International Journal of Engineering, Management and Humanities (IJEMH)
Volume 4, Issue 1, pp: 354-361 www.ijemh.com

Literature Survey on Cipher Decoder - MalwareDetection Using Deep Learning Methods

Sanket Goel Veer Dutta Tasensola Aier
Saurabh Naik
Assistant Professor -> Suman Mam
Department of Computer Science Engineering, Dayanand SagarCollege of Engineering

Date of Submission: 14-02-2023 Date of Acceptance: 27-02-2023

Abstract:
In the modern world, web is the wellspring of information and all the resources. Rapid growth in technology has made it possible to access the internet from anywhere and download the resources available. One can easily access the Internet on their smartphone or Desktop system. The Internet allows us to install Third-party applications. These third-party applications are suspicious. Security is the major issue as these applications can contain malware which is a threat to the computer system and stakeholders. One of the top priorities is preventing fraud by safeguarding stakeholder and end user data. Credulous users are unable to distinguish between these malevolent applications. Some of these applications can be malicious ones that can gain access to the user system and can easily tamper the resources. Attackers can inject various types of malware into these applications and can easily gain access to or control the system. In this paper, we have discussed various Algorithms to detect malware activities that are already designed by using various Deep learning techniques . Our study provides a thorough analysis of the inadequacies of existing malware detection techniques and the problems associated with security architecture, security considerations, and ways to improve efficiency.

Keywords:
Artificial Intelligence, Malware Detection, Malware Classification, Static analysis, Machine Learning, Deep Learning

I. Introduction

The scientific revolution, which led to the development of the computer, began in the early 1500s with the aid of contributions made by great scientist who simplified thecontext of computing. These individual include Von, Jacquard, Babbage, Herman, Cliffor d, Konard, Alken, Presper, Eckert, Remington, Ala n and Neumann and others. Early 1980s, mark the beginning of the Information Age when society saw a rapid transition from core technology to information technology. Advances in scientific technology bring a number of problems, especially in the field of computers and different types of malicious files that have arisen up to that time. Currently, 40000 types of viruses have been successfully identified, and the number keepson increasing exponentially.

Elk Cloner, created by a fifteen-year-old school student named Skrenta, was the first virus assault to be identified on a second-generation Apple IMAC system in 1982. Alvi and Farooq developed Brain named Personal Computer virus to prove that computer systems are not Immune. Inserting an infected floppy disc causes the PC to become infected since "Brain" was capable of reproducing itself using floppy discs. The entire procedure can be broken down into three conceptual phases: 1. Boot Loading 2. Replication 3. Projection. These viruses developed were harmless and were developed to point out the security issues present in the system.

As a result of the software technology's susceptibility, practises of deploying malware- based applications have since been quickly expanding. Elk Cloner and Brain were the two early computer viruses that were designed to highlight problems instead of causing any malfunctioning in computers. Malware, on the other hand, shifts in a harmful direction in order to interfere with computer operations, collect personal data, or access private computer systems.

A few examples of the countless malware programs that have been discovered over the last few decades include The Morris, ILOVEYOU, Melissa, CodeRed, Sasser, Slammer, Stuxnet, CryptoLocker, and Welchia. These viruses also underwent mutations as a result of technological advancement. All of these computer viruses have the ability to disseminate through ordinary usage or downloads, commercial software updates, malicious intent, or simply by clicking on a specially planted link, and they may disrupt any software programme used by the government, data centres, laboratories, businesses, corporations, or organisations. According to a researcher, since computer viruses do not emerge from anywhere, someone with access to the specific computing device must be persuaded into installing them there. Once it manifests, the outcome can be extremely disastrous, and several tragic losses have subsequently been documented.

As firewalls watch over incoming and outgoing connections to guard against attacks and disasters, scientists and researchers are working to develop security features and antivirus packages that are primarily used to protect, trace, and eliminate viruses, Trojan horses, worms, and other ransomware[11]. According to the study analysis conducted via Hotspot shield, the actual roots of the first antivirus are debatable. In 1987, Bernd Robert, a German computer security specialist, designed a program to remove Vienna, a virus that infected.com files on DOS-based systems, and it is believed that this was the first anti- virus tool to successfully eliminate a computer virus. For a variety of platforms, including workstations, servers, gateways, and mobile devices, there are several manuals and automatic malware control and protection methods accessible. These technologies provide updates on the identification process, and being proactive is the first step in the preventive procedure.

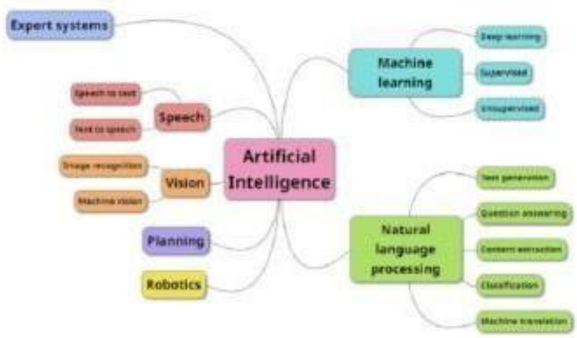
From the viewpoint of artificial intelligence, this study aims to give an examined summary of malware detection and prevention approaches. We will give a thorough review of the limits of existing malware detection systems' use of artificial intelligence (AI), as well as their potential for improvement. Finally, we will suggest solutions to these issues.

We research possible methods for detecting and preventing malware as well as the possibilities of artificial intelligence (AI). We present a comprehensive assessment of artificial intelligence-based methods for virus detection and prevention tools. We talk about the shortcomings of the current approaches and suggest areas for future study.

Artificial Intelligenceand Malware

Artificial Intelligence

AI has the potential to replace people by doing cognitive activities that were previously only possible with the human mind, many businesses are eager to capitalize on this technological development. AI is defined by Nones as the quickly developing field which can carry out process which requires human monitoring. However, according to academics, AI may be used to enhance Intelligence(IA) rather than replace the human brain, value in terms of being identified as a possible major force behind the present technological revolution. In order to construct modules that mimics human brain, consciousness, exploration, passionate information, thinking, organizing, creativity and the most important skill which is being a problem solver.



Machine learning is one of the numerous types and methods of achieving artificial intelligence, allows computers to mimic and adapt human like behaviour. Machine learning and natural language processing are two examples of the different forms and applications of artificial intelligence. The field of study known as ML can be summed up as automatic computing processes that allow computers to achieve AI without having to be defined by the programmer. Comprehension and experience using DL and ML serve as foundations for applications to stop viruses and malware.

Malware

Malware aka badware is an acronym for suspicious log and scripted files or harmful software. These programs can take a variety of forms like viruses, worms, ransomware, keyloggers etc. which are designed to damage the stakeholders and the owner of the system. Badware is the abbreviation for harmful software or applications, which expand beyond computer systems and into the web and other connected areas. In 1969 the first test with uses four machines statistics show that the number has increased by 1 billion. Growth of internet has exponentially increased the number of virus significantly. Rise of the Internet have grown gradually and significantly since then.

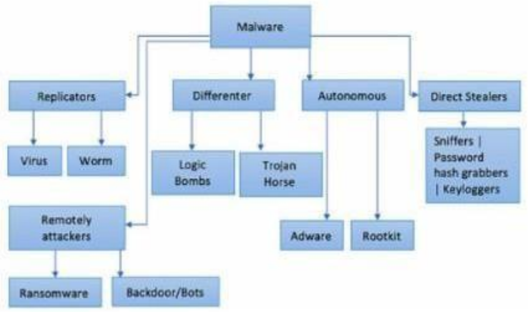


Fig. 2. Malware Classification by [28].

Malware is any software that has been intentionally created with nefarious intentions, and it can be categorized based on its intended use and method of dissemination. The classification of malware is shown in Fig.2. A malicious file is uploaded on the internet where the end users download them without knowing that the file contains virus, these files when executed starts executing and replicating themselves. These can spread from one system to another just like biological virus. Malware programmers replicate and destroys a computer without the permission or consent of owner. These harmful files or programmers can also be obtained through third parties, main source being the internet where all the suspicious and bad files are uploaded or automatically gets downloaded by clicking the bad links.

Research Methodology

The research on AI-based malware detection strategies is conducted via a comprehensive literature review. Finding, evaluating, and researching the top methodology is the main objective of the systematic review. We initially used a "Search Process" to look for potential research publications using pre-selected search phrases or strings, such as "Ai Technology" AND ("Malware" AND "Identification" OR "Preventative measures") OR "AI." We had to develop these search parameters, which are based on terms relevant to malware and ai technologies and their variations, acronyms, and popular synonyms, to screen out results from irrelevant research publications.

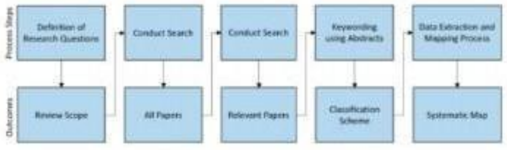


Fig. 3. Paper Classification Process [32]

Related Work

Malware detection protects the system form different harmful assaults with the use of anti-malware strategy. There are multiple detection techniques available today, but as malware technology advances, the integration of AI is required and successful virusprotection programs.

For identification, one must first locate the harmful source code. A technique known as source finder has been proposed by the researchers to find out malware repositories from largest database source available. The study discovered that these recommended technqiues can detect the malwares repo with 89% accuracy and 86% r2 score by first identifying the 7504 badware code using Source Finder, followed by examination of the different behaviour of files.

Machine learning algorithms are frequently used to detect malware. most likely a lot more. Niharika Sharma assesses malware detection techniques in her thorough analysis of the static, dynamic, and hybrid strategies. Additionally, by combining data mining and machine learning techniques, the author speeds the identification process. The study evaluates several malware detection techniques that rely on data mining and machine learning

For detection of badware using Artificial Intelligence techniques, Sanjay has proposed a technique which focus on opcode of file for detecting badware using ML techniques. Data Source has been taken from Kaggle challenge which includes comparison of different classifiers, including LMT, Random Forest, NBT. The proposed technique is demonstrated to be almost entirely accurate in identifying malware. A demonstration shows that the suggested method is virtually 100% accurate in malware detection.

In addition to machine learning, other approaches to malware detection include cloud computing, network-based detection systems, virtual machines, and the use of hybrid techniques and technologies. Malware detection today makes use of deep learning and artificial intelligence. Irina Baptista's et al study which was published in Science [37], proposes a novel approach for malware detection using binary visualization and self- organizing incremental neural networks. A test was conducted to show how malware payloads might be found in a variety of file formats, including Portal Document File (.pdf) and Microsoft Document File (.doc) files. According to the experimental findings, ransomware detection accuracy is 91.7% and 94.1%, respectively.

According to the authors, the recommended strategy successfully identified unknown malware in real time with an incremental detection rate.

In another research, Syam and Vankata [38] used artificial intelligence to build a virtual analyst that could detect hazards and perform the necessary measures. The researchers separate the data into supervised and unsupervised categories, turn the unsupervised data into supervised data using analyst input, and then automatically update the system. It evolves the algorithm over time using its own Active Learning Mechanism, making it stronger and more efficient.

A team of professionals from Kennesaw University suggested an unique Bayesian optimization-based technique that produces the required architecture. It is focused on NSl, a test dataset for intruder detection , and outputs results clearly show the usefulness. A significantly bigger intrusion is effectively detected by the resulting DNN architecture in terms of r2 score and precision. With BO obtaining the maximum accuracy ,the BO-GP technique outperforms the random search optimization strategy.

Malware Detection Using AI

The limits of current methodologies, DL based tech utilised to identify bad-ware and solutions to these issues are covered in this section

Malware Detection Techniques

Better bad-ware prevention will result from implementing various classifier types, and using DL will enhance the ability of identifying suspicious activities. Figure shows flowchart for artificial intelligence-based identification of unknown malware. Each method of malware detection is thoroughly reviewed in this section.

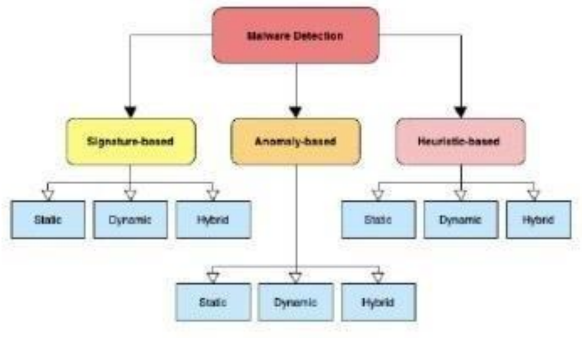


Fig. 4. Classification of Malware Detection Techniques

Signature-Based-Detection

The phrase "signature-based" detection technique refers to a strategy that aids in recognizing and detecting assaults by searching for certain patterns. It consists of four components. In this approach, developer scans the directory with a database that contains viral signatures and then analyze the information to look for malware in the database. When the pattern gets matched with the stored data file or directory is declared infected with virus. Limits of this approach is that it is unable in identifying undiscovered malware but works well for known malware. Tress pass Detection System maintains model which monitors the traffic which can be used for referring a directory. TDS takes traffic from different directories and compares the stats model to detect intrusions.

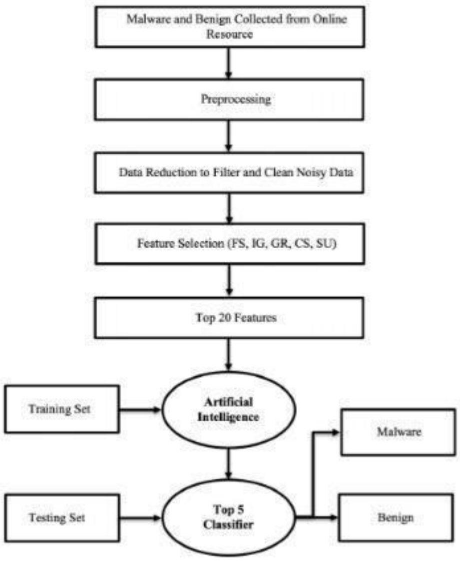

Malware and Benign Collected from Online Resource
Preprocessing
Data Reduction to Filter and Clean Noisy Data
Feature Selection (FS, IG, GR, CS, SU)
Top 20 Features
Training Set
Artificial Intelligence
Malware
Testing Set
Top 5 Classifier
Benign

Fig. 5. Flow chart of AI Based Unknown Malware Detection Techniques

Anomaly-based-Technique

This technique is essential for addressing security concerns and defending networks from malicious activity [43]. It allows us the identification of unidentified badware by using classification to the activities of the system, approaches amplifies the limit of pattern or footprint technique. An advantage of tracking activities is been given by the switch from pattern mappers to classification-basedapproach.

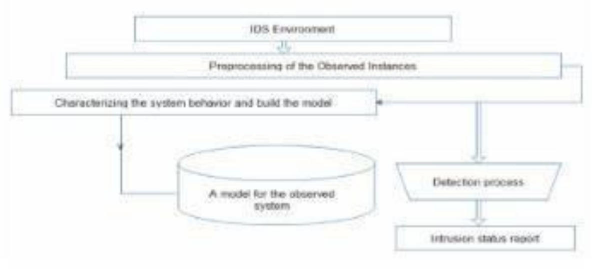

IDS Environment
Preprocessing of the Observed Instances
Characterizing the system behavior and build the model
A model for the observed system
Detection process
Intrusion status report

Fig. 8. Common anomaly-based network IDS [43]

Heuristic-based DetectionTechnique

The use of Deep Learning amplifies the badware detection when used with pattern and anomaly based approach. It combines the genetic algorithm and neural network and generates a framework that can detect distinct badwares in real time which improves the efficiency and performance. It utilizes the traits which includes the inheritance that helps to achieve desired results without knowing the system. It is improvised by combining the mathematical and pattern tools together. The characteristics of heuristic methods are show in Fig.

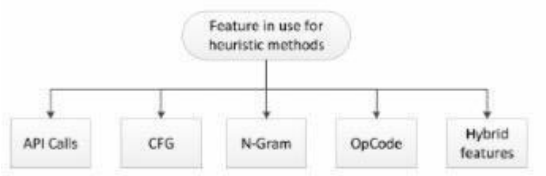


Fig. 10. Heuristic Methods Features [46]

Malware Detection byAdopting AI

Malware has been evolving and has large diversity, until now only some of them have been identified successfully. This makes it difficult to protect the system from cyberpunk.

Due to the fast growth in AI, various techniques have been developed which can be utilized to develop AV systems that can prevent, detect and remove badware from the system. Here we have discussed methods, their results and potential drawbacks.

Tal and Mendel were the first two guys who conducted the experiments and discovered a virtual monitoring technique that can be utilised to fight against the bad software and bad hardware.

They proposed a framework that increases the resistivity of the system by using a transparent Tresspass Detection System (TDS). Results from the experiments suggested that a VM monitor can utilize distinct moderate and primary host software interactions. The limitation of VM is that it can throw numericalerrors and resistance to tampering.

A graph network calls the API Sequence from the badware scripts and generates a Directed Graph. Designing is formulated by analyzing sub-components of the system. The performance of the approach is also examined and contrasted. The evaluation's findings show that the greatest accuracy is 98.32.

A lightweight machine learning-based approach is proposed by Yu and Wen[50] on badware on OS devices. Features are extracted using static and dynamic analysis. Brand new PCA-RELIEF approaches have been used for property identification and the removal of outliers. GCN classifiers have been utilized because of their lower error rate.

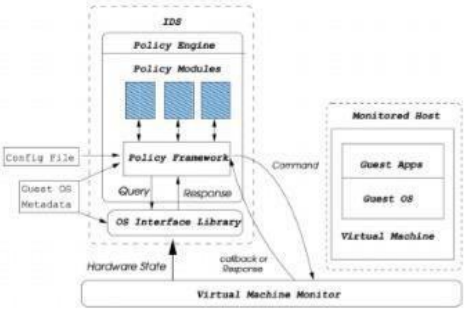


Fig. 11. A High-Level View of our VMI-Base [48]

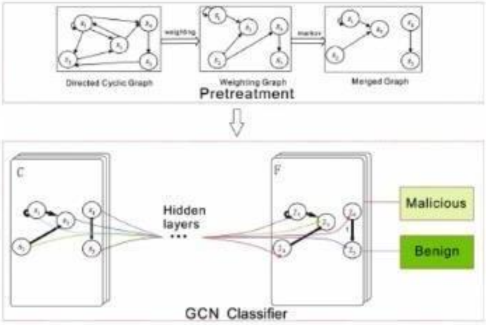


Fig. 12. GCN-based malware detection system framework [49]

Discussion and Limitations

The limitations of earlier techniques were covered in previous discussions of various malware detection methods. To cope with cutting-edge methods for malware detection and prevention, it is essential to anlayze the shortcomings of detection systems. We address the shortcomings of the techniques that are being used in this area and provide solutions.

The main drawback of pattern mapping is that it is unable to identify unidentified badware activity. Update Because some specific bad wares can alter the BIOS of the infected system, updating the directory solves the problem. The pattern scanning method was developed to address these problems, but it can't delete the bad files from the system. This method can still detect unknown viruses.

Heuristic analysis has two phases static and dynamic. Here code mapping process is performed which is challenging because badware has distinct properties that behave in different ways. Even though a dynamic procedure is a long procedure but it performs better than the static one. The drawback of dynamic phase is its inability for identifying executable virus in certain circumstances. The user might stop the heuristic dynamic analysis by completing any action. System Integration address problem of dynamic phase inability to consistently identify malware when performance discounted due to past failures. The beginning state of a file is usually assumed to be unaffected by integrity verification, however this is frequently untrue.

Multiple malware detection methods are actively looking for harmful software programmers. Dynamic solutions are required to cut down on the time spent analyzing malware features, and more advanced techniques should be used to identify harmful behavior which increases the classification strategies. The clever badware has evolved in recent years, and the use of DL tech which can be used for creation as well as protection has been enhanced.

II. Conclusion

Malware or malicious software may disrupt computer systems, websites, and applications across range of e-commerce, particularly educational institutions. The development of AV systems are benefited from the AI. With such a focus, this study provided overall analysis of malware classification and strategies. An effort to give a concise summary of badware, artificial intelligence, and it's storytelling. In section three, a discussion of the current state of malware detection system was followed by a list of the programmer's shortcomings.

Likely on any system, malware detection approaches have variety of drawbacks in addition to new properties. Research has shown that DL is potential domain which can be used for the creation of resistant system for detecting and deleting badware or threats associated with applications in the direction of a technological utopia. In order to make a conclusion, we examine a variety of solutions to the problem we've found ,with the stated goal of advancing Malware Detection and Prevention-related achievements.

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 tissues towards using computer technology into the efl classrooms,” Universal Journal of Educational Research, vol. 2, pp. 146–153, 2014.[4] 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.

[4]. S. Subramanya and N. Lakshmi Narasimhan, “Computer viruses,” Potentials, IEEE, vol. 20, pp. 16 – 19, 11 2001.

[5]. S. Levy and J. Crandall, “The program with a personality: Analysis of elk cloner, the first personal computer virus,”07 2020.

[6]. N. Milosevic, “History of malware,” 02 2013.

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

[8]. I. Khan, “An introduction to computer viruses: Problems and solutions,” Library Hi Tech News, vol. 29, pp. 8–12,09 2012.

[9]. M. Bishop, “An overview of computer viruses in a research environment,” USA, Tech.Rep., 1991.

[10]. D. B. Patil and M. Joshi, “A study of past, present computer virus performance of selected security tools,” Southern Economist, 12 2012.

[11]. A. Terekhov. History of the antivirus. [Online].Available: https://www.hotspotshield.com/blog/history-of-the-antivirus

[12]. M. J. Hossain Faruk, H. Shahriar, M. Valero, S. Sneha,S. Ahamed, and M. Rahman, “Towards blockchain-basedsecure data management for remote patient monitor-ng,” IEEE International Conference on Digital Health(ICDH), 2021.

[13]. M. J. Hossain Faruk, “Ehr data management:

Hyper-ledger fabric-based health data storing and sharing," TheFall 2021 Symposium of Student Scholars, 2021.

[14]. S. Ryan, R. Mohammad A, H. F. Md Jobair, 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.

[15]. D. G. Vigna. (2020) How ai will help in the fight against malware. [Online]. Available: https://techbeacon.com/security/how-ai-will-help-fight- against-malware.

[16]. 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.

[17]. A. I. Nones, A. Palepu, and M. Wallace. (2019) Artificial Intelligence (ai). [Online]. Available: cisse.info/pdf/2019/RR-01-artificial-intelligence.pdf.

[18]. (2020) Artificial intelligence - reasoning. [On-line].Available: britannica.com/technology/artificial-intelligence/Evolutionary-computing

[19]. 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 sup-porting big data business analytics in complex artificial intelligence environments," in 2019 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE), 2019, pp.1–6.

[20]. A. Cranage. (2019) Getting smart about artificial intelligence. [Online]. Available: https://sangerinstitute.blog/2019/03/04/getting-smart-about-artificial-intelligence

[21]. J. Alzubi, A. Nayyar, and A. Kumar, "Machine learning from theory to algorithms: An overview," Journal of Physics: Conference Series, vol. 1142, p. 012012, 112018.

[22]. T. Ayodele, Machine Learning Overview, 02 2010.

[23]. M. Ahmad, "Malware in computer systems: Problems and solutions," IJID (International Journal on Informatics for Development), vol. 9, p. 1, 04 2020.

[24]. N. Milosevic, "History of malware," Digital forensics magazine, vol. 1, no. 16, pp. 58–66, Aug. 2013.

[25]. S. Gupta, "Types of malware and its analysis," Inter-national Journal of Scientific Engineering Research, vol. 4, 2013. [Online]. Available: https://www.ijser.org/researchpaper/Types-of-Malware-and-its-Analysis.pdf

[26]. Statista. Number of worldwide internet hosts in the domain name system (dns) from 1993 to 2019. [Online].Available: https://www.statista.com/statistics/264473/number-of-internet-hosts-in-the-domain-

[27]. name-system/

[28]. S. Poudyal, D. Dasgupta, Z. Akhtar, and K.

[29]. D. Gupta," Malware analytics: Review of data mining, machine learning and big data perspectives," 12 2019.

[30]. 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.

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

[32]. B. A. Kitchenham and S. Charters, "Guidelines for performing systematic literature reviews in software engineering," Keele University and Durham University Joint Report, Tech. Rep. EBSE 2007-001, 07 2007.[Online].

[33]. Available: https://www.elsevier.com/data/promis misc/525444systematicreviewsguide.pdf

[34]. C. C. Agbo, Q. H. Mahmoud, and J. M. Eklund,"Blockchain technology in healthcare: A systematic review," Healthcare, vol. 7, no. 2, 2019.[Online].Available: https://www.mdpi.com/2227-9032/7/2/56

[35]. M. O. F. Rokon, R. Islam, A. Darki, E. Papalexakis, andM. Faloutsos, "Sourcefinder: Finding malware source-code from publicly available repositories," in RAID,2020.

[36]. N. Sharma and B. Arora, "Data mining and machine learning techniques for malware detection," in Rising Threats in Expert Applications and Solutions, V. S.Rathore, N. Dey, V. Piuri, R. Babo, Z. Polkowski, and J. M. R.

[37]. S. Tavares, Eds. Singapore: Springer Singapore,2021, pp. 557–567.

[38]. S. Sharma, R. Challa, and S. Sahay, Detection of Ad-vanced Malware by Machine Learning Techniques: Pro-ceedings of SoCTA 2017, 01 2019, pp. 333–342.

[39]. S. Saad, W. Briguglio, and H. Elmiligi, "The curious case of machine learning in malware detection," 2019.

[40]. I. Baptista, S. Shiaeles, and N. Kolokotronis,

"A novel malware detection system based on machine learning and binary visualization," 05 2019, pp. 1–6.

[41]. S. A. Repalle and V. R. Kolluru, "Intrusion detectionsystem using ai and machine learningalgorithm," 122017.

[42]. M. Mohammad, S. Hossain, H. Hisham, H.

[43]. F. Md Jobair,V. Maria, K. Md Abdullah, A. R. Mohammad,A. Muhaiminul I., C. Alfredo, and W.Fan, "Bayesian hyperparameter optimization for deep neural network-based network intrusion detection," IEEE International Conference on Big Data, 2021.

[44]. O. C. Onyedeke, E. Taoufik, M. Okoronkwo, U. Ihedioha, C. H.Ugwuishiwu, and O. .B, "Signature based network intrusion detection system using feature selection on android," International Journal of Advanced Computer Science and Applications, vol. 11, 012020.

[45]. Y. Ye, T. Li, Q. Jiang, Z. Han, and L. Wan, "Intelligent file scoring system for malware detection from the graylist," 01 2009, pp. 1385–1394.[42] S. Jyoti, A. Bhandari, V. Baggan, M. Snehi, and Ritu, "Diverse methods for signature based intrusion detection schemes adopted," 07 2020.[43] J. Veeramreddy and K. Prasad, Anomaly-Based Intrusion Detection System, 06 2019

[46]. D. Bolzoni and S. Etalle, "Aphrodite: an anomaly-based architecture for false positive reduction," ArXiv, vol.abs/cs/0604026, 2006.

[47]. S. Bridges, R. Vaughn, and A. Professor, "Fuzzy datamining and genetic algorithms applied to intrusion de-tection," 04 2002.

[48]. Z. Bazrafshan, H. Hashemi, S. M. Hazrati Fard, and A. Hamzeh, "A survey on heuristic malware detection techniques," 05 2013, pp. 113–120.

[49]. I. Baptista, S. Shiaeles, and N. Kolokotronis, "A novel malware detection system based on machine learning and binary visualization," in 2019 IEEE International Conference on Communications Workshops (ICC Workshops),2019, pp. 1–6.

[50]. T. Garfinkel and M. Rosenblum, "A virtual machine introspection based architecture for intrusion detection, "NDSS, vol. 3, 05 2003.

[51]. S. Li, Q. Zhou, R. Zhou, and Q.Lv, "Intelligent malware detection based on graph convolutional network," The Journal of Supercomputing, 08 2021.

[52]. L. Wen and H. Yu, "An android malware detection system based on machine learning," vol. 1864, 08 2017, p.020136

.