IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Artificial Intelligence In Cyber Security

RIA SINHA

Abstract.

Without substantial automation, individuals cannot manage the complexity of operations and the scale of information to be utilized to secure cyberspace. Nonetheless, technology and software with traditional fixed implementations are difficult to build (hardwired decision-making logic) in order to successfully safeguard against security threats. This condition can be dealt with using machine simplicity and learning methods in AI. This paper provides a concise overview of AI implementations of various cybersecurity using artificial technologies and evaluates the prospects for expanding the cybersecurity capabilities by enhancing the defence mechanism. We may infer that valuable applications already exist after the review of current artificial intelligence software on cybersecurity. First of all, they are used to protect the periphery and many other cybersecurity areas with neural networks. On the other hand, it was clear that certain cybersecurity problems would only be overcome efficiently if artificial intelligence approaches are deployed. In strategic decision making, for example, comprehensive information is important, and logical decision assistance is one of the still unanswered cybersecurity issues.

Keywords: Artificial Intelligence, Intelligent Agents, Neural networks, Smart Cyber Security methods.

1. Introduction

This is clear that only smart technologies can help defend against sophisticated cyber devices, with the sophistication of malware and cyber-arms increasing exponentially in the past two years. The following case of "On 15 January 2009, Conficker corrupted "Ultramar" the French Navy computer network. The service has then been quarantined, and flights at different airbases have been forced to land because they've not been able to update their flight schedules [1]. The United Kingdom Defence Ministry confirmed contamination of some of its key devices and computers. The virus has dispersed through government offices, Navy Star / N * desk departments and hospitals in the town of Sheffield have confirmed infections to more than 800 machines. In a report on 2 February 2009, over a hundred of their machines were compromised by the Bundeswehr, the Federal Republic of Germany's united armed forces. In January 2010, the Information Network of the Greater Manchester Police triggered a pre-emptive disconnection of the Police Central Database for three days. Staff had to contact certain forces to carry out regular searches on cars and individuals [2]. Cyber incidents are particularly hazardous with Network Centric Warfare (NCW), and cyber defence alterations are urgently needed. The use of artificial intelligence techniques and knowledge-intensive tools would be vital in new offensive methods like dynamic installation of protected perimeters and integral crisis management, fully automated reactions to attacks in networks [3].

Why has the role of smart apps escalated exponentially in cyber warfare?

You can see the following response if you look carefully at the cyber room. Firstly, the fast response to circumstances on the Internet requires artificial intelligence. Many data need to be managed very quickly in order to explain and interpret cyberspace activities and take the decisions needed. Before substantial technology, individuals cannot succeed in the speed of operations in addition to the volume of data to be used. Nevertheless, machines with normal, fixed algorithms (hardwired decision-making logic) are problematic to build to successfully defend against cyberspace attacks as new challenges continuously emerge. This is a forum for automated technologies of intelligence [4]. The latter part of this paper presents the areas of technology and science with artificial intelligence. In the third chapter, we will delve into the established cyber protection AI implementations, clumped by the methods of artificial intelligence. The fourth segment explores the possibilities and introduces new smart devices.

2. Research Methodology

To get an all-round impression of the junction between cybersecurity and AI, we used four databases: Scopus, Web of Science, ACM digital library also IEEE Xplore. Along with that, we also used the Google Scholar search engine. A set of keywords matching the topics were searched for in these databases.

To improve our search results and to make them more accurate, the authors refined various keywords from the search machine to obtain the maximum coverage [5]. In the additional step, obtained results were filtered.

3. AI in depth

As an area of study journal, artificial intelligence (AI) is about as ancient as computer systems (also called initial system intelligence). From the yesteryears of AI, it was "on the horizon" that devices/software/structures could be built cleverer than humans. The issue is that as time progresses, the time frame is going further. We saw a variety of machines, for example, playing really good chess, overcome sensibly complex problems [8]. The chess play was viewed during the initial periods of the computation as a test of intellectual ability. Although electronic chess was on the grandmaster during the seventies, a system that could defeat the global champion appeared almost difficult to develop. Yet quicker than anticipated, this happened. It has three reasons: improved computational power, design of powerful search algorithms. It could be utilized in several software beyond games like chess, see Check section below), and well-structured skill set which includes all possible chess information. The chess dilemma was basically solved as it was an abstract concern of the so-called small AI. Another example involves the translation of a particular AI from one dialect to the next [9]. In the 1960s, especially following N. Chomski 's research in computational linguistics, has been anticipated to address the issue of Natural Language Processing early. It hasn't yet occurred, even though certain unique programs such as Google's AI linguistics indicated initial success. This includes artificial intelligence gaining vast quantities of expertise in each aspect of human activities and obtaining the capacity to cope with it. AI can be regarded, in general, as an aspect of intellect, and broadly the creation of intelligent devices, as a technology that offers a solution to overcome difficult issues which cannot be solved without, for example, performing well or creating correct choices due to large quantities of smartness [10]. In this article, we apply the right line, propose the application of particular AI methods in cyber defense issues and respond to the latest Artificial intelligence as illustrated in(IOS Press, n.d.). 4. The Role of AI in Cyber Security

4.1 Is AI the future of cybersecurity?

Industries and private sector companies have already adopted AI programs, and as the White House notes, also many government departments utilize the tool. Why? Why? Since AI can easily save resources and time by scrolling through standardized data and comprehensively reading and studying unstructured data, numbers, speech patterns, and sentences. In fact, AI could save both tax dollars as well as national secrets. And there are gaps. Hackers are trying to figure out how to access the machines, slipping through cracks we didn't know were there. Years fly already then until a company finds a data leak [11]. By then, the hacker is long gone and all the sensitive data. On the other side, AI must sit back and collect data and wait until a hacker gets messy. AI checks for behavioral anomalies that hackers are expected to display for starters, whether a password is written, or when the user logs in. AI can detect those little signs that otherwise would have gone undetected and stop the hacking group in their routes. As Varughese noted, every device can be abused. Human hackers

always will interrogate the weak spots in every system including AI in the constant cybersecurity chess game. Artificial intelligence is human-controlled and may still, therefore, be vanquished. Although AI is remarkable in its capacity to link and process data, it can only function as well as it was designed [12]. As hackers adjust to the Artificial Intelligence systems, new defensive measures will have to be deployed by the programmers. The game of cat and mouse will proceed, but AI is a positive strengthening in the fight to secure data. Google introduced a graphical data learning model for Tensor Flow machine learning. search Implemented Neural Structured Learning (NSL), an opensource framework that uses the Neural Graph Learning technique to train data sets and data structures in neural nets.NSL works with the machine learning stage Tensor Flow and is designed to work for qualified besides incompetent machine learning professionals. NSL may render machine vision models, execute NLP, and run projections from interactive databases such as medical reports or graphs of information [13]. "The use of organized signals during training enables developers to deliver better predictive performance, particularly if the volume of data points is fairly limited," Tensor Flow engineers thought today in a blog post. "Structured-signal also exercises principals to more robust models. These methods have been widely used to improve the performance of the model in Google, such as learning semantic implanting of images [14]. NSL can work with monitored, semi-supervised, or unsupervised to construct representations that use graphic signals to regularize throughout development, with much less than ten code lines in certain instances. The original framework also contains tools that will help developer's structure data and APIs with little code for creating examples of vector quantization. In April, Google Cloud launched other organized data approaches, such as linked sheets in Big Query besides Auto ML Tables. In several other AI news, Google AI, formally known as Google Research, open-sourced SM3, a compiler for large-scale speech recognition models such as Google's BERT, too the GPT2 for Open AI [15].

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

The Capgemini Research Institute examined the position of information protection besides their study "Reinventing Cyber Protection with AI," which shows that it is important for companies to set up cybersecurity defenses with AI. It is partially because respondents from the survey (850 data security leaders, IT information management also IT operations around ten countries) think AI-enabled solution is important because hackers are now utilizing the technology to conduct cyber-attacks. Some of the other main points of the report include: 75 percent of the survey respondents say that AI enables their organization to respond to infringements more quickly. Sixty-nine percent of organizations agree that AI is required. [19] Three in five firms say that using AI makes cyber analysts more accurate and more efficient. Using artificial intelligence could even help bolster the perspectives of existing solutions to cybersecurity also rebuild the way of creating new ones. When networks develop wider and increasingly sophisticated, AI will be a huge boost to security defenses for the enterprise. To put it plainly, the increasing sophistication of the networks is beyond what humans can do on their own. So that's all right to recognize — you needn't be afraid. Yet it leaves you asking a crucial question: What do you do to ensure that the confidential details and consumer knowledge regarding your company are secure?

4.3 Addressing the vulnerabilities AI cybersecurity tools cause

The application of AI in information defence is generating new challenges to physical protection. Even as it is important to utilize AI technologies to help detect and combat malware threats, cyber attackers may also use AI tools to progressive behaviour attacks. It is partially because access to the advanced AI technologies besides machine learning strategies is cruising as costs of producing and applying these developments decline [22]. This ensures that computer attackers can, more quickly and at a reduced expense, build increasingly sophisticated and efficient malicious apps. The mixture of variables provides exposure to cybercriminal abuse.

4.4 Adversarial AI: how hackers can misuse AI against various organizations

The danger to information security, including artificial intelligence, falls in the context of adversarial AI, a word used for sinister purposes to apply to the growth also utilization of AI. Accenture defines adversarial AI as something that "causes machine learning algorithms to misunderstand inputs into the framework and respond in a way beneficial to the intruder." Basically, that occurs when neural networks in an AI program are fooled into misidentifying or falsely representing artifacts because of deliberately changed inputs [23]. Without the appropriate safeguards or precautions in effect, Cyber Security implementations may be nearly unlimited.

Fortunately, the risks associated with adversarial AI are recognized by cybersecurity researchers. As indicated by an article in IBM's Security Intelligence research blog, they give their white caps and are "building protections and making pre-emptive assault models test AI weaknesses." IBM's Dublin labs are additionally dynamic in the project and have made the IBM Adversarial Robustness Toolbox (ART) ill-disposed AI index.

5. Challenges

When you intend future study, production, and implementation of AI approach on cybersecurity, you will differentiate among imminent targets and long-term outlooks. Multiple AI approaches can be used on cybersecurity quickly, and urgent cybersecurity challenges need smarter solutions than they are actually applied. So far, these current immediate apps have been mentioned. The introduction of entirely new concepts of information processing in the management of circumstances and decisionmaking in the future would be exciting. Knowledge management for net central warfare is a demanding technology field. The rapid evaluation of the situation, which allows leaders and policymakers dominance at every point, is achieved only by automatic information management. The review gives an overview of the centralized and decentralized information model in the Bundeswehr modern command and control structure. Having a potential horizon in mind maybe we should not only rely on the Narrow AI for at least a couple of decades to come Some people are tempted that the AI's main goal – artificial cognition creation AGI can be accomplished in the mid-20th century. In 2008 the first AGI meeting took place at Memphis University. Founded in 2000, the Singularity Institute for Artificial Intelligence (SIAI) alerts investigators that there could be the risk of increasingly accelerated intelligence growth on machines. This can progress to Singularity, defined as follows: "Singularity is the technical advancement of intellect that is smarter than an individual. There are many developments that are commonly listed as a path forward. The most frequently discussed is currently Artificial Intelligence, but many other developments enable the development of intelligent intelligence, provided they meet a threshold degree of complexity.

7. Conclusion

In a scenario where malicious intelligence and cyber threats are rising exponentially, sophisticated cybersecurity strategies cannot be ignored. Also, security against large-scale threats, with very minimal resources, has been demonstrated from experience in DDoS prevention if smart approaches are used. Publications reviews indicate that studies into artificial neural networks offer the findings of AI most widely relevant to cybersecurity. Neural network implementations continue on cybersecurity. For many fields where neural networks weren't the most appropriate technologies, sophisticated cybersecurity approaches are still desperately needed. Such fields include decision support, understanding of the situation, and control of information. The most interesting in this scenario is expert machine development. Too fast general artificial intelligence has advanced cannot be known, but a possibility remains that the perpetrators will exploit a new form of artificial intelligence as long as it is accessible. This is not obvious. In addition, the latest technology in the understanding, interpretation, and management of information, particularly in the area of computer learning, would significantly improve systems' cybersecurity capabilities.

References

[1] Use of Artificial Intelligence Techniques / Applications in Cyber Defense. (n.d.). Retrieved 14 August, 2020,

[2] Ahmad, I., Abdullah, A. B., & Alghamdi, A. S. (2009). Application of artificial neural network in the detection of DOS attacks. SIN'09 - Proceedings of the 2nd International Conference on Security of Information and Networks, 229–234. https://doi.org/10.1145/1626195.1626252.

[3] Bai, J., Wu, Y., Wang, G., Yang, S. X., & Qiu, W. (2006). A novel intrusion detection model based on multi-layer self-organizing maps and principal component analysis. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 3973 LNCS, 255–260. https://doi.org/10.1007/11760191_37.

[4] Bitter, C., North, J., Elizondo, D. A., & Watson, T. (2012). An introduction to the use of neural networks for network intrusion detection. Studies in Computational Intelligence, 394, 5–24. https://doi.org/10.1007/978-3-642-25237-2_2.

[5] Carrillo, F. A. G. (2012). ¿Can Technology Replace the Teacher in the Pedagogical Relationship with the Student? Procedia - Social and Behavioral Sciences, 46, 5646–5655. https://doi.org/10.1016/j.sbspro.2012.06.490.

[6] Chang, R. I., Lai, L. Bin, & Kouh, J. S. (2009). Detecting network intrusions using signal processing with query-based sampling Filter. Eurasip Journal on Advances in Signal Processing, 2009. https://doi.org/10.1155/2009/735283.

[7] Chatzigiannakis, V., Androulidakis, G., & Maglaris, B. (2004). A Distributed Intrusion Detection Prototype using Security Agents. HP OpenView University Association, June 2014.

[8] Chmielewski, M., Wilkos, M., & Wilkos, K. (2010). Building a multiagent environment for military decision support tools with semantic services. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 6070 LNAI(PART 1), 173–182. https://doi.org/10.1007/978-3-642-13480- 7_19.

[9] Corral, G., Llull, U. R., Herrera, A. F., Management, H., Ignasi, S., & Llull, U. R. (2007). Innovations in Hybrid Intelligent Systems {--} Proceedings of the 2nd International Workshop on Hybrid Artificial Intelligence Systems (HAIS'07). 44/2008(June 2014). https://doi.org/10.1007/978-3-540-74972-1.

[10] Feyereisl, J., & Aickelin, U. (2009). S Elf -O Rganising M Aps. August, 1–30.

[11] Ghosh, A. K., Michael, C., & Schatz, M. (2000). A real-time intrusion detection system based on learning program behavior. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 1907, 93–109. https://doi.org/10.1007/3-540-39945-3_7.

[12] Hosseini, R., Qanadli, S. D., Barman, S., Mazinani, M., Ellis, T., & Dehmeshki, J. (2012). An automatic approach for learning and tuning gaussian interval type-2 fuzzy membership functions applied to lung CAD classification system. IEEE Transactions on Fuzzy Systems, 20(2), 224–234. https://doi.org/10.1109/TFUZZ.2011.2172616.

[13] IOS Press. (n.d.). Retrieved 14 August 2020, from https://www.iospress.nl/book/algorithmsand-architectures-of-artificial-intelligence/.

[14] Kotenko, I., & Ulanov, A. (2007). Multi-agent framework for simulation of adaptive cooperative defense against internet attacks. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 4476 LNAI, 212–228. https://doi.org/10.1007/978-3-540-72839-9_18.

[15] Kotenko, I. V, Konovalov, A., & Shorov, A. (2010). Agend-based Modeling and Simulation of Botnets and Botnet Defense. In Conference on Cyber Conflict (pp. 21–44). http://ccdcoe.org/229.html.

[16] Kotkas, V., Penjam, J., Kalja, A., & Tyugu, E. (2013). A model-based software technology proposal. MODELSWARD 2013 - Proceedings of the 1st International Conference on ModelDriven Engineering and Software Development, 312–315. https://doi.org/10.5220/0004348203120315.

[17] Pachghare, V. K., Kulkarni, P., & Nikam, D. M. (2009). Intrusion detection system using self organizing maps. 2009 International Conference on Intelligent Agent and Multi-Agent Systems, IAMA 2009, 4(12), 11–16. https://doi.org/10.1109/IAMA.2009.5228074.

[18] Parati, N., & Anand, P. (2017). Machine Learning in Cyber Defence. International Journal of Computer Sciences and Engineering, 5(12), 317–322.

[19] Protect yourself from the Conficker computer worm. (2009). Microsoft. http://www.microsoft.com/protect/computer/viruses/worms/conficker.mspx.

[20] R A Poell P C Szklrz R3 Getting | Course Hero. (n.d.). Retrieved 14 August, 2020,fromhttps://www.coursehero.com/file/p40hov9n/R-EFERENCES-1- httpenwikipediaorgwikiConficker-2-R-A-Poell-P-C-Szklrz-R3-Getting/.

[21] Rajani, P., Adike, S., & Abhishek, S. G. K. (2020). ARTIFICIAL INTELLIGENCE : THE NEW AGE. 8(2), 1398–1403.

[22] Rosenblatt, F. (1957). The Perceptron - A Perceiving and Recognizing Automaton. In Report 85, Cornell Aeronautical Laboratory (pp. 460–461). https://doi.org/85-460-1.

[23] Sadiku, M. N. O., Fagbohungbe, O. I., & Musa, S. M. (2020). Artificial Intelligence in Cyber Security. International Journal of Engineering Research and Advanced Technology, 06(05), 01–07. https://doi.org/10.31695/ijerat.2020.3612.

[24] Shankarapani, M. K., Ramamoorthy, S., Movva, R. S., & Mukkamala, S. (2011). Malware detection using assembly and API call sequences. Journal in Computer Virology, 7(2), 107– 119. https://doi.org/10.1007/s11416-010-0141-5.

[25] Tyugu, E. (2011). Artificial intelligence in cyber defense. 2011 3rd International Conference on Cyber Conflict, ICCC 2011 - Proceedings, 95–105