DOI:

Journal of Computers and Intelligent Systems

Vol. 3, No. 1, 2025, pages 49 - 57

Journal Homepage:

https://journals.iub.edu.pk/index.php/JCIS/

Performance of Deep Learning in Malware Classification

Humza Rana[1], Fatima Yousaf [2]

[1] Bahauddin Zakariya University, Multan, Pakistan

[2] Bahauddin Zakariya University, Multan, Pakistan

ARTICLE INFO

Article History:

Received: September24, 2024
Revised: March 22, 2025
Accepted: March 22, 2025
Available Online: March 23, 2025

Keywords:

Deep Learning
Malware Classification
Artificial Intelligence
Neural Networks

Classification Codes:

Funding:

This research received no specific grant from any funding agency in the public or not-for-profit sector.

ABSTRACT

The malware program is designed to harm the user's data and information. With the new advancements in technology, all the business systems now get through a network. Large-scale businesses are also now in online systems. The security of these systems is essential. The malware programmer developed an advanced type of code that breaks the user security, user information, and money. The malware is of different types. The deep learning is used to classify the modern type of malware. In this survey, the deep learning models that have been used in classifying the malware are studied. Their model performance, their datasets, and preprocessing are discussed in this paper. After an overview of the deep learning model in malware classification with their preprocessing and datasets, we discuss further research direction, to improve the security.

Corresponding Author's Email: Humza.Rana99@gmail.com

Citation:

1. Introduction

Malware is a malicious activity that destroys the functioning of the computer system. The malicious programs are in different categories each one different from one another [1]. A rapid increase in the use and transfer of information over the network around the globe may increase the risk of threats and theft of data. Malware in different forms may enter the user system without the user's knowledge the malware developers break the security and gain access to the most important data [2]. The malware developer uses different ideas to write harmful code that changes from moment to moment and cannot be captured easily. The old malware detector methods are now getting slowed. The signature base method to determine the malware is its limit because the caught the known malware information which is stored in its database. However, this method is unaware of new types of malware. The heuristic type method for determining the unknown malicious types contains a high

FPR [3]. The static and dynamic analysis also becomes useless because of the modern type of malware changes in behavior. This situation takes researchers towards artificial intelligence which provides accurate and in-time performance [4]. Different types of deep learning models were proposed for classifying the malware. In this paper, the model performance in classification is highlighted with their use of datasets.

A. Contribution

1. A brief study of all types of deep learning models for classifying the malware includes their metrics performance and classification efficiency.
2. A detailed study of the datasets used in model training for malware classification. Their performance comparison includes the dataset nature APIs, Opcodes, Images datasets, and different type datasets, etc.
3. A list of contributions in malware classification by the researchers. Highlight the contribution of the researcher in malware classification.
4. Compare the performance of different deep learning models in classifying malware with their training and testing accuracy.
5. Overview of feature selections used in existing deep learning models for malware classification.
6. Highlight the limitations of the deep learning models in malware classification. Include their covered families of malware.

2. Related Work

Malani et al. 2022 [5] implement a CNN, GRU, and RNN model to detect the malware. The Meraz 18, IIT Bhilai provides the dataset. It uses 55 features of the dataset. It contains two classes malicious and non-malicious. After the training by the deep learning models, the CNN 98.02% accuracy performance was achieved rather than other different networks. Liu et al. 2019 [6] implement different neural network models to detect the malware. It includes the BLSTM, GRU, BGRU, and LSTM on the malware dataset. The dataset contains malicious and non-malicious files. The experiment shows the BLSTM gives 97.85% excellent performance.

Venkata et al. 2022 [7] proposed a CNN model for detecting the malware. The image type dataset used in the experiment contains malicious and non-malicious data. After the experiment, a 95% percent accuracy performance is given by the model. The model accuracy needs to be improved the enhance the malicious classes. Schofield et al. [8] proposed CNN for malicious classification. The APIs call dataset to use with 8 different types of malicious family. The experiment shows 98.17% accuracy performance by the model. The proposed results compare with different ML performances which states the CNN model achieves better results than other algorithms. Kareem et al. 2021 [9] proposed a CNN algorithm using the PSO to classify malicious activity in an Android environment. It also uses the PCA as a feature extractor from data. The android-based dataset was collected from the Kaggle. The experiment shows 93.7% accuracy performance by the model. The model is implemented on two class dataset malicious and non-malicious.

Iqbal et al. 2022 [2] proposed LSTM to predict the malware. The PE dataset contains 1000 features with malicious and benign uses. After an experiment, the proposed model gives 99.6% accuracy performance in two classes of malicious activity. Zhangjie et al. 2021 [10] propose an LSTM model for classifying the malware using the transfer learning mechanism. The APK dataset generated for an experiment contains two classes of data malicious and non-malicious. After an experiment, the proposed model has 99.9% classification performance. Catak et al. 2020 [11] propose an LSTM algorithm for classifying the malware using Windows API calls. The experiment from the LSTM algorithm shows 98.5% accuracy performance in eight class malicious families.

Gupta et al. 2022 [12] proposed an ANN model for classifying malicious activity. The Microsoft Challenged dataset was used in the experiment. The dataset contains the 10 malicious families. The experiment by the

proposed model on the dataset achieved 90.17% accuracy performance. Shamr et al. [13] proposed an ANN-GWO model to detect the intrusion. The MIT Darpa 1998 dataset contains the four types of malicious families used in the experiment. The experiment shows a 98.26% accuracy performance for detecting intrusion. Jamal et al. 2022 [14] propose an ANN model for classifying the malware in IoT networks. The ToN_IoT dataset was used in the experiment. It contains ten malicious families. The experiment by the proposed model on the dataset shows a 98.17% classification performance in eight malicious families. The comparison with different ML models including KNN & NB shows that the proposed ANN model achieves the highest accuracy performance.

Almahmoud et al. 2021 [15] proposed an RNN model for classifying the malware. The dataset contains 2,830 malicious and non-malicious which are Android package kit files. The experiment of the proposed RNN model gives a 98.5% accuracy performance. Comparing the performance of the proposed model with the old ML model shows that RNN performance is better than old methods.

Table 1. Deep Learning Model Performance with Datasets in Malware Classification

No	Authors	DL Models	Datasets	Accuracy
1	Lin [16]	CNN Model	Microsoft Challenge Dataset	0.98%
2	Altunay [17]	CNN Model	CSE-CIC-IDS2018	0.988%
3	Cahyani [18]	ANN Model	Bitcoin Heist Data	0.97%
4	Kinkead [19]	CNN Model	Drebin benchmark dataset	0.98%
5	Cao [20]	CNN & GRU	UNSW_NB15, NSL-KDD, CIC-IDS2017	0.996%
6	Joshi [21]	ANN Model	CTU-13 dataset.	0.994%
7	Malgwi [22]	ANN Model	CICIDS2017	0.999%
8	Pinheiro [23]	DL Model	Dataset-I, Dataset-II	0.999%
9	Mai [24]	Dec-DCNN	BIG 2015 dataset	0.98%
10	Qiu [25]	MalShuffleNet	Malimg dataset	0.99%

Table 1 shows the different deep learning models with their use of datasets for training the model in classifying malicious activity. It contains accuracy performance by the models in classifying the malware activity. It contains big datasets, and small datasets, of different types including APIs, malicious images, opcodes, and normal malicious datasets.

Table 2 Deep Learning Model Performance According to Feature Selection in Malware Classification

No	Authors	Feature Selection	Accuracy
1	Alalhareth [26]	LRGU-MIFS	0.934%
2	Pashiri [27]	SCA-Algorithm	0.986%
3	Fu [10]	RF-Algorithm	0.999%
4	Alomari [28]	Correlation-Method	0.991%
5	Almotairi [29]	COA, VVS-PSO	0.986%
6	Smitha [30]	GA-Algorithm	0.985%

Table 2 shows different types of deep learning models that perform in the classification of malicious attacks using feature selection. Different types of feature selection techniques are used in deep learning models to achieve performance accuracy.

Table 3 Deep Learning Model Performance in Malware Families in Classification

No	Authors	Families	Accuracy
1	Viboonsang [31]	5-class	0.995%
2	Ma [32]	5-class	0.999%

3	Wei [33]	8-class	0.988%
4	Alzahrani [34]	5-class	0.982%
5	Awan [35]	25-class	0.971%
6	Alnajim [36]	25-class	0.981%
7	Aslan [37]	25-class	0.977%
8	Jamal [14]	9-class	0.971%

Table 3 shows the different deep learning models' performance in case of multiple classes in the malicious. It presents the different model's accuracy performance in multiclass malware classification datasets.

Table 4 Datasets Types Used in Malware Classification By Deep Learning

No	Authors	Datasets	Type	Accuracy
1	Smitha [30]	Andriod-Malware	Andriod-apps	0.938%
2	Catak [38]	Windows APIs	APIs Calls	0.985%
3	Kalyan [7]	Binaries	Images Data	0.951%
4	Iqbal [2]	Top-PE Imports	PE & DLLs	0.996%
5	Aslan [37]	Microsoft Big & Malimg	Images Type	0.978%
6	Almahmoud [15]	Andriod Malware Dataset	APKs Files	0.981%
7	KinKead [19]	Derbin Dataset	Apps	0.981%
8	Mayhem [39]	KDD Cup 1999 Dataset	Intrusion	0.955%
9	Maulana [40]	Malware Dataset	PE Files	0.986%
10	Mitsuhashi [41]	Malimg	Images	0.997%

Table 4 presents the different types of datasets used by deep learning models with their respective performance of malware classification. The dataset contains different types and gives different accuracy performances.

Table 5 Existing Contributions in Malware Classification By Deep Learning

No	Authors	Contribution
1	Ayub [42]	Proposed ANN model for detecting intrusion. The ransomware sample used belongs to 18 families with 99.7% performance achieved.
2	Pawlicki [43]	Proposed ANN model for detecting intrusion. Two datasets were used in the experiment which is multiclass 99,9% accuracy performance achieved in 13 families.
3	Kumar [44]	Proposed CNN-BiLSTM for detecting the malware. It uses PE headers file in experiment 99.2% accuracy performance with 8 malware class.
4	Mahendru [45]	Proposed an ANN model using the SOM method to detect the malware. The Android malware app used in the experiment had 98.7% accuracy achieved to unknown classes.
5	Imtiaz [46]	Proposed deep ANN model for detecting the malware. The two class and multiclass datasets are used in the experiment. It achieves 0.935% and 0.90% accuracy performance.

Table 5 shows the different contributions in malware classification by deep learning models. It contains the number of classes covered by the deep learning model in classifying the malware attacks which achieves up to 99% accuracy performance.

A. Limitation

In the above different authors' works presented malware classification by deep learning with efficient performance. However, there is a need to handle the proper class imbalance issue in the dataset. The improved feature extraction and selection technique for refining the data. The multiclass model achieves accuracy up to 99% but the time complexity and calculation need to be reduced to overcome the computational resources. Different hybrid models are proposed for malware classification but the high computation is required in these models the hyperparameters need to be implemented to reduce the computation power. The different types of techniques include the PSO and ACO to be used in the model to increase the performance. Large datasets with multiclass used in training the hybrid model are needed to evaluate the model performance in large scenarios for classifying the malware.

3. Methodology

This section contains the method for collecting all existing deep learning model performance. The main purpose is to highlight deep learning models' performance in malware classification. It contains papers from different repositories including IEEE, Google Scholar, etc. It mainly focuses on malware classification performance, datasets, and feature selection and covers the number of malicious families by deep learning approach. The papers about 60-70 have been studied and categorized only the deep learning models' performance including the CNN, LSTM, and other different models. It extracts the model performance with datasets with mentions the limitations of the research and future direction for further improving the cybersecurity research. The quantitative approach was used in this survey to compare the different deep learning models in terms of accuracy.

.

4. Results & Discussion

This section describes all existing research done in malware classification using deep learning techniques. The deep learning model CNN performance achieves best in the multiclass approach. The different types of datasets nature with used in feature selection are mentioned in it with their performance. It presents the datasets, deep learning model, feature selection, authors contribution, and covered malware families. The malware classification is accurate and efficient using a deep learning model.

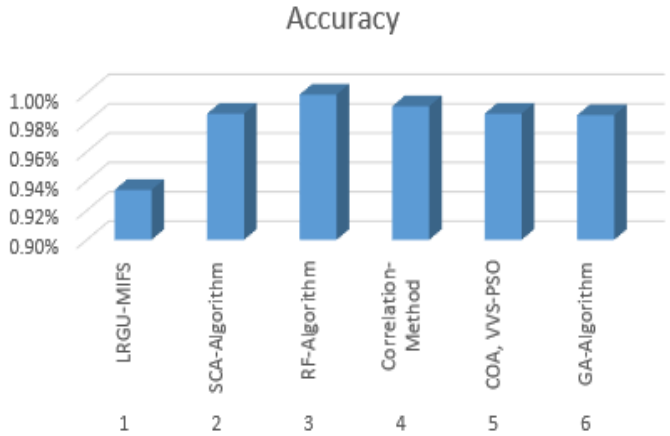

Figure 1 Feature Selection Performance in Malware Classification

Figure 1 shows the different types of feature selection performance in malware classification. The above graph shows the comparison of feature selection used in deep learning model for classify malware.

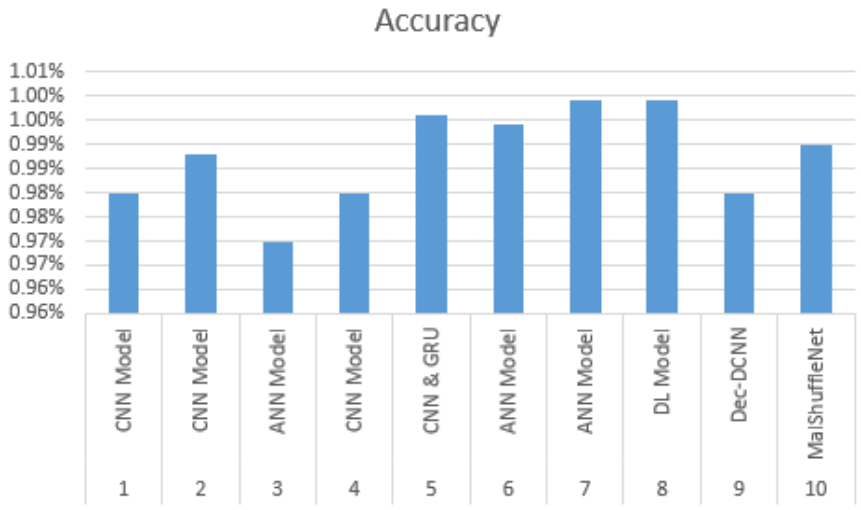

Figure 2 Deep Learning Model Performance

Figure 2 represents the different types of deep learning models including the CNN, LSTM, & GRU, etc. It presents the accuracy performance of the proposed approach till use in classifying the malware. The deep learning model approximately reaches 100% performance in malware classification.

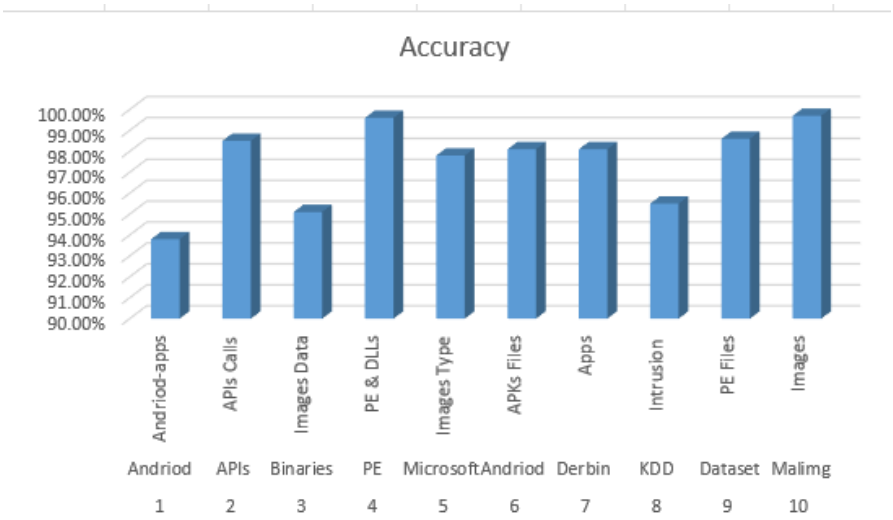

Figure 3 Deep Learning Model Performance in Classification with Different Datasets

Figure 3 shows the different dataset types and deep learning model performance in these datasets. It performs up to 99% on all datasets. It contains the APIs, images, PE files, and different malware binaries. The datasets may be in different classes of malware. It contains the binary and multiclass datasets.

5. Conclusion

In detail overview of existing work in classification of malicious using deep learning. The CNN model's performance in multiclass is best. However the time performance of deep learning CNN needs to be improved in multiclass. The

PSO and ACO algorithms need to be implemented to determine the performance. The hybrid deep learning model needs to be implemented in malware classification with efficient time performance and class balancing issues in the dataset.

6. References

1. D. Dang, F. Di Troia, and C. R. Mar, "Malware Classification Using Long Short-Term Memory Models," pp. 1–16, 2021.

2. S. Iqbal, A. Ullah, S. Adlan, and A. R. Soobhany, "Malware Prediction Using LSTM Networks," *Lect. Notes Networks Syst.*, vol. 350, pp. 583–604, 2022, doi: 10.1007/978-981-16-7618-5_51.

3. R. Tahir, "A Study on Malware and Malware Detection Techniques," *Int. J. Educ. Manag. Eng.*, vol. 8, no. 2, pp. 20–30, 2018, doi: 10.5815/ijeme.2018.02.03.

4. L. Saidia, M. Fisichella, G. Lax, and C. Qian, "Computers & Security Disarming visualization-based approaches in malware detection systems," vol. 126, 2023, doi: 10.1016/j.cose.2022.103062.

5. H. Malani, A. Bhat, S. Palriwala, J. Aditya, and A. Chaturvedi, "A Unique Approach to Malware Detection Using Deep Convolutional Neural Networks," *Proceedings, Int. Conf. Electr. Control Instrum. Eng. ICECIE*, vol. 2022-Novem, 2022, doi: 10.1109/ICECIE55199.2022.10000344.

6. Y. Liu and Y. Wang, "A robust malware detection system using deep learning on API calls," *Proc. 2019 IEEE 3rd Inf. Technol. Networking, Electron. Autom. Control Conf. ITNEC 2019*, no. Itnec, pp. 1456–1460, 2019, doi: 10.1109/ITNEC.2019.8728992.

7. E. Venkata Pawan Kalyan, A. Purushottam Adarsh, S. Sai Likith Reddy, and P. Renjith, "Detection Of Malware Using CNN," *2022 2nd Int. Conf. Comput. Sci. Eng. Appl. ICCSEA 2022*, 2022, doi: 10.1109/ICCSEA54677.2022.9936225.

8. M. Schofield *et al.*, "Convolutional Neural Network for Malware Classification Based on API Call Sequence," pp. 85–98, 2021, doi: 10.5121/csit.2021.110106.

9. K. A. Kareem, E. Sabah, and M. Ali, "Optimized Convolutional Neural Networks based malware detection," vol. 58, pp. 5036–5056, 2021.

10. Z. Fu, Y. Ding, and M. Godfrey, "An LSTM-Based Malware Detection Using Transfering Learning," *J. Cyber Secur.*, vol. 3, no. 1, pp. 11–28, 2021, doi: 10.32604/jcs.2021.016632.

11. F. O. Catak, A. F. Yazi, O. Elezaj, and J. Ahmed, "Deep learning based Sequential model for malware analysis using Windows exe API Calls," *PeerJ Comput. Sci.*, vol. 6, pp. 1–23, 2020, doi: 10.7717/PEERJ-CS.285.

12. K. Gupta, N. Jiwani, M. H. U. Sharif, R. Datta, and N. Afreen, "A Neural Network Approach For Malware Classification," *3rd IEEE 2022 Int. Conf. Comput. Commun. Intell. Syst. ICCCIS 2022*, pp. 681–684, 2022, doi: 10.1109/ICCCIS56430.2022.10037653.

13. A. Sharma and U. Tyagi, "A Hybrid Approach of ANN-GWO Technique for Intrusion Detection," 2021.

14. A. Jamal, M. Faisal Hayat, and M. Nasir, "Malware Detection and Classification in IoT Network using ANN," *Mehran Univ. Res. J. Eng. Technol.*, vol. 41, no. 1, pp. 80–91, 2022, doi: 10.22581/muet1982.2201.08.

15. M. Almahmoud, D. Alzu'bi, and Q. Yaseen, "Redroiddet: Android malware detection based on recurrent neural network," *Procedia Comput. Sci.*, vol. 184, pp. 841–846, 2021, doi: 10.1016/j.procs.2021.03.105.

16. W. C. Lin and Y. R. Yeh, "Efficient Malware Classification by Binary Sequences with One-Dimensional Convolutional Neural Networks," *Mathematics*, vol. 10, no. 4, pp. 1–14, 2022, doi: 10.3390/math10040608.

17. H. C. ALTUNAY and Z. ALBAYRAK, “Network Intrusion Detection Approach Based on Convolutional Neural Network,” *Eur. J. Sci. Technol.*, no. 26, pp. 22–29, 2021, doi: 10.31590/ejosat.954966.

18. N. Dwi, W. Cahyani, and H. H. Nuha, “Ransomware Detection on Bitcoin Transactions Using Artificial Neural Network Methods,” pp. 669–673, 2021.

19. M. Kinkead, S. Millar, N. McLaughlin, and P. O’Kane, “Towards explainable cnns for android malware detection,” *Procedia Comput. Sci.*, vol. 184, no. 2019, pp. 959–965, 2021, doi: 10.1016/j.procs.2021.03.118.

20. B. Cao, C. Li, Y. Song, Y. Qin, and C. Chen, “Network Intrusion Detection Model Based on CNN and GRU,” *Appl. Sci.*, vol. 12, no. 9, 2022, doi: 10.3390/app12094184.

21. C. Joshi, R. Kumar, and V. Bharti, “A Fuzzy Logic based feature engineering approach for Botnet detection using ANN,” *J. King Saud Univ. - Comput. Inf. Sci.*, no. xxxx, 2021, doi: 10.1016/j.jksuci.2021.06.018.

22. Y. M. Malgwi, I. Goni, and B. M. Ahmad, “Artificial Neural Network Model for Intrusion Detection System,” *Mediterr. J. Basic Appl. Sci.*, vol. 06, no. 01, pp. 20–26, 2022, doi: 10.46382/mjbas.2022.6103.

23. A. Pinhero *et al.*, “Malware detection employed by visualization and deep neural network,” *Comput. Secur.*, vol. 105, p. 102247, 2021, doi: 10.1016/j.cose.2021.102247.

24. J. Mai, C. Cao, F. Shi, and X. Chen, “Malware Variant Detection Based on Decomposed Deep Convolutional Network,” *2021 IEEE 6th Int. Conf. Big Data Anal. ICBDA 2021*, pp. 333–338, 2021, doi: 10.1109/ICBDA51983.2021.9403081.
25. J. Wang, S. Wang, and Y. Wang, “Malware Classification based on a Light-weight Architecture of CNN : MalShuffleNet,” pp. 2–5, 2022.

26. M. Alalhareth and S. Hong, “An Improved Mutual Information Feature Selection Technique,” 2023.

27. R. Talaei, P. Yaser, and R. Mohsen, “Spam detection through feature selection using artificial neural network and sine – cosine algorithm,” *Math. Sci.*, vol. 14, no. 3, pp. 193–199, 2020, doi: 10.1007/s40096-020-00327-8.

28. N. S. Sani, M. I. Esa, and B. A. Musawi, “SS symmetry Feature Selection,” *Symmetry (Basel).*, vol. 15, no. 123, pp. 1–21, 2023.

29. S. Almotairi, M. A. R. Khan, O. Alharbi, Z. Alzaid, Y. M. Hausawi, and J. Almutairi, *Detection of Android Malware Using Deep Learning Ensemble With Cheetah-Optimized Feature Selection*, vol. 41, no. 5. 2024. doi: 10.17654/0974165824026.

30. M. Sonia, C. B. N. Lakshmi, S. J. Hussain, M. L. Swarupa, and N. Rajeswaran, “Android Malware Detection Using Genetic Algorithm Based Optimized Feature Selection and Machine Learning,” *Lect. Notes Electr. Eng.*, vol. 1106, no. 12, pp. 207–215, 2024, doi: 10.1007/978-981-99-7954-7_19.

31. P. Viboonsang and S. Kosolsombat, “Network Intrusion Detection System Using Machine Learning and Deep Learning,” *Int. Conf. Cybern. Innov. ICCI 2024*, no. February, 2024, doi: 10.1109/ICCI60780.2024.10532673.

32. W. Ma, C. Gou, and Y. Hou, “Research on Adaptive 1DCNN Network Intrusion Detection Technology Based on BSGM Mixed Sampling,” *Sensors*, vol. 23, no. 13, 2023, doi: 10.3390/s23136206.

33. L. Wei, F. Xu, N. Zhang, W. Yan, and C. Chai, “Dynamic malicious code detection technology based on deep learning,” *ICOCN 2022 - 20th Int. Conf. Opt. Commun. Networks*, pp. 2022–2024, 2022, doi: 10.1109/ICOCN55511.2022.9901158.

34. A. I. A. Alzahrani, M. Ayadi, M. M. Asiri, and A. Al-rasheed, “Detecting the Presence of Malware and Identifying the Type of Cyber Attack Using Deep Learning and VGG-16 Techniques,” pp. 1–20, 2022.

35. M. J. Awan *et al.*, “Image-based malware classification using vgg19 network and spatial convolutional attention,”

Electron., vol. 10, no. 19, 2021, doi: 10.3390/electronics10192444.

36. A. M. Alnajim, S. Habib, M. Islam, R. Albelaihi, and A. Alabdulatif, "Mitigating the Risks of Malware Attacks with Deep Learning Techniques," *Electron.*, vol. 12, no. 14, 2023, doi: 10.3390/electronics12143166.

37. O. Aslan and A. A. Yilmaz, "A New Malware Classification Framework Based on Deep Learning Algorithms," *IEEE Access*, vol. 9, pp. 87936–87951, 2021, doi: 10.1109/ACCESS.2021.3089586.

38. F. O. Catak, A. F. Yazi, O. Elezaj, and J. Ahmed, "Deep learning based Sequential model for malware analysis using Windows exe API Calls," *PeerJ Comput. Sci.*, vol. 6, pp. 1–23, 2020, doi: 10.7717/PEERJ-CS.285.

39. M. Maithem and G. A. Al-Sultany, "Network intrusion detection system using deep neural networks," *J. Phys. Conf. Ser.*, vol. 1804, no. 1, 2021, doi: 10.1088/1742-6596/1804/1/012138.

40. R. J. Maulana and G. P. Kusuma, "Malware classification based on system call sequences using deep learning," *Adv. Sci. Technol. Eng. Syst.*, vol. 5, no. 4, pp. 207–216, 2020, doi: 10.25046/aj050426.

41. R. Mitsuhashi and T. Shinagawa, "High-Accuracy Malware Classification with a Malware-Optimized Deep Learning Model," no. August, 2020, [Online]. Available: http://arxiv.org/abs/2004.05258.

42. A. Continella and A. Siraj, "An I / O Request Packet (IRP) Driven Effective Ransomware Detection Scheme using Artificial Neural Network," pp. 319–324, 2020, doi: 10.1109/IRI49571.2020.00053.

43. M. Pawlicki and M. Choras, "Neurocomputing Intrusion detection approach based on optimised artificial neural network," vol. 452, pp. 705–715, 2021, doi: 10.1016/j.neucom.2020.07.138.

44. A. I. Journal and M. Kumar, "Scalable Malware Detection System Using Distributed Deep Learning Deep Learning," *Cybern. Syst.*, vol. 0, no. 0, pp. 1–29, 2022, doi: 10.1080/01969722.2022.2068226.

45. A. Mahindru and A. L. Sangal, *SOMDROID : android malware detection by artificial neural network trained using unsupervised learning*, vol. 15, no. 1. Springer Berlin Heidelberg, 2022. doi: 10.1007/s12065-020-00518-1.

46. S. I. Imtiaz, S. ur Rehman, A. R. Javed, Z. Jalil, X. Liu, and W. S. Alnumay, "DeepAMD: Detection and identification of Android malware using high-efficient Deep Artificial Neural Network," *Futur. Gener. Comput. Syst.*, vol. 115, pp. 844–856, 2021, doi: 10.1016/j.future.2020.10.008.