

A Comprehensive Review of Deep Learning Techniques for Malware Detection and Classification

¹Mohd Saif, ²Dr. Satyendra Kurariya

M. Tech. Scholar, Department of Computer Science and Engineering, Madhyanchal
Professional University (MPU), Bhopal, India¹

Professor, Department of Computer Science and Engineering, Madhyanchal Professional
University (MPU), Bhopal, India²

Abstract

The rapid growth of sophisticated cyber threats has made malware detection and classification a critical challenge in modern cybersecurity systems. Traditional signature-based malware detection techniques are effective against known threats but often fail to identify new, polymorphic, metamorphic, and zero-day malware variants. Deep learning (DL) has emerged as a promising approach for addressing these limitations because of its ability to automatically learn complex patterns and discriminative features from large-scale malware datasets. This paper presents a comprehensive review of deep learning techniques employed for malware detection and classification, including Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), Long Short-Term Memory (LSTM), Autoencoders, Deep Belief Networks (DBN), Generative Adversarial Networks (GAN), Transformer-based models, and hybrid deep learning architectures. The review examines different malware analysis approaches, including static, dynamic, and hybrid analysis, along with commonly used datasets, feature extraction methods, preprocessing techniques, and performance evaluation metrics such as accuracy, precision, recall, F1-score, and area under the ROC curve. Furthermore, the study compares the capabilities of different DL architectures in identifying malware families and distinguishing malicious software from benign applications. Key challenges, including data imbalance, adversarial attacks, obfuscated malware, computational complexity, model interpretability, and limited availability of representative datasets, are also discussed. Finally, emerging research directions such as explainable artificial intelligence, transfer learning, federated learning, graph neural networks, and Transformer-based malware analysis are highlighted. The review provides a comprehensive foundation for researchers and cybersecurity practitioners seeking to develop accurate, robust, and adaptive deep learning-based malware detection and classification systems.

Keywords: - Malware Classification, Deep Learning, Machine Learning

1. INTRODUCTION

The rapid expansion of the Internet, cloud computing, mobile applications, Internet of Things (IoT) devices, and connected digital services has significantly increased the number of potential entry points for cyberattacks. Among various cybersecurity threats, malware remains one of the most persistent and rapidly evolving threats to computer systems, networks, mobile devices, and critical infrastructure. Malware refers to malicious software designed to perform unauthorized or harmful activities, including stealing sensitive

information, disrupting services, damaging systems, encrypting files, monitoring user activities, and obtaining unauthorized access to computing resources. Common categories of malware include viruses, worms, Trojan horses, ransomware, spyware, rootkits, botnets, and other potentially unwanted malicious programs [1, 2]. The continuous emergence of new malware variants has created a significant challenge for conventional cybersecurity mechanisms and has increased the need for intelligent and automated malware detection and classification systems [3].

Traditional malware detection systems primarily rely on signature-based techniques, in which a previously identified malicious program is represented by a unique signature and compared with incoming files or applications. Although signature-based detection can provide efficient identification of known malware, its effectiveness decreases when attackers modify the structure or behavior of malicious program [4, 5]. Techniques such as code obfuscation, packing, polymorphism, metamorphism, and rapid generation of malware variants can allow malicious programs to evade conventional signatures. In addition, zero-day malware does not have a previously known signature, making its detection particularly difficult. To address these limitations, researchers have increasingly investigated machine learning (ML) and artificial intelligence (AI) techniques that can identify malicious patterns from extracted features rather than relying exclusively on predefined signatures [6].

Deep learning (DL), a major branch of artificial intelligence, has demonstrated significant potential for automated malware detection and classification because of its capability to learn hierarchical and complex representations directly from large-scale data. Unlike conventional machine learning methods that often require carefully engineered features, deep learning models can learn useful representations from raw or minimally processed data. Convolutional Neural Networks (CNNs), for example, have been applied to malware classification by representing executable files or byte sequences as images or spatial feature representations. Similarly, Recurrent Neural Networks (RNNs) and Long Short-Term Memory (LSTM) networks can analyze sequential characteristics of executable instructions, API calls, system calls, or behavioral traces. Autoencoders can be used for feature learning and anomaly detection, while Transformer-based architectures have recently attracted attention because of their ability to model long-range dependencies in sequential and contextual malware data [7]. Malware analysis can generally be categorized into static analysis, dynamic analysis, and hybrid analysis. Static analysis examines malware without executing the program and may utilize features such as byte sequences, opcode sequences, imported libraries, headers, strings, and control-flow information. Dynamic analysis observes malware behavior during execution and can collect information such as API calls, system calls, network traffic, registry modifications, memory behavior, and file operations. Hybrid analysis combines static and dynamic characteristics to obtain a more comprehensive representation of malicious behavior. Deep learning techniques can be applied to each of these analysis strategies, allowing researchers to develop automated systems capable of detecting malware and identifying its corresponding family or category [8, 9].

The classification of malware into different families is particularly important for cybersecurity because malware belonging to the same family may exhibit related characteristics, attack strategies, or propagation mechanisms. Accurate classification can assist security analysts in understanding the nature of a threat and selecting appropriate defensive measures. Several deep learning architectures have therefore been investigated for binary malware detection as well as multi-class malware family classification. CNN, LSTM, gated recurrent architectures, deep neural networks, autoencoders, ensemble deep learning models, and hybrid architectures have been explored using executable files, opcode sequences, API-call traces, network behavior, and malware images. More recently, Transformer models and graph-based deep learning approaches have provided additional opportunities for representing complex relationships between instructions, program components, and behavioral events [10].

Despite the promising performance of deep learning, several challenges remain. The quality and representativeness of the training dataset have a direct influence on model performance. Malware datasets may suffer from class imbalance, outdated samples, duplicated files, insufficient representation of newly emerging malware families, and variations in data collection procedures. Furthermore, malware authors continuously develop evasion techniques that can manipulate the input characteristics of malicious programs and reduce the reliability of trained models. Deep learning models may also require substantial computational resources and large amounts of labeled data. Another important concern is interpretability, since many deep learning models operate as complex black-box systems, making it difficult for cybersecurity analysts to understand why a particular file has been classified as malicious.

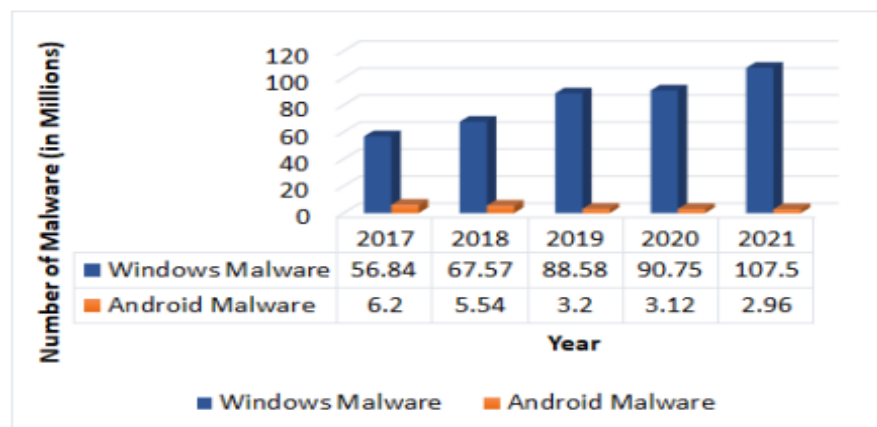


Fig. 1: Malware Statistics for Windows and Android Platforms

2. MALWARE DETECTION

Protecting the devices from malware is important since the smartphones today are used from normal phone calls to banking transactions, where highly sensitive information is accessed. The detection of any malware involves several sequences of steps. The steps involved in the process of malware detection are analysis of the sample, extraction of features, selection of appropriate features, feature reduction and finally using a suitable detection engine [11].

2.1 Mobile Malware

Mobile malware is one major threat to the security of any mobile devices. The first ever mobile malware is discovered in the year 2004. It is named as “Cabir”. This malware is designed with devices running on Symbian operating system, which is predominantly used by “Nokia”. Cabir worm is capable of spreading through Bluetooth. The malicious apps get installed to a device through a number of ways. Although the users download the apps from Play Store, there is a risk of getting infected from the malicious apps [12, 13].

2.2 Dynamic Analysis

Dynamic analysis of Android apps involves executing the application either in a virtual or a real device, to monitor the application’s run-time activities, and gathering features from the log file generated as a result of execution. Virtual devices are generally preferred for performing dynamic analysis since the changes made by the malware can be easily reverted, which is tedious with real devices. Android provides support for virtual device by a tool called “Android Emulator”. Using this tool Android device of any configuration is created. The most important dynamic feature is the system calls. As Android is a Linux based architecture, it uses system calls to communicate with various process. Thus by tracing of system calls several information is gained. Thus the work extracts the system call to analyze the Android applications to find traces of malware [14].

1.3 Feature Extraction

Feature extraction process involves collecting the required features from the information gathered during the analysis phase. Once the features are extracted, it is encoded so as to convert the text data into a form understandable by the classification algorithms. The feature vector constructed is generally very sparse and hence a technique is required to select features that are relevant from the entire set of features, and finally these are fed into classification algorithms for the purpose of detection. Some of the advantages of feature reduction are improved accuracy, avoids overfitting of the model, helps to speed up the training process, improved data visualization [15].

3. LITERATURE REVIEW

Alshoulie et al. [1] presented a comprehensive review of deep learning approaches for malware detection, focusing on the growing capability of intelligent models to identify increasingly sophisticated cyber threats. The study examined different deep learning architectures and their applications in malware analysis, highlighting the advantages of automated feature learning over conventional signature-based detection mechanisms. The authors discussed approaches based on static, dynamic, and hybrid malware analysis, where features such as byte sequences, opcodes, API calls, system behavior, and executable characteristics can be utilized for model training. Various deep learning architectures, including convolutional and recurrent neural networks, were considered for learning complex patterns associated with malicious software. The review also emphasized major challenges affecting deep learning-based malware detection, including malware obfuscation, polymorphic and metamorphic attacks, adversarial manipulation, data imbalance, dataset limitations, computational requirements, and model interpretability. The study further identified emerging research directions involving explainable AI, transfer learning, and

robust learning techniques. Overall, the work provides a broad understanding of how deep learning is being incorporated into modern malware detection systems and highlights the need for adaptive and robust models capable of handling continuously evolving malware variants.

P. Maniriho et al. [2] conducted a survey of recent advances in deep learning models for malware detection across both desktop and mobile computing platforms. The study highlighted the increasing complexity of malware and the limitations of traditional detection approaches in identifying previously unseen or modified malicious programs. The authors reviewed deep learning-based techniques developed for different malware analysis scenarios and examined how models can learn discriminative representations from executable files, behavioral information, API calls, system calls, and other malware-related features. Particular attention was given to the differences between malware detection on desktop systems and mobile platforms, where Android applications introduce additional challenges related to application permissions, code structure, and dynamic behavior. The review discussed several neural network architectures and their effectiveness in automated malware detection and classification. The authors also considered important issues such as dataset quality, class imbalance, feature representation, model generalization, and computational overhead. The study demonstrated that deep learning can significantly reduce dependence on manually engineered features; however, its practical deployment requires robust datasets and models capable of adapting to emerging malware variants. The survey provides a useful foundation for understanding the development of deep learning-based malware detection across heterogeneous computing environments.

H. Wang et al. [3] reviewed deep learning-based malware detection techniques with emphasis on the evolution of intelligent approaches for automatically identifying malicious software. The authors examined how deep learning can overcome several limitations of traditional machine learning and signature-based approaches by learning hierarchical representations from malware data. The review covered different forms of malware analysis, including static analysis, dynamic analysis, and hybrid analysis, and discussed the types of information that can be extracted from executable files and runtime behavior. Different deep learning architectures were analyzed according to their ability to process image-like representations, sequential information, and behavioral features. CNN-based methods are particularly useful for extracting spatial patterns from malware representations, whereas recurrent architectures can capture sequential relationships in instructions, API calls, or behavioral traces. The authors also discussed challenges associated with adversarial attacks, malware obfuscation, data scarcity, class imbalance, and the computational cost of deep models. In addition, the review indicated that future malware detection systems require improved generalization and robustness against newly emerging threats. This work is significant for understanding the methodological development of deep learning-based malware detection and the technical challenges that must be addressed before large-scale deployment.

A. Bensaoud, et al. [4] presented a comprehensive survey of malware detection techniques based on deep learning and examined the transition from conventional cybersecurity mechanisms toward data-driven intelligent detection. The authors discussed how malware can be represented using different feature types and how deep neural networks can automatically extract useful patterns from these representations. The study considered static and dynamic analysis approaches and reviewed the application of different deep learning architectures for malware detection and classification. Image-based malware analysis was identified as an important direction, in which binary files or executable code are transformed into visual representations that can subsequently be processed using CNN architectures. Sequential and behavioral representations can also be analyzed using recurrent and other deep learning models. The authors emphasized that the effectiveness of a malware detection model depends strongly on dataset characteristics, feature representation, preprocessing, and evaluation methodology. The survey also identified important limitations, including adversarial attacks, obfuscation, evolving malware families, lack of standardized datasets, and difficulty in interpreting complex deep learning decisions. The study suggests that future research should focus on developing more robust, explainable, scalable, and adaptive malware detection architectures capable of operating against rapidly changing cyber threats.

A. R. Redhu et al. [5] investigated the role of deep learning in modern cyberspace malware detection through a contemporary review of existing approaches, methodologies, and challenges. The authors discussed the increasing dependence on intelligent cybersecurity systems as malware becomes more diverse and difficult to identify using traditional signature-based mechanisms. The study examined the use of deep learning for extracting meaningful patterns from different types of malware-related data, including executable characteristics, byte sequences, behavioral information, and other system-level features. CNNs, recurrent neural networks, autoencoder-based approaches, and other neural architectures were discussed in the context of automated malware identification and classification. The review also emphasized the importance of combining effective feature representation with suitable deep learning architectures to improve detection performance. In addition, the authors highlighted practical challenges such as adversarial attacks, malware obfuscation, dataset imbalance, computational complexity, false-positive detection, and the requirement for continuously updated training data. The study concluded that deep learning provides substantial opportunities for improving cybersecurity defenses, but future malware detection systems need to become more robust, explainable, computationally efficient, and capable of detecting previously unseen malware. This work therefore provides a useful contemporary perspective on the application of deep learning techniques for intelligent malware detection in evolving cyberspace environments.

Omer Aslan et al. [6] have mechanical advances in the PC framework shift human existence from a real state to a virtual one. COVID-19 has accelerated this cycle. The dominance of digital gangs is also shifting from real life to virtual life. This is because cheating is more likely to occur on the Internet than in the real world. Malicious programming (malware) is unwanted programming commonly used by digital criminals to carry out digital attacks.

Malware variants continue to evolve using sophisticated disruptive and offensive techniques. These concealment strategies make malware detection and characterization a fundamental challenge. Successfully dealing with new malware variants requires employing new techniques that are very unique compared to traditional strategies. Traditional artificial intelligence (artificial intelligence) explicit AI (ML) computations are currently unable to detect all new and complex malware variants. Deep learning (DL) approaches are not exactly identical to traditional ML computations, but they may be a promising answer to the problem of identifying all malware variants.

K. Bhargavi et al. [7] in military cases, the Web of Things (IoT) is typically made of an assortment and hubs for the Web (for example Versatile military coats as well as symptomatic gear). This IoT framework and organization is a significant objective for malevolent, particularly for people financed by the state or without a doubt the political element. Malware use is a famous passage. This paper presents a strategy for tremendous data to introduce noxious on the Web of Combat zone Things (IoBT) or the web of military things (IoMT) through the OpCode grouping of both the framework. They change OpCodes in a vector field and execute a significant procedure for examining to recognize unsafe and fruitful programming. The particularity of certain proposed malware examination technique and the practical advancement towards infusion of trash programming dangers are without a doubt illustrated. At last, we have our Github pernicious investigation, that they accept will help continuous examinations (for example to advance appraisal of likely supporter of malware discovery).

M. D. AlGarni et al. [8], the prevalence of malicious programming attacks (malware) poses a serious threat to online security today. Malware poses a threat to anyone who uses the Internet because it can steal information and damage PC systems. Similarly, the prevalence of malware threats impacting large numbers of PC customers, organizations and the law has made malware identification an important topic of scientific research. Current malware detection techniques rely on static and dynamic inspection of malware marks and behaviors to incrementally detect unknown malware, which is slow and ineffective. This article then examines the role of deep convolutional brain networks in malware grouping and provides answers on using AI to distinguish and characterize malware families through movement learning. We proposed a pretrained CNN model to find ways to characterize malware families. The research was conducted using two network data sets, including Maling and ImageNet. We assembled a maling dataset that uses Practical Executable to convert malware pairs into malware images. The results show that the EfficientNet3 model achieved a high accuracy of 99.93%.

S. Kumar et al. [9] the proliferation of online gadgets can reach malicious targets for attackers. They use malicious projects to think of devices and use them to infect other devices as well. Security scientists strive to drive the process of accurately distinguishing all malware using powerful malware hardening techniques such as strong cryptography, obscurity, polymorphism, and transformation engines. In this particular case, this paper proposes a new malware order-with-tweak-convolution-brain organization model (MCFT-CNN).

Ö. Aslan et al. [10] malicious programming (malware) is growing at an alarming rate, according to new research, and some malware may use other obfuscation strategies to lurk on systems. Protecting PC frameworks and the web from malware requires identifying malware before it affects millions of frameworks. There has been quite a bit of research lately on where future malware is located. Either way, identifying residual malware is risky. Signature-based and heuristic-based localization approaches are fast and effective in distinguishing known malware, but signature-based detection methods in particular fail to identify obscure malware. On the other hand, behavior-based, model-validation-based, and cloud-based approaches work well against obscure and complex malware. The purpose of this article is to help researchers get an overview of malware detection approaches, the strengths and weaknesses of each identification approach, and the strategies employed by these methods.

Problem Formulation

Moreover, existing approaches use categorization of permission that is suggested by Google [9]. There are four categories of permissions according to Google: Normal, Dangerous, Signature, System. The normal permissions are automatically granted by the Android System, while the user's consent is required for the dangerous permissions. This conceptual categorization provided by Google is not working well when association of permissions is considered. For example, READ PHONE STATE is a normal permission according to Google, which reads some information from the mobile device like identifiers, IMEI numbers etc. But when it is present along with another permission, say INTERNET (normal permission as per Google Categorization), there are more chances that these information can be sent to some remote server and it might fall into the hands of hackers. Based on this motivation, many research groups focus on securing Android devices from malicious applications. In malware detection one of the research interests is to use machine learning techniques, to detect malware. Use of machine learning methodologies helps detect zero-day malware, as it allows an unknown application to be classified as suspicious or identify it as benign [10].

4. DEEP LEARNING

Deep learning is a subset of machine learning techniques focused on classification tasks and evolutionary algorithms [14]. There are three types of learning: supervised learning, semi-supervised and unsupervised. Deep-learning architectures incorporating deep learning models, fully connected networks, recurrent neural networks, and artificial neural networks were used in fields involving machine learning, artificial intelligence, computer vision, data analysis, realized, social media site filtering, computational linguistics, computational biology, drug design, information retrieval, and clear overview, among others [15]. Knowledge acquisition and decentralized organizational infrastructure in biological systems influenced artificial neural networks (ANNs). ANNs vary from the human brain in several ways. In particular, neural networks are constant and symbolic, whereas most functioning entities' biological brains are dynamic and analog.

Deep learning gets its name from the fact that it employs many layers in the network. Early research demonstrated that a linear perceptron cannot be used as a universal classifier but that

a network with a non-polynomial input layer and one unrestrained width hidden layer may [59]. Deep learning is a more recent variant involving many layers of bounded size, allowing for functional application and optimization while maintaining theoretical subjectivity under mild conditions. For the sake of performance, trainability, and intelligibility, deep learning structures are also allowed to be diverse and veer away widely from scientifically informed connectionist models, hence the "organized" portion [16].

The majority of new deep learning techniques focus on machine learning, especially convolutional neural networks (CNNs). They may also include propositional formulas or latent variables structured layer-wise in deep generative models like deep belief networks and deep Boltzmann machines. Each level of deep learning learns to turn the data it receives into a slightly more abstract and composite representation. The raw input in an image recognition program could be a matrix of pixels; the first representative layer could abstract the pixels and encode edges; the second layer could compose and encode edge arrangements; the third layer could encode a nose and eyes, and the fourth layer could recognize that the image contains a face. Importantly, a deep learning algorithm may figure out which features belong to which level on its own.

The term "deep learning" refers to the number of layers that the data is transformed through. Deep learning systems, in particular, have a significant credit assignment path (CAP) depth [5]. The CAP is the input-to-output transition chain. CAPs are used to define possible causal relationships between input and output. The depth of the CAPs in a feedforward neural network is equal to the network's depth plus the number of hidden layers plus one. The CAP depth in recurrent neural networks, where a signal can propagate through a layer multiple times, is theoretically unlimited. Although no generally agreed-upon depth level separates shallow and deep learning, most researchers agree that deep learning needs a CAP depth greater than 2. In the sense that it can imitate any function, CAP of depth two is a universal approximate [7].

5. CONCLUSION

Malware has become one of the major and continuously evolving cybersecurity threats due to the rapid growth of connected devices, cloud platforms, mobile applications, IoT environments, and digital services. Traditional signature-based malware detection techniques are effective for identifying previously known threats but have limitations in detecting new, polymorphic, obfuscated, and zero-day malware. The reviewed studies demonstrate that deep learning techniques provide an effective alternative because they can automatically learn complex and discriminative features from malware data without depending entirely on manually designed signatures. CNN, RNN, LSTM, autoencoder, transfer learning, and other deep learning architectures have been successfully investigated for malware detection and classification using static, dynamic, and hybrid analysis approaches.

The literature also indicates that the performance of deep learning-based malware detection depends strongly on the quality and diversity of datasets, feature representation, preprocessing techniques, and model architecture. Although deep learning models can achieve promising detection and classification performance, several challenges remain,

including class imbalance, malware obfuscation, adversarial attacks, computational complexity, limited availability of representative datasets, false positives, and lack of model interpretability. These limitations can reduce the reliability of intelligent malware detection systems when they are deployed against continuously changing real-world threats.

REFERENCES

- [1] M. Alshoulie and A. Mehmood, "Deep Learning Approaches for Malware Detection: A Comprehensive Review of Techniques, Challenges, and Future Directions," *IEEE Access*, vol. 13, pp. 118652–118677, 2025, doi: 10.1109/ACCESS.2025.3582875.
- [2] P. Maniriho, A. N. Mahmood, and M. J. M. Chowdhury, "A Survey of Recent Advances in Deep Learning Models for Detecting Malware in Desktop and Mobile Platforms," *ACM Computing Surveys*, vol. 56, no. 6, Art. 145, pp. 1–41, 2024, doi: 10.1145/3638240.
- [3] H. Wang, B. Cui, Q. Yuan, R. Shi, and M. Huang, "A Review of Deep Learning Based Malware Detection Techniques," *Neurocomputing*, vol. 598, Art. 128010, 2024, doi: 10.1016/j.neucom.2024.128010.
- [4] A. Bensaoud, J. Kalita, and M. Bensaoud, "A Survey of Malware Detection Using Deep Learning," *Machine Learning with Applications*, vol. 16, Art. 100546, 2024, doi: 10.1016/j.mlwa.2024.100546.
- [5] A. R. Redhu, P. Choudhary, K. S. Srinivasan, and T. K. Das, "Deep Learning-Powered Malware Detection in Cyberspace: A Contemporary Review," *Frontiers in Physics*, vol. 12, 2024, Art. 1349463, doi: 10.3389/fphy.2024.1349463.
- [6] Omer Aslan and Abdullah Asim Yilmaz, "A New Malware Classification Framework Based on Deep Learning Algorithms", *IEEE Access* 2021.
- [7] K. Bhargavi N. Vadivelan S. Kodati and M. Nalini "M. Secure internet of battlefield from malicious software using deep eigenspace learning" In *AIP Conference Proceedings* vol. 2405 no. 1 pp. 030002 2022.
- [8] M. D. AlGarni R. AlRoobaea J. Almotiri S. S. Ullah S. Hussain and F. Umar "An efficient convolutional neural network with transfer learning for malware classification" *Wireless Communications and Mobile Computing* pp. 1-8 2022.
- [9] S. Kumar "MCFT-CNN: Malware classification with fine-tune convolution neural networks using traditional and transfer learning in Internet of Things" *Future Generation Computer Systems* vol. 125 pp. 334-351 2021.
- [10] Ö. Aslan and R. Samet, "A comprehensive review on malware detection approaches," *IEEE Access*, vol. 8, pp. 6249–6271, Jan. 2020.
- [11] R. Komatwar and M. Kokare, "A survey on malware detection and classification," *J. Appl. Secur. Res.*, pp. 1–31, Aug. 2020.
- [12] A. A. Yilmaz, M. S. Guzel, E. Bostanci, and I. Askerzade, "A novel action recognition framework based on deep-learning and genetic algorithms," *IEEE Access*, vol. 8, pp. 100631–100644, 2020.

- [13] A. A. Yilmaz, M. S. Guzel, I. Askerbeyli, and E. Bostanci, “A vehicle detection approach using deep learning methodologies,” in Proc. Int. Conf. Theor. Appl. Comput. Sci. Eng., Nov. 2018, pp. 64–71.
- [14] A. A. Yilmaz, M. S. Guzel, I. Askerbeyli, and E. Bostanci, “A hybrid facial emotion recognition framework using deep learning methodologies,” in Human-Computer Interaction, T. Özseven, Eds. Hauppauge, NY, USA: Nova Science Publishers, 2020.
- [15] S. A. Roseline, S. Geetha, S. Kadry, and Y. Nam, “Intelligent vision-based malware detection and classification using deep random forest paradigm,” IEEE Access, vol. 8, pp. 206303–206324, 2020.
- [16] M. Nisa, J. H. Shah, S. Kanwal, M. Raza, M. A. Khan, R. Damaševičius, and T. Blažauskas, “Hybrid malware classification method using segmentation-based fractal texture analysis and deep convolution neural network features,” Appl. Sci., vol. 10, no. 14, p. 4966, 2020.
- [17] J. Love. (2018). A Brief History of Malware—Its Evolution and Impact. Accessed: Mar. 20, 2021. [Online]. Available: <https://www.lastline.com/blog/history-of-malware-its-evolution-and-impact/>
- [18] D. Palmer. (2017). Ransomware: Security Researchers Spot Emerging New Strain of Malware. Accessed: Mar. 20, 2021.
- [19] Ö. Aslan, “Performance comparison of static malware analysis tools versus antivirus scanners to detect malware,” in Proc. Int. Multidisciplinary Stud. Congr. (IMSC), 2017, pp. 1–6.
- [20] S. K. Pandey and B. M. Mehtre, “Performance of malware detection tools: A comparison,” in Proc. IEEE Int. Conf. Adv. Commun., Control Comput. Technol., May 2014, pp. 1811–1817.