IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 11, Issue 12, December 2022

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.118

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.118|

|| Volume 11, Issue 12, December 2022 ||

| DOI:10.15680/IJIRSET.2022.1112075 |

Network Attack and Defense Counter Measure Technology Based on Artificial Intelligence

Mr.Naveenkumar D, Mr.T.Saransujai M.E,

Department of Information Technology, KSR College of Engineering, Tiruchengode, Tamilnadu, India

ABSTRACT: Artificial intelligence techniques have grown rapidly in recent years, and their applications in practice can be seen in many fields, ranging from facial recognition to image analysis. In the cybersecurity domain, AI-based techniques can provide better cyber defense tools and help adversaries improve methods of attack. However, malicious actors are aware of the new prospects too and will probably attempt to use them for nefarious purposes. This survey paper aims at providing an overview of how artificial intelligence can be used in the context of cybersecurity in both offense and defense.

I. INTRODUCTION

Cybersecurity involves the devising of defense strategies that preserve computing resources, networks, programs, and data from unauthorized access, change, or destruction. Due to the dramatic advances in information and communication technologies, new cybersecurity threats are emerging and changing rapidly. Cybercriminals are adopting new and sophisticated techniques that increase the speed and scale of their attacks. Hence, there is a requirement for more flexible, adaptable, and robust cyber defense systems that are capable of detecting a wide variety of threats in real-time. In recent years, the adoption of artificial intelligence (AI) techniques has been rising and maintaining a crucial role in cyber threat detection and prevention.

While the concept of AI was proposed in the 1950s, in recent years, it has grown at a significant pace and is now influencing all aspects of communities and occupations. Many areas benefit from AI, such as gaming, natural language processing, health care, manufacturing, education, and others. This trend is also affecting the cybersecurity field where AI has been utilized for both attacking and defending in the cyberspace. On the offense side, cyber threats can employ AI to improve the sophistication and scope of their attacks. On the defense side, AI is utilized to enhance the defense strategies, so that the defense systems become more robust, flexible, and efficient, which involves being adaptive with changes in the environment to decrease the impacts occurred.

Recently, researchers presented several surveys in the domain of AI and cybersecurity. However, some of them just focused on the adopting machine learning methods for cyber problems such as those in. Other research just focused on deep learning methods. Additionally, there is a lack of literature dealing with the nefarious use of AI.Apruzzeseetal.performed a survey on ML and DL methods for cyber security. Nevertheless, their research was just covering attacks related particularly to network intrusion detection, malware investigation, and spam identification.

The author in discussed the intersection of AI and cybersecurity. More particularly, the paper reviewed some ML and DL approaches to counter against cyber attacks. What is more, the author introduced the possibility of attacking the AI model. Nevertheless, the paper just discussed adversarial attacks and ignored other kinds of attack using the AI model, such as poisoning data, and the extraction model.Another approach by the authors in pointed out the differences between traditional ML and DL methods for cybersecurity. However, their survey just concentrated on intrusion detection.Based on the above circumstances, this survey paper pursues a two-fold goal. The first is to carry out an exploration of the impact of AI in cybersecurity. The second is to replenish the literature with recent reviews on cyber applications of AI methods.

II. LITERATURE SURVEY

1. Artificial Intelligence Security: Threats and Countermeasures
Author: Yupeng Hu, WenxinKuang, Zheng Qin, Kenli Li,

In recent years, with rapid technological advancement in both computing hardware and algorithm, Artificial Intelligence (AI) has demonstrated significant advantage over human being in a wide range of fields, such as image

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.118|

|| Volume 11, Issue 12, December 2022 ||

| DOI:10.15680/IJIRSET.2022.1112075 |

recognition, education, autonomous vehicles, finance, and medical diagnosis. However, AI-based systems are generally vulnerable to various security threats throughout the whole process, ranging from the initial data collection and preparation to the training, inference, and final deployment. In an AI-based system, the data collection and pre-processing phase are vulnerable to sensor spoofing attacks and scaling attacks, respectively, while the training and inference phases of the model are subject to poisoning attacks and adversarial attacks, respectively. To address these severe security threats against the AI-based systems, in this article, we review the challenges and recent research advances for security issues in AI, so as to depict an overall blueprint for AI security. More specifically, we first take the lifecycle of an AI-based system as a guide to introduce the security threats that emerge at each stage, which is followed by a detailed summary for corresponding countermeasures. Finally, some of the future challenges and opportunities for the security issues in AI will also be discussed.

2. Research and implementation of network attack and defense countermeasure technology
Author: FeiShu; ShuTing Chen; Feng Li; JianYe Zhang; Jia Chen

Using artificial intelligence technology to help network security has become a major trend. At present, major countries in the world have successively invested R & D force in the attack and defense of automatic network based on artificial intelligence. The U.S. Navy, the U.S. air force, and the DOD strategic capabilities office have invested heavily in the development of artificial intelligence network defense systems. DARPA launched the network security challenge (CGC) to promote the development of automatic attack system based on artificial intelligence. In the 2016 Defcon final, mayhem (the champion of CGC in 2014), an automatic attack team, participated in the competition with 14 human teams and once defeated two human teams, indicating that the automatic attack method generated by artificial intelligence system can scan system defects and find loopholes faster and more effectively than human beings. Japan's defense ministry also announced recently that in order to strengthen the ability to respond to network attacks, it will introduce artificial intelligence technology into the information communication network defense system of Japan's self defense force.It can be predicted that the deepening application of artificial intelligence in the field of network attack and defense may bring about revolutionary changes and increase the imbalance of the strategic strength of cyberspace in various countries.

III. EXISTING SYSTEM

The purpose of Malware detection is to protect the system from various kinds of malicious attacks by following the policy of detection and prevention. There are various existing algorithms to detect malware, however, with the advancement of malware technology, the adoption of Artificial Intelligence is crucial for efficient, and robust malware prevention applications. In order to detection of malware, finding the malicious source code is the very first step. Researchers proposed a technique called SourceFinder to identify malware source code repositories which is the largest malware source code database. The research showed that the proposed approach identifies malware repositories with 89 % precision and 86 % recall while it identifies 7504 malware source code repositories using SourceFinder followed by analyzing properties and characteristics of repositories.

PROPOSED SYSTEM
Apart from machine learning, other techniques are also used in malware detection like cloud computing, networkbased detection system, virtual machine, or the use of hybrid methods and technologies. Nowadays Deep learning and Artificial are actively applied in malware detection. Irina Baptistaetalintroduces a novel approach for malware detection by utilizing binary visualization and self-organizing incremental neural networks. A demonstration was conducted on detecting malicious payloads in various file types including Portal Document File .pdf and Microsoft Document Files .doc files where the experimental results indicate a detection accuracy of 91.7% and 94.1% for ransomware respectively. According to the authors, the proposed technique performed well with an incremental detection rate, allowing for efficient real-time identification of unknown malware. In a separate study, Syam and propose a detection way where a virtual analyst was developed by using Artificial Intelligence to defend threats and take appropriate measurements.

Research Methodology
In order to carry out the study on Malware Detection Techniques using AI, we utilize a systematic literature review [31]. The main purpose of the systematic review is to identify, study, and investigate the suitable existing approaches. We first carried out a “Search Process” to identify potential research papers from the scientific databases using pre-

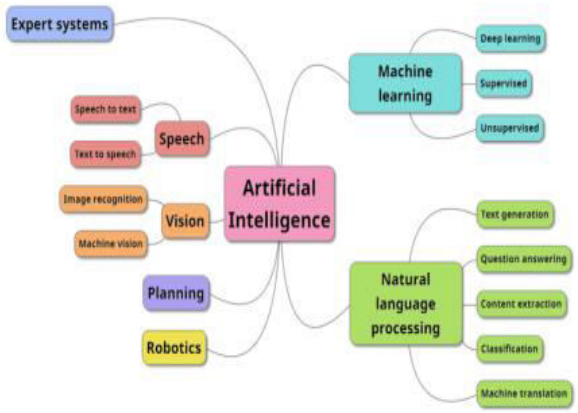
| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.118|

|| Volume 11, Issue 12, December 2022 ||

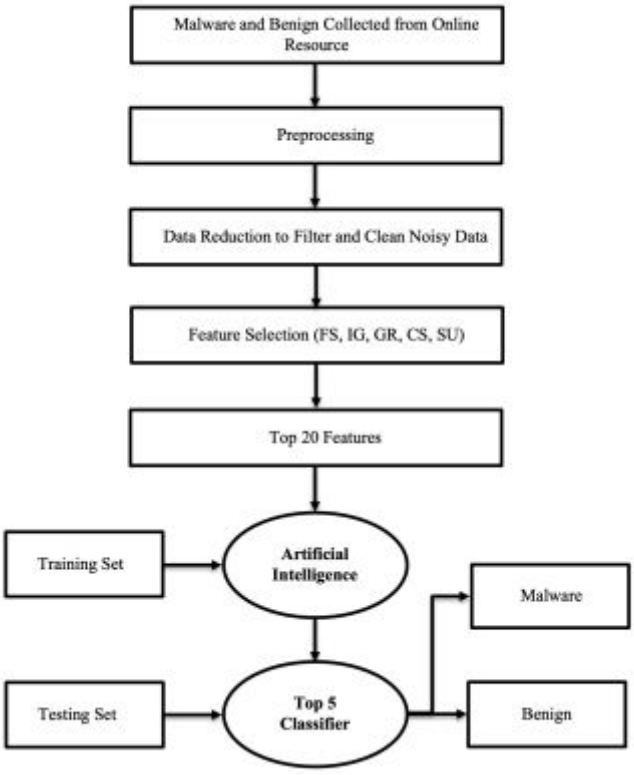
| DOI:10.15680/IJIRSET.2022.1112075 |

selected search keywords or strings including "Artificial Intelligence" AND ("Malware" AND "Detection" OR "Prevention") OR "AI". We had to identify these search strings to avoid findings from non-related research papers and those keywords are based on the Malware and Artificial Intelligence related terms and their derivatives, acronyms, and widely used synonyms. Besides, among various scientific databases, we used three digital database sources including
(i) IEEE Xplore
(ii) ScienceDirect, and
(iii) Springer Link.

Choosing these three bibliographic databases, our goal is to identify research papers that were published in reputable conferences, journals, and books.



RESULT



AI Based Unknown Malware Detection Techniques

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.118|

|| Volume 11, Issue 12, December 2022 ||

| DOI:10.15680/IJIRSET.2022.1112075 |

Heuristic analysis is divided into two parts- static and dynamic where it performs code mapping which is a difficult process as some characteristics of a virus can be implemented in various ways. Dynamic heuristic analysis is better comparably with static analysis regardless of its slow process. One of the limitations of dynamic processes is the failure not to detect certain active viruses in a certain situation. For instance, performing any operation by the user may interrupt the heuristic dynamic analysis. Integrity checking may solve the limitation of dynamic heuristic analysis, able to detect viruses with certainty if accuracy can be ignored because of its record in failure cases. Other than that, integrity checking always assumes that the starting state of a file is unaffected but this can be false often. Malware detection techniques are working simultaneously to detect malicious software applications. In order to improve the efficiency of malware detection techniques, improvement of existing limitations is a major fact and dynamic solutions are needed to reduce malware feature analysis time, and more sophisticated approaches should be applied to detect malicious activities. Utilizing artificial intelligence (AI) technology in the development of both malware detection and prevention needs to be increased to deal with intelligent malware that has grown in recent years.

IV. CONCLUSION

Malware or malicious applications may cause catastrophic damages to not only computer systems but also data centers, web, and mobile applications to various industries; particularly, financial and healthcare institutes. Ensuring the safety of stakeholders' data from malicious entities is a major challenge that leads us towards the concept of malware detection and prevention. Artificial Intelligence (AI) can be an effective solution that we can adopt for the development of AntiMalware Systems. Having such direction, this study presented a detailed review of malware detection techniques and approaches. At first, we attempted to provide a clear overview of malware, artificial intelligence, and its narration. An overview of existing malware detection systems was discussed in followed by identifying the limitations of existing applications. Likely every system, the malware detection approaches also consist of a number of limitations along with facilities and improvements from its previous version. So far, our findings indicate that AI can be utilized as a promising domain for the development of anti-malware systems for detecting and preventing malware attacks or security risks of software applications towards a technological wonderland. To draw a conclusion, we discuss scores of ideas to overcome the identified limitations and aim to continue our effort explicitly towards significant accomplishments around the domain of Malware Detection and Prevention.

REFERENCES

[1] O. Asaolu, "On the emergence of new computer technologies."Educational Technology Society, vol. 9, pp. 335–343, 01 2006.
[2] Z. Arsic and B. Milovanovic, "Importance of computer technology in realization of cultural and educational tasks of preschool institutions," International Journal of Cognitive Research in Science, Engineering and Education, vol. 4, pp. 9–15, 06 2016.
[3] A. P. Gilakjani, "A detailed analysis over some important issues towards using computer technology into the efl classrooms," Universal Journal of Educational Research, vol. 2, pp. 146–153, 2014.
[4] H. F. MdJobair, 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.
[5] S. Subramanya and N. Lakshminarasimhan, "Computer viruses," Potentials, IEEE, vol. 20, pp. 16 – 19, 11 2001.
[6] S. Levy and J. Crandall, "The program with a personality: Analysis of elk cloner, the first personal computer virus," 07 2020.
[7] N. Milosevic, "History of malware," 02 2013.
[8] A. P. Namanya, A. Cullen, I. Awan, and J. PagnaDiss, "The world of malware: An overview," 09 2018.
[9] I. Khan, "An introduction to computer viruses: Problems and solutions," Library Hi Tech News, vol. 29, pp. 8–12, 09 2012.
[10] M. Bishop, "An overview of computer viruses in a research environment," USA, Tech. Rep., 1991.
[11] D. B. Patil and M. Joshi, "A study of past, present computer virus performance of selected security tools," Southern Economist, 12 2012.
[12] A. Terekhov. History of the antivirus.[Online]. Available: https://www.hotspotshield.com/blog/history-of-the-antivirus

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.118|

|| Volume 11, Issue 12, December 2022 ||

| DOI:10.15680/IJIRSET.2022.1112075 |

[13] M. J. HossainFaruk, H. Shahriar, M. Valero, S. Sneha, S. Ahamed, and M. Rahman, "Towards blockchain-based secure data management for remote patient monitoring," IEEE International Conference on Digital Health (ICDH), 2021.
[14] M. J. HossainFaruk, "Ehr data management: Hyperledger fabric-based health data storing and sharing," The Fall 2021 Symposium of Student Scholars, 2021.
[15] S. Ryan, R. Mohammad A, H. F. MdJobair, S. Hossain, and C. Alfredo, "Ride-hailing for autonomous vehicles: Hyperledger fabric-based secure and decentralize blockchain platform," IEEE International Conference on Big Data, 2021.
[16] D. G. Vigna. (2020) Howai will help in the fight against malware. [Online]. Available: https://techbeacon.com/security/how-ai-will-helpfight-against-malware
[17] 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.
[18] A. I. Nones, A. Palepu, and M. Wallace. (2019) Artificial intelligence (ai).[Online]. Available: cisse.info/pdf/2019/RR-01- artificial-intelligence.pdf
[19] (2020) Artificial intelligence - reasoning. [Online]. Available: britannica.com/technology/artificial-intelligence/Evolutionarycomputing
[20] S. Ahn, S. V. Couture, A. Cuzzocrea, K. Dam, G. M. Grasso, C. K. Leung, K. L. McCormick, and B. H. Wodi, "A fuzzy logic based machine learning tool for supporting big data business analytics in complex artificial intelligence environments," in 2019 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE), 2019, pp. 1–6.
[21] A. Cranage. (2019) Getting smart about artificial intelligence. [Online]. Available: https://sangerinstitute.blog/2019/03/04/getting-smart-aboutartificial-intelligence
[22] J. Alzubi, A. Nayyar, and A. Kumar, "Machine learning from theory to algorithms: An overview," Journal of Physics: Conference Series, vol. 1142, p. 012012, 11 2018.
[23] T. Ayodele, Machine Learning Overview, 02 2010.
[24] M. Ahmad, "Malware in computer systems: Problems and solutions," IJID (International Journal on Informatics for Development), vol. 9, p. 1, 04 2020.
[25] N. Milosevic, "History of malware," Digital forensics magazine, vol. 1, no. 16, pp. 58–66, Aug. 2013.

INNO SPACE
SJIF Scientific Journal Impact Factor
Impact Factor: 8.118

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

Scan to save the contact details