iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** I **Month of publication:** January 2025

DOI: https://doi.org/10.22214/ijraset.2025.66213

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue I Jan 2025- Available at www.ijraset.com

Machine Learning in Malware Analysis: Current Trends and Future Directions

Sagar Verma[1], Narendra Kumar Upadhyay[2], Ayush Verma[3], Sakshi Tiwari[4]
[1]*MCA, Department of Computer Applications, Harlal Institute of Management & Technology, Greater Noida*
[2]*HOD, Department of Computer Applications, Harlal Institute of Management & Technology, Greater Noida*
[3]*Asst. prof, Department of Computer Applications, Harlal Institute of Management & Technology, Greater Noida*
[4]*Asst. prof, Department of Computer Applications, Harlal Institute of Management & Technology, Greater Noida*

Abstract: ***Malware analysis is essential in cybersecurity because of the increasing complexity and spread of harmful software. Machine learning plays a key role in this area by handling large datasets, identifying complex patterns, and adapting to changing threats. This paper reviews current research on using machine learning for malware analysis, focusing on the effectiveness of techniques like deep learning, transfer learning, and XML in improving malware detection and analysis. It also discusses challenges such as the need for distributed computing and image resizing to enhance training efficiency and visualization. As cyberattacks become more advanced and frequent, machine learning has become a vital tool for identifying and combating malware. Ongoing studies are exploring scalable deep learning systems for better malware detection. The research focuses on analyzing polymorphic malware to improve detection methods. Machine learning is being applied to uncover hidden patterns in malware behavior, particularly in Windows environments, to keep up with its constant evolution. The literature is categorized by goals, data features, and machine learning techniques used, highlighting current challenges and areas for future research. This study aims to strengthen cybersecurity by advancing malware detection and adapting to emerging threats.***

Keywords: malware analysis, cybersecurity, machine learning, malicious software, deep learning, transfer learning, xml techniques, malware detection

I. INTRODUCTION

The growing use of computers and internet connectivity has contributed to the constant evolution of malware. With more people depending on the internet for daily activities, cybercriminals have found new ways to exploit system vulnerabilities. Malware spreads through various channels such as email attachments, social media, and other online platforms. It includes threats like viruses, worms, Trojan horses, ransomware, and adware. Detecting and analysing malware is a challenging task due to the limitations of traditional methods and the difficulty in identifying new, unforeseen attacks. Malware analysis involves examining programs and networks to understand how malicious software behaves and changes over time. Techniques like signature-based detection and machine learning (ML)-based methods are commonly used for this purpose. While signature-based methods rely on predefined patterns to identify malware, ML-based approaches are more efficient at detecting new and unknown malware. ML, a branch of artificial intelligence, allows systems to learn from data and improve without requiring explicit programming for every task. By recognizing patterns, ML algorithms can identify both existing and emerging malware threats. As cyber threats become increasingly complex, traditional signature-based methods are less effective, making ML a crucial tool for malware detection, classification, behaviour analysis, and assessing system vulnerabilities. In conclusion, the increasing reliance on technology and the internet has given rise to more advanced and diverse malware. To address this growing challenge, ML-based methods are becoming essential for effective malware detection and analysis. These methods offer a more dynamic and reliable solution to protect against ever-changing cyber threats, ensuring better security in today's digital age.

II. METHODOLOGY

The application of machine learning in malware analysis involves several systematic steps, from data collection to model deployment. Below is a detailed breakdown of the methodology:

A. Data Collection

- Static Data: Collecting information from malware binaries, such as opcode sequences, file headers, and embedded strings [8].
- Dynamic Data: Gathering runtime behaviour data, including system calls, network activity, and memory usage [9], [15].
- Hybrid Data: Combining static and dynamic features to enrich the dataset [12].

©IJRASET: All Rights are Reserved

B. Data Preprocessing

- Feature Extraction: Identifying and extracting relevant characteristics from the collected data, such as n-grams of opcodes or API call sequences [29].
- Normalization and Encoding: Transforming raw data into numerical formats suitable for machine learning algorithms [31].
- Balancing Datasets: Addressing class imbalance using techniques like oversampling, under-sampling, or synthetic data generation (e.g., SMOTE) [5].

C. Model Selection

- Supervised Learning: Utilizing labeled datasets to train classifiers such as support vector machines (SVMs), random forests, or neural networks [30], [27].
- Unsupervised Learning: Employing clustering algorithms (e.g., k-means) or anomaly detection techniques for scenarios with limited labeled data.
- Deep Learning: Applying advanced architectures like convolutional neural networks (CNNs) and recurrent neural networks (RNNs) for complex pattern recognition [26], [29].

D. Model Training And Evaluation

- Training: Feeding pre-processed data into selected models and optimizing parameters to minimize loss functions.
- Validation: Using cross-validation techniques to tune hyper-parameters and avoid overfitting.
- Evaluation Metrics: Measuring model performance using metrics such as accuracy, precision, recall, F1-score, and area under the receiver operating characteristic (ROC) curve [15].

E. Deployment

- Real-Time Detection: Implementing models in production environments for live malware detection [6], [43], [35].
- Edge Computing: Deploying lightweight versions of models on endpoint devices for decentralized analysis.
- Integration: Embedding models into security platforms like intrusion detection systems (IDS) or antivirus software [46].

F. Continuous Learning

- Updating Models: Periodically retraining models with new data to adapt to evolving malware.
- Adversarial Training: Incorporating adversarial examples to enhance model robustness against evasion techniques [45].

III. CURRENT TRENDS IN MACHINE LEARNING FOR MALWARE ANALYSIS

This section discusses recent trends, techniques, and strategies in malware analysis and detection that utilize machine learning, highlighting dynamic improvements in the field proposed by researchers [15].

A. Feature Engineering

Feature engineering enhances machine learning by transforming raw data into useful features, crucial for model performance [22]. It focuses on selecting and transforming relevant data aspects, including binary, behavioural, and network information.

B. Deep Learning Approaches

Deep Learning (DL) is a sophisticated branch of Machine Learning (ML) that emulates the human brain's structure using layers of interconnected neurons. It learns abstract concepts autonomously from raw data, utilizing techniques like CNNs, RNNs, and transformers for applications such as malware classification and behaviour prediction [16], [50].

C. Transfer Learning and Pre-trained Models

Pre-trained models are adapted to malware datasets using transfer learning, which accelerates the learning process and decreases the need for extensive training data by leveraging existing knowledge from related tasks, enabling effective generalization [34], [36], [44].

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

D. Ensemble Methods

Ensemble methods in machine learning enhance detection and classification by combining multiple models, improving predictive performance, especially with limited datasets [30], [27].

E. Real-Time Detection

Efforts focus on achieving low-latency, high-accuracy detection in enterprise environments through real-time machine learning, combining object detection and tracking in video sequences [43], [35].

F. Adversarial Machine Learning

Adversarial machine learning (AML) manipulates ML systems to yield malicious results, posing challenges like evasion techniques and defensive strategies in cybersecurity contexts [5], [15].

IV. BENCHMARKING IN MALWARE ANALYSIS

Commonly used datasets in malware detection, such as (Virus Total, Ember, and Microsoft BIG), play an integral role in research. However, they come with limitations and inherent biases, underscoring the need for more diverse and updated datasets [31], [39]. Benchmark datasets are critical for developing and validating machine learning models, providing standardized tools for testing and comparison. They promote consistency in evaluations, enabling researchers to directly compare model effectiveness. The accessibility of these benchmark datasets ensures reproducibility in research, which is vital for establishing credibility and reliability [20], [42]. Additionally, their diversity often mirrors the complexities of real-world scenarios, pushing algorithms to generalize across varied examples. Many of these datasets also hold historical significance, allowing for the tracking of advancements in model performance and machine learning techniques over time [4].

V. CHALLENGES AND LIMITATIONS

Researchers are exploring alternative technologies for real-time malware detection, aiming to reduce false positives and enhance accuracy, due to the limitations and challenges identified in various malware detection trends discussed in previous section [1], [29].

A. Limitations and Challenges Found in Papers using Deep Learning

Rhode et al. [19] explored using RNNs for early-stage malware detection, presuming malicious activities occur within the first five seconds of execution. However, attackers may exploit this assumption by introducing delays or inactive periods at the start of malicious files, misleading the system into categorizing them as safe. It is suggested to enhance detection mechanisms by monitoring behaviours beyond this initial time frame, such as analysing system calls and network activity for a more comprehensive assessment of the file's intent. Meanwhile, Obaidat et al. [28] implemented deep learning (DL) for Java malware detection, highlighting the need for substantial labelled datasets to train effectively and noted that insufficient samples hinder the model's ability to capture essential features, while extensive data processing demands significant training time and computational power. Additionally, Catak et al. [21] reported on dataset imbalances, with certain malware categories vastly outnumbering others, which could negatively impact classification performance. To remedy this, data resampling techniques can be employed to balance instances across categories, improving model training outcomes.

B. Limitations and Challenges Found in Papers using Transfer Learning

The work of Panda et al. [42] highlights challenges in transferring knowledge for malware detection, particularly due to varying image sizes, which can hinder the model's capabilities to capture significant features. This requires pre-processing images by resizing them, which can result in losing important information and longer classification times when the model encounters unknown malware. Additionally, negative transfer can occur when knowledge from one domain is not useful or relevant to another task, reducing the model's performance. This mismatch can create noise that hinders the model's ability to make accurate predictions. A suggested solution is to use a group of models trained on different domains. By combining their strengths, the impact of negative transfer can be minimized. Additionally, Prima and Bouhorma [40], alongside Panda et al. [42] suggest that transfer learning typically relies on large datasets, which, despite yielding high accuracy, demand significant time and computational resources. Incremental learning emerges as a potential remedy, enabling sequential training on smaller data subsets to optimize resource usage and reduce training duration.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

C. Limitations and Challenges Found in Papers using XML

Alani and Awad's [48] work on malware detection is praised for its accuracy and efficiency, yet it struggles to identify unknown and obfuscated malware due to its reliance on static features. These features gather information without accounting for dynamic behaviours, which can be better captured through dynamic analysis. This approach enhances malware detection by revealing execution behaviours such as file modifications and network activity. Furthermore, a balance between model performance and interpretability is crucial, as advancing interpretability often compromises predictive accuracy, a challenge highlighted. The dataset division by Kinkead et al. [47] was criticized for lacking fairness; a balanced split is necessary to reflect accurate distributions of malware and benign samples, with cross-validation being the recommended technique for dataset resampling. Additionally, interpretability in these models lacks standardized evaluation metrics, complicating the comparison and assessment of various explainable machine learning (XML) methods.

VI. FUTURE DIRECTIONS

This section outlines future research directions to address limitations of malware detection, analysis, and classification systems, improving efficiency and effectiveness. We will discuss some future areas. that researchers can utilize to address the issues listed below.: [1], [2], [29]

A. Use of moderate-sized and Balanced Dataset:

A moderate-sized and balanced dataset is crucial for malware analysis in machine learning. It avoids overfitting, ensures diversity, and is computationally efficient. A balanced dataset with equal representation of malware and benign samples prevents model bias, improves evaluation metrics, and enhances generalization to real-world scenarios [21]. Challenges like dataset imbalance can be addressed using techniques like oversampling, under-sampling, or class-weighted loss. Best practices include extracting meaningful features, cross-validation, and real-time testing.

B. Domain Distance Measure

Domain distance measurement in machine learning is a promising future for malware analysis, focusing on quantifying similarity or divergence between different domains. Techniques like domain adaptation, transfer learning, and metric learning can enhance model generalization and make machine learning systems more resilient to concept drift and evolving threats [40]. Addressing negative transfer in transfer learning is crucial for better performance. Accurate domain distance measurement is essential for identifying relevant knowledge for transfer and making model adaptation more effective [21], [27].

C. Comparative Evaluation

Future research should focus on evaluating the quality of XML explanations through comparative evaluations. This involves comparing different XML methods on fixed benchmarks or datasets, focusing on interpretability. This approach is crucial in machine learning for malware analysis, promoting reproducibility and guiding the development of more effective solutions [21], [22]. By fostering transparency and collaboration, comparative evaluation can accelerate malware detection and improve machine learning system reliability [2].

D. Resizing Image and Standardization

Changing image size is a common pre-processing step in machine learning models, ensuring consistent input dimensions and format [37],[42]. However, it can lead to information loss. Standardization techniques can minimize loss, improve model accuracy, and enhance feature extraction. By focusing on resizing and standardization, researchers can create more robust pipelines for effective malware detection methods [6], [43], [35].

E. Integration with Threat Intelligence

Integration with threat intelligence is a key future direction in machine learning for malware analysis, enabling systems to leverage real-time data from global threat intelligence feeds [6], [43], [35]. By incorporating indicators of compromise (IOCs), behavioural patterns, and attack signatures, machine learning models can enhance their predictive accuracy and adapt to emerging threats. This integration allows for more comprehensive context-aware analysis, improving detection rates and reducing false positives [15]. Additionally, collaboration between machine learning systems and threat intelligence platforms fosters proactive defence mechanisms, enabling organizations to anticipate and mitigate cyber threats more effectively.

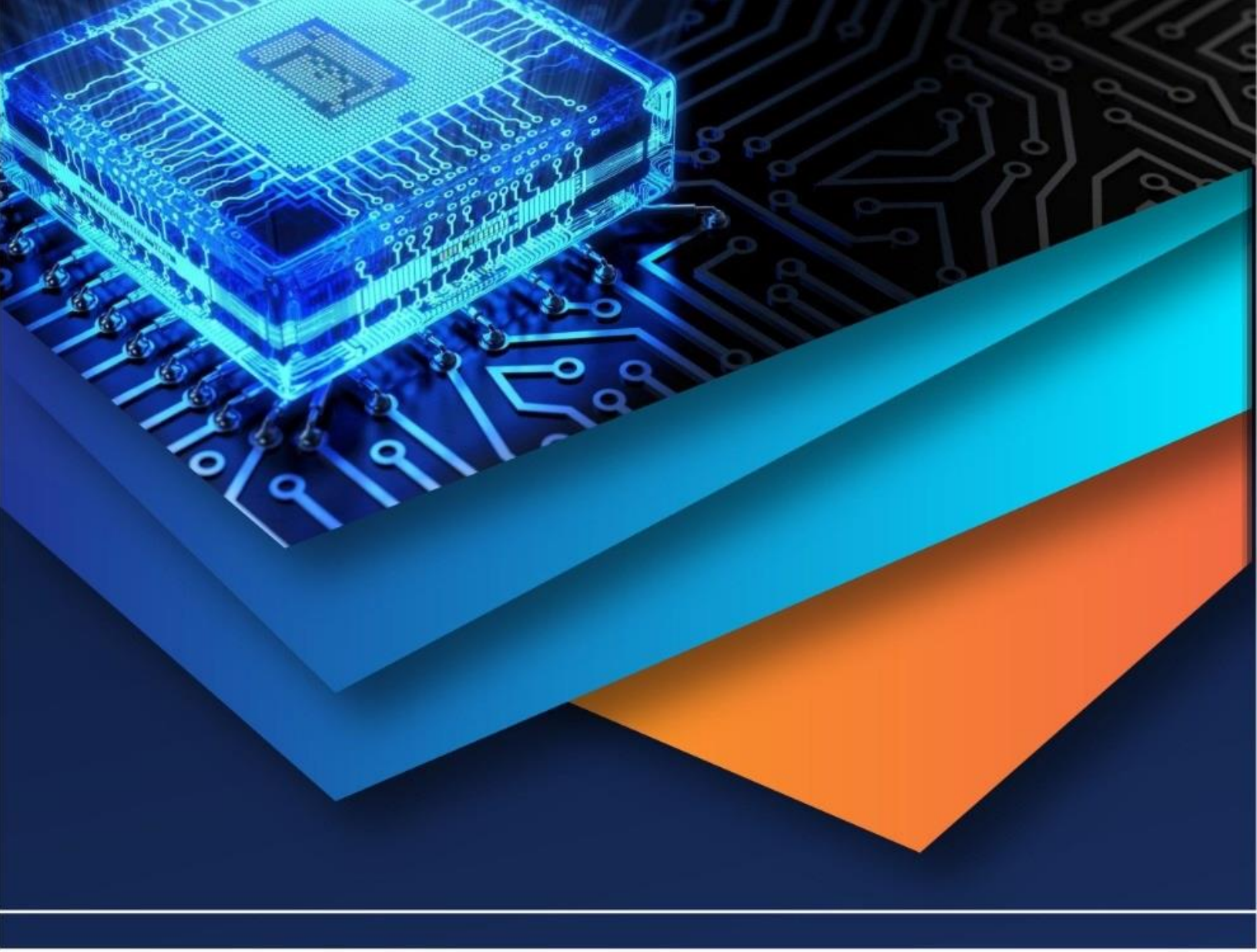
VII. CONCLUSIONS

Machine learning has revolutionized malware analysis by enhancing detection and understanding of malicious software. Innovations in hybrid methods, explainable AI (XAI), and adversarial defence are paving the way for a resilient future in ML-driven cybersecurity [5], [15]. Collaboration between academia, industry, and policymakers is crucial for shaping this future Malware analysis is an essential part of cybersecurity, especially as malware becomes more advanced and harder to detect. Machine learning (ML) plays a key role in this process by helping to analyse large amounts of data and detect complex patterns. This makes it highly effective in identifying and stopping malware attacks. [32] The survey highlights current trends in using ML for malware analysis and discusses how techniques like deep learning, transfer learning, and XML improve detection accuracy and make the process more transparent. It also explores the challenges in this field and offers suggestions for future research to further improve malware analysis. However, the paper has some limitations, such as a small sample size, which reduces the ability to apply its findings to a broader range of scenarios. To address this, further research with larger datasets is needed to make the results more reliable and applicable. In summary, the survey provides valuable insights into how ML is transforming malware analysis while also pointing out areas that require more study for better results in cybersecurity.[46]

REFERENCES

[1] N. Z. Gorment, A. Selamat, L. K. Cheng, and O. Krejcar, "Machine learning algorithm for malware detection: Taxonomy, current challenges and future directions," IEEE Access, 2023.
[2] U. V. Nikam and V. M. Deshmuh, "Performance evaluation of machine learning classifiers in malware detection," in 2022 IEEE International Conference on Distributed Computing and Electrical Circuits and Electronics (ICDCECE). IEEE, 2022, pp. 1–5.
[3] M. S. Akhtar and T. Feng, "Malware analysis and detection using machine learning algorithms," Symmetry, vol. 14, no. 11, p. 2304, 2022.
[4] D. Ucci, L. Aniello, and R. Baldoni, "Survey of machine learning techniques for malware analysis," Computers & Security, vol. 81, pp. 123–147, 2019.
[5] I. H. Sarker, A. Kayes, S. Badsha, H. Alqahtani, P. Watters, and A. Ng, "Cybersecurity data science: an overview from machine learning perspective," Journal of Big data, vol. 7, pp. 1–29, 2020.
[6] I. Sarker, "Machine learning: algorithms, real-world applications and research directions. sn comput sci 2: 160," 2021.
[7] M. T. Ahvanooey, Q. Li, M. Rabbani, and A. R. Rajput, "A survey on smartphones security: software vulnerabilities, malware, and attacks," arXiv preprint arXiv:2001.09406, 2020.
[8] O. Aslan and A. A. Yilmaz, "A new malware classification framework¨ based on deep learning algorithms," Ieee Access, vol. 9, pp. 87936– 87951, 2021.
[9] R. Komatwar and M. Kokare, "Retracted article: a survey on malware detection and classification," Journal of Applied Security Research, vol. 16, no. 3, pp. 390–420, 2021.
[10] M. Ijaz, M. H. Durad, and M. Ismail, "Static and dynamic malware analysis using machine learning," in 2019 16th International bhurban conference on applied sciences and technology (IBCAST). IEEE, 2019, pp. 687–691.
[11] J. Lee, H. Jang, S. Ha, and Y. Yoon, "Android malware detection using machine learning with feature selection based on the genetic algorithm," Mathematics, vol. 9, no. 21, p. 2813, 2021.
[12] N. Tarar, S. Sharma, and C. R. Krishna, "Analysis and classification of android malware using machine learning algorithms," in 2018 3rd International Conference on Inventive Computation Technologies (ICICT). IEEE, 2018, pp. 738–743.
[13] N. K. Gyamfi and E. Owusu, "Survey of mobile malware analysis, detection techniques and tool," 11 2018, pp. 1101–1107.
[14] V. Rao and K. Hande, "A comparative study of static, dynamic and hybrid analysis techniques for android malware detection," International Journal of Engineering Development and Research, vol. 5, no. 2, pp. 1433–1436, 2017.
[15] U.-e.-H. Tayyab, F. B. Khan, M. H. Durad, A. Khan, and Y. S. Lee, "A survey of the recent trends in deep learning based malware detection," Journal of Cybersecurity and Privacy, vol. 2, no. 4, pp. 800–829, 2022.
[16] N. Shone, T. N. Ngoc, V. D. Phai, and Q. Shi, "A deep learning approach to network intrusion detection," IEEE transactions on emerging topics in computational intelligence, vol. 2, no. 1, pp. 41–50, 2018.
[17] N. Rusk, "Deep learning," Nature Methods, vol. 13, no. 1, pp. 35–35, 2016.
[18] Karthick Jonagadla, "Deep learning in financial markets," https://www.quantace.in/deep-learning-application-financial-markets/, 2023, accessed: November 9, 2023.
[19] M. Rhode, P. Burnap, and K. Jones, "Early-stage malware prediction using recurrent neural networks," computers & security, vol. 77, pp. 578–594, 2018.
[20] O. N. Elayan and A. M. Mustafa, "Android malware detection using deep learning," Procedia Computer Science, vol. 184, pp. 847–852, 2021.
[21] F. O. Catak, A. F. Yazı, O. Elezaj, and J. Ahmed, "Deep learning based sequential model for malware analysis using windows exe api calls," PeerJ Computer Science, vol. 6, p. e285, 2020.
[22] A. McDole, M. Gupta, M. Abdelsalam, S. Mittal, and M. Alazab, "Deep learning techniques for behavioral malware analysis in cloud iaas," Malware analysis using artificial intelligence and deep learning, pp. 269–285, 2021.
[23] V. Ravi, M. Alazab, S. Selvaganapathy, and R. Chaganti, "A multi-view attention-based deep learning framework for malware detection in smart healthcare systems," Computer Communications, vol. 195, pp. 73–81, 2022.
[24] E. Calik Bayazit, O. Koray Sahingoz, and B. Dogan, "Deep learning based malware detection for android systems: A comparative analysis," Tehnicki vjesnik˘ , vol. 30, no. 3, pp. 787–796, 2023.
[25] M. ˙Ibrahim, B. Issa, and M. B. Jasser, "A method for automatic android malware detection based on static analysis and deep learning," IEEE Access, vol. 10, pp. 117334–117352, 2022.
[26] R. Patil and W. Deng, "Malware analysis using machine learning and deep learning techniques," in 2020 SoutheastCon, vol. 2. IEEE, 2020, pp. 1–7.

[27] C. Rodrigo, S. Pierre, R. Beaubrun, and F. B. El Khoury, "A hybrid machine learning-based malware detection model for android devices. electronics 2021, 10, 2948," 2021.
[28] I. Obaidat, M. Sridhar, K. M. Pham, and P. H. Phung, "Jadeite: A novel image-behavior-based approach for java malware detection using deep learning," Computers & Security, vol. 113, p. 102547, 2022.
[29] L. Alzubaidi, J. Zhang, A. J. Humaidi, A. Al-Dujaili, Y. Duan, O. AlShamma, J. Santamar´ıa, M. A. Fadhel, M. Al-Amidie, and L. Farhan, "Review of deep learning: Concepts, cnn architectures, challenges, applications, future directions," Journal of big Data, vol. 8, pp. 1–74, 2021.
[30] P. Maniriho, A. N. Mahmood, and M. J. M. Chowdhury, "A survey of recent advances in deep learning models for detecting malware in desktop and mobile platforms," arXiv preprint arXiv:2209.03622, 2022.
[31] Q. Wang, W. Guo, K. Zhang, A. G. Ororbia, X. Xing, X. Liu, and C. L. Giles, "Adversary resistant deep neural networks with an application to malware detection," in Proceedings of the 23rd ACM sigkdd international conference on knowledge discovery and data mining, 2017, pp. 1145–1153.
[32] R. Ribani and M. Marengoni, "A survey of transfer learning for convolutional neural networks," in 2019 32nd SIBGRAPI conference on graphics, patterns and images tutorials (SIBGRAPI-T). IEEE, 2019, pp. 47–57.
[33] C. Tan, F. Sun, T. Kong, W. Zhang, C. Yang, and C. Liu, "A survey on deep transfer learning," in Artificial Neural Networks and Machine Learning–ICANN 2018: 27th International Conference on Artificial Neural Networks, Rhodes, Greece, October 4-7, 2018, Proceedings, Part III 27. Springer, 2018, pp. 270–279.
[34] H. M. K. Barznji, "Transfer learning as new field in machine learning," 2020.
[35] M. Ranaweera and Q. H. Mahmoud, "Virtual to real-world transfer learning: A systematic review," Electronics, vol. 10, no. 12, 2021. [Online]. Available: https://www.mdpi.com/2079-9292/10/12/1491
[36] L. Chen, "Deep transfer learning for static malware classification," arXiv preprint arXiv:1812.07606, 2018.
[37] N. Bhodia, P. Prajapati, F. Di Troia, and M. Stamp, "Transfer learning for image-based malware classification," arXiv preprint arXiv:1903.11551, 2019.
[38] M. Ahmed, N. Afreen, M. Ahmed, M. Sameer, and J. Ahamed, "An inception v3 approach for malware classification using machine learning and transfer learning," International Journal of Intelligent Networks, vol. 4, pp. 11–18, 2023. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2666603022000252
[39] S. Acharya, U. Rawat, and R. Bhatnagar, "A computationally inexpensive method based on transfer learning for mobile malware detection," in Proceedings of Fourth International Conference on Computer and Communication Technologies: IC3T 2022. Springer, 2023, pp. 263– 274.
[40] B. Prima and M. Bouhorma, "Using transfer learning for malware classification," The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences, vol. 44, pp. 343–349, 2020.
[41] Z. Zhao, S. Yang, and D. Zhao, "A new framework for visual classification of multi-channel malware based on transfer learning," Applied Sciences, vol. 13, no. 4, 2023. [Online]. Available: https://www.mdpi.com/2076-3417/13/4/2484
[42] P. Panda, O. K. CU, S. Marappan, S. Ma, and D. Veesani Nandi, "Transfer learning for image-based malware detection for iot," Sensors, vol. 23, no. 6, p. 3253, 2023.
[43] M. Tasyurek and R. S. Arslan, "Rt-droid: a novel approach for real-time android application analysis with transfer learning-based cnn models," Journal of Real-Time Image Processing, vol. 20, no. 3, pp. 1–17, 2023.
[44] Z. He, A. Rezaei, H. Homayoun, and H. Sayadi, "Deep neural network and transfer learning for accurate hardware-based zero-day malware detection," in Proceedings of the Great Lakes Symposium on VLSI 2022, 2022, pp. 27–32.
[45] M. V. Ngo, T. Truong-Huu, D. Rabadi, J. Y. Loo, and S. G. Teo, "Fast and efficient malware detection with joint static and dynamic features through transfer learning," in International Conference on Applied Cryptography and Network Security. Springer, 2023, pp. 503–531.
[46] U. Bhatt, A. Xiang, S. Sharma, A. Weller, A. Taly, Y. Jia, J. Ghosh, R. Puri, J. M. Moura, and P. Eckersley, "Explainable machine learning in deployment," in Proceedings of the 2020 conference on fairness, accountability, and transparency, 2020, pp. 648–657.
[47] M. Kinkead, S. Millar, N. McLaughlin, and P. O'Kane, "Towards explainable cnns for android malware detection," Procedia Computer Science, vol. 184, pp. 959–965, 2021.
[48] M. M. Alani and A. I. Awad, "Paired: An explainable lightweight android malware detection system," IEEE Access, vol. 10, pp. 73214– 73228, 2022.
[49] Y. Liu, C. Tantithamthavorn, L. Li, and Y. Liu, "Explainable ai for android malware detection: Towards understanding why the models perform so well?" in 2022 IEEE 33rd International Symposium on Software Reliability Engineering (ISSRE). IEEE, 2022, pp. 169–180.
[50] G. ladarola, F. Mercaldo1, F. Martinelli, and A. Santone, "Assessing deep learning predictions in image-based malware detection with activation maps," in Security and Trust Management: 18th International Workshop, STM 2022, Copenhagen, Denmark, September 29, 2022, Proceedings, vol. 13867. Springer Nature, 2023, p. 104.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)