International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Recent Advances in Image based Malware Classification through the Lens of Deep Learning - A Systematic Literature Review

Kajal Jaisinghani[1], Dr. Santosh Singh[2]

Submitted:24/04/2023 **Revised**:23/06/2023 **Accepted**:04/07/2023

Abstract: Image-based malware classification using deep learning (DL) models has shown as a promising approach for detecting and classifying malware on various platforms such as Windows, Android, and IoT devices. In this systematic literature review, we explore recent advancements in image-based malware classification through the lens of deep learning. We reviewed 30 research papers published between 2019 and 2023, which employed different DL models such as ResNet, CNN, Inception-v1, LSTM, VGG-16, DenseNet, Inception-v3, and EfficientNetB0 CNN for image-based malware classification. Our review found that transfer learning is a popular technique for training DL models for malware detection. In order to improve the performance of deep learning models and increase the size of the training datasets, data augmentation techniques were also used. Visualization-based techniques like class activation mapping and saliency mapping were used to interpret the results and identify the regions of an image responsible for malware detection. The review also highlighted some limitations of existing research, including the limited availability of large-scale annotated datasets for training deep learning models, high false positive and false negative rates in object detection, limited generalizability of deep learning models to new environments and scenarios, and privacy concerns with using image-based malware detection, especially when it comes to collecting and using personal data. Future research directions include developing more robust deep learning models that are less sensitive to changes in the data distribution and incorporating human expertise to improve model interpretability. Furthermore, the creation of larger, diverse, and representative datasets for training and testing deep learning models is essential to ensure that the models can perform well in real-world settings. In conclusion, our review suggests that deep learning-based techniques have great potential for detecting and classifying malware through image-based approaches. Further research in this area can lead to more effective malware detection and improved security for various devices.

Keywords: *Image-based malware classification, Deep learning, Malware detection, Transfer learning, Visualization-based malware detection, Malware classification*

1. Introduction

The threat of malware attacks has been on the rise in recent years, with ransomware attacks being one of the most significant contributors. According to Fedor [1], there were 623.3 million detected ransomware attacks in 2021, and 76% of organizations experienced at least one attack in the same year. Negligence from managers or administrators accounted for 43% of the attacks, while user actions caused 42%. The impact of these attacks has been significant, with hackers successfully encrypting data in 65% of the attacks, resulting in an 82% rise in ransomware incidents. The need for organizations to adopt robust security measures to prevent and detect advanced threats has become more critical than ever.

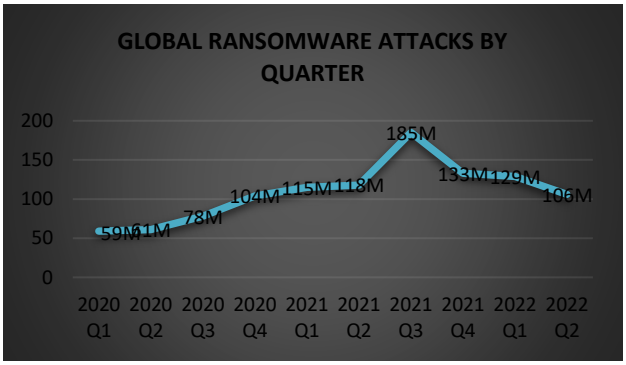


Fig 1: Global ransomware attacks by quarter [1]

The SolarWinds attack, carried out by a state-sponsored actor, highlighted the need for proactive and multi-layered security measures to prevent and detect advanced threats. The attack emphasized the importance of implementing regular software updates, network segmentation, and the use of threat intelligence and incident response solutions to mitigate the risk of similar attacks in the future [2]. The Ryuk ransomware attack, which emerged in 2019, continues to be a significant threat to organizations across various industries, causing significant financial damage and disruption. To prevent and mitigate the impact of such attacks, organizations must have robust backup and disaster recovery solutions in place, as well as implement strong security measures such as network segmentation, security

[1]*Research Scholar, Department of Information Technology, University of Mumbai, Maharashtra State*
[2]*HOD, Thakur College Autonomous, Kandevali, Mumbai, Maharashtra State*

information and event management, and endpoint detection and response solutions [3].

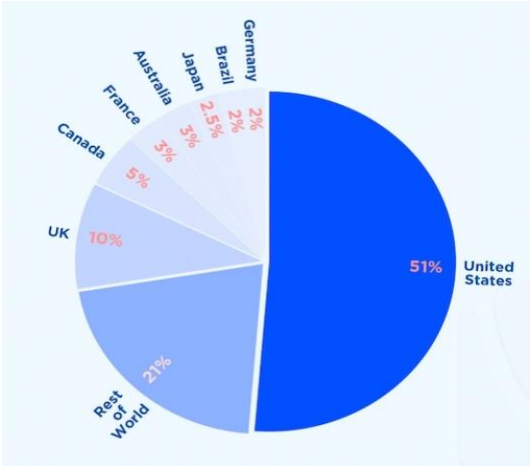


Fig. 2: Countries most attacked by Malware [1]

The recent malware attacks on organizations and government agencies have had a significant impact on their operations and data security. As an example, in 2021, a Chinese hacker group launched an attack on Microsoft Exchange Server vulnerabilities, impacting a large number of organizations worldwide, numbering in the tens of thousands [4]. Similarly, the Darkside ransomware attack on Colonial Pipeline in May 2022 resulted in the shutdown of the largest fuel pipeline in the United States and caused widespread fuel shortages in the Southeast [5]. New strains of malware, such as Babuk ransomware and the Exim vulnerability exploit, have emerged in 2023, posing significant risks to organizations worldwide [6] [7].

To mitigate the risks posed by these types of attacks, organizations can implement software patches and updates promptly, adopt multi-factor authentication, and implement backup and disaster recovery plans. Security awareness training for employees can also help to reduce the risk of successful attacks by educating them on best practices for avoiding phishing and other social engineering tactics used by attackers [8].

The significance of malware detection has become more apparent with the increasing sophistication and prevalence of malware attacks. Malware detection involves identifying malicious software and mitigating its potential harm through various techniques, ranging from traditional signature-based methods to advanced methods based on machine learning. Liu *et al.* [13] explored that deep learning (DL) outperforms traditional signature-based methods and other machine learning-based techniques in detecting Android malware. This has paved the way for deep learning to become a promising approach in the field of malware detection.

The use of DL in malware detection is a relatively new field that requires additional research and development. Deep learning-based methods can be susceptible to overfitting, adversarial attacks, and a lack of diverse training data, which can impact their accuracy. Therefore, it is crucial to continually update and enhance the training data and algorithms used in deep learning-based malware detection. Additionally, a multi-layered defense approach that combines deep learning with other methods like static analysis, dynamic analysis, and hybrid analysis can provide a more comprehensive and effective defense against malware attacks.

Image-based malware classification using DL models has shown promising results for detecting and classifying malware [9]. Recent studies have demonstrated that deep learning models can effectively classify malware images based on their visual features, surpassing traditional signature-based and behavioral-based approaches [10] [11]. Deep neural network models achieved higher accuracy on the Malimg dataset [12]. In addition, deep learning models have advantages over traditional methods as they can learn features automatically and can detect zero-day attacks.

Therefore, this article aims to present a thorough comprehension of recent advances in image-based malware classification through the lens of deep learning, as well as the challenges and opportunities in this field. This paper discusses various studies and researches that focus on image-based malware classification using DL techniques. The major aspirations of this study are:

- To provide an overview of recent advances in image-based malware classification using DL techniques.
- To critically review image-based malware classification techniques for windows, Android and IoT environments.
- To analyse the effectiveness of different DL models for image-based malware classification, and to identify their potential limitations.
- To discuss how different factors, such as the size of the dataset, imbalanced class distribution, and feature engineering techniques, influence the effectiveness of image-based classification methods for identifying malware.
- To propose potential avenues for future research in the area of detecting malware through analyzing images.

2. Related Work

There has been a growing interest in using deep learning models for malware classification in recent years. In this section, we summarize the key findings and limitations from several recent studies on this topic.

Liu *et al.* [13] provided a comprehensive overview of the use of DL techniques for detecting Android malware, including a review of different algorithms and their performance. The authors found that deep learning approaches generally outperformed traditional methods in terms of accuracy, but they also noted that there were limitations in terms of the generalizability of the models, the need for large, diverse training datasets, and the limitations of existing algorithms.

Tayyab *et al.* [14] provided an overview of the latest trends in DL based malware detection and highlights the strengths and weaknesses of different approaches. The authors noted that deep learning-based approaches generally had higher accuracy and faster detection times than traditional methods, but they also highlighted limitations such as the need for large training datasets and the difficulty of interpretability of the models.

Catal *et al.* [15] focused on the use of DL for detecting malware in mobile devices and provides a comprehensive overview of different algorithms and their performance. The authors found that deep learning approaches generally outperformed traditional methods, but they also noted limitations such as the need for large, diverse training datasets and the limitations of existing algorithms.

Wang *et al.* [16] provided an overview of the use of DL techniques for detecting Android malware and highlights the advantages and limitations of different algorithms. The authors

found that deep learning approaches generally had higher accuracy and faster detection times than traditional methods, but they also highlighted limitations such as the difficulty of interpretability of the models and the need for large, diverse training datasets.

The use of deep neural networks for Android malware detection and the effectiveness of various algorithms were extensively reviewed by Qiu *et al.* in their study [17]. The authors found that deep neural networks generally outperformed traditional methods in terms of accuracy, but they also noted limitations such as the need for large, diverse training datasets and the limitations of existing algorithms.

Kumars *et al.* [18] provided a comprehensive overview of the use of various intelligent techniques, including deep learning, for detecting Android malware and their performance. The authors found that intelligent techniques generally outperformed traditional methods, but they also noted limitations such as the need for large, diverse training datasets and the limitations of existing algorithms.

Despite of having many reviews related to malware detection in recent years, it is important to note that these studies do not focus specifically on image-based malware classification. The existing reviews have also ignored to review different platforms such as Windows, Android, and IoT-based malware detection. The existing literature did not cover the most recent advances in a field, and did not follow a rigorous, predetermined methodology for searching and evaluating articles related to malware detection.

3. Review Methodology

The Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) flow diagram is a useful tool for documenting the screening process in Systematic Literature Reviews (SLRs). It is used to visually represent the flow of articles from the initial identification to the final inclusion or exclusion in the review.

The typical flow of a PRISMA flow chart in an SLR methodology is as follows:

1. Identification: In this step, the SLR team identifies the potential articles by searching various databases and sources, such as scientific journals, conference proceedings, and online repositories.
2. Screening: The identified articles are screened based on their title, abstract, and keywords to determine their eligibility and relevance to the research question. Articles that do not meet the eligibility criteria are excluded at this stage.
3. Full-text review: The full text of the eligible articles is obtained and reviewed in detail to confirm their eligibility.
4. Eligible articles: The articles that meet the eligibility criteria and are relevant to the research question are included in the final analysis.
5. Excluded articles: The articles that were excluded at the screening stage or the full-text review stage are documented in the flow chart along with the reason for exclusion.

4. Research Questions

1. What are the recent advances in image-based malware classification using DL in Windows, Android and IoT environments?
2. What are the current challenges for image-based malware classification, utilising deep learning?
3. How accurate are image-based classification techniques for classifying different types of malware families and variants, and how do they compare with other malware detection approaches?

5. Article Selection Strategy

Article segregation strategy was employed to select relevant publications for answering the research questions. A systematic search process was used, including keywords such as "image-based malware classification" and "deep learning," to identify a shortlist of articles that comprehensively addressed the concerns. The search was limited to articles published from 2019 to 2023, resulting in over 96 research papers. After a thorough examination of the title, abstract, and contents, 30 papers were selected for inclusion in the review.

6. Data Analysis And Synthesis

Deep learning models for image-based malware classification is an effective approach to classifying malware from images by analyzing their visual features [19]. The process typically involves collecting a large dataset of image malware samples, preprocessing the data, training a deep learning model such as a CNN, evaluating the model's performance, and deploying it in a real-world environment [20]. One of the main benefits of this approach is its ability to detect previously unseen or unknown malware, as the model can learn to recognize patterns and features that are not explicitly programmed into it [21].

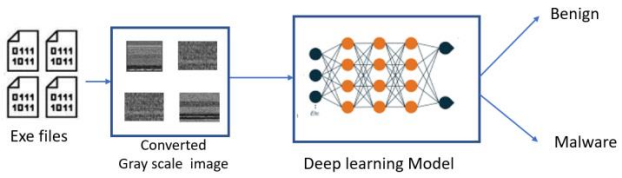


Fig. 3. Image-based malware classification using deep learning

In this section, we will critically review recent research efforts on image-based malware classification using various deep learning models. Table 1, 2, 3 summarizes image-based malware classification on Windows operating systems, Android platform, and Internet of Things (IoT) environments.

Table 1: Windows

Author	Model used	Dataset Used	Accuracy	Limitation
Bhodia et al. 2019 [22]	ResNet	Malimg and Malicia dataset and windows dataset	96.5%	Robustness
Marastoni et al. 2021 [23]	CNN, LSTM	Malimg and Microsoft 2015 datasets	98.5%	Poor dataset size
Khan et al., 2019 [24]	1. ResNet 2. Inception-v1	Microsoft 2015	1. 88.36% 2. 74.5%	Limited dataset used
Alzahrani et al. 2022 [25]	VGG-16	Malicia dataset	99%	New malware types and dataset quality affects accuracy
Darem et al. 2021 [26]	CNN	Malimg malware dataset	99.12%	Based on Gray image only
Hemalatha et al. 2021 [27]	DenseNet	1. Malimg 2. Microsoft 2015 3. MaleVis 4. Malicia	1. 98.2% 2. 98.46% 3. 98.2% 4. 89.48%	Need to focus false negatives to achieve an optimal solution
Obaidat et al. 2022 [28]	CNN	Real time dataset	98.4%	Java malware detection and limited dataset
Rizvi et al. 2022 [29]	FANN	Real time dataset	98.09%	Limited to malicious Portable Executable Files only
Huang et al. 2021 [30]	VGG16	Real time dataset	94.70%	Poor performance on older malwares and QQ password stealer trojans.
Deng et al. 2023 [31]	Malware Classification method based on Three-channel Visualization and Deep learning (MCTVD)	Microsoft dataset	99.44%	Limited to small and uniform malware images

Table 2: Android

Author	Model used	Dataset Used	Accuracy	Limitation
Bakour, & Ünver, 2021 [32]	DeepVisDroid (1D-CNN)	Realtime datasets	98%	Some techniques of code camouflage and obfuscation were not detected.
Bakour, & Ünver, 2020 [33]	ResNet and Inception-v3	5 grayscale image datasets with 4850 samples each were created from Android malware sample sources.	98.2%	Hindered by code obfuscation and manipulation, and may not detect certain injection attacks.
Yadav et al. 2022 [34]	EfficientNetB0 CNN	ImageNet database	100%	Disconnected stages may lack adversarial resiliency testing.
Daoudi et al. 2021 [35]	1-D CNN	Malware and benign apps from AndroZoo	97%	Selective Compatibility
Sihag et al. 2022 [36]	CNN	Real collected dataset	98.44%	Not focused on low-level technical details such as system calls and network statistics.
Geremias et al. 2022 [37]	CNN	CICMalDroid dataset	98.7%	addressed limited Android malwares
Zhu et al. 2023 [38]	Multi-Head Squeeze-and-Excitation Residual Network (MSerNet)	VirusShare &	96.48%	Potential dataset bias affecting performance
Şahin et al. 2023 [39]	Deep neural networks, 1D CNN, and 2D CNN	Malgenome and Drebin datasets	96.1%	Not able to detect new and unknown types of malwares
Ren et al. 2020 [40]	1. DexCNN (Dexterous Convolutional Neural Network) 2, DexCRNN (Dexterous Convolutional Recurrent Neural Network)	Realtime dataset	1. 93.4% 2. 95.8%	Limit on the file size of the input samples
Vasan et al. 2020 [41]	Image based Malware Classification using Fine-tuned Convolutional Neural Network Architecture (IMCFN)	IoT android mobile dataset	97.35%	Dependency on colour information, being limited to image-based detection, specific datasets, and static analysis

Table 3: IoT

Author	Model used	Dataset Used	Accuracy	Limitation
Namanya et al., 2020 [42]	CNN	Real time dataset	91%	
Nguyen et al. 2020 [43]	CNN	ELF files dataset	98.7%	Poor runtime information.
Dib et al. 2021 [44]	CNN and LSTM	IoTPOT	99.78%	Obfuscated malware not considered.
Chaganti, Ravi, & Pham, 2022 [45]	Bidirectional-Gated Recurrent Unit-Convolutional Neural Network (Bi-GRU-CNN) and RNN	IoT malware dataset (obtained from multiple sources, including the IoTPOT honeypot and VirusTotal and VirusShare)	99%	Unable to classify latest malware types like xorddos, pnscan.
Ghahramani et al. 2022 [46]	CNN	Real time collected dataset (set of 10,000 emails)	45.1%	Ignored to investigate alternative approaches to multi-objective optimization learning, label

				flipping, or vulnerability identification
Li et al. 2021 [47]	CNN	Real time dataset	95.31%	Limited dataset
Anand et al. 2021 [48]	CNN-DMA (Detect Malware Attacks)	Malimg dataset	99%	Dataset bias, scalability challenges, interpretability issues, implementation challenges, and limited focus on other security concerns.
Asam et al. 2022 [49]	iMDA (CNN-based IoT malware detection architecture)	A benchmark IoT dataset.	97.93%	Ignored to test the generalizability of the proposed iMDA on other datasets or real-world scenarios.
Naeem, Alshammari, & Ullah, 2022 [50]	Inception-v3	ImageNet	98.5%	Lack of training with large scale datasets
Wang et al. 2021 [51]	Depthwise Efficient Attention Module (DEAM)	MalImg dataset	98.5%	Lack of Pre processing

Deep learning models used for image based malware classification:

CNN:

Convolutional Neural Networks (CNNs) are a type of deep learning model used primarily for image recognition tasks. They are particularly well-suited for identifying patterns in large datasets of visual information, making them ideal for detecting image-based malwares. The basic architecture of a CNN consists of several layers, each with a specific purpose [26] [47] [36]. When using CNNs for malware classification, the input images are represented as byte-level images, and the CNNs are trained to recognize patterns in the byte-level image data that are indicative of a specific malware family. For this classification problem, Yadav *et al.* [34] presented EfficientNetB0 CNN, a particular CNN design that has been demonstrated to have great performance and computational performance.

Inception-v3:

A CNN model called Inception-v3 has undergone pretraining for the purpose of detecting malware in Android and IoT devices. The model is utilized in this study to identify the most important features of malware present in Android Dalvik Executable File (DEX) images, which are then classified using a SoftMax classifier. Inception-v3 is specifically chosen in a study [50] due to its ability to effectively extract features from complex images, which is particularly useful when dealing with polymorphic and obfuscated malware. The model is fine-tuned to improve its performance in identifying IoT device malware, with a global max-pooling layer applied to further refine the feature extraction process.

RNN:

Recurrent neural networks, or RNNs, are a specific kind of neural network created with the purpose of processing sequential input, such as text or time-series data. Chaganti, Ravi, and Pham [45] utilized RNNs to process byte sequences of the Executable and Linkable Format (ELF) binary files, which represent malware in IoT devices. This enabled them to extract important features for the classification of different malware families.

LSTM:

LSTM, which stands for Long Short-Term Memory, is a type of RNN that is commonly used for natural language processing and time series analysis, but can also be applied to image-based classification tasks, including object detection and image captioning. Recent research has demonstrated that LSTMs can be used for malware detection as well. Dib *et al.* [44] used a multi-level deep learning architecture with LSTM to classify IoT malware families and analyze the sequence of pixel values in images of malware samples. Marastoni *et al.* [23] used LSTM in conjunction with a CNN to classify obfuscated binaries from images, and transfer learning was used to improve classification accuracy. Overall, the use of LSTMs in malware detection has shown promising results in recent research.

ResNet:

ResNet (Residual Network) is deep learning model type used for image recognition because of their combination of performance and efficiency and their ability to train deep neural networks [22]. For the experiments, the ResNet models were pre-trained on the ImageNet dataset, which comprises more than a million images categorized into 1,000 classes. The author tested various ResNet variants, including ResNet34, ResNet50, ResNet101, and ResNext50, but found that ResNet34 was sufficient for the experiments and also experimented with various combinations of hyperparameters to optimize the ResNet model's performance.

FANN

The Feature Attention-based Neural Network (FANN) is a neural network type specifically developed for malware classification [29]. FANN incorporates an Attention Block (AB) to assess the significance of each feature and its relationship with other features. To learn feature representation without ground-truth cluster membership labels, FANN is trained on pseudo labels obtained through k-means clustering. FANN is composed of an input layer, output layer, AB, and three hidden layers, all of which are fully connected.

VGG16

The VGG16 (Visual Geometry Group 16) network is a well-known deep learning architecture that has shown impressive performance on image recognition tasks. In this method, Huang *et al.* [30] used a hybrid visualization approach, combining static and dynamic analysis of malware samples. The dynamic analysis is carried out using Cuckoo Sandbox, and the results are visualised as images, and the neural network is trained using these images along with static images and shown effectiveness in detecting unknown malware.

DenseNet:

DenseNet is a deep learning model that has shown great success in image classification tasks. It is based on the concept of dense connections, where each layer receives feature maps from all preceding layers, allowing for a more efficient flow of information through the network. Regarding malware detection, the initial step involves converting malware binaries into two-dimensional images, which can then be classified using the DenseNet model. Hemalatha et al. [27] addressed class imbalance in malware datasets by using the DenseNet model in conjunction with a reweighted class-balanced loss function. Also, the author demonstrated higher accuracy in detecting novel malware samples while decreasing false-positive rates and retaining low computational time. The authors established that a deep learning

and DenseNet-based malware detection approach is a dependable and efficient alternative to traditional methods for mitigating malware.

In the context of malware detection, the malware binaries are first converted into two-dimensional images, which can then be input into the DenseNet model for classification. By using the DenseNet model with a reweighted class-balanced loss function, the proposed system can effectively handle the issue of class imbalance in malware datasets. Hemalatha *et al.* [27] shown higher accuracy in detecting new malware samples, while also reducing false-positive rates and maintaining low computational time. The authors shown that the malware detection solution based on deep learning and DenseNet is a reliable and effective alternative to traditional malware mitigation techniques.

7. Performance Analysis

This thorough investigation showed that authors typically evaluated at accuracy as a system performance of their suggested DL models. The comparative analysis of several DL approaches is highlighted in this section.

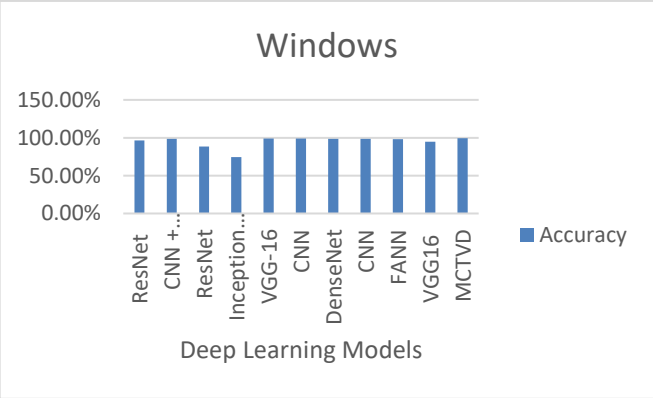


Fig. 4: Performance Analysis of various Deep Learning Models on Windows

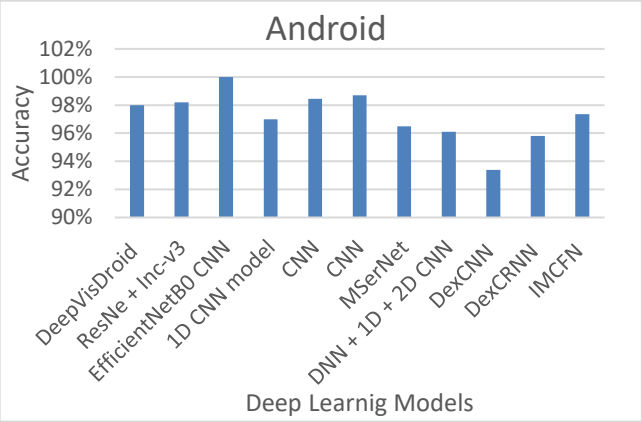


Fig. 5: Performance Analysis of various Deep Learning Models on Android

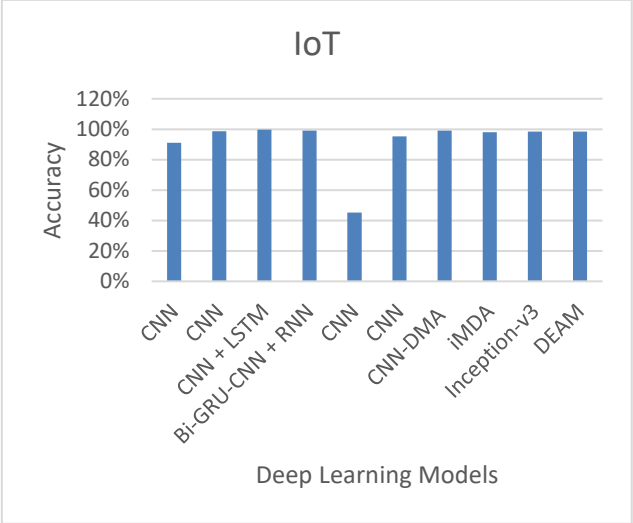
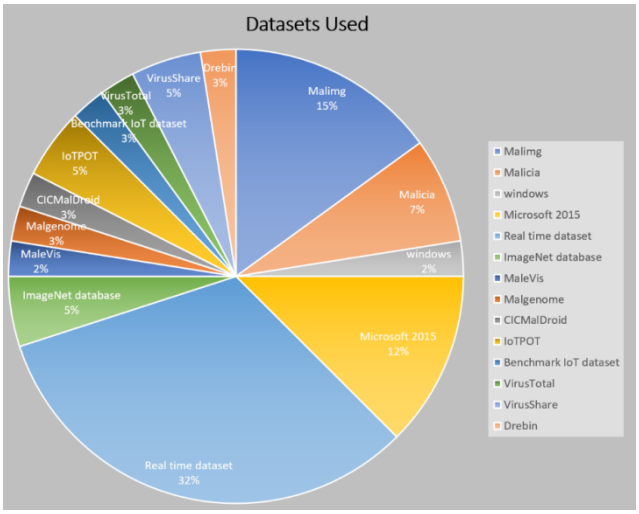


Fig. 6: Performance Analysis of various Deep Learning Models on IoT

8. Dataset Used



9. Discussion

The systematic literature review examines recent developments in deep learning-based image classification for malware detection. From the findings presented in the preceding section, it is evident that the CNN model attained the highest accuracy in the Windows environment, with a score of 99.12%. In the IoT environment, the highest accuracy achieved was 99.78%, which was obtained by the CNN + LSTM model. On the other hand, for the Android environment, the EfficientNetB0 CNN model achieved the highest accuracy of 100%. Regarding the dataset used in these studies, the Real-time dataset was the most widely used dataset, with 13 studies using it. The Malimg dataset was used in six studies, while the Microsoft 2015 and Malicia datasets were used in five and three studies, respectively. Other datasets such as ImageNet database, VirusTotal, and VirusShare were also used in the studies.

In summary, the Windows environment showed good performance with the CNN model, the IoT environment yielded the highest accuracy with the CNN + LSTM model, and the EfficientNetB0 CNN model outperformed other models in the Android environment. Moreover, the Real-time dataset was the most commonly used dataset among the studies reviewed. recent studies on image-based malware classification through deep

learning have demonstrated high accuracy in detecting and classifying malware images. Deep learning models can serve as an extra layer of protection against malware attacks by eliminating the necessity for manual feature engineering. Nevertheless, these models need a substantial amount of high-quality data to be trained effectively, and their interpretability can be challenging. Adversarial attacks and the high computational requirements of these models are also potential limitations that need to be addressed to ensure their effectiveness and robustness in real-world scenarios.

10. Metric Used

Here is the comparison of the various metrics for image-based malware classification using different deep learning models.

- **F-score**: This metric considers the false positive and false negative rates to assess a model's accuracy and precision.
- **Precision**: This metric calculates the proportion of true positive identifications out of all the positive detections generated by the model.
- **False Positive (FP)**: A false positive is a prediction made by the model that is not actually an object of interest.
- **False Negative (FN)**: A false negative is a prediction that a model fails to identify as an object of interest when it should have.
- **Recall:** Measures the percentage of true positive detections among all the objects in the dataset.
- **True Positive (TP):** A true positive is a prediction that a model correctly identifies as an object of interest.
- **The Area Under the Receiver Operating Characteristic Curve (AUC):** AUC is a metric that quantifies how effectively a model can differentiate between positive and negative instances.
- **Computational Complexity:** Refers to the amount of time and computational resources required to run the model

11. Research Gaps

The limitations identified in this study suggests that while deep learning-based image classification techniques have shown promise in detecting malware, there are significant gaps in their efficacy and generalizability. These include limitations such as poor dataset size, reliance on image-based detection, and bias in the available datasets, among others. As potential research gaps, it may be worth exploring the use of other techniques beyond deep learning-based image classification, such as graph-based approaches, to improve malware detection. Additionally, there is a need for further investigation into the generalizability and robustness of these techniques to new and unknown malware types and for addressing the challenges posed by obfuscation and manipulation techniques. Furthermore, given the limitations in dataset size and quality, there is a need to explore strategies for generating larger and more diverse datasets that are better suited for evaluating and improving the effectiveness of malware detection techniques

12. Research Implication and Practice

The use of applying deep learning approaches to identify malware through images shows promise in improving the security of these systems against malware attacks. However, the studies also highlight several research gaps, including exploring newer deep learning models, improving robustness against adversarial attacks, and investigating the effectiveness of these techniques on more complex types of malwares. From a practical standpoint, the findings suggest that image-based malware detection can be an effective supplement to traditional detection methods, which rely on identifying malicious code or behaviours. The research implications and practical applications of deep learning-based image classification for malware are promising, yet further research is needed to explore its potential in other environments and to improve its effectiveness and reliability.

13. Challenge and Strength

One of the biggest challenges in applying deep learning approaches to identify malware through images is the constantly evolving nature of malware. Malware creators are constantly finding new ways to obfuscate and hide their code, making it more difficult to detect using traditional methods, let alone image-based detection. Additionally, there is a risk of false positives and negatives in detecting image-based, as the visual representation of a file or program may not always accurately reflect its malicious intent. Another challenge is the computational complexity of some deep learning models, which can require significant resources to train and run.

Despite these challenges, image-based detection has several strengths that make it a promising approach for malware detection. First, it can be more effective at detecting malware that has been designed to evade traditional detection methods. Second, it can potentially detect malware that has not yet been seen before, as it relies on the visual representation of a file or program rather than a signature or behavior pattern. Third, it can be used across various operating systems and devices, making it a versatile approach to malware classification. Lastly, the use of deep learning allows for the creation of more sophisticated and accurate detection models, which can continue to evolve as malware threats change. In general, even though utilizing deep learning for malware detection through images comes with its set of difficulties, the possible advantages are significant enough to merit further investigation and advancement.

14. Limitation

This paper review primarily focuses on malware detection utilizing deep learning models and image-based techniques. However, there are several other effective methods, such as graph-based and signature-based techniques, as well as machine learning-based techniques that were not included in this review. Moreover, this review solely concentrates on recent publications, which could limit the scope of knowledge to recent years and overlook the fundamental works and their benefits in this field.

15. Conclusion and Future Directions

In conclusion, the systematic literature review highlights the recent advances in deep learning techniques for image based malware classification. The review demonstrates that these techniques have the potential to effectively classify malware through image-based approaches on various environments, such as Windows, Android, and IoT devices. The review also identifies the challenges in this field, such as the need for larger annotated datasets for model training, the computational cost of

deep learning model training, and the susceptibility of these models to false positives and false negatives.

Future research should focus on improving the robustness of deep learning models to adversarial attacks and enhancing their interpretability to facilitate better understanding of their decision-making processes. Additionally, research should be conducted on utilising deep learning for malware classification in industrial control systems and other critical infrastructure. Furthermore, the review highlights the need for research on the use of deep learning models for malware detection and classification in new and complex types of malwares. Future research should also focus on the Generative deep learning models and concept drift detection techniques that would be useful for malware detection, particularly in scenarios where the malware is evolving rapidly and traditional signature-based methods may not be effective. Finally, future studies should address the ethical and privacy concerns associated with the use of deep learning techniques for malware detection and classification.

References

[1] O. Fedor, "93 Must-Know Ransomware Statistics 2022]," Antivirus Guide, 2022. Online]. Available: https://www. antivirusguide .com/ cybersecurity/ransomware-statistics/?gclid=CjwKCAiAlp2fBh BPEiwA2Q10D7CFIAhWIQvYVNcVVwt8DiCfGyz6gxM hL W0sfhphyviVxMHgoC6p ThoC7rsQAvD_BwE.

[2] SolarWinds, "SolarWinds supply chain attack explained: Why organizations were not prepared," CSO Online, 2020. Online]. Available: https://www.csoonline.com/article/3601508/solarwinds-supply-chain-attack-explained-why-organizations-were-not-prepared.html.

[3] C. Burdova, "What Is Ryuk Ransomware?," Avast, 2022. Online]. Available: https://www.avast.com/c-ryuk-ransomware.

[4] "Microsoft Exchange Server Vulnerabilities," Microsoft, 2021. Online]. Available: https://www.microsoft.com/en-us/microsoft-365/security/office-365-security/microsoft-exchange-server-vulnerabilities.

[5] "Darkside ransomware," CISA, 2022. Online]. Available: https://us-cert.cisa.gov/ncas/alerts/aa21-062a.

[6] "Babuk ransomware," TrendMicro, 2023. Online]. Available: https://www.trendmicro.com/en_us/research/21/b/babuk-ransomware-targets-enterprises.html.

[7] "Exim vulnerability exploit," NIST, 2023. Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2019-15846.

[8] M. Rees, "What Is Security Awareness Training And Why Is It Important?," Expert Insights, 2022. Online]. Available: https://expertinsights.com/insights/what-is-security-awareness-training-and-why-is-it-important/.

[9] S. Venkatraman, M. Alazab, and R. Vinayakumar, "A hybrid deep learning image-based analysis for effective malware detection," Journal of Information Security and Applications, vol. 47, pp. 377-389, 2019.

[10] K. He and D. S. Kim, "Malware detection with malware images using deep learning techniques," in 2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), 2019, pp. 95-102.

[11] Y. Jian, H. Kuang, C. Ren, Z. Ma, and H. Wang, "A novel framework for image-based malware detection with a deep neural network," Computers & Security, vol. 109, p. 102400, 2021.

[12] A. Bensaoud, N. Abudawaood, and J. Kalita, "Classifying malware images with convolutional neural network models," International Journal of Network Security, vol. 22, no. 6, pp. 1022-1031, 2020.

[13] Y. Liu, C. Tantithamthavorn, L. Li, and Y. Liu, "Deep learning for android malware defenses: a systematic literature review," ACM Journal of the ACM (JACM), vol. 69, no. 2, pp. 1-36, 2022.

[14] 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.

[15] C. Catal, G. Giray, and B. Tekinerdogan, "Applications of deep learning for mobile malware detection: A systematic literature review," Neural Computing and Applications, pp. 1-26, 2022.

[16] Z. Wang, Q. Liu, and Y. Chi, "Review of android malware detection based on deep learning," IEEE Access, vol. 8, pp. 181102-181126, 2020.

[17] J. Qiu, J. Zhang, W. Luo, L. Pan, S. Nepal, and Y. Xiang, "A survey of android malware detection with deep neural models," ACM Computing Surveys (CSUR), vol. 53, no. 6, pp. 1-36, 2020.

[18] R. Kumars, M. Alazab, and W. Wang, "A survey of intelligent techniques for Android malware detection," in Malware Analysis Using Artificial Intelligence and Deep Learning, Cham: Springer, 2021, pp. 121-162.

[19] D. Pant and R. Bista, "Image-based Malware Classification using Deep Convolutional Neural Network and Transfer Learning," in 2021 3rd International Conference on Advanced Information Science and System (AISS 2021), 2021, pp. 1-6.

[20] R. Kumar, Z. Xiaosong, R. U. Khan, I. Ahad, and J. Kumar, "Malicious code detection based on image processing using deep learning," in Proceedings of the 2018 International Conference on Computing and Artificial Intelligence, 2018, pp. 81-85.

[21] M. Xiao, C. Guo, G. Shen, Y. Cui and C. Jiang, "Image-based malware classification using section distribution information," Computers & Security, vol. 110, p. 102420, 2021.

[22] N. Bhodia, P. Prajapati, F. Di Troia, and M. Stamp, "Transfer learning for image-based malware classification," arXiv preprint arXiv:1903.11551, 2019.

[23] N. Marastoni, R. Giacobazzi, and M. Dalla Preda, "Data augmentation and transfer learning to classify malware images in a deep learning context," Journal of Computer Virology and Hacking Techniques, vol. 17, pp. 279-297, 2021.

[24] R. U. Khan, X. Zhang, and R. Kumar, "Analysis of ResNet and GoogleNet models for malware detection," Journal of Computer Virology and Hacking Techniques, vol. 15, pp. 29-37, 2019.

[25] A. I. Alzahrani, M. Ayadi, M. M. Asiri, A. Al-Rasheed, and A. Ksibi, "Detecting the Presence of Malware and

Identifying the Type of Cyber Attack Using Deep Learning and VGG-16 Techniques," Electronics, vol. 11, no. 22, pp. 3665, 2022.

[26] A. Darem, J. Abawajy, A. Makkar, A. Alhashmi, and S. Alanazi, "Visualization and deep-learning-based malware variant detection using OpCode-level features," Future Generation Computer Systems, vol. 125, pp. 314-323, 2021.

[27] J. Hemalatha, S. A. Roseline, S. Geetha, S. Kadry, and R. Damaševičius, "An efficient densenet-based deep learning model for malware detection," Entropy, vol. 23, no. 3, pp. 344, 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, pp. 102547, 2022.

[29] S. K. J. Rizvi, W. Aslam, M. Shahzad, S. Saleem, and M. M. Fraz, "PROUD-MAL: static analysis-based progressive framework for deep unsupervised malware classification of windows portable executable," Complex & Intelligent Systems, pp. 1-13, 2022.

[30] X. Huang, L. Ma, W. Yang, and Y. Zhong, "A method for windows malware detection based on deep learning," Journal of Signal Processing Systems, vol. 93, pp. 265-273, 2021.

[31] H. Deng, C. Guo, G. Shen, Y. Cui, and Y. Ping, "MCTVD: A malware classification method based on three-channel visualization and deep learning," Computers & Security, vol. 126, p. 103084, 2023.

[32] K. Bakour and H. M. Ünver, "DeepVisDroid: android malware detection by hybridizing image-based features with deep learning techniques," Neural Computing and Applications, vol. 33, pp. 11499-11516, 2021.

[33] K. Bakour and H. M. Ünver, "VisDroid: Android malware classification based on local and global image features, bag of visual words and machine learning techniques," Neural Computing and Applications, vol. 33, pp. 3133-3153, 2020.

[34] P. Yadav, N. Menon, V. Ravi, S. Vishvanathan, and T. D. Pham, "A two-stage deep learning framework for image-based android malware detection and variant classification," Computational Intelligence, vol. 38, no. 5, pp. 1748-1771, 2022.

[35] N. Daoudi, J. Samhi, A. K. Kabore, K. Allix, T. F. Bissyandé, and J. Klein, "Dexray: a simple, yet effective deep learning approach to android malware detection based on image representation of bytecode," in Deployable Machine Learning for Security Defense: Second International Workshop, MLHat 2021, Virtual Event, August 15, 2021, Proceedings 2, Springer International Publishing, 2021, pp. 81-106.

[36] V. Sihag, S. Prakash, G. Choudhary, N. Dragoni, and I. You, "DIMDA: Deep Learning and Image-Based Malware Detection for Android," in Futuristic Trends in Networks and Computing Technologies: Select Proceedings of Fourth International Conference on FTNCT 2021, Singapore, Springer Nature Singapore, Nov. 2022, pp. 895-906.

[37] J. Geremias, E. K. Viegas, A. O. Santin, A. Britto, and P. Horchulhack, "Towards multi-view android malware detection through image-based deep learning," in 2022 International Wireless Communications and Mobile Computing (IWCMC), IEEE, May 2022, pp. 572-577.

[38] H. J. Zhu, W. Gu, L. M. Wang, Z. C. Xu, and V. S. Sheng, "Android malware detection based on multi-head squeeze-and-excitation residual network," Expert Systems with Applications, vol. 212, p. 118705, 2023.

[39] D. Ö. Şahin, B. K. Yazar, S. Akleylek, E. Kiliç, and D. Giri, "On the Android Malware Detection System Based on Deep Learning," in Smart Applications with Advanced Machine Learning and Human-Centred Problem Design, Cham, Springer International Publishing, 2023, pp. 453-466.

[40] Z. Ren, H. Wu, Q. Ning, I. Hussain, and B. Chen, "End-to-end malware detection for android IoT devices using deep learning," Ad Hoc Networks, vol. 101, p. 102098, 2020.

[41] D. Vasan, M. Alazab, S. Wassan, H. Naeem, B. Safaei, and Q. Zheng, "IMCFN: Image-based malware classification using fine-tuned convolutional neural network architecture," Computer Networks, vol. 171, p. 107138, 2020.

[42] A. P. Namanya, I. U. Awan, J. P. Disso, and M. Younas, "Similarity hash based scoring of portable executable files for efficient malware detection in IoT," Future Generation Computer Systems, vol. 110, pp. 824-832, 2020.

[43] H. T. Nguyen, Q. D. Ngo, and V. H. Le, "A novel graph-based approach for IoT botnet detection," International Journal of Information Security, vol. 19, no. 5, pp. 567-577, 2020.

[44] M. Dib, S. Torabi, E. Bou-Harb, and C. Assi, "A multi-dimensional deep learning framework for iot malware classification and family attribution," IEEE Transactions on Network and Service Management, vol. 18, no. 2, pp. 1165-1177, 2021.

[45] R. Chaganti, V. Ravi, and T. D. Pham, "Deep learning based cross architecture internet of things malware detection and classification," Computers & Security, vol. 120, p. 102779, 2022.

[46] M. Ghahramani, R. Taheri, M. Shojafar, R. Javidan, and S. Wan, "Deep Image: A precious image based deep learning method for online malware detection in IoT Environment," arXiv preprint arXiv:2204.01690, 2022.

[47] Q. Li, J. Mi, W. Li, J. Wang, and M. Cheng, "CNN-based malware variants detection method for internet of things," IEEE Internet of Things Journal, vol. 8, no. 23, pp. 16946-16962, 2021.

[48] A. Anand, S. Rani, D. Anand, H. M. Aljahdali, and D. Kerr, "An efficient CNN-based deep learning model to detect malware attacks (CNN-DMA) in 5G-IoT healthcare applications," Sensors, vol. 21, no. 19, p. 6346, 2021.

[49] M. Asam, S. H. Khan, A. Akbar, S. Bibi, T. Jamal, A. Khan, et al., "IoT malware detection architecture using a novel channel boosted and squeezed CNN," Scientific Reports, vol. 12, no. 1, pp. 1-12, 2022.

[50] H. Naeem, B. M. Alshammari, and F. Ullah, "Explainable Artificial Intelligence-Based IoT Device Malware Detection Mechanism Using Image Visualization and Fine-Tuned CNN-Based Transfer Learning Model," Computational Intelligence and Neuroscience, 2022.

[51] C. Wang, Z. Zhao, F. Wang, and Q. Li, "A novel malware detection and family classification scheme for IoT based on DEAM and DenseNet," Security and Communication Networks, pp. 1-16, 2021.

[52] enifa Sabeena, S. ., & Antelin Vijila, S. . (2023). Moulded RSA and DES (MRDES) Algorithm for Data Security. International Journal on Recent and Innovation Trends in Computing and Communication, 11(2), 154–162. https://doi.org/10.17762/ijritcc.v11i2.6140

[53] Esposito, M., Kowalska, A., Hansen, A., Rodríguez, M., & Santos, M. Optimizing Resource Allocation in Engineering Management with Machine Learning. Kuwait Journal of Machine Learning, 1(2). Retrieved from http://kuwaitjournals.com/index.php/kjml/article/view/115