JCRES
Journal of Current Research in Engineering and Science
Bi-Annual Online Journal (ISSN : 2581 - 611X)

Volume 7-Issue 1, January 2024
Paper: 75

Envisioning and Proposing an Innovative Imaged based Malware Detection using Transfer Learning

[1]*DR.Amirtha lakshmi T.M* ,[2]*Mahinder P.M*, [3]*Mohammed Shafi S and* [4]*Bhavani Sai K.B*

Department of Computer Science and Engineering,
SRM Institute of Science and Technology, Ramapuram, Chennai, India
amirthatm@gmail.com ,
mahitm2002@gmail.com,
mohammedshafisms10@gmail.com,
bhavanisaikb@gmail.com

Abstract: The increase in malware proliferation has become a significant concern for cybersecurity experts. Malware authors are continually devising new techniques to evade traditional security measures. Static and dynamic analysis techniques are among the most commonly used methods for detecting malware, but they have significant limitations. These approaches are often ineffective against new and sophisticated threats and require significant memory and time resources to process.Machine learning-based malware detection systems have emerged as an effective alternative to traditional analysis techniques. However, the effectiveness of these systems is limited by the use of handcrafted features. Additionally, class imbalance in malware datasets can lead to performance degradation in malware detection systems.To address these limitations, this paper proposes a visualization-based approach that represents malware binaries as two-dimensional images. The images are fed into a deep learning model that classifies them as malicious or benign. The proposed approach outperforms traditional signature-based and behavior-based methods and is capable of detecting unknown malware variants with similar characteristics.The proposed method uses a layered ensemble approach that replicates the salient features of deep learning while reducing complexity and eliminating the need for backpropagation or hyperparameter tuning. The method is capable of identifying and extracting unique features for each infection and can adjust to each malware variant's changes, making it an effective solution against zero-day malware threats.In conclusion, the proposed visualization- based approach shows promising results in detecting malware threats and addressing the limitations of traditional malware detection methods. This method has the potential to significantly improve the effectiveness of malware detection systems and enhance the overall security of computer systems.

Keywords: CNN (Convolutional Neural Network), Transfer Learning Algorithm, PE files(Portable Executable)

INTRODUCTION

The internet has become an essential part of our daily routine, and it has simplified many aspects of our lives. However, it has also exposed users to various risks, particularly malware. Malware, which initially started as a hobby for tech enthusiasts, has evolved into a profit-making venture for cybercriminals. They often use email and phishing as the primary means of infecting their targets. Cyberattacks are most common in the food industry, logistics sector, and non-profit organizations. In recent times, information similar to what was used in banking Trojans has emerged as a new threat.

The escalating level of malware is becoming one of the most severe cybersecurity threats, posing a significant challenge for the industry. Cybercriminals continue to develop and deploy new forms of malware, with increasing complexity, making it difficult for conventional mitigation techniques to keep pace with these attacks. Malicious hacker groups are using advanced malware techniques, including code obfuscation, polymorphism, and metamorphism, which have become prevalent and beat many established malware mitigation techniques.Companies are frequently targeted by attackers who use various types of malware, including backdoors, miners, spyware, and information stealers, among others. Data-stealing malware, such as Emotet and TrickBot, use malicious spam to infiltratecomputers, making them vulnerable to cyber-attacks. The increasing prevalence of malware attacks calls for more advanced cybersecurity solutions and proactive measures to thwart cybercriminals' attempts.To examine malware instances, static and dynamic analysis techniques are commonly used. Static analysis techniques disassemble the code logic without executing the malware, whereas dynamic analysis examines the malware's behaviour by executing it in a controlled and secure environment. However, static detection techniques are not effective in detecting new malware as the signatures used by them are not universal. Dynamic behaviour-based approaches offer better accuracy, but they have significant overheads.Deep learning, a branch of machine learning that uses multiple levels of learning to enhance its understanding of input data, is a promising technique for detecting and mitigating malware attacks. However, traditional dynamic malware analysis techniques are becoming increasingly ineffective against sophisticated malwareattacks, which render them useless. As such, the cybersecurity industry needs to develop more advanced techniques to address the evolving threats posed by malware.

Convolutional Neural Networks, or CNNs for short, were developed with the primary aim of advancing computer vision through deep learning. These models are built to incorporate numerous complex features that are learned during training, with convolutional layers requiring millions of values. However, one major issue with deep learning models is that they are susceptible to overfitting. When a model is overfit, it

performs well on the training data, but poorly on new, unseen data. This is often caused by the model's inability to generalize well, meaning that it is unable to recognize similar patterns in new data that it hasn't seen before.To address this issue, one approach is to utilize transfer learning, which is the idea that the knowledge and skills acquired while learning one model can be applied to improve the performance of another model on different tasks. In the case of computer vision, pre-trained CNNs can be used to improve the detection and classification of malware images, for example. Pre-trained CNNs are models that have been trained on large, well- defined datasets like ImageNet, and they can be fine-tuned for a specific task, rather than trained from scratch.CNNs are constructed with increasing depth as they become more complex, but this can result in the loss of input data before it reaches the top layer ofthe network. To address this issue, ResNet and other CNNs create shorter pathways between layers, which allows input data to flow more easily through the network. This approach has been shown to improve the performance of CNNs, particularly for tasks like image classification and object detection.

LITERATURE SURVEY

S. Abijah Roseline, S. Geetha, Seifedine Kadry, and Yunyoung Nam [1] The authors have proposed an adaptation of vision-based malware analysis techniques. This approach involves using the grayscale representation of malwareexecutable files to access global features, without the need for reverse engineering or a deep understanding of opcodes or assembly language, as required in static and dynamic analysis.The visual features are engineered and extracted to be clean, simple, powerful, and straightforward. In static analysis,the executable binary file is examined by disassembling it withoutrunning it, and malware is detected using signature-based or pattern-matching techniques. Dynamic analysis, on the other hand, focuses on monitoring the runtime behavior of the executables and addresses the limitations of static analysis. Features such as N-grams, API/system call sequences, control flow graphs, and operational code (opcode) sequences are recovered via dynamic analysis. The work presented in [1] involves retrieving byte code sequences from executables and turning them into n-gram features, which are then matched with the malware signature database. Other features collected from these methods include hash signatures, string sequences, byte sequences, and system resource information. However, conventional signature-based techniques and antivirus software that rely on hash values of binary files are ineffectiveagainst disguised malware and have scalability issues due to the exponential growth of malware signature databases.

R. Vinayakumar , Mamoun Alazab , K. P. Soman , Prabaharan Poornachandran and Sitalakshmi Venkatraman [2] In today's digital landscape, cyberattacks pose a significant threat to businesses, governments, and computer users. Malware, a type of malicious software, is a common form of cyberattack that is evolving at a rapid pace. As a result, malware detection has become a popular research area due to its impact on security. However, existing malware detection techniques have limitations in identifying unknown malware in real-time. Static and dynamic analysis methods have been used, but they require a significant amount of time and resources. In recent years, machine learning algorithms (MLAs) have emerged as apromising approach to effectively analyze malware. These algorithms have been successful because new malware is often a variation of previously detected malware.However, MLAs require extensive feature engineering, feature learning, and feature representation to perform effectively. Additionally, these algorithmsare often biased, which can limit their applicability in real-world scenarios. To overcome these limitations, researchers are developing new methods for efficient zero-day malware detection.This study aims to compare the performance of deep learning architectures and traditional MLAs for malware detection, classification, and categorization using various public and private datasets. By using multiple partitions of these datasets to train and test the model in a disjoint manner, the researchers aim to eliminate dataset bias. Furthermore, they propose a unique image processing method with the best settings for MLAs and deep learning architectures to create a model that is effective at detecting zero-day malware.The study's thorough comparative analysis revealed that the suggested deep learning architectures outperformed traditional MLAs. By reducing bias and assessing these approaches independently, this study provides valuable insights into the development of more effective zero-day malware detection techniques.

Aviad Cohen , Nir Nissim and Yuval Elovici [3] Over the pastfew years, there has been a rise in cyberattacks targeting individuals, businesses, and organizations. Cybercriminals are always looking for new and efficient ways to spread malware to their targets, and they have found that photos are a particularly effective channel. Although many people use photos on a daily basis and consider them to be safe, some types of images may contain dangerous payloads that can carry out harmful functions. The JPEG image format is the most widely used due to its lossy compression, and it is present on nearly all devices, from smartphones and digital cameras to websites and social media platforms. Because JPEG photos are so ubiquitous, cybercriminals often use them as an attack vector because they are perceived as innocuousbut carry a high risk of abuse.Despite the effectiveness of machine learning in detecting known and unknown malware in various domains, machine learning approaches have not yet been used specifically for the identification of malicious JPEGimages. This is where our study comes in. We introduce MalJPEG, a novel machine learning-based approach for accurately identifying unknown malicious JPEG images. We believe that this is the first machine learning-based solution that has been specifically designed for the identification of malicious JPEG images. With our approach, we aim to improve the detection of malware in photos and enhance the security of individuals, businesses, and organizations against cyberattacks.

Yuntao Zhao , Wenjie Cui , Shengnan Geng , Bo Bo , Yongxin Feng and Wenbo Zhang [4] As IoT and 5G technology continue to advance, the importance of cyberspace in social and economic development and national security has grown. The detection of malware and its variations is crucial for cybersecurity, but identifying it has become increasingly difficult due to its increasing sophistication, including encryption, polymorphism, and obfuscation. This paper proposes an improved approach for malware detection using an upgraded Faster RCNN that incorporates transfer learning. By using visualisation technologies to map dangerous code into matching images with common textural qualities, we are able to classify malware. Specifically, the paper suggests a method for detecting malicious code visualisation that is basedon a faster RCNN that incorporates transfer learning. To achieve this, the paper converts the malicious samples' PE files into binary files for static disassembly and then translates these binary bits into grayscale images of the corresponding harmful codes using computer vision technologies.

Jueun Jeon , Jong Hyuk Park and Young-Sik Jeong [5] The IoT technology serves as the basic structure for a hyperconnected world where everything is linked and communicates through the Internet. To be applied in different areas, like smart cities and factories, IoT is merged with 5G and AI. With the rising need for IoT, security concerns have also increased, particularly against the infrastructure, apps, and devices. Several studies have been conducted to identify and prevent the risks of malicious code, but detecting new and variant malware can be challenging. IoT gadgets are frequently targeted by malware writers, especially those with Linux environmentsdue to their numerous attack points and vulnerable products. As most IoT devices have ARM processors, the number of IoT malware samples targeting them has grown. While many studies have been carried out to analyze and detect IoT malware, the subjective selection and classification of representative malware behaviors by analysts can make it difficult to detect new and variant IoT malwaredue to its intelligent evolution.

Jinting Zhu , Julian Jang-Jaccard and Paul A. Watters [6] The paper presents a new neural network model for malware detection, which is based on one-shot learning. Unlike previous models, this model is able to effectively detect unknown malware and optimizes the feature space to ensure that positive samples from the same class have a higher local distance than those from other malware classes. The study results show that this algorithm outperforms other standard techniques such as Siamese Neural Network and KNN. The authors plan to incorporate additional measure learning in their future research to improve recognition accuracy. To avoid losing malicious code information, they also intend to include the Spatial Pyramid Pooling layer into the Siamese network. This layer allows the convolutional network to handle images of any size.

Suyeon Yoo , Sungjin Kim and Brent Byunghoon Kang [7] The paper assessed traditional machine learning algorithms and deep learning architectures that use Static analysis, Dynamic analysis, and image processing techniques for malware detection. The study also developed a scalable framework called ScaleMalNet that detects, categorizes, and classifies zero-day malware. The framework uses a two-stage method for malware analysis and employs deep learning to analyze malware samples gathered from end-user hosts.

Seoungyul Euh , Hyunjong Lee , Donghoon Kim and Doosung Hwang [8] The research analyzed tree-based ensemble techniques and investigated malware properties for static analysis. To address the limitations of commonly used malware feature representations such as changeable length, high-dimensional representation, and high storage utilization, the study proposed a modified malware feature representation.The results showed that the proposed malware features demonstrated better ensemble method generalization in terms of training time and performance than the initial training features. The modified malware features can be advantageous in operations that are frequently used, domain knowledge, or entropy discretization. Malware features do not require fixed-length selection or padding when training data is adequate for feature vectorization for machine learning.

Nuno Martins , Jos Magalhes Cruz , Tiago Cruz and Pedro Henriques Abreu [9] The study examined several papers that utilize advertising machine learning techniques to analyze malware and intrusion. One of the papers reviewed was N. Martins et al.'s "Use of Adversarial Machine Learning to Malware and Intrusion Scenarios: detecting scenarios for systematic reviews." The researchers first presented several key concepts that can help in understanding the basics of adversarial machine learning, as well as adversarial attack and defense strategies.

Existing System:

The continuous emergence of thousands of new malware programs each day poses a significant challenge to cyber security. Many of these programs are highly advanced and canalter their functionalities and structures to bypass security measures. However, accurately detecting the different variants of these malware programs remains a challenge. Existing methods for identifying malware variants mainly rely on staticfeatures such as opcodes and function flows extracted from thephysical structure of the malware files. However, these static features are susceptible to obfuscation and code shelling, which reduces their effectiveness. While malware strains may be able to modify their structures and functions, they cannot conceal their destructive behavioural patterns during execution. To address this issue, a malware variant detection model that combines several behavioural actions can improve detection accuracy and reducethe false-negative rate.This paper proposes a Deep-Ensemble and Multifaceted Behavioral Malware Variant Detection Model Using Sequential Deep Learning and Extreme Gradient Boosting Methods. The modeluses various behavioural features extracted from the dynamic analytic environment. Sequential deep learning and the Extreme Gradient Boosting algorithm are used to develop a multifaceted and deep ensemble behavioral-based malware variant detection scheme. The proposed approach incorporates multiple sets of behavioural variables to identify malware variants. Each type of behavioural feature can automatically extract the final hidden layer of a trained deep sequential learning model, which can indicate the goodness or malice of the investigated program. Four deep learning models were built using different sets of behavioural variables, such as the sequence of API requests, file access patterns, registry access, and network traffic. Overall, this model can significantly enhance the detection of malware variants and improve cyber security..

Existing System Issues:

The current methods of malware detection are inadequate due to the destructive nature of malware attacks and the frequent production of zero-day malware. Additionally, these methods are only effective when dealing with limited amounts of data and require significant computing power. Packed malware is particularly challenging to detect due to its high entropy and lack of visible patterns. While new techniques show potential, their practical application is limited by computational complexity. Furthermore, the challenges in improving performance of these methods mean they cannot meet the expectations of today's network businesses, as they generally have lengthy polynomial running times.

Proposed Architecture:

The size of executable files varies, and for learning purposes, fixed-size input is required. Two methods are used to create fixed-size images: resizing and truncation. In each test of the -d CNN, two convolutional layers and three fully connected layers are employed. A grayscale image with one channel is inputted into the first convolutional layer, which uses a kernel size of three, padding of two, and stride of one to produce data with channels. The output of the second convolutional layer is also channels, with the same other parameters as the first layer. The output of the first fully connected layer is a dimension vector, which is then transmitted to the second fullyconnected layer, where relu activation is utilised to convert theoutput to a dimensional vector. Finally, the data is passed to the lastfully connected layer, which is -dimensional and used for classification. To reduce the expense of training on large images, we use epochs for image sizes smaller than. All layerswere frozen for VGG- except and. Two additional fully connected neuron layers were added to decrease the output dimension from to, and all transfer learning trials were trained for epochs with learning rates of. and.The image dimensions were adjusted to match those required by ResNet and VGG, which are both.

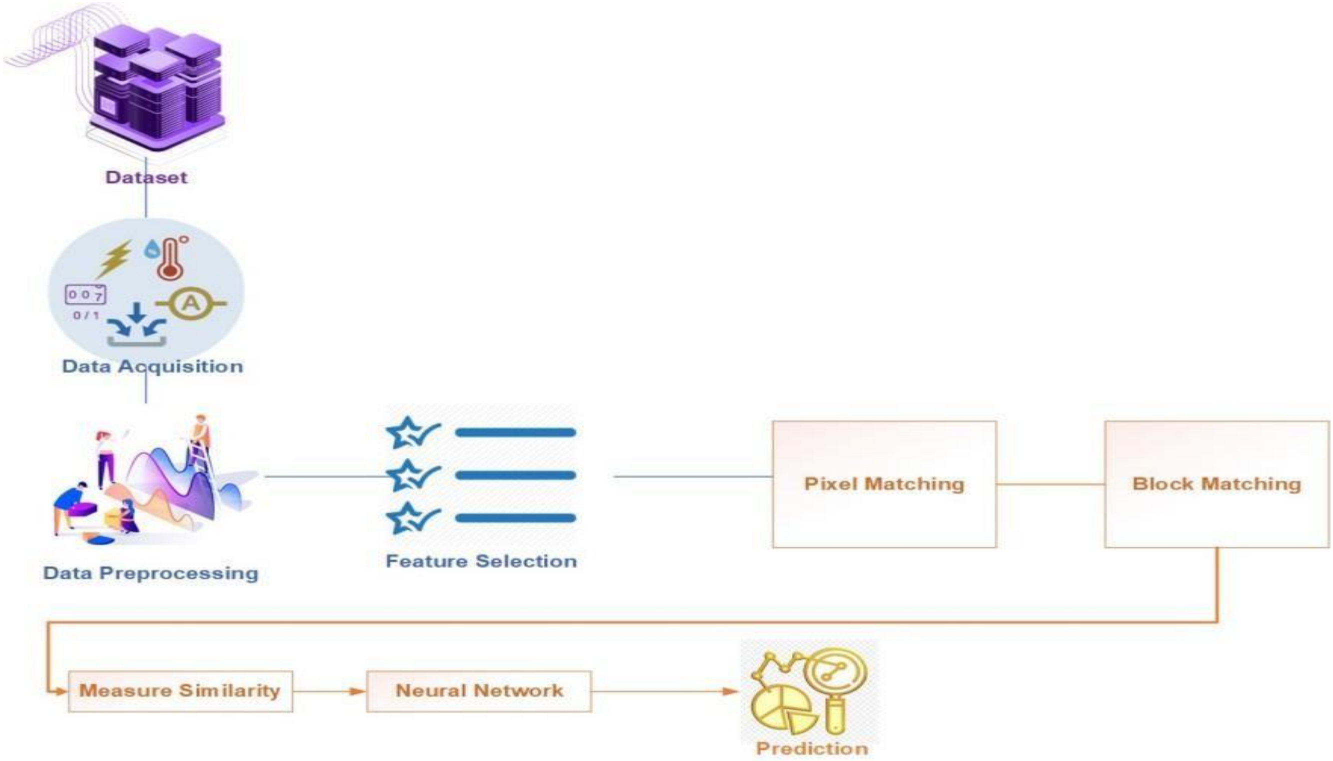

Fig. 1: Proposed Architecture Diagram

Advantages of Proposed System:

To improve the ensembling, a technique called the local mean method was used to reduce the image size. This approach effectively combines local and global features to classify malware and ensures that the model can generalize well to new data from the same distribution as the training set. Compared to the current method, this approach is more reliable, accurate, and generalizable. Moreover, it can significantly reduce the risk of false detection when dealing with a large volume of recently added data.

Algorithms:

Existing Algorithm: Multifaceted Behavioral Malware Variant Detection Model. Algorithm Advantages of Proposed Algorithm Transfer Learning Algorithm are improved performance at the baseline, Address issues including the lack of readily available labelled data and Cutting-edge Performance

Modules:

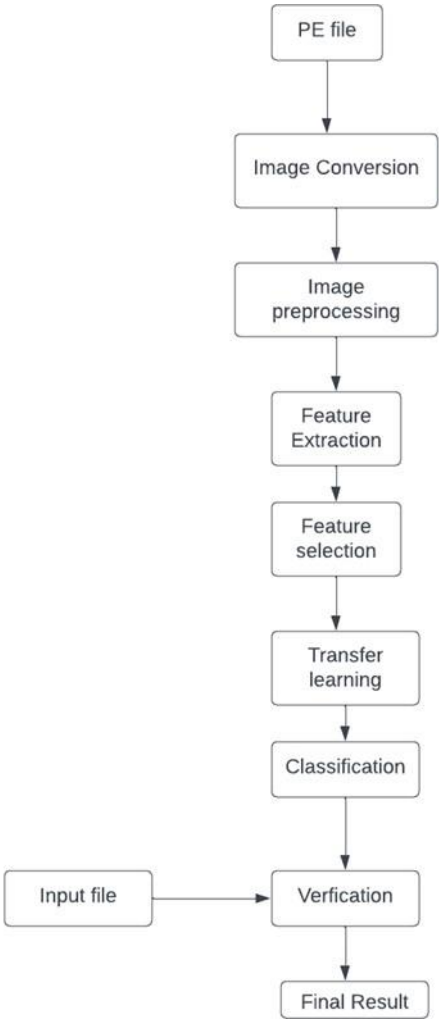

Fig. 2: Block diagram

(1) Image Preprocessing: Deep learning models performanceis dependent on the calibre and volume of data fed into the system. Dueto potential pre-existing noise and irregularity in the photos, raw data as input can hardly account for the highest achievableperformance of the model. Hence, a clear preprocessing flow is necessary to improve model training. The suggested model receives thePE binary files (either malicious or cleanware) as input. Each file contains a representation of its binary data in hexadecimal form.Each binary is transformed using a method that creates.png images from hexadecimal data. Each set of eight characters from a binary isfirst put in an array after each line has been scanned. The decimal equivalent of each byte is then calculated and placed in a different array. Every of the binary file's lines go through this conversion procedure again and again. A Python Imaging Library (PIL) library is used to visualize binary images from the array of decimal values.

(2) Feature Extraction: The feature learner known as the neural network, which usually has two parts and has a tremendous amount of learning the ability to autonomously extract key characteristics from input data. Feature extractor isthe initial stage, which includes a convolutional layer, layer pooling, and automated characteristic learning from raw data. The classification from the first section is then carried out by the completely connected layer using the learned attributes. iterative layer is made up of the individual values that represent the smallest input unit, whereas the output layer consists of as many outputs as there are categories in the specificclassification issue. By transforming one layer to the one before it, the convolutional layer conducts a convolution operation to small, localized regionsSpecifically, this is used to extract the feature from the original data. Convolutional layers are followed by pooling layers, which reduce the number of factors involved and the degree of computational complexity..

(3) Create Transfer Learning Model and Predict Malware: Thetraining data was divided into testing and training validating parts. Each iteration used a small number of Epochs. In total,% of the data were chosen for training, and% were kept for testing and validation. Both the last layer's parameters and the other layers' parameters have learning rates set to e-. Adamoptimizer and cross-entropy loss are utilised with a batch size of (i) Pooling Layer: Topology of the data has already been retained in feature maps when they are detected. Locational information consequently loses significance. Spatial invariance is achieved by applying the pooling process on feature maps with lower resolution. Every feature map in the pooling layer corresponds to a particular feature map in the layer beneath it. As a result, the current layer's feature mappings are equal to those in the prior layer. (ii) Fully Connected Layer: Many inner-product layers, including merging and pooling layers, are typically followed by a fully-connected layer. Each node (neuron) in the layer with complete connectivity contacts all the nodes in the layer below. By multiplying the nodes in the preceding layer by all of their weights, as well as by the activation function, the output of the node is calculated. (iii) Dropout Layer: During training, the activity levels of a few randomly selected neuronsare zeroed out using the regularisation approach known as dropout. Instead of relying on the prediction abilities of a small group of network neurons, this constraint drives the network to acquire more reliable features. This concept was further developed by Tompson et al. to convolutional networks with spatial dropout, which eliminates entire feature maps rather than single neurons.(iv) Batch Normalization Layer: The set of activations in a layer is normalised using batch normalisation, another regularisation technique. The batch mean is subtracted from each activation before being divided by the batch standard deviation to achieve normalisation. This normalising method is a common one used in the preprocessing of pixel values, coupled with standardisation.

CONCLUSION AND FUTURE WORK

Conclusion:

Despite numerous ongoing research projects aimed at malware detection and classification, malware continues to pose a significant danger in the online environment. Bypassing malware detection with escape strategies like code obfuscation, packing, etc. leaves detection methods useless. In order to detect and identify malware efficiently this study suggests a diverse deep forest model. The system aims to improve the current malware detection tools in three ways. First, D grayscale pictures are created from the PE binary files. Second, the pictures are processed in two stages: the cascade layering stage and the sliding window scanning stage. The scanning step of convolutional neural networks uses sliding windows to analyse each pixel, allowing for the consideration of important features that improve prediction.While the cascade layering step also uses layers similar to deep learning, it does not use backpropagation to create feature vectors. Third, cross validation performance is used to determine whether to continue or halt the layering process.

Future work:

Future research might involve using a threshold to detect unknown samples of untrained families.

REFERENCES

[1] S. Abijah Roseline , S. Geetha , Seifedine Kadry and Yunyoung Nam, "Intelligent Vision-Based Malware Detection and Classification Using Deep Random Forest Paradigm", 2020.

[2] R. Vinayakumar , Mamoun Alazab, K. P. Soman , Prabaharan Poornachandran and Sitalakshmi Venkatraman, "Robust Intelligent Malware Detection Using Deep Learning",2019..

[3] Aviad Cohen , Nir Nissim and Yuval Elovici, "MalJPEG: Machine Learning Based Solution for the Detection of Malicious JPEG Images", 2020.

[4] Yuntao Zhao , Wenjie Cui , Shengnan Geng , Bo Bo , Yongxin Feng and Wenbo Zhang, "A Malware Detection Method of Code Texture Visualization Based on an Improved Faster RCNN Combining Transfer Learning ", 2020.

[5] Jueun Jeon , Jong Hyuk Park and Young-Sik Jeong, "Dynamic Analysis for IoT Malware Detection With Convolution Neural Network Mode", 2020.

[6] Jinting Zhu , Julian Jang-Jaccard and Paul A. Watters"Multi-Loss Siamese Neural Network With Batch Normalization Layer for Malware Detection", 2020.

[7] Suyeon Yoo , Sungjin Kim and Brent Byunghoon Kang, "The Image Game: Exploit Kit Detection Based on Recursive Convolutional Neural Networks", 2020.

[8] Seoungyul Euh , Hyunjong Lee , Donghoon Kim and Doosung Hwang, "Comparative Analysis of Low-Dimensional Features and Tree-Based Ensembles for Malware Detection Systems", 2020

[9] Nuno Martins , Jos Magalhes Cruz , Tiago Cruz and Pedro Henriques Abreu, "Adversarial Machine Learning Applied to Intrusion and Malware Scenarios: A Systematic Review", 2020

[10] W. K. Wong , Filbert H. Juwono and Catur Apriono., "Vision-Based Malware Detection: A Transfer Learning Approach Using Optimal ECOC-SVM Configuration" , 2021.

[11] Michael L. Santacroce , Daniel Koranek and Rashmi Jha, "Detecting Malware Code as Video With Compressed, Time-Distributed Neural Networks" ,2020

[12] Q. Wang, W. Guo, K. Zhang, A. G. Ororbia, X. Xing, X. Liu, and C. L. Giles, Adversary resistant deep neural networks with an application to malware detection, in Proc. , rd ACM SIGKDD Int. Conf. Knowl.

[13] S. Wu, P. Wang, X. Li, and Y. Zhang, Effective detectionof Android malware based on the usage of data ow APIs and machine learning, Inf.Art. no. B56.

[14] F. Ahmed, H. Hameed, M. Z. Shaq, and M. Farooq, Using spatio- temporal information in API calls with machine learning algorithms for malware detection, in Proc. , nd ACM Workshop Secur. Artif. Intell.

[15] Y. Ding, X. Xia, S. Chen, and Y. Li, A malware detectionmethod based

[16] F. Ahmed, H. Hameed, M. Z. Shaq, and M. Farooq, Using spatio- temporal information in API calls with machine learning algorithms for malware detection, in Proc. , nd ACM Workshop Secur. Artif. Intell..

[17] P. L. Bartlett, The sample complexity of pattern classication with neural networks

[18] L. Nataraj, A Signal Processing Approach To malware Analysis. Santa Barbara, CA, USA: Univ. California 2020.

[19] H. S. Anderson and P. Roth. (,). EMBER: An open dataset for abs.

[20] W. Wang, M. Zhao, and J. Wang, Effective Android malware detection with a hybrid model based on deep autoencoder and convolutional neural Aug

[21] P. Trinius, T. Holz, J. Gobel, and F. C. Freiling, Visual analysis of malware behavior using treemaps and thread graphs, presented at the , th Int. Workshop Vis. Cyber Secur., Atlantic City, NJ, USA

[22] T. A. Alghamdi, Convolutional technique for enhancing security in wire- less sensor networks against malicious nodes, Hum.-Centric Comput. Inf 2020. ,

[23] Y. Zhao, Deep learning: , days of practical caffe, Electron.Ind. Press, Jul