IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Advanced Image-Based Malware Detection Leveraging Sparse Lstm Networks For Intelligent Feature Recognition And Classification

Student Name: Ketki Dattatray Gavhane

College Name : Trinity College Of Engineering And Research

S.No. 25 27, Kondhwa-Saswad Road, Pisoli Pune - 411048

Study of Year – Second year

Department - Computer Engineering

Abstract: Malware is a form of malicious software designed to cause harm to computer systems. In recent years, the proliferation of malware for illegal and malicious purposes has grown significantly. To counter these threats, several machine learning and deep learning techniques have been employed for the detection and classification of malware. One promising approach is image-based malware detection, which leverages machine learning and compuer vision models to analyse the visual representation of malware, such as binary images or screenshots, for detecting malicious behaviours. This method has the potential to identify hidden or polymorphic malware variants, providing an additional layer of defence against emerging cyber-attacks. In this study, a new approach is introduced that utilizes a Sparse Long Short-Term Memory (LSTM) network for image-based malware classification. The primary objective of this method is to employ an optimized deep learning model to efficiently identify and classify malware images. The Sparse LSTM network is used to extract crucial feature vectors from the malware images, enhancing the classification process. By integrating attention mechanisms, the model effectively captures significant patterns for malware recognition. The technique is evaluated using the Malimg malware data set, demonstrating promising results in comparison to existing methods.

I. INTRODUCTION

The rapid evolution of the digital ecosystem has fundamentally reshaped how individuals, businesses, and governments operate. However, this growth has also introduced significant cyber security challenges, with malware short for malicious software emerging as a major threat. Malware is designed to infiltrate, disrupt, or damage computer systems, leading to data breaches, financial losses, and operational disruptions. Over the years, the rise of sophisticated malware variants, including polymorphic and metamorphic types, has rendered traditional detection methods increasingly ineffective. These advanced malware types dynamically alter their code or structure, enabling them to evade signature-based detection systems, which rely on predefined patterns to identify malicious files. Heuristicbased detection methods, which aim to identify suspicious or anomalous behaviors, have been developed to address these limitations. However, these approaches often struggle with high false positive rates and fail to detect dormant malware that behaves benignly until fully activated. To counter these challenges, machine learning (ML) and deep learning (DL) techniques have emerged as promising solutions. These methods excel at identifying complex patterns within large datasets, making them highly effective for detecting evolving malware threats. A particularly innovative approach in this domain is image-based - detection. This method involves converting malware binaries into visual formats, such as gray scale images, and leveraging computer vision models to analyze

their unique spatial features. By visualizing malware data, this technique enables the detection of hidden, obfuscated, or polymorphic malware variants that traditional methods struggle to identify.

Figure No.1. Comparison between Traditional Detection Methods and Image-Based Malware Detection Approaches

Recent advancements in deep learning architectures, such as Convolutional Neural Networks (CNNs) and Long ShortTerm Memory (LSTM) networks, have demonstrated their effectiveness in extracting spatial and temporal features from malware images. Sparse LSTM networks, in particular, offer improved performance by efficiently handling temporal dependencies in malware data. These models, when combined with attention mechanisms, can focus on the most relevant patterns, enhancing the accuracy and reliability of malware classification. Evaluations on benchmark datasets, such as the Malimg dataset, have shown the significant potential of this approach in realworld applications. This project introduces a state-of-the-art solution for image-based malware detection by integrating Sparse LSTM networks with attention mechanisms. The proposed method extracts critical feature vectors from malware images, providing a scalable and robust solution for identifying advanced malware variants. This approach aligns with emerging technologies, such as IoT, 5G, and edge computing, and ensures compliance with modern cyber security standards. By addressing key challenges in malware detection, this study contributes to the development of more effective and adaptable defenses against evolving cyber threats.

Literature Review : Benchadi et al. [1] propose a malware analysis framework that leverages subspace-baseed techniques to identify representative image patterns within malware binaries. This approach reduces the computational burden typically associated with malware analysis, enabling faster and more efficient processing. By focusing on subspace methods, their framework isolates relevant features in image representations, improving accuracy in detecting malicious software. Their work, published in IEEE Access, demonstrates that image-based detection models, when combined with subspace techniques, can offer high precision with reduced computational cost, making it feasible for realtime analysis. Hai et al. [2] introduce an advanced Endpoint Detection and Response (EDR) system that incorporates image-based malware detection. The EDR system transforms malware binaries into visual representations, which allows the detection algorithms to analyse structural patterns visually rather than relying on traditional feature extraction methods. This visual approach enhances detection capability, particularly for sophisticated malware that evades conventional EDR systems. Hai et al.'s findings emphasize the potential of integrating image-based malware detection in EDR frameworks to improve organizational cyber security, demonstrating improved detection accuracy and adaptability to evolving threats. Jin et al. [3] explore the use of auto encoders in malware detection, focusing on extracting features from malware images for improved classification. Their approach

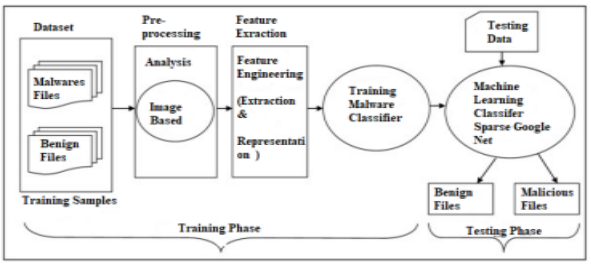
employs deep auto encoder models to identify hidden features within image representations of malware, particularly effective in mobile ad hoc networks and sensor systems where computational resources are constrained. By reconstructing malware images through auto encoders, the model captures distinctive features that enhance the detection process. Jin et al.'s study illustrates the potential of auto encoders in feature extraction, paving the way for more resource-efficient, image-based malware detection solutions in mobile and sensor-driven environments. Nguyen et al. [4] investigate generative adversarial networks (GANs) as a means of augmenting malware datasets with synthetic images for classification. Their innovative approach enhances classification accuracy by creating artificial images that closely resemble malware samples, thus expanding the training dataset without requiring more real-world samples. This study illustrates how GANs can generate diverse representations of malware, improving model robustness and reducing over fitting. Nguyen et al. demonstrate that GAN-augmented datasets improve the performance of image-based classifiers, offering a novel way to tackle the challenge of limited dataset diversity in malware detection. Yadav et al. [5] present a two-stage deep learning framework aimed at Android malware detection. Their method involves transforming Android binaries into images and applying deep learning techniques to detect and classify malware variants effectively. The framework uses convolutional layers in combination with sequential processing methods to detect subtle differences between malware types, enhancing security for mobile platforms. Yadav et al.'s findings highlight the advantages of a twostage process, showing that this structure improves detection rates for Android-specific threats and helps in variant classification, contributing to mobile device security. Yaseen et al. [6] introduce a unique approach that converts machine code directly into images for malware classification. By transforming low-level code into visual representations, this method broadens the scope of imagebased malware detection to analyse underlying code structures. This approach is particularly useful for capturing minute differences in code that signify malicious intent, which are often missed by traditional methods. Yaseen et al. demonstrate that by examining low-level code patterns visually, their method provides insights into malware behaviour, offering a new dimension for feature extraction in cyber security. Ketebu et al. [7] review existing methods in image-based malware classification, with a focus on convolutional neural networks (CNNs). Their work categorizes various imagebased detection techniques and assesses the effectiveness of CNNs for pattern recognition in malware images. By highlighting the strengths and limitations of current methodologies, Ketebu et al. provide a well-rounded perspective on the advancements in image-based malware detection. Their survey emphasizes CNNs' capabilities in detecting intricate patterns, offering valuable insights into the challenges and potential improvements in the field. Pant et al. [8] investigate the effectiveness of deep convolutional neural networks (DCNNs) combined with transfer learning for malware classification. Their study leverages pre-trained models, which are then fine-tuned on malware images, significantly boosting detection performance. This approach illustrates the practical application of transfer learning in image-based malware detection, making it accessible for real-world scenarios. Pant et al. show that transfer learning not only enhances classification accuracy but also reduces training time, providing a viable solution for cyber security applications requiring quick adaptability to new malware. Reilly et al. [9] assess the robustness of image-based malware classifiers by training their models with GANgenerated images. Their research indicates that GANs improve detection models' resilience against adversarial attacks, which are often used by malicious entities to bypass standard detection mechanisms. By strengthening model robustness through GANs, Reilly et al. contribute to the development of more secure detection systems capable of withstanding adversarial manipulation, reinforcing the role of GANs in building resilient cyber security defences. Prajapati et al. [10] conduct an empirical evaluation of various image-based learning techniques for malware classification. Their study assesses different models' performance on malware image datasets, analysing the effectiveness of each in accurately classifying malware. By identifying strengths and weaknesses across techniques, Prajapati et al. provide a foundational understanding of image-based approaches, helping researchers determine the most suitable methods for different cyber security applications. This work serves as a comparative analysis that aids in selecting appropriate models based on specific detection requirements.

Research Gap : Despite the advancements in image-based malware detection, several gaps remain that hinder its widespread application. Current approaches often rely on limited datasets, restricting the diversity and generalizability of the models across different malware variants and platforms. Scalability is another challenge, as many methods are computationally expensive and require high processing power, limiting their applicability in real-time scenarios or on resource-constrained devices. Additionally, while deep learning models achieve high detection accuracy, their decision-making processes often lack transparency, raising concerns about interpretability. The integration of attention mechanisms could further enhance detection accuracy by focusing on critical features, yet this aspect remains underexplored. Furthermore, the application

of image-based malware detection techniques across domains such as IOT and cloud environments has not been thoroughly examined, leaving an opportunity to assess cross-domain applicability. Establishing standardized benchmarks for evaluating performance in real-world settings could also enhance the reliability and adoption of these techniques, addressing gaps in both research and practical applications of image-based malware detection.

Problem Statement :The increasing sophistication of malware, especially polymorphic and metamorphic variants, poses a significant challenge to traditional detection methods that rely on static signatures or heuristic analysis. These conventional approaches often struggle to accurately identify malware that frequently changes its structure to avoid detection. As cyber threats grow more complex, there is a pressing need for advanced, scalable, and efficient detection systems that can adapt to these evolving tactics. This study addresses this gap by developing a novel image-based malware detection system using Sparse LSTM networks, which leverages deep learning to improve detection accuracy and efficiency for modern cyber security needs.

Proposed System : Introduction to System Architecture for Image-Based Malware Detection: The rapid growth of malware has created significant challenges for cyber security, demanding advanced and automated detection methods. Traditional techniques like signature-based detection and heuristic analysis often fail to identify new and evolving malware variants. To overcome these limitations, machine learning and deep learning approaches have emerged as effective alternatives. Among these, image-based malware detection has gained prominence, where malware files are converted into visual representations and analyzed using image classification techniques to identify malicious patterns. The proposed system architecture for image-based malware detection consists of two main phases: Training and Testing. In the training phase, malware and benign files are pre-processed into image formats, followed by feature extraction and model training. In the testing phase, the trained model classifies new files as benign or malicious based on learned patterns. Leveraging advanced neural networks, such as Google Net or Sparse Google Net, the system enhances detection accuracy by identifying subtle patterns that traditional methods might miss. This innovative approach offers a scalable and robust solution for real-time malware detection, addressing critical cyber security challenges with high precision



Methodology for Image-Based Malware Detection:

Dataset Collection:

Training Samples: Gather a dataset of files, including both malware files and benign (non-malicious) files. The dataset should represent various types of malware to improve model generalization.

Pre-processing:

Image-Based Analysis: Convert each file in the dataset to a visual format (image-based representation). This may involve interpreting binary code, assembly code, or file structure in a way that each sample becomes an image. This transformation allows the system to analyze patterns in a way similar to image classification.

Feature Extraction:

Feature Engineering:

Perform feature extraction on the image-based dataset. This process involves extracting and representing specific characteristics or patterns from the image, which helps distinguish between malware and benign files. Techniques may include texture analysis, colour pattern recognition, and structural element extraction.

Training Phase:

Training Malware Classifier: Use the extracted features to train a machine learning classifier. A neural network model, such as Google Net (or a variant like Sparse Google Net as indicated), can be trained to identify malicious patterns within the visual representations of files. The classifier learns to recognize differences between images representing malware and those representing benign files.

Testing Phase:

Testing Data: Prepare a separate testing dataset with labelled files (malware and benign) that were not used in the training phase.

Machine Learning Classifier Application: Apply the trained classifier to the testing data to evaluate its performance in categorizing files as either benign or malicious. The classifier's accuracy and effectiveness can be determined by how well it categorizes these testing files.

Classification Output: The model outputs classifications for each tested file, labelling them as either Benign or Malicious, based on the features detected in their image representations.

Algorithm-Sparse Google Net

Deep convolutional neural networks (CNNs) have achieved notable success across various computer vision tasks, such as object classification, detection, and segmentation malware detection, the depth of neural networks has played a crucial role in advancing detection accuracy and robustness. From the early success of models like Alex Net to VGG Net and Google Net, end that network externally boosted performance across visual tasks. However, as demonstrated in experiments, merely stacking layers without modifying the net wore can degrade performance due to the vanishing gradient problem, where gradients diminish as the network depth increases. To address this, He introduced Res Net, a residual learning framework that enables o surpass 1000 layers by using identity-mapping shortcuts.

This approach extended the depth of Res Net to over 1000 layers, achieving state-of-the-art performance on image classification tasks, which has implications for applications such as malware image classification. Recognizing the potential for over fitting in very deep networks (e.g., beyond 1000 layers), Huang proposed a new training strategy called stochastic depth, which effected over fitting in Res Net by randomly dropping residual modules during training. This process helped alleviate the vanishing gradient problem by training shallower sub-networks within the overall architecture. The stochastic depth method demonstrated improved performance on image classification, even in networks exceeding 1000 layers, and holds potential for further enhancing image-based malware detection models by addressing over fitting concerns in deep architectures.

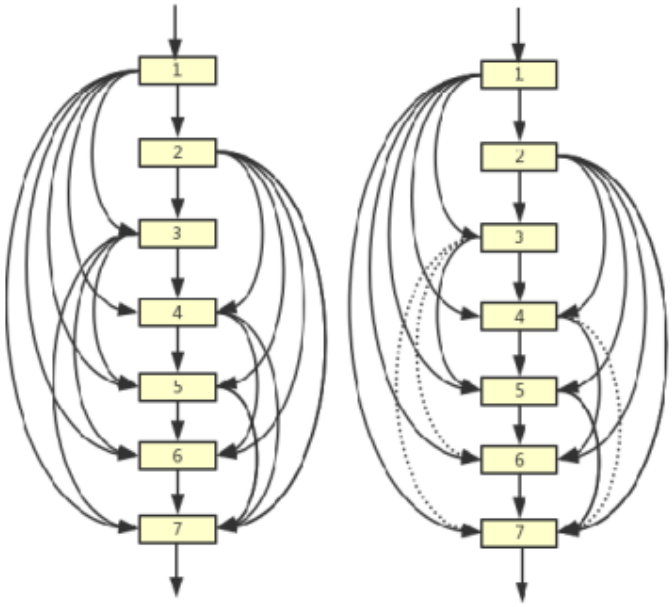


Figure No.3: Left Is Dense Net, Inputs to Layers Are From All Previous Layers; Right Is Sparse Net, Dotted Lines Are Dropped Connections. Input To Layers Is From At Most Two Previous Layers.

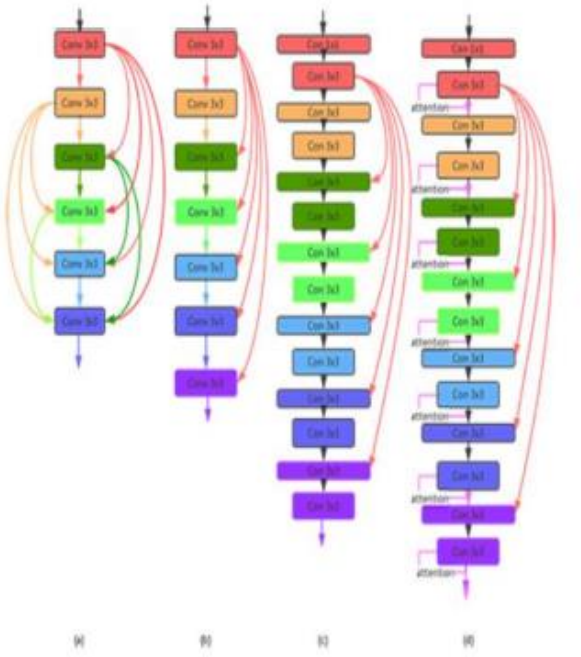


Figure No.4: A is Dense net; B is Sparse net (Path=2); C Is Sparse net-BC; D Is Sparse net ABC.

Another innovation in network architecture came from Zagoruyko, who introduced a wider and shallower Res Net variant. This “Wide Res Net” with ores outperformed the original Res Net with over 1000 layers, largely due to the increased number of channels in convolutional layers. Wider networks benefit from faster training and the ability to harness GPU parallelism effectively, which is advantageous for computationally intensive tasks like image-based malware detection. Further, Han expanded on this approach by introducing deep pyramidal residual networks, where network eases progressively rather than doubling only after down sampling. In the original Res Net architecture, each module's width is fixed (e.g., Conv2_x at 64, Conv3_x at 128, Conv4_x at 256, and Conv5_x at 512), while pyramidal residual networks have increasing width across residual units, regardless of their module. This structure has demonstrated enhanced generalization capabilities, suggesting that balanced increases in both depth and width could similarly improve the performance of networks for image-based malware detection. Applying these architectural advances to image-based malware detection can offer significant advantages, enabling models to effectively

learn intricate features and patterns unique to malware, including polymorphic and metamorphic variants that evade traditional detection methods.

Conclusion

This study explored the use of deep learning techniques, particularly Sparse LSTM networks and image-based representation, to address the challenges in malware detection. Traditional methods, such as signature-based detection, struggle to keep up with evolving malware, especially polymorphic and metamorphic variants that change appearance to evade detection. By converting malware binaries into images, this approach allows deep learning models to leverage computer vision techniques, uncovering unique visual patterns and textures that characterize malicious files. The integration of Sparse LSTM networks, along with attention mechanisms, enhances the detection accuracy by focusing on critical sections within the malware image, which is particularly valuable for detecting obfuscated malware variants. The results demonstrate that the proposed method outperforms conventional detection approaches, improving scalability, adaptability, and speed. This project also highlights the potential of applying deep convolutional neural networks and temporal analysis to cyber security tasks, expanding the scope of AI-driven solutions for real-world malware detection challenges. The findings reinforce the importance of advanced deep learning methods in tackling sophisticated cyber threats, offering a practical framework that can be integrated into industry-standard security tools, such as endpoint detection and response systems, for enhanced protection against modern malware.

References

- D. Y. M. Benchadi, B. Batalo and K. Fukui, "Efficient Malware Analysis Using Subspace-Based Methods on Representative Image Patterns," in IEEE Access, vol. 11, pp. 102492-102507, 2023, doi: 10.1109/ACCESS.2023.3313409.

- Hai, Tran Hoang, et al. "A proposed new endpoint detection and response with image-based malware detection system." IEEE Access 11 (2023): 122859- 122875.

- Jin, Xiang, et al. "A malware detection approach using malware images and auto encoders." 2020 IEEE 17th International Conference on Mobile Ad Hoc and Sensor Systems (MASS). IEEE, 2020.

- Prajapati, Pratik Kumar, and Mark Stamp. "An empirical analysis of image-based learning techniques for malware classification." Malware analysis using artificial intelligence and deep learning (2021): 411-435.