WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Cyber Threat Detection to Protect Our Digital Ecosystem Using Machine Learning

Ms. Sahana Bisalapur [a], Soundarya c. k [b], Nisarga k [c], Pooja Arakeri [d], Srushti Sannaki [e]

[a,b,c,d,e] *Department of Computer Science and Engineering, S.G Balekundri Institute of Technology , Belagavi-590009, India*

A B S T R A C T

Malware, the lethal weapon of cyber attackers, is becoming increasingly sophisticated rapid adoption and distribution. In addition, modern malware is one of the most destructive forms of cybercrime because it can evade detection, making digital forensics almost real-time impossible, and the consequences of sophisticated avoidance strategies can be severe and far-reaching. This It must be detected early and independently to ensure effective analysis. This work proposes a new systematic approach for modern malware detection using dynamic depth learning-based methods combined with heuristic approaches using five state-of-the-art classification and detection malware families: adware, radware, rootkits, SMS malware and ransomware. Our symmetry Artificial intelligence research and cybersecurity analytics improve malware detection, analytical and mitigation capabilities that provide cyber systems resilient to cyber threats. We have confirmed our approach using a dataset specifically containing recent malware to demonstrate this the model achieves its goals and meets the actual performance and requirements effectiveness Experimental results show that the combination of behaviors deep learning and heuristic approaches to malware detection and classification outperform static usage deep learning methods.

Keywords: Artificial Intelligence, Malware, Detection System, Malware Prevention Technology, Software Security.

1. Introduction

Despite the significant improvement in technology and its positive impact on facilitation people's lifestyle and the rapid growth of internet usage in people's daily life, all these evolution offers malware authors a great opportunity to expand their work and expand their operations spread malware. This increase was particularly evident in the last two years under review record due to COVID-19 [1]. The pandemic forced people to switch to remote work and increase daily internet usage during shutdown. international 2021 statistics from the Telecommunications Union (ITU) showed that 2019 has started during the pandemic, about 54% of the world's population of about 4.1 billion people used the Internet. in 2020 The number of Internet users increased by 10.2%, which is a jump according to statistics reported [2]. This number continues to grow; used by almost two-thirds of the world's population Internet [3].

In connection with this growth, malicious programs (Malware) are considered a major threat. worldwide, which continues to grow exponentially. According to a recent study [4] by the AVTest Institute, approximately 450,000 malware cases are detected every day. Originally malware the authors target computer users, especially Windows users, but through development technology makes people less dependent on computers and other operating systems (DICTIONARY); Android, iOS. This creates a new opportunity for malware authors to distribute their malware through other operating systems.

Figure 1 illustrates how Android users are growing compared to others DICTIONARY. Malware authors extend their targeting to more than one platform, making containment difficult the spread of malware.

Figure 1: Operating System Market

Malware comes in many forms; Viruses, worms, rootkits, ransomware, etc. Ransomware [6] It is considered the most severe of them because it encrypts the victim's files and demands a ransom switch to decryption, causing attackers to use it widely in business. In addition, they target organizations and not just individuals [7].

Based on previous research in the area of malware detection, analyze the malware sample there there are two methods; static analysis and dynamic analysis. Static analysis [8][9] depends examine a suspect sample without doing so. Static analysis [8][9] depends examine a suspect sample without doing so. Traditionally based on static analysis Heuristic and signature-based methods. Heuristic analysis involves a set of rules that are determined by experts, while signature-based depends on signatures that are the unique identifier of the binary file. Both methods are effective and easy to detect malware with a limited false positive rate. However, these technologies cannot detect anything variants of this malware in addition to not being able to detect unknown malware.

On the other hand, dynamic analysis [10] involves running a suspect sample in a vault an environment that allows analysts to observe its behavior, for example; Application programming Interface (API) calls, system calls or network traffic try to find suspicious activity. On the other hand, dynamic analysis

[10] involves running a suspect sample in a vault an environment that allows analysts to observe its behavior, for example; Application programming Interface (API) calls, system calls or network traffic try to find suspicious activity Dynamic analysis is more effective than static [11] because it can identify new and unknown malware. However, dynamic analysis takes time and resources the presence of avoidance methods prevents dynamic analysis if the sample shrinks it functionality when it detects that it is working in an isolated environment [12], making it difficult improved malware detection.

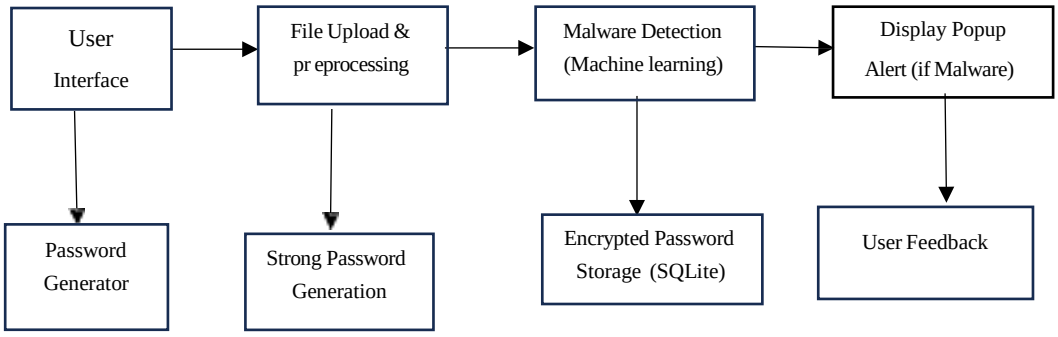
Artificial intelligence (AI), with all its advances, can provide effective detection advanced malware. By combining harmful and benevolent behavior modeling, it can be successful facilitates the detection of harmful. Researchers aim to create models that are can detect different types of malware, including unknown and zero-day malware. In the year Various AI-based malware detection techniques, including machines, have been proposed in the literature Learning (ML) [13][14][15] and Deep Learning (DL) [16][17][18].

This paper reviews the literature on malware detection using artificial intelligence techniques. especially ML and DL techniques in both desktop and mobile malware. In addition, this paper discusses the analysis methods, state-of-the-art data, limitations and challenges which researchers face.

2. Methodology

The method adopted for this research andquot; malware detection and prevention using artificial intelligence techniques and quot; includes an in-depth study of existing literature that examines various artificial intelligence techniques used in industry. It is based on deep analysis of machine learning algorithms, deep learning models and natural language processing. The research further explores the datasets used to train and test AI models, highlighting their diversity and characteristics to shed light on real-world challenges. The effect of feature selection and extraction methods on detection accuracy is investigated, while evaluation of training and testing protocols, including metrics such as precision and recall, provides insight into model performance.

In addition, the study explores the integration of artificial intelligence into traditional malware detection methods, with an emphasis on real-time detection and prevention capabilities. The paper examines an important aspect of adversarial attacks against AI models and suggests strategies to improve their resilience. Real-world case studies and practical applications are thoroughly explored and provide valuable insights into the application of AI in various organizational settings. Finally, the study outlines possible future directions and identifies emerging technologies and areas that require further research to advance malware detection and prevention using artificial intelligence



3. Comparison Table

References	Algorithm/classifiers	Techniques	Results	Limitation	Accuracy
Md Jobair Hossain Faruk ∗, Hossain Shahriar†, Maria Valero†, Farhat Lamia Barsha‡, Shahriar Sobhan¶ Md Abdullah Khan§, Michael Whitman¶, Alfredo Cuzzocreak , Dan Lo§, Akond Rahman‡ and Fan Wu∗∗	genetic algorithm along with neural network	statistical and mathematical techniques	Malware Detection and Prevention using Artificial Intelligence Techniques	It has limitations in detecting unknown malware. Analyzing the limitations of detection systems is vital to deal with novel techniques for malware detection and prevention.	98.32%
Hend Faisal1, 2, Hanan Hindy1, Samir Gaber2,3, Abdel-Badeeh Salem1	Recurrent Neural Networks (RNN), Convolutional Neural Networks (CNN), Multilayer Perceptron (MLP), Deep Belief Network (DBN)and Long Short Term Memory Network (LSTM)	Hybrid	A Survey on artificial intelligence Techniques for malware detection	Anti-analysis Techniques, Obfuscation and Packing, Dataset, Evolution of malware, AI Obstacles	96%
Amir Djenna 1,*, Ahmed Bouridane 2, Saddaf Rubab 3, and Ibrahim Moussa Marou 1	Deep learning algorithms (CNN and DNN) machine learning algorithms (RF and DT).	Static, Dynamic	Artificial Intelligence-Based Malware Detection, Analysis, and Mitigation	Deep learning-based methods often face difficulties in identifying and analyzing different variants of malware in real time.	Accuracy results are not mentioned .
Dhanashree Paste1, Trupti Wadkar2	Support Vector Machine (SVM) algorithm and the Decision Tree algorithm	Static, Dynamic and Hybrid	Malware: Detection, Classification and Protection	Traditional machine learning algorithms are often difficult to process large unknown anonymous samples of malware.	97.8%

4. Conclusion

The battle between malware analysts and malware threat actors is a never-ending battle. Therefore, it is necessary to constantly find new effective ways to detect malware. In addition, there is artificial intelligence is widely used in many research fields, including malware detection. This article introduced a literature review on malware detection using different AI methods, mostly ML and DL. The evaluated works were categorized into computer-based and Android-based platforms because the incredibly fast evolution of malware. Articles are compared according to the approaches used, classification algorithms, datasets and techniques. In addition, the paper shows how the function extraction and selection processes affect the accuracy of the recognition model both as ML and DL can be effective in detecting malware. In addition, the article highlights and discusses various challenges and limitations facing malware detection research. Although different Malware detection approaches have been proposed, but none is claimed to detect all the endless evolution of malware. New approaches should be proposed as future work increase detection speed and fight advanced malware.

References

[1] Md Jobair Hossain Faruk∗, Hossain Shahriar†, Maria Valero†, Farhat Lamia Barsha‡, Shahriar Sobhan¶ Md Abdullah Khan§, Michael Whitman¶ Alfredo Cuzzocreak, Dan Lo§, Akond Rahman‡ and Fan Wu∗∗" Malware Detection and Prevention using Artificial Intelligence Techniques" 2021 IEEE International Conference on Big Data. https://www.researchgate.net/publication/357163392

[2] Amir Djenna 1 ,*, Ahmed Bouridane 2, Saddaf Rubab 3 and Ibrahim Moussa Marou 1. "Artificial Intelligence-Based Malware Detection, Analysis, and Mitigation" 8 March 2023

[3] Hend Faisal1,2, Hanan Hindy1, Samir Gaber2,3, Abdel-Badeeh Salem1, "A SURVEY ON ARTIFICIAL INTELLIGENCE TECHNIQUES FOR MALWARE DETECTION"

[4] Dhanashree Paste1, Trupti Wadkar2 "Detection, Classification and Protection" 08 Issue: 08 | Aug 2021"

[5] Hend Faisal1,2, Hanan Hindy1, Samir Gaber2,3, Abdel-Badeeh Salem1, "A SURVEY ON ARTIFICIAL INTELLIGENCE TECHNIQUES FOR MALWARE DETECTION" pp. 91-108, 2022. CS & IT - CSCP 2022

[6] N. A. Khan, S. N. Brohi, and N. Zaman, "Ten deadly cyber security threats amid COVID-19 pandemic," 2020. TechRxiv, doi: 10.36227/techrxiv.12278792.v1.

[7] Facts and figures, "Internet use," 2021. Available: https://www.itu.int/itud/reports/statistics/2021/11/15/internet-use/ Accessed: (10 June 2022).

[8] P. O'Kane, S. Sezer, and D. Carlin, "Evolution of ransomware," Iet Networks, vol. 7, no. 5, pp. 321– 327, 2018.

[9] B. A. S. Al-rimy, M. A. Maarof, and S. Z. M. Shaid, "Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions," Computers & Security, vol. 74, pp. 144– 166, 2018.

[10] O. Or-Meir, N. Nissim, Y. Elovici, and L. Rokach, "Dynamic malware analysis in the modern era—a state of the art survey," ACM Computing Surveys (CSUR), vol. 52, no. 5, pp. 1–48, 2019.

[11] H. F. Md Jobair, M. Paul, C. Ryan, S. Hossain, and C. Victor, "Smart connected aircraft: Towards security, privacy, and ethical hacking," International Conference on Security of Information and Networks, 2022.

[12] S. Subramanya and N. Lakshminarasimhan, "Computer viruses," Potentials, IEEE, vol. 20, pp. 16 – 19, 11 2001.

[13] N. Milosevic, "History of malware," 02 2013.

[14] H. Hassani, E. Silva, S. Unger, M. Tajmazinani, and S. MacFeely, "Artificial intelligence (ai) or intelligence augmentation (ia): What is the future?" AI, vol. 1, p. 1211, 04 2020.

[15] A. P. Namanya, A. Cullen, I. Awan, and J. Pagna Diss, "The world of malware: An overview," 09 2018.

[16] O. Adebayo, M. A., A. Mishra, and O. Osho, "Malware detection, supportive software agents and its classification schemes," International Journal of Network Security Its Applications, vol. 4, pp. 33–49, 11 2012.

[17] A. K.S., "Impact of malware in modern society," Journal of Scientific Research and Development, vol. 2, pp. 593– 600, 06 2019.