Nodes. Electronics (Switzerland), 2021, 10, 1241. | 1.8 | 16 |

| # | Article | IF | Citations |
|---|---|---|---|
| 77 | A systematic review on Deep Learning approaches for IoT security. Computer Science Review, 2021, 40, 100389. | 10.2 | 52 |
| 78 | On the undetectability of payloads generated through automatic tools: A humanâ€oriented approach. Concurrency Computation Practice and Experience, 2021, 33, e6351. | 1.4 | 1 |
| 79 | Ensemble Detection Model for IoT IDS. Internet of Things (Netherlands), 2021, 16, 100435. | 4.9 | 34 |
| 80 | A review of artificial intelligence based malware detection using deep learning. Materials Today: Proceedings, 2023, 80, 2678-2683. | 0.9 | 7 |
| 81 | Cross-Architecture Intemet-of-Things Malware Detection Based on Graph Neural Network. , 2021, , . | | 9 |
| 82 | Internet of Things attack detection using hybrid Deep Learning Model. Computer Communications, 2021, 176, 146-154. | 3.1 | 107 |
| 83 | IoT-Based Intrusion Detection Systems: A Review. Smart Science, 2022, 10, 265-282. | 1.9 | 4 |
| 84 | Comprehensive Analysis of IoT Malware Evasion Techniques. Engineering, Technology & Applied Science Research, 2021, 11, 7495-7500. | 0.8 | 6 |
| 85 | A secure and efficient authentication and data sharing scheme for Internet of Things based on blockchain. Journal of Systems Architecture, 2021, 117, 102112. | 2.5 | 38 |
| 87 | Markov Decision Process based Model for Performance Analysis an Intrusion Detection System in IoT Networks. Journal of Telecommunications and Information Technology, 2021, 3, 42-49. | 0.3 | 3 |
| 88 | Deep learning in the information service system of agricultural Internet of Things for innovation enterprise. Journal of Supercomputing, 2022, 78, 5010-5028. | 2.4 | 4 |
| 89 | Generative adversarial network to detect unseen Internet of Things malware. Ad Hoc Networks, 2021, 122, 102591. | 3.4 | 29 |
| 90 | IoT-Malware Classification Model Using Byte Sequences and Supervised Learning Techniques. Lecture Notes in Networks and Systems, 2021, , 51-60. | 0.5 | 0 |
| 91 | DL-FHMC: Deep Learning-Based Fine-Grained Hierarchical Learning Approach for Robust Malware Classification. IEEE Transactions on Dependable and Secure Computing, 2022, 19, 3432-3447. | 3.7 | 15 |
| 92 | IoT Malware Classification Based on Lightweight Convolutional Neural Networks. IEEE Internet of Things Journal, 2022, 9, 3770-3783. | 5.5 | 16 |
| 93 | Security in 5G-Enabled Internet of Things Communication: Issues, Challenges, and Future Research Roadmap. IEEE Access, 2021, 9, 4466-4489. | 2.6 | 40 |
| 94 | Artificial Intelligence and Machine Learning for Ensuring Security in Smart Cities. Advanced Sciences and Technologies for Security Applications, 2021, , 23-47. | 0.4 | 29 |
| 95 | HybriDroid: an empirical analysis on effective malware detection model developed using ensemble methods. Journal of Supercomputing, 2021, 77, 8209-8251. | 2.4 | 14 |

| # | Article | IF | Citations |
|---|---|---|---|
| 96 | Deep neural network based anomaly detection in Internet of Things network traffic tracking for the applications of future smart cities. Transactions on Emerging Telecommunications Technologies, 2021, 32, e4121. | 2.6 | 46 |
| 97 | Analysis of APT Actors Targeting IoT and Big Data Systems: Shell_Crew, NetTraveler, ProjectSauron, CopyKittens, Volatile Cedar and Transparent Tribe as a Case Study. , 2019, , 257-272. | | 3 |
| 98 | Internet of Things for Sustainable Community Development: Introduction and Overview. Internet of Things, 2020, , 1-31. | 1.3 | 21 |
| 99 | Feature-Based Semi-supervised Learning to Detect Malware from Android. Learning and Analytics in Intelligent Systems, 2020, , 93-118. | 0.5 | 10 |
| 100 | Anomaly Detection in Cyber-Physical Systems Using Machine Learning. , 2020, , 219-235. | | 19 |
| 101 | Privacy and Security in Smart and Precision Farming: A Bibliometric Analysis. , 2020, , 305-318. | | 11 |
| 102 | Industrial Big Data Analytics: Challenges and Opportunities. , 2020, , 37-61. | | 14 |
| 103 | Applications of Big Data Analytics and Machine Learning in the Internet of Things. , 2020, , 77-108. | | 16 |
| 104 | A Comparison of State-of-the-Art Machine Learning Models for OpCode-Based IoT Malware Detection. , 2020, , 109-120. | | 7 |
| 105 | Enhancing Network Security Via Machine Learning: Opportunities and Challenges. , 2020, , 165-189. | | 12 |
| 106 | PerbDroid: Effective Malware Detection Model Developed Using Machine Learning Classification Techniques. Intelligent Systems Reference Library, 2020, , 103-139. | 1.0 | 10 |
| 107 | A Comparison Between Different Machine Learning Models for IoT Malware Detection. , 2020, , 195-202. | | 9 |
| 108 | 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 |
| 109 | A Multilabel Fuzzy Relevance Clustering System for Malware Attack Attribution in the Edge Layer of Cyber-Physical Networks. ACM Transactions on Cyber-Physical Systems, 2020, 4, 1-22. | 1.9 | 22 |
| 110 | LAMBDA. Transactions on Embedded Computing Systems, 2020, 19, 1-31. | 2.1 | 7 |
| 111 | A survey of methods supporting cyber situational awareness in the context of smart cities. Journal of Big Data, 2020, 7, . | 6.9 | 19 |
| 113 | A Novel IoT Based Smart Energy Meter with Backup Battery. International Journal of Computing, 0, , 357-364. | 1.5 | 2 |
| 114 | Botnet attack detection in Internet of Things devices over cloud environment via machine learning. Concurrency Computation Practice and Experience, 2022, 34, e6662. | 1.4 | 40 |

| # | Article | IF | Citations |
|---|---|---|---|
| 115 | Subgraph-Based Adversarial Examples Against Graph-Based IoT Malware Detection Systems. Lecture Notes in Computer Science, 2019, , 268-281. | 1.0 | 9 |
| 116 | A Survey of Machine Learning Techniques Used to Combat Against the Advanced Persistent Threat. Communications in Computer and Information Science, 2019, , 159-172. | 0.4 | 2 |
| 117 | Forensic Investigation of Cross Platform Massively Multiplayer Online Games: Minecraft as a Case Study. , 2019, , 153-177. | | 0 |
| 118 | Distributed Filesystem Forensics: Ceph as a Case Study. , 2019, , 129-151. | | 2 |
| 119 | Detection of Advanced Linux Malware Using Machine Learning. Advances in Intelligent Systems and Computing, 2021, , 185-194. | 0.5 | 1 |
| 120 | Active Spectral Botnet Detection Based on Eigenvalue Weighting. , 2020, , 385-397. | | 10 |
| 121 | On the Applicability of Users' Operation-action Characteristics for the Continuous Authentication in IIoT Scenarios. , 2020, , . | | 0 |
| 122 | Cross Platform IoT-Malware Family Classification Based on Printable Strings. , 2020, , . | | 17 |
| 123 | Enabling Smart Cities with Cognition Based Intelligent Route Decision in Vehicles Empowered with Deep Extreme Learning Machine. Computers, Materials and Continua, 2020, 66, 141-156. | 1.5 | 4 |
| 124 | Big Data and Privacy: Challenges and Opportunities. , 2020, , 1-5. | | 8 |
| 125 | Statically Dissecting Internet of Things Malware: Analysis, Characterization, and Detection. Lecture Notes in Computer Science, 2020, , 443-461. | 1.0 | 4 |
| 126 | Intrusion Detection Systems for Internet of Things. Advances in Information Security, Privacy, and Ethics Book Series, 2020, , 148-171. | 0.4 | 0 |
| 127 | Detecting Block Cipher Encryption for Defense Against Crypto Ransomware on Low-End Internet of Things. Lecture Notes in Computer Science, 2020, , 16-30. | 1.0 | 3 |
| 128 | Big Data Application for Security of Renewable Energy Resources. , 2020, , 237-254. | | 1 |
| 129 | IoT Malware Analysis and New Pattern Discovery Through Sequence Analysis Using Meta-Feature Information. IEICE Transactions on Communications, 2020, E103.B, 32-42. | 0.4 | 3 |
| 130 | Privacy Preserving Abnormality Detection: A Deep Learning Approach. , 2020, , 285-303. | | 0 |
| 131 | Machine Learning Framework to Analyze IoT Malware Using ELF and Opcode Features. Digital Threats Research and Practice, 2020, 1, 1-19. | 1.7 | 30 |
| 132 | Scalable malware detection system using big data and distributed machine learning approach. Soft Computing, 2022, 26, 3987-4003. | 2.1 | 7 |

| # | Article | IF | Citations |
|---|---|---|---|
| 133 | Review on the Security Threats of Internet of Things. International Journal of Computer Applications, 2020, 176, 37-45. | 0.2 | 9 |
| 134 | Build a malware detection software for IOT network Using Machine learning. , 2021, , . | | 2 |
| 135 | Evaluation of Machine Learning Algorithms on Internet of Things (IoT) Malware Opcodes. , 2022, , 177-191. | | 1 |
| 136 | IoT Privacy, Security and Forensics Challenges: An Unmanned Aerial Vehicle (UAV) Case Study. , 2022, , 7-39. | | 3 |
| 137 | Detection of Enumeration Attacks in Cloud Environments Using Infrastructure Log Data. , 2022, , 41-52. | | 1 |
| 138 | Adaptive Neural Trees for Attack Detection in Cyber Physical Systems. , 2022, , 89-104. | | 0 |
| 139 | Cyber Threat Attribution with Multi-View Heuristic Analysis. , 2022, , 53-73. | | 4 |
| 140 | Machine Learning for OSX Malware Detection. , 2022, , 209-222. | | 1 |
| 141 | Evaluating Performance of Scalable Fair Clustering Machine Learning Techniques in Detecting Cyber Attacks in Industrial Control Systems. , 2022, , 105-116. | | 4 |
| 142 | Scalable Fair Clustering Algorithm for Internet of Things Malware Classification. , 2022, , 271-287. | | 1 |
| 143 | Evaluation of Supervised and Unsupervised Machine Learning Classifiers for Mac OS Malware Detection. , 2022, , 159-175. | | 2 |
| 144 | Cyber-Attack Detection in Cyber-Physical Systems Using Supervised Machine Learning. , 2022, , 131-140. | | 4 |
| 145 | Mapping CKC Model Through NLP Modelling for APT Groups Reports. , 2022, , 239-252. | | 1 |
| 146 | Mac OS X Malware Detection with Supervised Machine Learning Algorithms. , 2022, , 193-208. | | 3 |
| 147 | Evaluation of Scalable Fair Clustering Machine Learning Methods for Threat Hunting in Cyber-Physical Systems. , 2022, , 141-158. | | 0 |
| 148 | A Survey of Machine Learning Techniques for IoT Security. Communications in Computer and Information Science, 2021, , 139-157. | 0.4 | 3 |
| 149 | Smart Detection and Preservation of Privacy Concerns in Iot Systems: A Systematic Literature Review. SSRN Electronic Journal, 0, , . | 0.4 | 0 |
| 151 | IoT Bonet and Network Intrusion Detection using Dimensionality Reduction and Supervised Machine Learning. , 2020, , . | | 5 |

| # | Article | IF | Citations |
|---|---|---|---|
| 152 | A Comparative Analysis of Machine Learning Techniques for Classification and Detection of Malware. , 2020, , . | | 8 |
| 153 | Passive User Authentication Utilizing Behavioral Biometrics for IIoT Systems. IEEE Internet of Things Journal, 2022, 9, 12783-12798. | 5.5 | 3 |
| 154 | The Approach for IoT Malware Detection Based on Opcodes Sequences Pattern Mining. , 2021, , . | | 0 |
| 155 | A Study of Classifying Advanced Persistent Threats With Multi-Layered Deep Learning Approaches. , 2021, , . | | 0 |
| 156 | On the Applicability of Multi-Characteristics for the Continuous Authentication in IIoT Scenarios. , 2021, , . | | 1 |
| 158 | A Sensitivity Analysis of Poisoning and Evasion Attacks in Network Intrusion Detection System Machine Learning Models. , 2021, , . | | 6 |
| 159 | Security threat model under internet of things using deep learning and edge analysis of cyberspace governance. International Journal of Systems Assurance Engineering and Management, 2022, 13, 1164-1176. | 1.5 | 5 |
| 160 | A comprehensive survey on machine learning approaches for malware detection in IoT-based enterprise information system. Enterprise Information Systems, 2023, 17, . | 3.3 | 64 |
| 161 | Machine learning and the Internet of Things security: Solutions and open challenges. Journal of Parallel and Distributed Computing, 2022, 162, 89-104. | 2.7 | 30 |
| 162 | State-of-the-art survey of artificial intelligent techniques for IoT security. Computer Networks, 2022, 206, 108771. | 3.2 | 37 |
| 164 | Wireless Transmissions, Propagation and Channel Modelling for IoT Technologies: Applications and Challenges. IEEE Access, 2022, 10, 24095-24131. | 2.6 | 23 |
| 165 | Intelligent Malware Defenses. Lecture Notes in Computer Science, 2022, , 217-253. | 1.0 | 2 |
| 166 | Malware Detection Using Decision Tree Based SVM Classifier for IoT. Computers, Materials and Continua, 2022, 72, 713-726. | 1.5 | 3 |
| 167 | A Comparative Analysis of Network Intrusion Detection System for IoT Using Machine Learning. Lecture Notes in Electrical Engineering, 2022, , 211-221. | 0.3 | 1 |
| 168 | Artificial intelligence empowered threat detection in the Internet of Things: A systematic review. Concurrency Computation Practice and Experience, 2022, 34, . | 1.4 | 1 |
| 169 | A comprehensive study of Mozi botnet. International Journal of Intelligent Systems, 2022, 37, 6877-6908. | 3.3 | 8 |
| 170 | Applications of Wireless Sensor Networks and Internet of Things Frameworks in the Industry Revolution 4.0: A Systematic Literature Review. Sensors, 2022, 22, 2087. | 2.1 | 232 |
| 171 | A wrapper method based on a modified two-step league championship algorithm for detecting botnets in IoT environments. Computing (Vienna/New York), 0, , 1. | 3.2 | 3 |

| # | Article | IF | Citations |
|---|---|---|---|
| 172 | Malware Multi Perspective Analytics with Auto Deduction in Cybersecurity. , 2021, , . | | 6 |
| 173 | A GAN Based Malware Adversaries Detection Model. , 2021, , . | | 0 |
| 174 | IIoT Deep Malware Threat Hunting: From Adversarial Example Detection to Adversarial Scenario Detection. IEEE Transactions on Industrial Informatics, 2022, 18, 8477-8486. | 7.2 | 9 |
| 175 | A Knowledge Transfer-based Semi-Supervised Federated Learning for IoT Malware Detection. IEEE Transactions on Dependable and Secure Computing, 2022, , 1-1. | 3.7 | 13 |
| 176 | A novel intelligent cognitive computing-based APT malware detection for Endpoint systems. Journal of Intelligent and Fuzzy Systems, 2022, 43, 3527-3547. | 0.8 | 6 |
| 177 | Scalable Malware Detection System Using Distributed Deep Learning. Cybernetics and Systems, 2023, 54, 619-647. | 1.6 | 4 |
| 178 | A survey on deep learning for cybersecurity: Progress, challenges, and opportunities. Computer Networks, 2022, 212, 109032. | 3.2 | 35 |
| 179 | Intrusion Detection in Internet of Things Systems: A Review on Design Approaches Leveraging Multi-Access Edge Computing, Machine Learning, and Datasets. Sensors, 2022, 22, 3744. | 2.1 | 23 |
| 180 | ThingNet: A Lightweight Real-time Mirai IoT Variants Hunter through CPU Power Fingerprinting. , 2022, , . | | 1 |
| 181 | Detection of Botnets in IoT Networks using Graph Theory and Machine Learning. , 2022, , . | | 3 |
| 182 | Hardware-Assisted Machine Learning in Resource-Constrained IoT Environments for Security: Review and Future Prospective. IEEE Access, 2022, 10, 58603-58622. | 2.6 | 21 |
| 183 | Machine Learning Applications to Smart Cities. Advances in Electronic Government, Digital Divide, and Regional Development Book Series, 2022, , 169-213. | 0.2 | 0 |
| 184 | DS-SWIPT: Secure Communication with Wireless Power Transfer for Internet of Things. Security and Communication Networks, 2022, 2022, 1-11. | 1.0 | 0 |
| 185 | Multilayer Backbones for Internet of Battlefield Things. Future Internet, 2022, 14, 186. | 2.4 | 3 |
| 186 | Cybersecurity for Battlefield of Things â€" A Comprehensive Review. Journal of Circuits, Systems and Computers, 2022, 31, . | 1.0 | 1 |
| 187 | A Brief Overview on Security Challenges and Protocols in Internet of Things Application. , 2022, , . | | 5 |
| 188 | A Low Computational Cost Method for Mobile Malware Detection Using Transfer Learning and Familial Classification Using Topic Modelling. Applied Computational Intelligence and Soft Computing, 2022, 2022, 1-22. | 1.6 | 3 |
| 189 | Local Intrinsic Dimensionality ofÂIoT Networks forÂUnsupervised Intrusion Detection. Lecture Notes in Computer Science, 2022, , 143-161. | 1.0 | 1 |

| # | Article | IF | Citations |
|---|---|---|---|
| 190 | Generating realistic cyber data for training and evaluating machine learning classifiers for network intrusion detection systems. Expert Systems With Applications, 2022, 207, 117936. | 4.4 | 9 |
| 191 | Few-shot IoT attack detection based on RFP-CNN and adversarial unsupervised domain-adaptive regularization. Computers and Security, 2022, 121, 102856. | 4.0 | 3 |
| 192 | Deep Learning Models for Cyber Security in IoT Networks. Advances in Digital Crime, Forensics, and Cyber Terrorism, 2022, , 112-127. | 0.4 | 0 |
| 193 | HeuCrip: a malware detection approach for internet of battlefield things. Cluster Computing, 2023, 26, 977-992. | 3.5 | 4 |
| 194 | On the use of artificial intelligence to deal with privacy in IoT systems: A systematic literature review. Journal of Systems and Software, 2022, 193, 111475. | 3.3 | 7 |
| 195 | Empirical Analysis of Vulnerabilities in Blockchain-based Smart Contracts. Sir Syed Research Journal of Engineering & Technology, 2022, 12, 78-85. | 0.2 | 1 |
| 196 | Improved Ant Colony Optimization and Machine Learning Based Ensemble Intrusion Detection Model. Intelligent Automation and Soft Computing, 2023, 36, 849-864. | 1.6 | 6 |
| 197 | Machine and Deep Learning for IoT Security and Privacy: Applications, Challenges, and Future Directions. Security and Communication Networks, 2022, 2022, 1-41. | 1.0 | 9 |
| 198 | A Survey of the Recent Trends in Deep Learning Based Malware Detection. Journal of Cybersecurity and Privacy, 2022, 2, 800-829. | 2.4 | 26 |
| 199 | Security Risk Analysis and Design Reengineering for Smart Healthcare. Lecture Notes in Electrical Engineering, 2022, , 599-612. | 0.3 | 7 |
| 200 | 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 |
| 201 | Deep Learning Methods for Malware and Intrusion Detection: A Systematic Literature Review. Security and Communication Networks, 2022, 2022, 1-31. | 1.0 | 7 |
| 202 | Cyber Situational Awareness Frontiers. , 2022, , 43-75. | | 0 |
| 203 | Cooperative Scheduling for Directional Wireless Charging With Spatial Occupation. IEEE Transactions on Mobile Computing, 2024, 23, 286-301. | 3.9 | 4 |
| 204 | Malware Detection Using Genetic Cascaded Support Vector Machine Classifier in Internet of Things. , 2022, , . | | 2 |
| 205 | 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 |
| 206 | Attack Detection by Using Deep Learning for Cyber-Physical System. , 2023, , 155-179. | | 0 |
| 207 | Malware Detection in Internet of Things (IoT) Devices Using Deep Learning. Sensors, 2022, 22, 9305. | 2.1 | 8 |

| # | Article | IF | Citations |
|---|---|---|---|
| 208 | A Review of Emerging Technologies for IoT-Based Smart Cities. Sensors, 2022, 22, 9271. | 2.1 | 21 |
| 209 | A Review on Malware Analysis for IoT and Android System. SN Computer Science, 2023, 4, . | 2.3 | 0 |
| 210 | Evaluation of Machine Learning Algorithms for Malware Detection. Sensors, 2023, 23, 946. | 2.1 | 8 |
| 211 | IoT Commercial and Industrial Applications and AI-Powered IoT. , 2023, , 465-500. | | 7 |
| 212 | Efficient and Secured Mechanisms for Data Link in IoT WSNs: A Literature Review. Electronics (Switzerland), 2023, 12, 458. | 1.8 | 7 |
| 213 | Malware Detection Classification using Recurrent Neural Network. , 2022, , . | | 0 |
| 214 | Artificial Algae Optimization with Deep Belief Network Enabled Ransomware Detection in IoT Environment. Computer Systems Science and Engineering, 2023, 46, 1293-1310. | 1.9 | 0 |
| 215 | Attack Detection in IoT Using Machine Learningâ€"A Survey. , 2023, , 211-228. | | 0 |
| 216 | GCDroid: Android Malware Detection Based on Graph Compression With Reachability Relationship Extraction for IoT Devices. IEEE Internet of Things Journal, 2023, 10, 11343-11356. | 5.5 | 5 |
| 217 | Hybrid classification model with tuned weight for cyber attack detection: Big data perspective. Advances in Engineering Software, 2023, 177, 103408. | 1.8 | 0 |
| 218 | Malware detection in IOMT (MDI) using RNN-LSTM. , 2023, 3, 99-106. | | 0 |
| 219 | Insider Intrusion Detection Techniques: A State-of-the-Art Review. Journal of Computer Information Systems, 2024, 64, 106-123. | 2.0 | 1 |
| 220 | Comprehensive Survey on Detecting Security Attacks of IoT Intrusion Detection Systems. Advances in Science and Technology, 0, , . | 0.2 | 3 |
| 221 | Toward support-vector machine-based ant colony optimization algorithms for intrusion detection. Soft Computing, 2023, 27, 6297-6305. | 2.1 | 3 |
| 222 | Tensor Recurrent Neural Network With Differential Privacy. IEEE Transactions on Computers, 2024, 73, 683-693. | 2.4 | 8 |
| 223 | Malware Threat on Edge/Fog Computing Environments From Internet of Things Devices Perspective. IEEE Access, 2023, 11, 33584-33606. | 2.6 | 10 |
| 224 | Mitigating Malware Attacks using Machine Learning: A Review. , 2023, , . | | 0 |
| 225 | Cybersecurity in Internet of Things Networks using Deep Learning Models. , 2023, , . | | 1 |

| # | Article | IF | Citations |
|---|---|---|---|
| 226 | AI Approaches for IoT Security Analysis. Advances in Intelligent Systems and Computing, 2021, , 47-70. | 0.5 | 0 |
| 230 | IoT Security Vulnerabilities and Defensive Measures in Industry 4.0. Advanced Technologies and Societal Change, 2023, , 71-112. | 0.8 | 7 |
| 242 | Role of AI for Data Security and Privacy in 5G Healthcare Informatics. , 2023, , 29-62. | | 0 |
| 247 | A Review of IoT Security Solutions Using Machine Learning and Deep Learning. Lecture Notes in Networks and Systems, 2023, , 115-132. | 0.5 | 0 |
| 249 | Preprocessing Network Traffic using Topological Data Analysis for Data Poisoning Detection. , 2023, , . | | 0 |
| 251 | A Comparative Analysis of IoT Malware Detection Using CNN and Deep Learning. , 2023, , . | | 0 |