Malware Classification Using Deep Learning

Weerasinghe D M G S.
faculty of computing
Sri Lanka Institute of Information Technology
malabe, Sri Lanka
it21829956@my.sliit.lk

***Abstract*— The review covers a wide range of approaches used by CNNs, RNNs, or hybrid systems in the field of malware classification when utilising deep learning methodologies. We will only examine the most recent advancements in feature extraction and model efficacy in an effort to fully comprehend issues arising from dynamic malware patterns. The review demonstrates how deep learning approaches can achieve state-of-the-art malware detection performance; it also emphasises issues concerning dataset quality, computational cost, and adaptability to emerging threats. The paper will provide insights into potential future research directions that can improve the robustness and functionality of malware classification frameworks.Keywords—malware classification, deep learning, malware analysis, artificial intelligence of malware classification**

I. Introduction

The Malware-associated risks have evolved in complexity that has made it imperative to employ detection measures that are equally evolved and far-reaching from traditional signature-based methodologies. In evolving as a powerful tool to offer the ability to learn complex patterns from very large data sets, in recent times, deep learning has now found its way into malware classification too. This review paper studies in detail the state of the art regarding deep learning applied to the realm of malware categorization. The primary purpose of this study is to focus on several deep learning architectures, including convolutional neural networks (CNN), recurrent neural networks (RNN), and their applicability in the detection task. The rest of this manuscript is organized as follows: the next section opens with a detailed discussion of techniques adopted in malware classification, followed by a review of popular work conducted in malware classification and concludes with a discussion on the challenges and future direction that should be taken within this area.

II. Methodology

For this review, I systematically searched in peer-reviewed journals, conference proceedings, and relevant databases, such as IEEE Xplore, ACM Digital Library, and ScienceDirect. The search string consisted of the keywords 'malware classification,' 'deep learning,' 'CNN,' 'RNN,' and 'cybersecurity.' Selection criteria were relevance to the study, importance of the citations, novelty, and original contribution to the subject area. The structure of the paper is given here: deep learning methodologies, types of malware studied, reported benchmarks—all focused on obtaining the best snapshot of all key advances and challenges in malware classification using deep learning techniques.

III. Review of Literature

The following section presents an overview of related works with respect to deep learning-based malware classification and the key works that have been made in the field. For instance, Cakir and Doggu (2018) have achieved good classification for opcode-based malware by using a combination of Word2Vec and Gradient Boosting Machine, but their overreliance on very outdated datasets reduces the generalizability of their results. For instance, the very comprehensive survey by Ucci et al., in 2019, where the need for updated data sets and challenges from anti-analysis techniques emerged, many more are using Markov images with deep CNNs like the one from Yuan et al. in 2020 and others, where the best accuracy up to now yields 99.26% but still with problems like the variability in data sets' distributions. While the general trends that this review indicates point to hybrid models, those that marry static analysis techniques with dynamic ones, it also underlines the promise of newly emerging techniques such as transfer learning and adversarial training for addressing current limitations.

[1]. The research article, "Malware Classification Using Deep Learning Methods," authored by Bugra Cakir and Erdogan Dogdu and released in 2018, focuses on the key problem of automated malware identification in cybersecurity. The work utilizes deep learning methodologies, notably using Word2Vec for extracting features and Gradient Boosting Machine (GBM) for classifying, to analyze malware based on their opcodes. This study is unique because it utilizes Word2Vec, a technique often used in natural language processing, to represent malware assembly code. This approach improves the model's capacity to understand the structural and meaning-based connections within the data. The findings indicate a high level of accuracy in categorization, with a success rate of up to 96%, which confirms the usefulness of the suggested technique. Nevertheless, the research encounters two notable limitations: firstly, the dataset employed is antiquated, thereby potentially failing to capture present-day malware patterns; secondly, although GBM demonstrated encouraging outcomes, contemporary models such as Convolutional Neural Networks (CNNs) or Recurrent Neural Networks (RNNs) might yield superior performance in effectively managing the intricacies of malware data. Updating the dataset and conducting experiments with sophisticated deep-learning architectures can tackle these challenges and improve the model's resilience and precision.

[2]. In the paper "Survey of Machine Learning Techniques for Malware Analysis" by Daniele Ucci, Leonardo Aniello, and Roberto Baldoni, the authors address the escalating complexity and volume of malware, presenting a comprehensive overview of how machine learning techniques are employed for malware analysis, particularly focusing on Windows Portable Executables (PEs). The survey categorizes existing research based on analysis objectives, extracted features, and utilized machine learning algorithms. Objectives include malware detection, similarity analysis, and category detection, while features span from byte sequences and opcodes to API/system calls and network activities. The paper also highlights current challenges such as anti-analysis techniques employed by malware, the selection of relevant features, and dataset limitations. Additionally, it introduces the concept of malware analysis economics, which examines trade-offs between analysis accuracy, speed, and cost. The authors argue for

the need for updated and well-labeled datasets to improve reproducibility and effectiveness in malware analysis and suggest potential research directions like malware attribution, triage, and prediction of future variants. This survey is crucial for researchers and practitioners aiming to leverage machine learning for robust and scalable malware defense mechanisms.

[3]. Ucci, Aniello, and Baldoni. (2019) publishes a study in their paper Survey of machine learning techniques for malware analysis. The authors discuss the growing problem of malware which is becoming more sophisticated and pervasive. They survey many machine learning algorithms in order to find an appropriate classifier for use in malware analysis generally and for Portable Executable files on Windows systems specifically. Ucci, Aniello, and Baldoni categorise the surveyed studies according to the aims they addressed, the features that were used as input for classification and the algorithm(s) that were employed. The chapter also notes that new malicious software is released at such a rate that new solutions are required to determine zero-day vulnerabilities with similar speed or more powerful techniques will need to acquire the same results in a shorter time (if it becomes economically feasible). This concept of ‘malware analysis economics’ can involve trade-offs between conflicting metrics such as accuracy vs cost or privacy vs efficiency. It is concluded that while there are many promising results published using machine learning as an aid, especially as a detection mechanism used alongside other tools in malware discovery, there remain several large challenges before machine learning is likely to replace any existing entire security toolset like antivirus tools or static disassemblers/ de-compilers/ debuggers etc (e.g.) both with respect to quality supervised training data sets from which features can be distilled from Portable Executable files as well as how this distillation is done (what classifies something not relevant?). There are several shortcomings related to these issues with respect particularly to unsupervised -organising methods: clustering (/grouping), with pruning having an enhanced trend over growing; thus most detected similarities between malicious code would appear trivial resulting in effectively less useful information about new threats than otherwise possible. Specifically how -based supervised classifiers function is not made clear either so nor how they overcome potentially confounding duplication(s) of certain bits – esp. – of program executables in training instances yet apparently avoid in doing so misclassification during live code execution instances.

[4]. In their 2020 study titled "Byte-level malware classification based on markov images and deep learning," Baoguo Yuan, Junfeng Wang, Dong Liu, Wen Guo, Peng Wu, and Xuhua Bao address the critical problem of efficiently and accurately classifying malware due to its rapid evolution and increasing sophistication. Traditional machine learning approaches are hindered by the necessity of feature engineering and their inefficiency in handling large volumes of malware data. The authors propose a novel methodology called MDMC (Markov-based Deep Malware Classification), which converts malware binaries into Markov images using byte transfer probability matrices and employs deep convolutional neural networks (DCNNs) for classification. This method significantly improves classification accuracy, achieving up to 99.264% on the Microsoft dataset and 97.364% on the Drebin dataset. However, the reliance on labeled training samples remains a challenge, and the technique's performance might vary with different dataset distributions. Despite these drawbacks, MDMC presents a robust framework for malware classification, outperforming existing methods based on gray images and deep learning.

[5]. The paper deals with the rapid growth of malware varieties, and the substantive threat they pose to information security. The authors propose in their paper a machine-learning-based malware analysis and classification solution. Their system has three modules that offer data processing, decision making, and new virus detection. Originality in the work: grey-scale picture, opcode n-gram, and import function-based feature extractions applied. The accuracy of the classification turned to be 98.9%. Their approach turned out to be able to detect 86.7% of new malware. However, there are some drawbacks of the research: first of all, system performance directly depends on the quality and variability of training datasets, second of all, issues in processing high-dimensional data exist. Their work contributed a great deal to the field of malware detection and classification but, at the same time, gave a hint that future improvements would be necessary to compensate for these limitations.

[6]. In the paper "Ensemble Malware Classification System Using Deep Neural Networks" by Barath Narayanan Narayanan and Venkata Salini Priyamvada Davuluru, published in 2020, the authors address a very critical aspect of malware classification. This paper attempts to address the problem of escalating sophistication and volume of malware, which is turning out to be a mammoth threat to cybersecurity. The authors have proposed an ensemble classification system where Convolutional Neural Networks and Long Short-Term Memory networks are combined to distinguish malware programs. Their methodology consisted of using the dataset obtained from the Microsoft Malware Classification Challenge, BIG 2015. The compiled files in this dataset are visualized as images in view to classification using CNN, and the assembly files are fed into LSTM networks. The originality of this study is an ensembling approach, which will integrate features extracted by CNNs and LSTMs that will then be classified using support vector machines or logistic regression. The results are amazing: accuracy obtained was 97.2% with LSTM networks, 99.4% for CNN architectures, and a total accuracy of 99.8% using the proposed ensembling method, setting a new benchmark in malware classification. The research has a few drawbacks, such as high dependence on the availability of large volumes of heterogeneous and high-quality

training datasets and processing high-dimensional data efficiently remains a challenge. To avoid these limitations, this research markedly pushes forward malware detection and classification with deep learning techniques and potentially holds huge promise for improving cybersecurity defenses.

[7]. The paper "A comprehensive survey on deep learning-based malware detection techniques" by Gopinath M. and Sibi Chakkaravarthy Sethuraman, published in 2023, raises the challenging problem of developing malware threats and fails traditionally applied techniques of detection. It is basically oriented to the research problem of conventional methods for malware detection that cannot keep pace with growing malware sophistication and quantity. It surveys some of the recent advances in deep learning approaches for malware detection. Some of the discussed methodologies include the use of grayscale images, opcode n-grams, and import functions for feature extraction. This paper thus describes several new techniques based on DL and explores their performance in detecting new variants of malware, which is much better compared to traditional approaches. Results indicate that such models can make fast, very accurate predictions of malware, thus greatly raising detection rates. Conversely, the paper highlights several deficiencies: dependence on high quality and variety in the training datasets, and challenges related to high-dimensional data processing. This comprehensive survey underlines the potential of DL for pushing the boundaries of the current state of malware detection and also shows how much more research needs to be done to mitigate such limitations in this domain.

[8]. The paper "Ensemble Malware Classification System Using Deep Neural Networks" by Barath Narayanan and Venkata Salini Priyamvada Davuluru, published in 2020, related to the timely problem of malware classification in conditions of fast evolution of malicious software. The authors present a new ensemble classification system in which Convolutional Neural Networks and Long Short-Term Memory networks are applied to increase the accuracy and efficiency of malware detection. In this research, Microsoft's dataset for the Malware Classification Challenge, BIG 2015, is used, including assembly and compiled files for every malware instance. The novelty in this research work lies in the fact that it uses CNNs to process compiled files visualized as images and LSTMs for the analysis of sequences of opcodes in assembly files. Their ensemble approach combines features extracted from these two deep architectures using support vector machines or logistic regression, hence achieving very high accuracy rates: 97.2% for LSTM, 99.4% for CNN, and an overall accuracy of 99.8%. The authors also mention the limitations of this research, such as dependency on high-quality labeled datasets and computational resources, keeping in view that much improvement is still needed to handle large-scale and diverse malware samples. This will, therefore, be a comprehensive framework that gives very useful insights and a robust methodology to enhance the capability of malware detection in cybersecurity applications.

[9]. The paper "Robust Intelligent Malware Detection Using Deep Learning" by R. Vinayakumar, M. Alazab, K. P. Soman, P. Poornachandran, and S. Venkatraman, published in 2019, relates to a very important aspect of malware detection in the digital age. The problem statement of the research revolves around the inadequacy of traditional malware detection methods that fail to identify new and evolving malware in real time. This is on account of their reliance upon static and dynamic analysis for malware signatures. The authors have proposed a scale deep learning-based framework called ScaleMalNet, which empowers image processing techniques to strengthen zero-day malware detection. This includes, but is not limited to, the performance evaluation of classic machine learning algorithms and deep learning architectures on several public and private datasets. To this end, this work makes a new contribution because of using a hybrid approach that loads static, dynamic, and image-processing-based techniques in robust and scalable malware detection. Results show that deep learning architectures proposed in the study outperform traditional machine learning methods with a reasonable improvement in accuracy and efficiency. However, it also points out the high computational requirements and large training datasets involved. Overall, this research helps enhance the capability of malware detection, hence opening avenues for more effective solutions in real-time cybersecurity.

[10]. The paper "DAEMON: Dataset/Platform-Agnostic Explainable Malware Classification Using Multi-Stage Feature Mining" is by Ron Korine and Danny Hendler, published in 2021. In their research, authors set the problem that malware variants are developing so fast and starting to bypass signature baselines. Authors propose a new malware classifier, DAEMON, which is dataset-agnostic and platform-aided. This classifier uses a multi-stage feature mining approach to extract platform-independent features, making it it very adaptable to different datasets without any algorithmic changes or parameter tuning. Shows high accuracy in testing with large-scale datasets of x86 binaries. In the meanwhile, the experiment shows that it obtains a high precision across several dataset, with malicious Android application examples. One of the main novelties of this work is that it focuses on explainability by means of the features used by DAEMON to understand the distinctive behavior of the families of malware. The results had shown that it was way better than the other classifiers to correctly classify this malware. The study, therefore, also mentions some disadvantages: for example, it may reduce the efficiency of processing very large datasets because of the extensive feature mining process. In conclusion, DAEMON greatly improved the field of malware classification by providing a strong, explainable solution fit for different environments.

[11]. In the paper, the authors propose a solution to one of the critical problems of malware against Android. It presents a novel approach to malware family detection by exploiting audio features. The researchers converted Android application files into audio files in .wav format and extracted features from them based on audio. They applied four feature selection methods for finding out the most discriminative features: CFS-Subset, ReliefF, Information Gain, and Gain Ratio. The novelty of this study is the usage of audio-based features against malware. Although this field of study is not as explored as the traditional static or image-based analysis, the experimental results proved the effectiveness of this approach. In particular, the ReliefF method combined with K-Nearest Neighbors gave the highest F-measure score of 0.966. Nevertheless, the authors also pin down some drawbacks of the technique: specifically, dependence on the quality of the audio transformation process and computational overhead for the extraction of audio features. The contribution this research brings to malware detection is huge, as it brings a completely new view and promising results, yet with an indication of further areas of improvement.

[12]. The paper by R. Korine and D. Hendler, 2021, "DAEMON: Dataset/Platform-Agnostic Explainable Malware Classification Using Multi-Stage Feature Mining," is about a very important issue of malware classification in the fast-changing landscape of cyber threats. It tries to locate a research problem in implementing, a robust and explainable malware classification system, which is not bound to specific datasets or platforms. The methodology used incorporates multi-stage feature mining, including static and dynamic analysis techniques to extract relevant features from malware samples. Therefore, it is new in that it applies multistage feature mining in a platform-agnostic way, hence improving generalization ability on different environments or datasets. The results showed high efficiency and robustness in the classification and analysis of a variety of diverse malware families, with very significant improvements over previous techniques. The authors still pointed out one drawback: the fact that the multistage analysis adds some complexity to the approach and computational cost, likely reducing its applicability in real-time scenarios. This research is useful for cybersecurity since this paper provides a breakthrough tool to classify malware, ensuring both accuracy and explainability.

[13]. The paper "Fusing Feature Engineering and Deep Learning: A Case Study for Malware Classification," by Daniel Gibert, Jordi Planes, Carles Mateu, and Quan Le, 2022, focused on one of the most challenging problems posed to cybersecurity: malware classification. One of the main research problems addressed is related to traditional signature-based and heuristic-based approaches that fail in the detection of new, sophisticated malware threats that are very different. The authors of this paper have given a hybrid methodology that merges manual feature engineering along with deep techniques in learning. What the authors have come up with is quite unique: integrating expert-defined features with deep learning-extracted features for the classification of malware with enhanced accuracy. More specifically, they use N-gram features from assembly language instructions and bytes of malware, texture patterns from grayscale images, and shapelet-based features from structural entropy. Their results against the Microsoft Malware Classification Challenge dataset achieve state-of-the-art performance in classification accuracy with a value of 99.81% and logarithmic loss of 0.0040. The study indicates drawbacks to this approach: high dimensionality might be a source of overfitting in case of combined features being too large, and it is highly dependent on the quality and variety of a training dataset. While this significantly enhances malware detection and classification, it still requires further work on the optimal selection of features and overfitting concerns.

[14]. The paper "Transfer Learning Approach for Malware Images Classification on Android Devices Using Deep Convolutional Neural Network" by Zahraddeen Bala, Fatima Umar Zambuk, Badamasi Ya'u Imam, Abdulsalam Ya'u Gital, Fatima Shittu, Muhammad Aliyu, and Mustapha Lawal Abdulrahman, published in 2022, describes a solution to the increasing threat of malware attacks on Android devices. Conventionally, signature-based approaches used to identify malware are proven to be useless against the increased complexity and high amount of malware. The authors present an Android malware image classifier that uses transfer learning on CNN architectures in this regard. The approach will leverage the pre-trained model on large datasets of images and reduce the need for extensive feature engineering from scratch. The novelty here is to represent malware binaries as grey-scale images, while a fine-tuned pre-trained ResNet model is used to set them for classification tasks. Experimental results showed that the proposed model has a high detection accuracy of 97.24%, much better than that of other methods, such as the hybrid DBN-GRU with 96.82%. Obviously, that reduces training time and largely improves model accuracy. However, it also has drawbacks: maybe the computational cost of the hybrid model could still be very large, and it needs further optimization in order to handle small-scale data effectively. Notwithstanding, this research has pointed out the potential of transfer learning to enhance the detection of malware on Android devices.

[15]. The paper "AI-HydRa: Advanced hybrid approach using random forest and deep learning for malware classification" by Suyeon Yoo, Sungjin Kim, Seungjae Kim, and Brent Byunghoon Kang, 2021, is devoted to the very serious problem of malware propagation via the Internet. To be more specific, the problem in the literature lies in the fact that machine learning-based models have different detection rates due to differences in features and classification methodologies. The methodology incorporates a hybrid decision model that combines random forest with deep learning, having 12 hidden layers, in which static and dynamic features are

utilized together with rules of voting for improving accuracy. It is rather the hybrid approach—combining machine learning and deep learning models—that would bring improved detection rates while minimizing the false positives. The results have a quite promising improvement in the detection rate, where it reaches a very high value of 85.1% detection at a very low false positive of 0.006. Nevertheless, two major limitations that bound the model's effectiveness were: computational complexity of feature extraction and the possibility of being vulnerable to anti-VM attacks. Notwithstanding the drawbacks, the Hybrid model portrayed better results than traditional single classifier models for malware classification.

[16]. This paper, published in 2018 by Quan Le, Oisín Boydell, Brian Mac Namee, and Mark Scanlon, addresses the challenge of malware detection and classification using deep learning techniques that require no expert domain knowledge. Formulation of the research problem: Traditional approaches to malware detection are manual and knowledge-intensive with respect to extracting signatures and behaviors from malware. The authors propose a completely data-driven approach using a deep learning model for learning complex patterns and features from raw binary files. The authors represent the raw binary files as one-dimensional sequences and use a Convolutional Neural Network combined with a Bidirectional Long Short-Term Memory network for classification.. This allows not having to worry about complex feature engineering and makes the approach really accessible to people who might not be domain experts. It is totally new in its simplicity, with raw bytecode used as input and no need for domain-specific preprocessing. The results are impressive: this proposed model classifies malware into nine distinct classes at a very high accuracy of 98.2%. Another underline of the model's efficiency is the fact that each binary file was processed in just 0.02 seconds on a regular desktop workstation.It, however, also highlights the disadvantages in terms of a probable loss of semantic meaning in the bytecode because of the down-sampling process and the one-dimensional representation. This work has been able to come up finally with a solution that realizes a high mark in the domain of malware classification, making classifying malware practical and highly improving efficiency while dispensing with a need for deep domain expertise.

[17]. A paper by Ahmed Bensaoud, Jugal Kalita, and Mahmoud Bensaoud entitled "A survey of malware detection using deep learning" was published in the Machine Learning with Applications journal in 2024. It focusses attention to the challenging issue of malware detection and categorisation, basically highlighting that in the current sector, there is not a single solution perfect in itself. The authors present a summary of some of the recent developments in malware detection utilising deep learning approaches on several operating systems such as MacOS, Windows, iOS, Android, and Linux. In the review, it is given how effective the DL classifiers are, yet unable to explain their judgements for developers, thus the necessity for Explainable Machine Learning, sometimes referred to as Interpretable Machine Learning programs. The research discusses numerous concerns linked with the adversarial assaults impacting DL models that impair their generalization capabilities. A main feature of this study is to do an extensive investigation of state-of-the-art DL models across distinct malware datasets, offering insights relevant to performance and problems. The findings reveal that, despite great accuracy in malware detection obtained by DL classifiers, there are limitations; for example, it shows computational cost of the defensive mechanisms and susceptibility of the models to adversarial assaults. The authors conclude the work by urging for additional research toward efficiency and resilience in malware detection using DL models.

[18]. In the 2024 paper "MADRAS-NET: A Deep Learning Approach for Detection and Classification of Android Malware Using Linknet," Yi Wang and Shanshan Jia address a very important topic connected with the detection of Android malware. The overall subject of the research is aimed at growing trends and the complexity of Android malware, which will surely one day become a serious concern for cybersecurity itself. The authors propose MADRAS-NET, a deep learning framework that uses LinkNET for the classification of Android malware. Their methodology is to preprocess input data using Max Abs Scaler, and then classify it using the LinkNET architecture. This new method differentiates between benign users, Penetho malware, and FakeAV malware. The experimental results for MADRAS-NET have been outstanding, with accuracy going up to 99.81%, when most other models such as LSTM, GAN, and DBN have scored a mere 93.11%, 94.42%, and 96.75%, respectively. This study originally combines the Max Abs Scaler with the LinkNET architecture for better detection of malware. A drawback could be that its performance would not be reliable for rarer types of malware, so more work is needed to deal with a broader spectrum of threats. The overall contribution of MADRAS-NET is toward enhancing the detection and classification of Android malware; it showcases the potential of deep learning techniques in improving cybersecurity measures.

[19]. In the paper "From Malware Samples to Fractal Images: A New Paradigm for Classification," Ivan Zelinka, Miloslav Szczypka, Jan Plucar, and Nikolay Kuznetsov presented a new paradigm in the classification of malware using fractal geometry in the year 2024. The paper addresses the question of how to effectively distinguish malware from goodware, which are malicious software of growing complexity. Traditional approaches typically rest on static or dynamic code analysis, which is a little narrow in the range of its features. These authors have come up with representations that transform the dynamic sequence of API function calls by malware into fractal patterns, Julia sets, and then use such visualizations to perform classification through deep learning networks. The novelty of this approach comes with the application of

fractal geometry to the visualization of malware, which presents an absolutely new line of research in cybersecurity. Their experiments demonstrate a very promising accuracy in the classification using their fractal-based approach on a large dataset supplied by ESET.However, the paper has also included in the discussion the downside to the said approach: the overly high processing cost to create and work with fractal images and the further development needed for better accuracy and productivity. This is still a work that paves the way for new horizons of the malware analysis and classification, where compatibility between certain mathematical ideas and the highest level of computation means can be showcased.

[20]. The paper "Android malware detection and identification frameworks by leveraging the machine and deep learning techniques: A Comprehensive Review" by Santosh K. Smmarwar, Govind P. Gupta, and Sanjay Kumar is related to the increasing danger that malware poses to Android-based systems, IoT devices, and other connected kinds of systems. This research problem arises because traditional signature-based methods of malware detection are unable to counter these sophisticated evasion methods of modern malware with techniques like obfuscation, packing, and encryption. The authors report a deep literature review in which they mainly divide existing works into three parts: techniques of feature selection, machine-learning-based methods, and deep-learning-based methods. They underline that one of the novelties proposed herein is the hybrid analysis method in which static and dynamic analyses are combined, improving the detection rate. This review identified a number of novel frameworks in ML and DL which have proven very promising in improving the accuracy of malware detection. However, drawbacks like high computational cost, inefficiency in the processing of high-dimensional data, and class imbalance issues have been discussed. The study concludes with the need for further research to address such limitations and construct more robust and efficient malware detection frameworks. It has, in general, contributed a valuable synthesis of current methodologies but outlined at the same time future research directions in order to enhance malware detection and identification.

[21]. In the paper "An inception V3 approach for malware classification using machine learning and transfer learning," Mumtaz Ahmed, Neda Afreen, Muneeb Ahmed, Mustafa Sameer, and Jameel Ahamed present their research in this very domain. Basically, the paper focuses on the ever-increasing problem of malware attacks that have turned into a potential threat to cybersecurity. The authors proposed a technique that constructs malware signatures as 2D image representations and applied deep learning methods to classify these signatures. Logistic regression, artificial neural network, convolutional neural network, long short-term memory, and finally, a transfer learning strategy using InceptionV3 were the applied methodologies. Such a key novelty in the work is transfer learning combined with deep learning, which provides an opportunity to enhance classification accuracy with the help of pre-trained models. It is shown that the accuracy achieved 98.76% using a test dataset in accordance with the InceptionV3 model. However, some drawbacks are also mentioned in this research: large computational resources should be spent to train deep neural networks, and to perform transfer learning, large and labeled datasets are needed for good performance. This paper presents a large contribution of potent deep learning techniques in enhancing malware detection and classification.

[22]. In the 2024 publication, S. Poornima and R. Mahalakshmi contributed to a very critical issue known as "Automated Malware Detection Using Machine Learning and Deep Learning Approaches for Android Applications." Due to the tremendous increase in usage, there has been increased cyber threats benchmarking with the Android platform. They have proposed a new framework, MAD-NET, which uses Deep Belief Networks to accurately detect and classify malware. The methodology followed here is feature extraction using the CICAndMal2017 dataset, which again can be divided into signature-based and behavior-based data. Afterwards, the extracted features will be processed and as inputs to the DBN model for classification. What is new in this approach is that it uses a hybrid analysis technique, bringing together both static and dynamic features in order to be more accurate. The results obtained are impressive—99.83% overall accuracy for DBN against models like ANN, GAN, and LSTM. The study also points toward some drawbacks of high computational complexity and heavy feature engineering in the model. However, considering both of these issues to a great extent, the proposed MAD-NET framework finally leads to the development of a robust malware detection system on Android devices. Further work may be oriented toward decreasing the computational burden and further improving processes related to feature selection.

[23]. This is a research paper entitled "A study of the relationship of malware detection mechanisms using Artificial Intelligence" written by Jihyeon Song, Sunoh Choi, Jungtae Kim, Kyungmin Park, Cheolhee Park, Jonghyun Kim, and Ikkyun Kim, published in 2024. The authors have put forth a complex and evolving problem regarding malware detection and how AI can be used to enhance the detection and classification of varied malware types. The authors have tried to present the current state of AI-based malware detection mechanisms in some organized way, focused on shallow and deep learning models. The methodologies applied in this study are the state-of-the-art review of the literature, the classification of mechanisms related to detection, and developing a taxonomy for malware detection criteria. The paper is furnished with a table

for classification and a flow chart showing the relationships and citation paths between a large number of studies, which provides an overview of the situation regarding the studies in insight. It is also among the novelties of this research that the overall contents related to malware detection methodology with AI are organizationally so well detailed as to help understand primary contents and performance of various features and models. In addition, it is also outstanding in that the research work has listed related works by year, explaining the citation relationship, which offers a clear perspective of how the field has evolved.The results of this study represent the high detection accuracy and performance of AI models in malware detection, with an emphasis on the efficacy of different feature extraction methods and model learning methods. The authors of this paper clearly specified the weaknesses in this approach: the painful task of collecting and labeling large datasets, and comparing performance across different detection mechanisms remains challenging because the datasets vary as do the evaluation metrics. There is no doubt that the paper enriches the literature by way of the succinct summarization of recent research trends and the very clear outline of future directions toward the negation of the current limitations in AI-based malware detection.

[24]. This work, by Shoayee Dlaim Alotaibi et al., "Bioinspired Artificial Intelligence-Based Android Malware Detection and Classification for Cybersecurity Applications," 2024, presents a breakthrough in the development of malware detection and classification against Android devices; this therefore offers an improved level of cybersecurity. The authors have combined an improved cockroach swarm optimization algorithm for feature selection, a bidirectional gated recurrent unit model for malware detection, and an arithmetic optimization algorithm for hyperparameter tuning. The originality here is how bioinspired algorithms are integrated with deep learning to elevate the approach of detecting and classifying Android malware. The BAI-AMDC technique was evaluated with the CICAndMal2017 dataset and had an accuracy average of 99.83%. However, according to the authors, the study had some limitations in the sense that threats can adapt themselves in real-time and continuous refinement is required in order to be able to cope with the emerging malware variations. Although somewhat promising for the detection of Android malware, the BAI-AMDC system generally needs further development in the light of current limitations.

[25]. The research document "On the Resilience of Shallow Machine Learning Classification in Image-based Malware Detection" by Rosangela Casolare, Giovanni Ciaramella, Giacomo Iadarola, Fabio Martinelli, Francesco Mercaldo, Antonella Santone, and Michele Tommasone addresses the challenge of malware detection in real-world environments with the help of shallow machine learning models. The authors have gone a step further in probing the resilience of such models in detecting malware that was unseen during the training phase by rendering Android application binaries in grayscale and RGB images and extracting features for classification. In this paper, the authors have trained several shallow supervised machine learning algorithms like Random Forest, J48, and REPTree and evaluated them for their performance over different time periods. This work is novel in that it brings forth temporal resiliency aspects of malware detection models, which have not been very evident until now, showing that model effectiveness wanes off as the gap between training and testing samples increases temporally. Results indicate that models trained on older malware samples struggle to detect newer variants. This paper thus reflects the need for constant updating and improvement of malware detection techniques if they are to be effective over a long period. The authors could, however extend deeper learning models and further integrate more features for more improvement in terms of resiliency and accuracy in detection.

[26]. The paper "Machine Learning for Android Malware Detection: Mission Accomplished? A Comprehensive Review of Open Challenges and Future Perspectives" by Alejandro Guerra-Manzanares, 2024, performs a critical reassessment of the state of affairs of machine learning-based Android malware detection. This is accomplished through the rectification of the belief that high-performance metrics of different studies have already sufficed in identifying Android malware. Literature was insightfully scoured for major challenges that still remain unabated and are the causes of ineffective malware detection in the long run.
It reviewed and qualitatively analyzed more than 230 papers on Android malware detection. The challenges are, according to Guerra-Manzanares, problems in five major domains: use of outdated and imbalanced datasets; mistaken assumptions of consistency across different platforms; overlooking concept drift; shallow exploration of model security; and too much attention toward model performance, as opposed to model understanding and explainability. Such innovation is at the heart of this work, relational and qualitative in its assessment of the literature, giving voice to several relevant blind spots that do not seem to be focused on dataset quality or adaptive measures against concept drift. Results from this in-depth analysis demonstrate that the problem related to Android malware detection is far from being solved, and there are many discrepancies between data representativeness, model robustness, and performance in the long run.
Some major disadvantages are connected with the use of old datasets like MalGenome and Drebin, which, as it was noted earlier, do not represent today's threat landscape, and continuous usage of static features instead of dynamic/hybrid ones, thus allowing proposed solutions barely to fight against obfuscation and encryption techniques used by modern malware. In summary, Guerra-Manzanares contributes valuable

insight together with future research directions into the development of more efficient and robust Android malware detection systems. This review underlines the fact that further studies have to be conducted for improvements in methodologies in order to meet new challenges.

[27]. The paper "Adversarial superiority in android malware detection: Lessons from reinforcement learning based evasion attacks and defenses" by Hemant Rathore, Adarsh Nandanwar, Sanjay K. Sahay, and Mohit Sewak, published in 2023, resolves a pressing puzzle related to how one could build a robust Android malware detection model resilient against adversarial attacks. The problem statement is how most of the constructed models for malware detection are very prone to adversarial attacks, which may bring down their efficiency considerably. The problem was solved by generating thirty-six malware detection models that had two features and eighteen classification algorithms. They then developed two novel reinforcement learning-based evasion attacks to run these models: TRPO-MalEAttack and PPO-MalEAttack. The average fooling rates for such highly efficient attacks were 95.75% and 96.87%, respectively, at very small perturbations that much reduced models' accuracies. What is new in this research, however, is the MalVPatch defense strategy in adversarial retraining to improve the robustness of the model. With improved adversarial robustness, the MalVPatch defense increased the average detection accuracy enough to lower the fooling rate down to 2.49% for TRPO-MalEattack and 3.77% for PPO-MalEattack. These results clearly show the relevance of adversarial robustness in malware detection, evidencing how one advanced model can become easily fooled without proper defenses. Most of this work refers to white-box attacks; therefore, generalizability to defense against other attacks remains unexplored. Moreover, it was based on features that had already been extracted outside of static features; therefore, it may further limit the models' applicability in dynamic environments. The current research explains the critical nature of adversarial robustness testing of the models for malware detection, and rather quite a promising avenue for defense mechanisms with a clear path to future research on resilient cybersecurity solutions.

[28]. The paper by W. K. Wong, F. H. Juwono, and C. Apriono, 2021, "Vision-Based Malware Detection: A Transfer Learning Approach Using Optimal ECOC-SVM Configuration", deals with one of the most challenging problems in malware detection, that is, inventing new techniques to raise malware detection. The main research problem addressed in the paper is the need for effective methods for malware detection, which would be able to adapt to new and continuously changing hazards. The authors propose another perspective related to transfer learning, combined with Error-Correcting Output Code support vector machine configuration for better accuracy in malware detection. One of the nice novelties of this research is the integration of vision-based techniques for detection into machine learning models, in particular within the framework of ECOC-SVM optimized for that purpose. Results: High improvement in accuracy and robustness compared to classic approaches; could hold appreciable detection rates among different malware samples. It has a few deficiencies, such as probable computational overhead due to complex model training and optimization that may create a barrier to its real-time detection scenarios. This work has contributed immensely in this area with regard to insights and methodologies that can be derived simply by demonstrating the potential of advanced machine learning techniques in enhancing cybersecurity defenses.

[29]. The paper titled "Improved chimp optimization algorithm (ICOA) feature selection and deep neural network framework for internet of things (IOT) based android malware detection" by Tirumala Vasu G, Samreen Fiza, ATA. Kishore Kumar, V. Sowmya Devi, Ch Niranjan Kumar, and Afreen Kubra, published in 2023, addresses the critical problem of detecting malicious Android applications in the Internet of Things (IoT) environment. The research focuses on overcoming the limitations of traditional malware detection systems which struggle with the increasing quantity and variety of Android malware. The methodology involves an innovative approach using the Improved Chimp Optimization Algorithm (ICOA) for feature selection and a Deep Neural Network Framework (DNNF) based on Long Short-Term Memory (LSTM) for accurate malware detection. The novelty of this study lies in integrating the ICOA with DNNF to enhance the feature learning and selection process, leading to better detection accuracy. The results demonstrate a high recognition accuracy, significantly outperforming existing state-of-the-art methods. However, the research also highlights some drawbacks, such as the need for extensive computational resources and the potential challenges in handling real-time malware detection scenarios. This study contributes significantly to the field by proposing a robust framework for improving Android malware detection using advanced optimization and deep learning techniques.

[30]. DImproved Chimpanzee Optimization Algorithm for Feature Selection and DNN Framework for Android Malware Detection in IoT Based on Android: Kishore Kumar, V. Sowmya Devi, Ch Niranjan Kumar, Afreen Kubra, 2023 The proposed paper develops and proposes much-required detection mechanisms for malignant Android applications over this actually mammoth

landscape of IoT, in which the present protection paradigms turn out to be ineffective because of this continuous variation in malware. The authors proposed a system that looked toward feature selection via ICOA, coupled with a deep neural network framework to increase accuracies in malware detection. Probably unique about the work is the usage of ICOA to actually design the feature selection itself: the one which would determine differential input into a later DNNF making use of LSTM for robust classification. The results of the experiment show increased accuracy in detection, explaining that the proposed system is efficient in its nature. The drawback noticed is that in the case of the integration of ICOA and DNNF, it may bring real-time applications forward as impracticable if the computational expenses are excessive. Nonetheless, that still remains quite ahead of Android malware detection with IoT; it kicks the door open for the following studies to ensure computationally efficient measures without any compromise in the performance of detection.

[31]. In the paper "Explainability in AI-based Behavioral Malware Detection Systems," Antonio Galli, Valerio La Gatta, Vincenzo Moscato, Marco Postiglione, and Giancarlo Sperlì, 2024, the authors address a very important problem in explainability within AI-driven malware detection systems. Traditional methods for malware detection are usually ineffective, as they cannot adapt to the continuous changeability of malware. The problem statement is focused on gaining insight and increasing transparency into AI models used for detecting behavioral malware, which normally act as "black boxes." In this respect, the authors propose a framework that integrates eXplainable Artificial Intelligence methodologies, notably SHAP, LIME, LRP, and attention mechanisms, applied to deep recurrent architectures such as LSTM and GRU. This is a new approach to making AI decisions interpretable, ranking the importance of API calls in malware detection. The results indeed show that SHAP and LRP provide the most reliable explanations, significantly improving understanding with respect to model predictions. It has, however, been noted that this comes at an increased computational complexity and variable explanation quality across different datasets. This work is, therefore, a very important step toward the integration of explainability in AI-based cybersecurity tools. It offers insight into both the strengths and limitations of current XAI techniques.

[32]. The paper "EvadeDroid: A practical evasion attack on machine learning for black-box Android malware detection" by Hamid Bostani and Veelasha Moonsamy, published in 2024, focuses on the problem of how machine learning-based malware detectors could be evaded in a black-box setting. Precisely, it is the problem of how Android malware detectors are vulnerable to adversarial examples, especially in real-world scenarios where zero knowledge is available about the targeted classifiers by attackers. This paper proposes a new methodology within the context of EvadeDroid's evasion attack, which uses a problem-space transformation-based approach, utilizes benign apps code snippets, and manipulates malware applications incrementally so that they will look benign. In such a context, it brings novelty with query efficiency, applying an optimization algorithm using the least number of transformations to very high evasion rates. Results show that EvadeDroid can be pretty effective in evading most malware detectors; it has an overall evasion rate between 80% and 95%, and the average evasion rate against commercial antivirus products is as high as 79%. However, this paper points out some limitations to the work with respect to the potential disruption of malware functionality and the challenge of making sure executable adversarial examples are ensured. Although there are some drawbacks, EvadeDroid has still made a very huge contribution towards the line of inquiry on adversarial robustness in Android malware detection systems.

[33]. The paper "Explainability in AI-based behavioral malware detection systems" by Antonio Galli, Valerio La Gatta, Vincenzo Moscato, Marco Postiglione, and Giancarlo Sperlì, published in 2024, deals with one of the most stringent challenges: to increase explainability in AI-powered malware detection. The identified research problem is that AI models are black boxes by design, and until now, this feature has limited their applicability in real-world cybersecurity scenarios where transparency is a must. The authors have come up with a new different framework including eXplainable Artificial Intelligence techniques—SHAP, LIME, LRP, and Attention mechanisms—all aimed at explaining AI models' decision-making processes in malware detection. In this methodology, these XAI methods will be evaluated against three separate datasets using recurrent deep architectures, notably an LSTM and a GRU model. This work provides the first well-controlled effectiveness and efficiency comparison between some top-performing XAI techniques, making the respective strengths and weaknesses known to the community. These results unequivocally indicate that incorporating these explanation-based AI methods into malware detection systems significantly improves their interpretability without performance degradation. The downside is that most of these XAI techniques incur large computational overheads, hence severely limiting their applicability in resource-constrained deployment scenarios. This thus brings an overall substantial advancement in the quest for making AI-driven solutions of cybersecurity more transparent and trustworthy.

[34]. Another paper, "Transferable Features from 1D-Convolutional Network for Industrial Malware Classification" by Liwei Wang, Jiankun Sun, Xiong Luo, and Xi Yang, published in 2022, is

expected to solve the problem of malware threats in growing connectivity of industrial systems to the Internet. It means that it focuses on the challenge of identifying and classifying new malware variants, especially in industrial malware detection scenarios where training data is usually in short supply. In this paper, a 1D-convolutional network architecture empowered by transfer learning is provided to mitigate the small sample size problem. Basically, these authors follow a methodology by which the feature spaces are aligned according to the GloVe word embedding and then train a 1D-convolutional network with the goal of evaluating three convolutional strategies on six transfer learning tasks. The originality of the paper is in proving that the 1D-convolutional network can learn transferable features for malware classification, with the first two convolutional layers being most efficiently transferable. Results: Transfer learning significantly reduces the training time with improved classification accuracy. The downside, however, is that this improvement has been proven slight, or even negative, in those cases where the target domain contains few training instances. This paper demonstrates the potential of transfer learning in enhancing industrial malware classification systems.

[35]. Younghoon Ban, Myeonghyun Kim, and Haehyun Cho pointed out, in 2024, some weaknesses of ML and DL classifiers against adversarial examples in the paper "An Empirical Study on the Effectiveness of Adversarial Examples in Malware Detection." This research will provide valuable results to argue against the hostility of attacks in the malware detection domain since AEs are created in such a way to avoid classification by any ML/DL-based classifier. Seven of the perturbation techniques that the authors have chosen include overlay append and section append. In such techniques, ambiguities are used in the PE format for the generation of AEs that remain evading in detection yet staying executable with malicious behavior. In this paper, the authors have shown that as high as 65.6%, the evasion rate is possible against ML-based classifiers and as high as 99% against DL-based classifiers using the proposed attack method. Novelty presented in this paper consists of using benign content and perturbation techniques for creating transferable AE and proposes a defense model using Trend Locality Sensitive Hashing, which can mitigate such attacks. Experiments show that more than 90% of the generated AE instances can be counterattacked by the defense models. The limitations in this study are that it focused on one aspect of the static analysis-based classifiers, which may have no bearing on dynamic analysis-based systems, and the behavior of the AEs possibly varies since it was not executed within a sandbox environment.

[36]. The paper by Omar N. Elayan and Ahmad M. Mustafa, "Android Malware Detection Using Deep Learning," was published in 2021, covering one of the most important concerns related to malware detection in the Android device environment. Traditional techniques of detection, including signature-based approaches, are known not to be able to identify new and evolving malware. The authors provide a novel detection method against this: Gated Recurrent Unit, a form of Recurrent Neural Network. The methodology describes the extraction of static features from Android applications, more precisely API calls and permissions. The model used in this paper is trained and tested by the dataset CICAndMal2017. The results obtained gave an accuracy of 98.2%, thus showing that this proposed deep learning approach is better than other traditional machine learning approaches. The novelty of the study is in using GRU for malware detection, which resonates with the potential of deep learning in cybersecurity. However, some limitations were underlined by the research: first of all, a large and representative dataset should be guaranteed to make the model robust and generalizable. In spite of the challenges discussed here, the present work makes a major contribution toward the field of Android malware detection, as it illustrates how deep learning techniques can enhance cybersecurity measures.

[37]. A 2023 paper by R. Aiyshwariya Devi and A.R. Arunachalam, "Improved Elliptic Curve Cryptography-based IoT device security enhancement and deep LSTM-based malware detection," has taken into consideration the growing security concerns for IoT infrastructures. A new mechanism with respect to this is described, being integrated with the improved ECC algorithm and the deep LSTM model for the enhancement of security of IoT devices and malware detection. It will involve identification of the attack nodes through contextual anomalies, deep LSTM malware classification, and improved ECC algorithms for secure data transmission. This is one of the key novelties in which the best keys will be optimized by using a hybrid MA-BW for selection and dynamically generate the keys to develop efficient and safe IoT communication. In this work, the proposed model turned in an accuracy of 95% with very low error rates and false positive rates. However, the intricacies involved in the deep learning model itself challenge real-time applications in terms of implementation and resource requirements within a resource-constrained IoT environment. The research provides a strong framework toward improving security in IoT by underlining the requirement for advanced cryptographic techniques and machine learning.

[38]. In the paper "An in-depth review of machine learning based Android malware detection," Ali Muzaffar, Hani Ragab Hassen, Michael A. Lones, and Hind Zantout have discussed one of the most critical issues: detection of malware in Android using machine learning techniques. Research question actually was framed on the inadequacies of traditional signature-based malware detection techniques since they are normally slow to match up with quickly altering nature of malware.

The authors survey all of the past works related to android malware detection using machine learning and organize them based on whether they used static, dynamic, or hybrid features. In this survey, methodologies such as Supervised, Unsupervised, Deep Learning, and Online Learning have been discussed. It contributes one of the novel aspects to this survey through a comprehensive taxonomy of Android malware detection techniques, providing an overview of different techniques and their efficacy. The results of the review underline that machine learning techniques, in particular hybrid analysis, allow for multiple improvements in the detection of new and unknown malware. On the other side, this study also underlines a few weaknesses: large, labeled datasets used for learning and high computational complexity of ML in some models. These results show that there is huge potential for machine learning to improve Android security; they also indicate areas in which further research is needed to engineer efficient and scalable solutions ready for deployment into real-world applications.

[39]. This paper, by Daniel Gibert, Carles Mateu, and Jordi Planes, entitled "The rise of machine learning for detection and classification of malware: Research developments, trends, and challenges," was published in 2020. Basically, the authors have focused on the critical point relating to evolving malware threats and the limitation of traditional methods for its detection in the paper. It provides an overview of the literature, systematically addressing the application of ML and DL techniques in the detection of malware. It is patently underlined since the beginning that sophisticated malware resurges with traditional signature-based and heuristic methods of detection. Static methodologies directly include static, dynamic, and hybrid approaches for feature extraction and model training. Novel contributions include the comprehensive taxonomy of techniques related to machine learning, an in-depth review of neural network-based methods, and the investigation of multimodal approaches to learning. The results obtained in the conducted study trace back the effectiveness of both ML and DL models with respect to accuracy in detection and handling large volumes of data. The same study, at the same time, reveals the drawbacks of these techniques: concept drift, adversarial learning, and class imbalance. This finally concludes with some recommendations to the future research directions in this regard by pointing out the need for continuous innovation on this so that malware evolution can be kept at bay.

[40]. This paper is titled "An in-depth review of machine learning-based Android malware detection" by Ali Muzaffar, Hani Ragab Hassen, Michael A. Lones, and Hind Zantout, 2022. The problem is that it is critical to know how to detect Android malware through very high usage rates of the platform and associated security risks. This paper surveys the various ML methodologies in the detection of Android malware: it focuses on approaches of supervised, unsupervised, deep learning, and online learning. The research pointed out that traditional signature-based techniques are inefficient for dealing with the huge and ever-changing landscape of Android malware and emphasized that ML techniques are better at identifying zero-day attacks without any use of already-identified malicious signatures. Novel contributions to the comparison of different ML models with different techniques of feature extraction are done. Results portray the efficiency of ML models toward better detection accuracy. On the other hand, it also highlighted major drawbacks such as high computational cost and large well-labeled datasets, which basically challenge their practical deployment. It also exposes some important current trends and future directions that may be useful in the enhancement of Android malware detection using machine learning.

[41]. A paper by Ron Korine and Danny Hendler entitled "DAEMON: Dataset/Platform-Agnostic Explainable Malware Classification Using Multi-Stage Feature Mining", 2021, focused on the problem of the automatic classification of malware variants into their respective families. Traditional anti-malware techniques often miss malware due to the ever-growing employment of obfuscation methods by malware vendors. The line that has been proposed is a new solution: DAEMON, the dataset-agnostic explainable malware classifier. This is based on an effective multistep feature mining process in which large N-grams have features extracted and selected for high-accuracy classification. Three large datasets containing Windows and Android malware were tested and demonstrated that DAEMON can produce high classification accuracy without any change in algorithms, re-engineering of features, or any kind of parameter tuning. This establishes its robustness and flexibility across different platforms. Again, although DAEMON's approach to feature selection brings considerable improvements to explainability, it remains resource-intensive in terms of computational resources required for training and model generation. This paper presents a highly accurate and explainable classification model, which is adaptable to many malware datasets and computing platforms; however, it still has a very high resource demand.

[42]. The paper "Self-Attentive Models for Real-Time Malware Classification" by Qikai Lu, Hongwen Zhang, Husam Kinawi, and Di Niu, published in 2022, deals with the important challenge of high accuracy in malware classification at low inference latency in real-time. Specifically, this research is guided by a concern with the inefficiency of state-of-the-art CNN classifiers in processing the high throughput of today's modern networks. The authors introduce two new transformer-based classifiers: SeqConvAttn and ImgConvAttn, for replacing traditional CNNs. A new file-size-aware two-stage framework is

proposed for combining these models to optimize this accuracy–latency tradeoff. This paper shows that transformer-based models significantly outperform the classification accuracy compared to the CNN-based models. Moreover, this two-stage framework can effectively reduce the average latency of model inference with high accuracy. The main novelty lies in the fact that there is an embedded file-size-aware mechanism that will prematurely direct larger files to a more appropriate classifier for efficient processing. However, it has to be realized that transformer models are greatly complex and resource-intensive compared to traditional methods. This work has achieved giant strides in the real-time classification of malware files by proving a robust framework that can be adapted with respect to different malware file sizes.

[43]. The paper by Xiaojian Liu, Xi Du, Qian Lei, and Kehong Liu, entitled "Multifamily Classification of Android Malware With a Fuzzy Strategy to Resist Polymorphic Familial Variants" from 2020, solves a very relevant problem related to the classification of Android malware into their respective families against challenges related to code obfuscation and polymorphic variants. These methodologies express malware behavior through regular expressions of security-sensitive API calls and adopt a two-step fuzzy processing strategy to ensure resilience to code obfuscation techniques. It provides novel contributions to a new approach in the fuzzy matching of regular expressions together with text mining techniques to train a 1-NN classifier based on a data set composed of 3270 samples from 65 families. These results provided an average accuracy of 97.8%, which is better than most state-of-the-art methods. Some limitations of the study have also been realized, including ICCs that may be affecting the comprehensive analysis of malware behavior. In general, research contributions significantly relate to the domain of Android malware detection, especially in terms of becoming more powerful against polymorphic and obfuscated malware.

[44]. The paper "RMDNet: Deep Learning Paradigms for Effective Malware Detection and Classification" by S. Puneeth, Shyam Lal, Mahendra Pratap Singh, and B. S. Raghavendra from 2024 also takes into consideration the further complication of malware threats and how the traditional approaches have failed to detect these new threats. The authors have come up with a new deep learning-driven methodology called RMDNet. It has a robust malware detection network that will enhance the accuracy and efficiency in the classification of malware. It is applied to datasets obtained from binary visualization images and malware samples, which have been converted into gray-scale images. The depth-wise convolution and concatenation increase the feature extraction and classification accuracy of the model. The experimental results prove that RMDNet outperforms the existing models of deep learning, like ResNeXt, VGG19, LiverNet, EfficientNet-B0, and DenseNet121 in all parameters with better accuracy and computational efficiency. This result is very promising, but still raises the question of interpretability and transparency of deep learning models—the most common drawback for the domain. This work thus significantly contributes to the development of malware detection techniques by proving that specifically designed deep learning architectures can be of very good performance for this task.

[45]. A 2023 work by Aurangzeb and Aleem, "Evaluation and Classification of Obfuscated Android Malware through Deep Learning using Ensemble Voting Mechanism," was focused on one of the most current and serious problems in malware: that which is using obfuscation is highly sidestepping in traditional ways of detection and posing a serious threat to user security. In this paper, these authors have proposed another approach where static and dynamic analysis methods are combined within the ensemble voting framework to improve the accuracy of the detector. In this paper, the authors have implemented a deep learning algorithm that evaluates malware at both real and emulator-based platforms. Another major contribution of this research is finding quite a small subset of features that perform very well consistently in the case of non-obfuscated malware, while with obfuscation, it changes drastically, hence turning into an important one in classifying benign from malicious applications. Results from this experiment proved that the proposed model was able to efficiently detect and classify obfuscated malware. However, the limitations of the adopted feature set are still pointed out here because obfuscation techniques used by malware vary greatly. All this simply requires further refinements to be carried out on this part and testing on a bigger dataset. It simply puts a case forward of how sophisticated machine learning techniques can help fortify cybersecurity against the ever-evolving malware threats.

[46]. This research tackles the critical issue of ever-increasing vulnerability of IoT devices against sophisticated malware attacks. The approach presented in the paper includes the following steps: preprocessing by scaling, normalization, and de-noising of data; feature selection with one-hot encoding; and an ensemble classifier that assimilates Convolutional Neural Networks and Long Short-Term Memory. The novelty consists in the totally comprehensive approach toward feature selection and CNN integration with LSTM, which will aid in the robust detection of malware. Results from empirical evaluations indicate that the proposed method outperforms existing state-of-the-art techniques, achieving very impressive average accuracy of 99.5% on standard datasets. The study, however, points out potential limitations to the generalizability of the model across different IoT environments and the computational overhead traditionally associated with deep learning models. In sum, the research accomplished a huge improvement in the detection of malware in IoT

devices but still requires further efforts to guarantee its real-world scenarios scalability and efficiency.

[47]. The paper "MalFuzz: Coverage-guided fuzzing on deep learning-based malware classification model" by Yuying Liu, Pin Yang, Peng Jia, Ziheng He, and Hairu Luo from 2022 deals with highly relevant security vulnerabilities in deep learning-based malware detection models. In more detail, the research problem was that specially designed test methods for the models were missing, which were increasingly applied in real-world malware detection scenarios. MalFuzz applies coverage-guided fuzzing for testing these models. Although already applied to models of images and natural language processing, this is the first application of this technique on malware detection models. MalFuzz uses neuron values from the first and last layers of the model to represent its state and follows up with a fast approximate nearest neighbor algorithm for the calculation of coverage. It concretely designs the seed selection and mutation strategies for malware detection model testing but represents results regarding MalFuzz's effectiveness against modified TensorFuzz and MAB-malware in detecting model classification errors while maintaining malware functionality. Besides, this work contributes a specially designed fuzzing technique for malware detection models that has proven very effective in error detection and model robustness. However, it is limited to some certain tested models, such as MalConv, Convnet, and CNN 2-d, and shall need further validation across different malware datasets and models.

[48]. The paper "OpCode-Level Function Call Graph Based Android Malware Classification Using Deep Learning" was written by Weina Niu, Rong Cao, Xiaosong Zhang, Kangyi Ding, Kaimeng Zhang, and Ting Li, published in the journal Sensors in 2020. In this paper, the authors focus on a very relevant and timely problem of Android malware classification, which represents one of the most dangerous factors for privacy and security. Therefore, flowing directly from the foregoing, the problem statement of the research is how to counter this inability of traditional signature-based methods of malware detection against unknown and obfuscated malware. In that regard, authors introduce a new approach toward the solution of such a problem through static analysis at the OpCode level FCG with LSTM deep learning models. The authors of this paper make a completely novel contribution in the integration of OpCode-level FCG with LSTM in malware detection to obtain an accuracy of 97% against a dataset containing 1796 malware samples and 1000 benign apps, hence outperforming the techniques developed earlier. However, the authors also mention a few limitations: slightly degraded performance on large and heterogeneous datasets and modeling complex malware behaviors. Although this survey is useful to some degree in using deep learning techniques for improving the detection of Android malware, validation on broader datasets is still better.

[49]. The work "Deep learning-based Sequential model for malware analysis using Windows exe API Calls" was done in 2020 by Ferhat Ozgur Catak, Ahmet Faruk Yazı, Ogerta Elezaj, and Javed Ahmed. In this paper, the authors raised one of the major challenges to metamorphic malware, which is advanced malware and hence very challenging to be detected by conventional techniques of signature-based for antivirus solutions. This implies security in the design of the classification method related to the behavioral characteristics of malware, which relate to API calls against an operating system such as Windows. In connection to this, authors have produced a totally new dataset of API calls covering all the spectrums of behaviors of malware: Adware, Backdoor, Downloader, Dropper, Spyware, Trojan, Virus, and Worm. They used an LSTM neural network model appropriate for sequential data to classify this form of malware. The accuracy in this case is high: it stands at 95%, while the F1-score is 0.83. That is high compared to other reported studies. Another significant development this research has contributed to the field is the development and release of a completely new dataset for the category of malware, based on Windows OS. This work reduces generalizability of the models to new or modifying malware types. Moreover, it might not identify malware variations of behavior that would exist in real-world scenarios since the model is trained on a single dataset.

[50]. The research "AMDDLmodel: Android smartphones malware detection using deep learning model" was published in 2024 by Muhammad Aamir, Muhammad Waseem Iqbal, Mariam Nosheen, M Usman Ashraf, Ahmad Shaf, Khalid Ali Almarhabi, Ahmed Mohammed Alghamdi, and Adel A Bahaddad. This paper presents the significant problem of malware detection and classification for Android smartphones, which is really urgent due to the fact that Android devices are used and popular worldwide. Most of the traditional detection techniques, including signature-based ones, miss the detection of new and evolving malware. This paper presents a deep learning-based approach using a convolutional neural network to improve accuracy in malware detection. In the methodology, the model is tested against the Drebin dataset with 215 features. It recorded an accuracy rate of 99.92%, beating all the traditional prior techniques. This makes the study novel with respect to innovative feature engineering and overall model performance evaluation. Scant research is done on the computational overhead and resource requirements that a model of this nature can potentially incur when being deployed on resource-constrained mobile devices. Overall, the AMDDL model advances Android malware detection with a robust solution showing very promising accuracy and performance metrics.

IV. Discussion

Aggregating the data throws up multiple themes. While deep learning models, especially CNNs and RNNs, offer superior results for various applications and malware classification, at times how well the training datasets represent the situation could be poor. In addition, computational complexity hampers the real-time detection capability of such models, especially in resource-constrained environments. It also leads to more evidence that hybrid approaches could link assessment-based methodologies to static and dynamic analysis with a promising attitude in enhancing their detection rate. One of the main formidable reasons for explaining deep learning remains a significant obstacle to a wider diffusion of these methods in cybersecurity. Follow-up work should aim to make models more interpretable, not just robust. Research now sought will aim at mechanisms for transfer learning and adversarial robustness to better adapt such systems to novel and evolving threats.

Study	Deep Learning Technique	Dataset	Accuracy	Limitations
Cakir & Dogdu (2018)	Word2Vec + Gradient Boosting Machine (GBM)	Custom	96%	Outdated dataset, limited by the older malware patterns.
Ucci et al. (2019)	Survey of various ML techniques	Various	N/A	Need for updated datasets; anti-analysis techniques pose challenges.
Yuan et al. (2020)	Markov Images + Deep CNN	Microsoft, Drebin	99.26% (Microsoft) 97.36% (Drebin)	Performance may vary with different dataset distributions; relies heavily on labeled training samples.
Narayanan & Davuluru (2020)	Ensemble (CNN + LSTM)	Microsoft Malware Classification Challenge	99.8%	High dependence on large, high-quality datasets; computational complexity.
Vinayakumar et al. (2019)	ScaleMalNet (Image processing + DL)	Public and Private	N/A	High computational requirements; large datasets needed.
Korine & Hendler (2021)	DAEMON: Multi-stage Feature Mining	Multiple (Windows, Android)	High	Computationally intensive; may not scale well to very large datasets.
Bala et al. (2022)	Transfer Learning + CNN	Android	97.24%	High computational cost; needs further optimization for small datasets.
Gopinath & Sethuraman (2023)	Survey of DL techniques	Various	N/A	High computational cost, inefficiency in processing high-dimensional data.
Gibert et al. (2022)	Hybrid: Feature Engineering + Deep Learning	Microsoft Malware Classification Challenge	99.81%	Risk of overfitting due to high dimensionality; dependent on the quality of training data.

References

[1] B. Cakir and E. Dogdu, "Malware classification using deep learning methods," in Proceedings of the ACMSE 2018 Conference, Richmond, Kentucky, USA, Mar. 2018, pp. 10-14. doi: 10.1145/3190645.3190692.

[2] D. Ucci, L. Aniello, and R. Baldoni, "Survey of machine learning techniques for malware analysis," Computers & Security, vol. 81, pp. 123-147, 2019. doi: 10.1016/j.cose.2018.11.001.

[3] B. Yuan, J. Wang, D. Liu, W. Guo, P. Wu, and X. Bao, "Byte-level malware classification based on Markov images and deep learning," Computers & Security, vol. 92, p. 101740, 2020. doi: 10.1016/j.cose.2020.101740.

[4] B. N. Narayanan and V. S. P. Davuluru, "Ensemble Malware Classification System Using Deep Neural Networks," Electronics, vol. 9, no. 5, p. 721, May 2020. doi: 10.3390/electronics9050721.

[5] R. Vinayakumar et al., "Robust Intelligent Malware Detection Using Deep Learning," IEEE Access, vol. 7, pp. 46717-46738, 2019. doi: 10.1109/ACCESS.2019.2906934.

[6] R. Korine and D. Hendler, "DAEMON: Dataset/Platform-Agnostic Explainable Malware Classification Using Multi-Stage Feature Mining," IEEE Access, vol. 9, pp. 78382-78399, 2021. doi: 10.1109/ACCESS.2021.3082173.

[7] Z. Bala, F. U. Zambuk, B. Y. Imam, A. Y. Gital, F. Shittu, M. Aliyu, and M. L. Abdulrahman, "Transfer Learning Approach for Malware Images Classification on Android Devices Using Deep Convolutional Neural Network," Procedia Computer Science, vol. 212, pp. 429-440, 2022. doi: 10.1016/j.procs.2022.11.027.

[8] G. M. and S. C. Sethuraman, "A comprehensive survey on deep learning based malware detection techniques," Computer Science Review, vol. 47, p. 100529, Feb. 2023. doi: 10.1016/j.cosrev.2022.100529.

[9] D. Gibert, J. Planes, C. Mateu, and Q. Le, "Fusing feature engineering and deep learning: A case study for malware classification," Expert Systems with Applications, vol. 207, 2022, Art. no. 117957. doi: 10.1016/j.eswa.2022.117957.

[10] S. Yoo, S. Kim, S. Kim, and B. B. Kang, "AI-HydRa: Advanced hybrid approach using random forest and deep learning for malware classification," Information Sciences, vol. 546, pp. 420-435, 2021. doi: 10.1016/j.ins.2020.08.082.

[11] Q. Le, O. Boydell, B. M. Namee, and M. Scanlon, "Deep learning at the shallow end: Malware classification for non-domain experts," Digital Investigation, vol. 26, Supplement, pp. S118-S126, 2018. doi: 10.1016/j.diin.2018.06.003.

[12] A. Bensaoud, J. Kalita, and M. Bensaoud, "A survey of malware detection using deep learning," Machine Learning with Applications, vol. 16, 2024, Art. no. 100546. doi: 10.1016/j.mlwa.2024.100546.

[13] Y. Wang and S. Jia, "MADRAS-NET: A Deep Learning Approach for Detecting and Classifying Android Malware Using Linknet," Measurement: Sensors, vol. 33, p. 101113, 2024. doi: 10.1016/j.measen.2024.101113.

[14] I. Zelinka, M. Szczypka, J. Plucar, and N. Kuznetsov, "From malware samples to fractal images: A new paradigm for classification," Mathematics and Computers in Simulation, vol. 218, pp. 174-203, 2024. doi: 10.1016/j.matcom.2023.11.032.

[15] S. K. Smmarwar, G. P. Gupta, and S. Kumar, "Android malware detection and identification frameworks by leveraging the machine and deep learning techniques: A comprehensive review," Telematics and Informatics Reports, vol. 14, p. 100130, 2024. doi: 10.1016/j.teler.2024.100130.

[16] M. Ahmed, N. Afreen, M. Ahmed, M. Sameer, and J. Ahamed, "An inception V3 approach for malware classification using machine learning and transfer learning," International Journal of Intelligent Networks, vol. 4, pp. 11-18, 2023. doi: 10.1016/j.ijin.2022.11.005.

[17] S. Poornima and R. Mahalakshmi, "Automated malware detection using machine learning and deep learning approaches for android

applications," Measurement: Sensors, vol. 32, 2024, Art. no. 100955. doi: 10.1016/j.measen.2023.100955.

[18] J. Song, S. Choi, J. Kim, K. Park, C. Park, J. Kim, and I. Kim, "A study of the relationship of malware detection mechanisms using Artificial Intelligence," ICT Express, vol. 10, no. 3, pp. 632-649, 2024. doi: 10.1016/j.icte.2024.03.005.

[19] S. Dlaim Alotaibi, B. Alabduallah, Y. Said, S. B. H. Hassine, A. A. Alzubaidi, M. Alamri, S. Al Zanin, and J. Majdoubi, "Bioinspired artificial intelligence based android malware detection and classification for cybersecurity applications," Alexandria Engineering Journal, vol. 100, pp. 142-152, 2024. doi: 10.1016/j.aej.2024.05.038.

[20] R. Casolare, G. Ciaramella, G. Iadarola, F. Martinelli, F. Mercaldo, A. Santone, and M. Tommasone, "On the Resilience of Shallow Machine Learning Classification in Image-based Malware Detection," Procedia Computer Science, vol. 207, pp. 145-157, 2022. doi: 10.1016/j.procs.2022.09.047.

[21] A. Guerra-Manzanares, "Machine Learning for Android Malware Detection: Mission Accomplished? A Comprehensive Review of Open Challenges and Future Perspectives," Computers & Security, vol. 138, 2024, Art. no. 103654. doi: 10.1016/j.cose.2023.103654.

[22] H. Rathore, A. Nandanwar, S. K. Sahay, and M. Sewak, "Adversarial superiority in android malware detection: Lessons from reinforcement learning based evasion attacks and defenses," Forensic Science International: Digital Investigation, vol. 44, 2023, Art. no. 301511. doi: 10.1016/j.fsidi.2023.301511.

[23] W. K. Wong, F. H. Juwono, and C. Apriono, "Vision-Based Malware Detection: A Transfer Learning Approach Using Optimal ECOC-SVM Configuration," IEEE Access, vol. 9, pp. 159262-159270, 2021. doi: 10.1109/ACCESS.2021.3131713.

[24] T. Vasu, S. Fiza, A. K. Kumar, V. S. Devi, C. N. Kumar, and A. Kubra, "Improved chimp optimization algorithm (ICOA) feature selection and deep neural network framework for internet of things (IOT) based android malware detection," Measurement: Sensors, vol. 28, 2023, Art. no. 100785. doi: 10.1016/j.measen.2023.100785.

[25] A. Galli, V. La Gatta, V. Moscato, M. Postiglione, and G. Sperlì, "Explainability in AI-based Behavioral Malware Detection Systems," Computers & Security, vol. 141, pp. 103842, 2024. doi: 10.1016/j.cose.2024.103842.

[26] H. Bostani and V. Moonsamy, "EvadeDroid: A practical evasion attack on machine learning for black-box Android malware detection," Computers & Security, vol. 139, 2024, Art. no. 103676. doi: 10.1016/j.cose.2024.103676.

[27] X. Liu, X. Du, Q. Lei, and K. Liu, "Multifamily Classification of Android Malware With a Fuzzy Strategy to Resist Polymorphic Familial Variants," IEEE Access, vol. 8, pp. 156900-156914, 2020. doi: 10.1109/ACCESS.2020.3019282.

[28] S. Puneeth, S. Lal, M. P. Singh, and B. S. Raghavendra, "RMDNet: Deep Learning Paradigms for Effective Malware Detection and Classification," IEEE Access, vol. 9, pp. 78382-78399, 2021. doi: 10.1109/ACCESS.2021.3082173.

[29] R. S, S. Latif, S. M. Usman, S. S. Ullah, A. D. Algarni, A. Yasin, A. Anwar, H. Elmannai, and S. Hussain, "Malware Detection in Internet of Things (IoT) Devices Using Deep Learning," Sensors (Basel), vol. 22, no. 23, p. 9305, 2022. doi: 10.3390/s22239305.

[30] Y. Liu, P. Yang, P. Jia, Z. He, and H. Luo, "MalFuzz: Coverage-guided fuzzing on deep learning-based malware classification model," PLoS One, vol. 17, no. 9, p. e0273804, 2022. doi: 10.1371/journal.pone.0273804.

[31] W. Niu, R. Cao, X. Zhang, K. Ding, K. Zhang, and T. Li, "OpCode-Level Function Call Graph Based Android Malware Classification Using Deep Learning," Sensors (Basel), vol. 20, no. 13, p. 3645, 2020. doi: 10.3390/s20133645.

[32] F. O. Catak, A. F. Yazı, O. Elezaj, and J. Ahmed, "Deep learning based Sequential model for malware analysis using Windows exe API Calls," PeerJ Comput Sci, vol. 6, 2020. doi: 10.7717/peerj-cs.285.

[33] M. Aamir, M. W. Iqbal, M. Nosheen, M. U. Ashraf, A. Shaf, K. A. Almarhabi, A. M. Alghamdi, and A. A. Bahaddad, "AMDDLmodel: Android smartphones malware detection using deep learning model," PLoS One, vol. 19, no. 1, 2024. doi: 10.1371/journal.pone.0296722.

[34] O. N. Elayan and A. M. Mustafa, "Android Malware Detection Using Deep Learning," Procedia Computer Science, vol. 184, pp. 847-852, 2021. doi: 10.1016/j.procs.2021.03.106.

[35] R. Aiyshwariya Devi and A. R. Arunachalam, "Enhancement of IoT device security using an Improved Elliptic Curve Cryptography algorithm and malware detection utilizing deep LSTM," High-Confidence Computing, vol. 3, no. 2, p. 100117, 2023. doi: 10.1016/j.hcc.2023.100117.

[36] A. Muzaffar, H. R. Hassen, M. A. Lones, and H. Zantout, "An in-depth review of machine learning based Android malware detection," Computers & Security, vol. 121, p. 102833, 2022. doi: 10.1016/j.cose.2022.102833.

[37] D. Gibert, C. Mateu, and J. Planes, "A Comprehensive Review of Machine Learning and Deep Learning Techniques for Malware Detection," Journal of Network and Computer Applications, vol. 153, p. 102526, 2020. doi: 10.1016/j.jnca.2019.102526.

[38] A. Galli, V. La Gatta, V. Moscato, M. Postiglione, and G. Sperlì, "Explainability in AI-based behavioral malware detection systems," Computers & Security, vol. 141, p. 103842, 2024. doi: 10.1016/j.cose.2024.103842.

[39] Q. Lu, H. Zhang, H. Kinawi, and D. Niu, "Self-Attentive Models for Real-Time Malware Classification," IEEE Access, vol. 10, pp. 95970-95985, 2022. doi: 10.1109/ACCESS.2022.3202952.

[40] X. Liu, X. Du, Q. Lei, and K. Liu, "Multifamily Classification of Android Malware With a Fuzzy Strategy to Resist Polymorphic Familial Variants," IEEE Access, vol. 8, pp. 156900-156914, 2020. doi: 10.1109/ACCESS.2020.3019282.

[41] R. Korine and D. Hendler, "DAEMON: Dataset/Platform-Agnostic Explainable Malware Classification Using Multi-Stage Feature Mining," IEEE Access, vol. 9, pp. 78382-78399, 2021. doi: 10.1109/ACCESS.2021.3082173.

[42] Q. Lu, H. Zhang, H. Kinawi, and D. Niu, "Self-Attentive Models for Real-Time Malware Classification," IEEE Access, vol. 10, pp. 95970-95985, 2022. doi: 10.1109/ACCESS.2022.3202952.

[43] X. Liu, X. Du, Q. Lei, and K. Liu, "Multifamily Classification of Android Malware With a Fuzzy Strategy to Resist Polymorphic Familial Variants," IEEE Access, vol. 8, pp. 156900-156914, 2020. doi: 10.1109/ACCESS.2020.3019282.

[44] S. Puneeth, S. Lal, M. P. Singh, and B. S. Raghavendra, "RMDNet: Deep Learning Paradigms for Effective Malware Detection and Classification," IEEE Access, vol. 9, pp. 78382-78399, 2021. doi: 10.1109/ACCESS.2021.3082173.

[45] R. S, S. Latif, S. M. Usman, S. S. Ullah, A. D. Algarni, A. Yasin, A. Anwar, H. Elmannai, and S. Hussain, "Malware Detection in Internet of Things (IoT) Devices Using Deep Learning," Sensors (Basel), vol. 22, no. 23, p. 9305, 2022. doi: 10.3390/s22239305.

[46] Y. Liu, P. Yang, P. Jia, Z. He, and H. Luo, "MalFuzz: Coverage-guided fuzzing on deep learning-based malware classification model," PLoS One, vol. 17, no. 9, p. e0273804, 2022. doi: 10.1371/journal.pone.0273804.

[47] W. Niu, R. Cao, X. Zhang, K. Ding, K. Zhang, and T. Li, "OpCode-Level Function Call Graph Based Android Malware Classification Using Deep Learning," Sensors (Basel), vol. 20, no. 13, p. 3645, 2020. doi: 10.3390/s20133645.

[48] F. O. Catak, A. F. Yazı, O. Elezaj, and J. Ahmed, "Deep learning based Sequential model for malware analysis using Windows exe API Calls," PeerJ Comput Sci, vol. 6, 2020. doi: 10.7717/peerj-cs.285.

[49] M. Aamir, M. W. Iqbal, M. Nosheen, M. U. Ashraf, A. Shaf, K. A. Almarhabi, A. M. Alghamdi, and A. A. Bahaddad, "AMDDLmodel: Android smartphones malware detection using deep learning model," PLoS One, vol. 19, no. 1, 2024. doi: 10.1371/journal.pone.0296722.

[50] O. N. Elayan and A. M. Mustafa, "Android Malware Detection Using Deep Learning," Procedia Computer Science, vol. 184, pp. 847-852, 2021. doi: 10.1016/j.procs.2021.03.106.