ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com
International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 10, Issue 5, May 2024

Review on Artificial Intelligence in Cyber Security

[1]Akshay M, [2] Vikas M N [3] Madhura B S [4] Daneshwari Sajjanar
[5] Dr.Mohideen Badhusha S
Alva's Institute of Engineering and Technology, Moodbidre,
[1]akshay.mckm56@gmail.com,[2]vikasgowda411@gmail.com ,
[3]madhurabsmadhura@gmail.com[4]daneshwarisajjanar@gmail.com

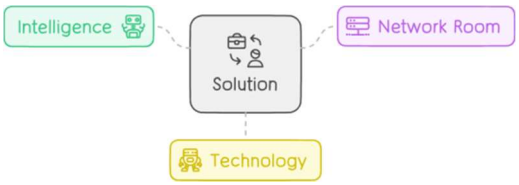
Abstract:
Humans are unable to handle the volume of data and the complexity of processes required to sustain cyberspace without complete automation. Hardened decision logic is a type of software that is difficult to design, as is typical technology for security protection. The ease of use of intelligence learning and technology can help solve this issue. This article assesses the potential for increasing network security through the development of repair defensive mechanisms and gives a brief review of the use of artificial intelligence technology in network security. We can presume that practical applications already exist based on the cybersecurity AI software that is now in use. Through neural networks, they are mostly employed to safeguard the environment and several other safety nets.

Introduction:

increasingly than two years ago, spyware and cyberweapons became increasingly powerful, proving that linked devices can only be protected by smart technology. the file below Conficker had an impact on the French Navy's "Ultramar" computer network on January 15, 2009. After that, the service was shut down, and because the flight schedule wasn't updated, planes from different air bases were compelled to land."[1] Over 800 machines have been proven to be infected. The Admiralty/N* station and hospital's vital equipment and computers have been certified to be contaminated by the UK Ministry of Defence and government offices located in the city of Sheffield. According to a report dated February 2, 2009, the unified army of the Federal Republic of Germany, the Bundeswehr, assaulted more than a hundred of its equipment. The Greater Manchester Police News Network searched the police database for three days in January 2010. Employees must routinely use their authority to search persons and vehicles[2]. Network-centric warfare (NCW) cyber mishaps carry a high risk, hence cyber defense improvements are desperately needed. For new attacks, the utilization of cutting-edge technology and information tools is crucial. Installing environmental protection and crisis management dynamically, responding fully to attacks, and expanding networks [3].

Why are intelligent apps becoming increasingly crucial in cyberwarfare situations?

The solution is visible below if you examine the network room closely. First, intelligence is needed to respond quickly to the network environment. Rapidly managing vast amounts of data is required to recognize and clarify cyberspace activity and make the required judgments. Before the advent of widespread technology, individuals could not swiftly achieve anything without expertise. Building devices with conventional, fixed algorithms (hardened decision logic) to effectively ward off internet attacks, however, gets more difficult as new problems keep coming up. This topic is about technology related to intelligent automation [4]. This article's second part provides an introduction to the science and art of intelligence. We shall delve further into developing AI derived from in Chapter 3. Artificial Intelligence for Cyber Defense. In Chapter Four, new smart gadgets are shown and the possibilities are explored.



Research Methodology:
We employ four databases—Scopus, Web of Science, ACM Digital Library, and IEEE Xplore—to gain a deeper understanding of the relationship between cybersecurity and intelligence. We also utilize the search engine

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com
International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 10, Issue 5, May 2024

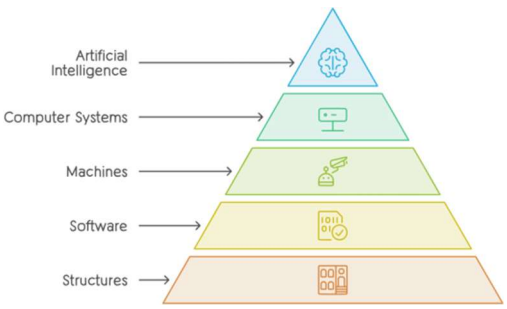
Google Scholar. The theme-matched keywords are searched for in this document. The writers altered a lot of search engine content to obtain the best assistance in order to enhance and increase the accuracy of our research findings [5].The results are filtered in the following stage. Since the purpose of this paper is to offer new models of intelligence in the firm security network, the study results we were able to get are restricted to data that has been published within the last four years. Lastly, the research findings are split by the total number of citations.

Furthermore, this paper, which was discussed in more detail more than five times, was chosen. Conversely, fresh research publications that included novel method(s) but had fewer than five published articles or documents were also chosen. sources that satisfy the criteria for monitoring [6] After approval: Documents whose names are not relevant to this study. III Books, citations, technical papers, and patent filings. There is no English publication for this article. In order to filter pertinent data, we examined the findings that weren't in the summary in the third stage. These procedures assist writers in figuring out the privacy policy's scope in order to understand the relationship between intelligence and cybersecurity. As a result, the documents that best met our goals and had the most pertinent information were chosen. The procedure is to perform a thorough analysis of the data andfind any gaps. This study carries on the trend by integrating them pacts of many fields, the use of security expertise, the techniques employed, and the techniques suggested. It is employed to produce an extensive manual for upcoming studies in this specific area [7].

AI in depth

Science claims that artificial intelligence (AI) predates computer systems, which are referred to as the original artificial intelligence. As we can see from the history of artificial intelligence, it will be "very soon" before machines, software, or structures surpass human intellect in intelligence. The issue is that the time frame likewise grows longer over time. For instance, we witness a variety of machines that are rather skilled at playing chess and solving challenging puzzles [8]. Chess was considered an intelligence test in the early days of computer technology. Even if electronic chess was a breakthrough in the 1970s, building a system that might defeat world champions appears challenging. But this came to pass sooner than anticipated. This is due to three factors: boosting the capacity of computers and producing strong search algorithms. It has a good skill set that encompasses all potential chess knowledge, and it may be utilized in various software applications outside of games like chess (see testing part below). Since the chess problem deals with low intellect knowledge, it can be solved in principle. Translating specialized knowledge between languages is another example [9].

He believed that early solutions to natural language processing issues may be found, particularly in light of N. Chomsky's work in the field of speech computing. This has not yet occurred, despite the early successes of a few particular programs, including Google's Artificial Intelligence Linguistics. This involves developing intellectual abilities, such as the capacity to learn a great deal about the many facets of human labor and the ability to solve problems with them. Artificial intelligence can be broadly defined as the development of technologically intelligent instruments to handle complicated issues that human performance is generally incapable of solving or that require decision-making for a variety of reasons. intellect [10]. In this piece, we draw the appropriate conclusions and advise using particular intelligence to cyberprotection issues and take action according to the most recent information, as demonstrated in (IOS Press, n.d.).



4.The Role of AI in Cyber Security

4.1 Is AI the future of cybersecurity?

AI has already been embraced by businesses and commercial enterprises, and as the White House pointed out, numerous government organizations continue to exploit the technology. Where did you get it? Where did you get it? By traversing through standard

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com
International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 10, Issue 5, May 2024

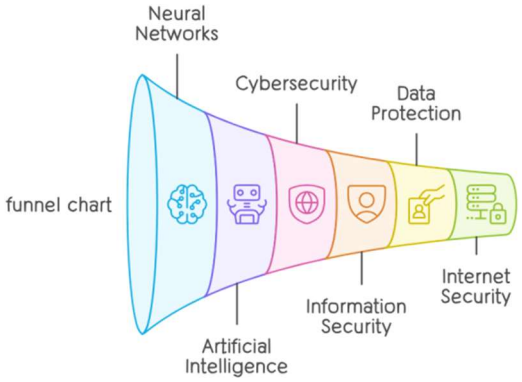
papers and reading and understanding data without structure, numbers, patterns, words, or phrases, artificial intelligence may quickly and effectively save time and resources. Actually, state secrets and taxes can both be saved by artificial intelligence. There are also gaps. Hackers are attempting to discover ways to gain access to computers via undiscovered vulnerabilities. Before the company finds out that the data has been released, time flies [11]. The hacker had already vanished by that point, as had all important data. However, AI must wait for hackers to escape by gathering data and sitting back. That. Artificial intelligence can identify malicious activity that a hacker would like to reveal to a new user—even if theydon't submit a password or log in. AI has the ability to spot subtle indicators that humans would miss, which can halt hacking groups in their tracks. As noted by Varughese, any material can be abused. Human hackers are continually examining the weaknesses of any system, even intelligence, in the never-ending chess game of cybersecurity.

Since wisdom is subject to human control, it is defeatable. Artificial intelligence can only function as intended, despite having excellent connectivity and information processing capabilities [12]. Programmers must create new defences as hackers adapt to artificial intelligence. The game of cat and mouse Will will go on, but artificial intelligence plays a significant part in safeguarding data. TensorFlow is a machine learning model for graph data that is available from Google. 03.09.2019 Data and data models are trained in neural networks using neural graph learning techniques by Neural Structured Learning (NSL) Research, an open-source project. NSL is intended to be used with both professional and non-technical students and operates on a Tensor Flow level learning engine. NSL is capable of doing NLP, building machine vision models, and projecting data from interactive databases like infographics and medical records [13]. Tensor Flow Engineer stated in a daily post that "using problem signals during training allows developers to provide better predictions, especially when data points are limited." The blog article states as much. "The set model continues to use the stronger model's model. This technique is frequently used to enhance Google models' performance, such as when learning semantic image embedding [14]. Throughout the development process, NSL can efficiently operate with graphs to build supervised, semi-supervised, or unsupervised agents, some of whom are connected by fewer than ten legal lines. Additionally, the original system has tools and APIs to assist developers in creating files and vectorized models with minimal scripting. Google Cloud debuted Automated ML Tables in April along with other data organization options including linked tables in Big Questions. In other AI news, the apparatus for large-scale speech recognition models, like Google's BERT, is called Google AI (also known as Google Research) open SM3.GPT2for Open AI [15].

investment banks in stopping trillions of dollars in recorded fraud. But what about the application of their Information Security?

Does artificial intelligence present an opportunity or a threat to digital job security? However, information management is still helpful today since it makes crimes easier for security experts to assess, look into, and comprehend. In order to prevent cybercrime and support businesses and consumers in staying safe, it fortifies enterprises' digital management methods. However, AI may require a lot of resources [16]. Any application may not be able to accomplish this. Actually, it may also turn into a potent tool in the hands of cybercriminals who utilize technology to create and enhance their cyberattacks. Information security has nothing to do with the discussion surrounding intelligence. Information is, after all, the secret to current cybersecurity developments. Thus, there is no better way to examine data than by using computers with millisecond processing speeds and then carry out things that would take a lot longer for humans? Artificial intelligence has grown in importance within the field of computer security. We'll examine developments in AI security technologies and their effects on businesses, hackers, and end users. Let's clear the air on everything. Why does the protocol for automatic data protection successfully increase the security of the Internet? You have multiple levels of protection, including media, network, edge, equipment, and computer storage, even if your business is expanding like many others.[17].

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com
International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 10, Issue 5, May 2024



4.2 What AI executives think the use of AI in information security?

The Capgemini Research Institute examined the situation of data protection in addition to the study "Using Artificial Intelligence to Reshape Network Protection." This indicates that departments must leverage intelligence to build a secure network. Because hackers are now utilizing the technology to attack, this is one of the reasons survey respondents (850 information security managers, IT information managers, and IT personnel from ten countries) think AI is a significant solution. The following are some salient points from the report: According to 75% of survey participants, AI helps their company react to risks more quickly. 69% of businesses concur that having skills is crucial. [19] Artificial intelligence, according to three out of five businesses, can increase the effectiveness and efficiency of cyber analysts. Artificial intelligence can be used to increase the dependability of already-available cybersecurity remedies or create fresh ones.

Artificial intelligence will be helpful for network security protection organizations as networks grow larger and more complicated. The intricacy of the Internet has just outpaced human comprehension. Thus, be aware that there's no reason to panic. However, this raise crucial query: How can you maintain the privacy of information about your business and clientele?

4.3 Artificial intelligence technology: How do you add AI to your defence?

It is now impossible to fully integrate data protection with intelligence technology. As you may expect, in order to make sure that projects and personnel can be utilized to their fullest potential, planning, training, and preparation require time [20]. In a Forbes article, Allerion's CEO and creator, Naveen Joshi, listed many ways that artificial intelligence may strengthen corporate network security. capacities consist of: Develop precise biometric password-based access technology ™ Use predictive analytics to identify dangers and questionable activity Enhance your reasoning by discussing and disclosing facts ™ Security analysis and following the request's connection >Your data intelligence professionals and other IT leaders need to understand how they can be productive right now if you include AI into your data protection. It takes time to do this. e and planning. Proceed with prudence and don't minimize the investment you have made inyour company's workforce. A deeper look at the industry as a whole show that a lot of big companies are now using AI into their products. Well-known companies that are now using AI cybersecurity include [21] Palo Alto Networks, Crowd Strike, Check Point, Fortinet, Log Rhythm, Fire Eye, SophosSymantec, and others. While there are many advantages to using intelligence in security awareness, there are also disadvantages to consider.There are various disadvantages of using AI for data protection over creative non- computer approaches, not the least of which is that it requires more time and money. This is partially the fault of intellectual property-based information protection technologies.

4.4 Addressing the vulnerabilities AI

cybersecurity tools cause

Physical protection faces additional difficulties with the application of artificial intelligence in data protection. Cybercriminals can employ AI techniques to alter behaviour in addition to detecting and neutralizing malware attacks. This is partially due to the fact that machine learning and artificial intelligence technologies are becoming more widely available as their production costs and applications drop [22]. This makes it possible for cybercriminals to establish a network more quickly and affordably and to install harmful software.Cybercriminals are more likely to take advantage of a combination of variables.4.5 Adversarial AI: How Cybercriminals Abuse Technology to Target All Types of Organizations Artificial

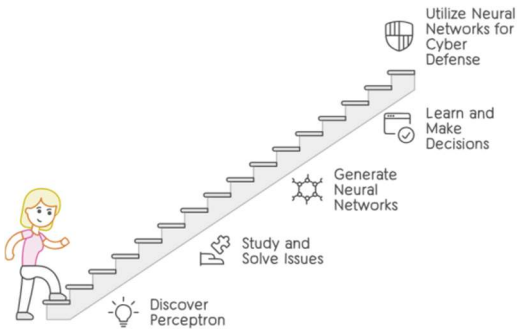
ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com
International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 10, Issue 5, May 2024

Intelligence (AI) and its risks are contextualized in the battle between Development of artificial intelligence is a concept that is used maliciously. "Enabling machine learning algorithms to interpret the false message based on it and respond based on the intruder's interests" is how Accenture describes artificial intelligence. This basically happens when an artificial intelligence program's neural network incorrectly interprets or misrepresents an artifact as a result of intentionally altering inputs [23].Cybersecurity's potential is nearly limitless in the absence of appropriate safeguards or preventative measures. Thankfully, academics studying cybersecurity are becoming aware of the dangers posed by AI assaults. They provide white hats and "develop protection and use pre-interception models to test AI against vulnerabilities," per an article on IBM's Security Intelligence Research Blog. IBM Regarding the project, the Dublin Lab is also quite involved. and depart from the AI The IBM Adversarial Robustness Toolbox (ART) index is not in good condition.

Offerings that we have cyber security reveals that there are numerous significant aspects to this subject. Peripheral firing neural networks were the earliest applications for them.[28] However, it is evident that a great deal of network security issues can be resolved using clever approaches. Effective decision making is one of the most challenging issues in network security, examining technological items for as it necessitates the use of copious amounts of information. Numerous techniques have been created in the field of artificial intelligence to address challenging scenarios involving human intellect [24]. Many of these methods have advanced to the point that particular algorithms built using them can be put into practice. Many techniques are deemed so significant that they defy common sense. They currently have become a component of certain artificial intelligence area applications, like data mining algorithms.

5.1 Neural Nets

The perceptron, one of the most widely used neural network components, was discovered by Frank Rosenblatt in 1957, and thus marked the beginning of the long history of mesh neural networks. One can study and solve intriguing issues with limited combination
knowledge. Nonetheless, neural networks can be used to generate most other neural networks. Neural networks therefore possess the ability to learn from networks and make decisions [26]. The most crucial choice he makes is how frequently to work. These consist of threat response compilations, learning models, groups, and ((4) Using Artificial Intelligence Technologies/Applications in Cyber Défense, n.d.). It helps with identification. They can be utilized electronically or within the app. Neural network avoidance suppression techniques are also applicable. There are programmes for malware analysis, bot identification, spam filtering, DoS detection, software worm detection, forensic science, and spam filtering. Acceleration—whether in graphics chipsets or hardware—will make deep learning in computer security even more crucial. Third-generation artificial intelligence networks, a rapidly developing field of machine learning that may teach the brain more effectively and efficiently, are a new advancement in neural networks. A excellent method for swiftly building a neural network and making it adaptable to changes in risk is to use Field Gate Arrays, or FPGAs. They could be fascinating.



5.2 Expert Systems

Specialist programs are undoubtedly the AI techniques that are used the most frequently. An expert program is a technology that looks for answers to issues brought up by users or specific technologies within a specific technology domain. This might be specifically used to decision support in the areas of finance, virtual worlds, and healthcare. Different optimization strategies can be used to solve a wide range of challenging problems, from very complex hybrid systems to microscopic analytical medical diagnosis. A knowledge base containing the expert analysis of a particular application field makes up a scheme of expertise [27]. This has a deduction engine built in to advise the knowledge base,

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com
International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 10, Issue 5, May 2024

providing solutions predicated on that comprehension. The term "current plastic understanding" refers to the motor of implication and vacant knowledge.

5.3 Intelligent Agents

Three intelligent operational capabilities—proactive, ACL, and reactive—distinguish computational intelligence software components from one another (the ability to determine and make specific judgments). Software programs are intelligent agents. They are able to measure, plan, and arrange. Within the software development community, the notion of software workers is recognized as a remnant of the web language, which is considered to be its least utilized instrument. Concepts, even those with exact definitions, might be continuous and lack communication comprehension, in contrast to agents and concepts. In order to defend against DDoS assaults and define simulation that may successfully shield the agent from such attacks, smart agents are employed. Practical implementation of the "cyber police" of mobile police officers will be achievable if all contractual and managerial issues.

Search

Numerous study designs have been created with the goal of addressing certain research issues. It is uncommon to apply research methods that were created outside of artificial intelligence to the field of artificial intelligence, despite the fact that these methods are widely employed in many applications. Firstly, search is not regarded as an AI feature because it is integrated into the application stack. Thus, the primary goal of dynamic analysis programming is to address security-related issues. Cybersecurity choices can benefit from the usage of techniques like control tree elimination, αβ indexing, and random indexing with minimum entry inserted, which are commonly employed in game-oriented applications. The αβ search algorithm was initially created for the computer game program chess, specifically as an adaptation of the "divide and conquer" concept that helped solve problems when two candidates had to decide which price is best.

5.5 Learning

By growing, improving, or honing the knowledge base, learning fortifies the data structure. One of the most significant and well-researched facets of artificial intelligence is this. Mathematics currently requires computer learning to achieve new concepts, new skills, and new ways of collaborating information. Learning challenges range from diverse forms of abstract learning, such teaching behaviour and practicality, to conceptual learning, syntactic learning, and parametric learning (i.e., understanding the meaning of these terms). Both supervised (trained) and unsupervised learning modalities are offered by artificial intelligence. When there are big files, the aforementioned is quite crucial. This is widely used in network security and will be found by numerous engines. Information initially only originates from unbridled intelligence. Self-organizing neural networks may be the basis for unsupervised learning.

Challenges

Future AI research, development, and applications for cybersecurity will be considered with a distinction between short- and long-term objectives. Numerous AI techniques are now available for cybersecurity, and urgent cybersecurity issues demand more intelligent solutions than are now achievable. So far, existing applications have been taken into consideration. He would be pleased to present fresh ideas on information processing for future decision-making in environmental management. The region requires information management of a network based around combat. The only way to swiftly analyse the situation and provide managers and policy makers authority over each location is through autonomous data management. An outline of the centralized and decentralized systems that make up the Bundeswehr's daily command and control is given in this review.Maybe we shouldn't depend solely on intelligence's limited scope. Regarding prospective horizons, at least temporarily Some are seeing artificial intelligence as the primary objective of intelligence in the upcoming years.Permit the development of artificial intelligence that is universal. In the middle of the 20th century, it was finished. The inaugural AGI Conference took place at the University of Memphis in 2008. Established in 2000, the Singularity Institute for Artificial Intelligence (SIAI) alerts scientists to the possibility that machines could acquire artificial intelligence. The Singularity, which is described as "the advancement of intelligence that is smarter than humans," can be addressed in this way. Numerous innovations are frequently cited as the path forward. While artificial intelligence is now a

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com
International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 10, Issue 5, May 2024

topic of much discussion, many other advancements can

Conclusion

It is impossible to overlook the need for sophisticated network security strategies as cyber threats and hostile intelligence grow. Additionally, if a clever strategy is applied Experience with DDoS protection has shown that even with little resources, significant threats can be avoided. According to the published review, the top AI research findings for cybersecurity come from neural network research. Neural networks are still being used in cyber security. Cybersecurity methods are still desperately needed in many domains where neural networks are not the best available instrument. Information management, situational awareness, and decision support are some of these areas. The development of technology is the most intriguing aspect of this situation. Artificial intelligence is developing too quickly to predict, but criminals may still be able to utilize new varieties of intelligence, provided that it is achievable. It's unclear what this means. Furthermore, the most recent advancements in computer science-specific technologies
is the most intriguing aspect of this situation**.**

References

[1] Cyber defense using intelligence technology and applications. (no specific date). From https://www.researchgate.net/publication/333477899_Use_of_Artificial_Intelligence_Techniqu es_Applications_in_CyberDéfense, retrieved August 14, 2020.

[2] Ahmad, I. (2009). In DOS, the use of artificial neural networks halts detection. The 2nd International Conference on Information and Network Security Proceedings, SIN-09, 229-234. 10.1145/1626195.1626252 can be found online.
Journal of Physics: Conference Series 1964 (2021) 042072 ICACSE 2020
IOP releasing with doi:10.1088/1 doi: 10.1088/1742-659 published
09 IOP64/1964/042072

[3] Yang Shuai, Qiu Wei, Bai Jian, Wu Yong, and Wang Goguen (2006). Based on multi-layered, self-generated maps and fundamental content analysis, the new approach offers access.
Computer Science Lectures, 3973 LNCS, 255–260 (includes Bioinformatics Lectures and Computer Science Lectures Subseries). This link points to 10.1007/11760191_37.

[4] Watson, T.; Elizondo, D.A.; North, J.; Bitter, C. (2012). Introduce the concept of network inference using neural networks. Research on Computational Intelligence,

[5] F.A.G. Carrillo (2012). Is it possible for technology to alter the dynamic of instruction between educators and learners? Social and Behavioural Sciences Procedia, 46, 5646–5655.
10.1016/j.sbspro.2012.06.490 can be found here.

[6] Kouch, J. S., Chang, R.I., and Lai, L. Bin (2009). Examine how networks interact by employing filter model-based queries and signal processing. Journal of Advances in Signal Processing: Eurasip, 2009, vol. 10.1155/2009/735283 can be found at this link.

[7] Andreoulakis, G., Chatzigiannakis, V., and Maguaris, B. (2004). Security guards are part of a decentralized intrusion detection paradigm. HP June 2014, OpenViewUniversity Association.

[8] Wilkos, K., M., and M. Chmielewski (2010). Construct a multi-agent environment with semantic services for military decision support systems. Lecture Notes in Computer Science (including Lecture Notes in Bioinformatics and Lecture Notes in was li Artificial Intelligence Subreddits), 6070 LNAI (Part 1), 173–182. The publication number is 10.1007/978-3-642-13480-7[9] Ignasi, S., Management, H., Herrera, A.F., Corral, G., & Lull, U.R. (2007).
Hybrid Intelligent Systems Innovation {--} 44/2008 (June 2014), Proceedings of the Second International Conference on Hybrid Artificial Intelligence Systems (HAISâ07).
The Doi value is 10.1007/978-3-540-74972-1.

[10] Hicklin, U. and J. Feiereisel (2009). making a report for oneself. August 1–30. [11] Michael, C., Schatz, M., and A. K. Ghosh (2000). Instant access to behaviour-based learning through searches. 1907, Lecture Notes in Computer Science (containing the subseries Lecture Notes on Bioinformatics and Lecture Notes on Artificial Intelligence), 93-109.

10.1007/3-540-39945-3_7 is the URL to be used.

[12] Mazzinian, M., Barman, S., Hosseini, R., Qandil, S.D., Ellis, T., and Demoski, J. (2012). A successful technique for developing and fine-tuning a type 2 fuzzy association function with Gaussian intervals for use in lung CAD classification.

[13] No date given by IOS Press. taken from http://www.iospress.nl/book/algorithmsand-architectures-of-artificial-intelligence/ on August 14, 2020.

[14] Ulanov, A. & Kotenko, I. (2007). A multi-agent system to simulate joint protectionagainst cyberattacks that is adaptive. IncludingLecture Notes in the Artificial Intelligence Subseries and Lecture Notes in Bioinformatics, Lecture Notes in Computer Science, 4476 LNAI, 212-228. The publication number is 10.1007/978-3-540-72839-9_18.

[15] Sharov, A., Konovalov, A., and I. V. Kotenko (2010). Botnet modelling and defines using agent-based simulation. Social media (pages 21–44).
ccdcoe.org/229.html is the URL. [16] Tugu, E., Kalja, A., Penjam, J., and Kotkas, V. (2013). Software Technology Offerings Based on Models. Model-Driven Engineering and Software Development: First International Conference Proceedings, MODELSWARD 2013, 312-315.

10.5220/0004348203120315 is the DOI.
[17] Nikam, D.M., Kulkarni, P., and Pachauri, V.K. (2009). 2009 Access to locate the system with a self-made map.

[13] No date given by IOS Press. taken from http://www.iospress.nl/book/algorithmsand-architectures-of-artificial-intelligence/ on August 14, 2020...

[14] Ulanov, A. and I. Kotenko (2007). A framework with several agents

[18] N. Parbati and P. Anand (2017). Cyber defines using machine learning. International Journal of Engineering and Computer Science, 5(12), 317–322.

Journal of Physics: Conference Series 1964 (2021) 042072 ICACSE 2020 IOP Publishing 10.1088/ 1742-6596/1964/4/042072 10: /doi.org/10.26438/ijcse/v5i12.317322.

[19] Guard against the Conifer computer virus (2009). Microsoft.
the Conficker.mspx file at http://www.microsoft.com/protect/computer/viruses/worms.

[20] Citations 1 2 R A Poell Computer Szekler R3 Overview Course Hero (no date). from https://www.coursehero.com/file/p40hov9n/R-EFERENCES-1-httpenwikipediaorgwikiConficker-2-R-A-Poell-P-C-Szklrz-R3-Getting /, retrieved August 14, 2020.

[21] Rajani, P.; Abhishek, S.G.K.; Adie, S. (2020). 8(2), 1398–1403; Artificial Intelligence: A New Era.
Rosenblatt, F. (1957) [22]. Perceptron: Perceptual and Recognition Automaton. Cornell Aeronautical Laboratory Report 85.

[23] Sadiku, M.N.O., Musa, S.M., and Fagbohungbe, O.I. (2020). Cybersecurity is a feature of artificial intelligence. Advanced Technology, International Journal of Engineering Research, 06(05), 01–07. The doi:10.31695/ijerat.2020.3612 is available here.

[24] Chakrapani, M.K., Movva, R. S., Mukkamala, S., and Ramamoorthy, S. (2011). Arrays are an API and component used in malware detection. Journal of Computer Virology, 7(2), 107– 119. https://doi.org/10.1007/s11416-010-0141-5.

[25] Thyagu, E. (2011). AI has Cyber Défense. 2011 3rd International Conference on Cyber Conflict, ICCC 2011 - Proceedings, 95–105.

[26] Venkatesh, G.K., Nadarajan, R.A., Botnet, H., Use, D., & Learning, A. (2017). Venkatesh, G. K., Nadarajan, R.A. Using a multilayer feedforward neural network with an adaptive learning rate, HTTP botnet detection Refer to this version using the HAL ID, hal-01534315. detection of HTTP botnets