Artificial Intelligence in Cyber Security

Ms. Divya Shinde[1], Mrs. Ashwini Sheth[2], Mrs. Gauri Malwadkar[3]
Student, M.Sc.IT.[1]
Assistant Professor, Department of I.T[2,3]
I.C.S. College, Khed, Ratnagiri

Abstract: *Without significant automation, individuals will not be able to handle the complexity of the operations and the amount of information to be used to protect cyberspace. However, in the case of traditional, fixed technology and software implementations, it is challenging to construct the hard wired logic of decision-making in order to effectively protect against security risks. This condition can be remedied through machine simplicity and the learning method in Artificial Intelligence (AI).*

This paper provides a brief overview of the AI implementations of various types of cybersecurity using artificial technologies. It also evaluates the prospects for increasing the cybersecurity capabilities by improving the defence mechanism. We may conclude that valuable applications are already available after reviewing the current artificial intelligence software for cybersecurity. First, they are used for protecting the periphery as well as many other cybersecurity areas using neural networks. However, it was evident that certain cybersecurity problems will only be effectively solved if artificial intelligence approaches were deployed. For instance, in strategic decision making, comprehensive information is very important. Logical decision assistance is also one of the yet unanswered cybersecurity issues.

As cyber threats become more sophisticated, the relationship between AI and cybersecurity is becoming increasingly important in strengthening digital defences.

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

I. INTRODUCTION

It is evident that only advanced technology can provide protection against advanced cyber devices, with malware and cyber-weapons having become increasingly sophisticated over the last two years. An example of this is the Conficker attack on the French Navy's computer network on 15 January 2009, which resulted in the service being quarantined and flights being forced to land at various airbases due to a lack of capacity to update flight schedules. The UK Defence Ministry has since confirmed the contamination of some of their key devices and computers, with the virus having spread to government offices, the Navy Star/N * desk departments, and hospitals in the city of Sheffield, where infections have been confirmed for over 800 machines. On 2 February 2009, the Bundeswehr reported that more than 100 of their machines had been compromised by the cyber-attack, and in January 2010, In order to carry out regular searches of vehicles and individuals, Greater Manchester Police had to pre-emptively disconnect their Information Network for a period of three days.

Network Centric Warfare is a particularly dangerous form of cyber attack, and the need for changes to cyber defence is pressing. Smart apps have become increasingly important in cyber warfare, as they are able to respond quickly to situations on the internet.

Artificial intelligence is a key component in the management of large volumes of data, as it must be able to interpret and make decisions without substantial technology. However, it is difficult to construct machines with traditional fixed algorithms in order to protect against cyber-attacks due to the constant emergence of new threats. This paper provides a platform to explore the areas of technology and science related to artificial intelligence. In the third chapter, the focus will be on the current cyber protection AI implementations, and in the fourth section, the possibilities and introduction of new smart devices.

II. RESEARCH METHODOLOGY

In order to gain a comprehensive understanding of the relationship between cybersecurity and artificial intelligence, four databases were utilized: Scopus (Scopus), Web of Science (Web of Science), ACM digital Library (ACM Digital Library), and IEEE XplORE (IEEE Xplore). Additionally, a set of keywords corresponding to the topics in these databases were searched for. To improve the accuracy of the search results, various keywords were refined from the search engine to ensure the maximum coverage.

Finally, the results were filtered to only include papers published within the past four years, in order to capture the most recent trends in cybersecurity. The findings were then categorised by certifications. Those documents with over five citations were selected, while those with fewer than five citations but innovative methods and approaches were also chosen.

The sources that met the standards were subsequently accepted. The exceptions were those with titles that connected to subjects external of the choice of the research paper.

Technical Reports, Patent Documents, Books, citations.

Papers that had not been published in English.

In the third step, the conclusions were examined in addition to the abstracts to filter the relevant data. This step enabled the authors to determine whether the confidential papers related to the same topic in order to identify the connection between cybersecurity and artificial intelligence. Consequently, those papers that had the most pertinent data and met the desired criteria were selected. The methodology employed was a comprehensive literature review to identify the discrepancies. This study closed the gap by combining the impact of multiple domains, AI use in the Security area, the methods employed, and the methods presented. It is employed to create a general framework for future exploration in this particular area

III. AI IN DEPTH

Artificial Intelligence (AI) has been around since the early days of computers, and it seemed like it was only a matter of time before we saw machines that were smarter than humans. But as time went on, we started to see machines that could play really well at chess, solve complex problems, and even beat the world champion.

This was because of three things: better computing power, designing powerful search algorithms, and the fact that AI could be used in more than just chess. Eventually, the chess dilemma was solved, but it was all in the abstract.

Translating an AI from one language to another is just one example. Back in the 60s, it was thought that N.Chomski's work on computational linguistics would solve the problem of natural language processing early on. But it hasn't happened yet, even though some programs like Google's AI-Linguistics have had some success. This is because AI has a lot of knowledge in all aspects of human life and has the ability to handle it. Basically, AI can be seen as a part of intelligence, and more specifically, the development of intelligent devices. It's a technology that can solve tough problems that can't be solved without performing well or making the right decisions because of a lot of smartness. In this post, we'll apply the correct line, suggest how specific AI methods can be used in cyber defense, and answer the latest questions about Artificial Intelligence as illustrated in IOS Press (n.d.).

IV. THE ROLE OF AI IN CYBER SECURITY

4.1 The Future of Cybersecurity: Is Artificial Intelligence (AI) the Future of Cybersecurity?

Industrial and private sector organizations have already implemented Artificial Intelligence (AI) programs, and, according to the White House, many government departments are also taking advantage of the tool. This is due to the fact that AI can significantly reduce resource and time consumption by analyzing standardized data and comprehending unstructured information, such as data sets, figures, and speech patterns. In reality, AI could potentially save both tax revenues and national confidential information. However, there are drawbacks. Hackers attempt to gain access to the machines by exploiting vulnerabilities that we may not have known existed. It can take years for a company to discover a data leak, by which time the hacker has disappeared and all the confidential data has been collected. On the contrary, AI must remain passive, collecting data and waiting for a hacker to make a mess.

Artificial Intelligence (AI) is capable of detecting behavioral anomalies that are expected to be observed by hackers, such as when a password is entered, or when a user logs in, and can thus prevent the hacking group from gaining access to the data. As noted by Vishnu Varuge, any device can be misused. Human hackers will always seek out the weaknesses in any system, including AI, in the ever-changing cybersecurity game. As AI is controlled by humans, it is possible that it will still be defeated, however, AI is a valuable asset in the battle for data security.

Additionally, structured-signal exercises can be used to progress models to more robust principles, which have been extensively used to enhance the model's performance in Google, for example, by learning to implicate images in a semantic way [14]. Additionally, NSL can be used with monitored, Sem supervised, and unsupervised methods to construct representations which use graphic signals for regularization during development, with significantly fewer than ten lines of code in some cases. The initial framework also includes tools that will assist developers in structuring data and providing APIs with minimal code for creating vector quantization examples. In April of this year, Google Cloud released additional organized data approaches in Big Query, in addition to Auto ML Tables, as well as in a number of other AI news. Google AI (formerly Google Research) has opened-sourced a compiler, SM3, which is designed to be used for large scale speech recognition models, such as Google BERT, as well as GPT2, for Open AI.

AI has revolutionized many areas of information security, from speech recognition apps like Siri to facial recognition tools like Facebook. Payment card companies use AI to help stop billions of dollars in fraud.

4.2 How Do AI Executives Feel About Using AI in Information Security?

The research from Capgemini showed that it's important for businesses to set up cyber defenses with AI, since hackers are now using AI to attack. The survey of 850 data security leaders and IT information management staff in 10 countries showed that 75% of respondents said AI allowed them to respond more quickly to infringements, and 69% of organizations said AI was needed. Three-quarters of companies said AI made cyber analysts more reliable and efficient. The report also said that AI could help bolster existing cybersecurity solutions and also help create new ones. But it also left you wondering what to do to make sure your company's confidential info and consumer data are safe.

4.3 How do you use AI in your defence?

Integrating AI into information defence networks isn't something that can be done right away. It takes time to get the programs and staff up to speed, train them, and make sure they're using the technology to its full potential. Allerin's CEO and founder Neel Joshi wrote in Forbes that there are lots of ways AI systems can help make cybersecurity operations more sustainable. Here are some of the features they look for:

- Developing exact, biometric password-based log-in technique/s
- Detection of dangers and suspicious action by prescient investigation
- Improved considering and translation by way of normal discourse acknowledgment
- Securing distinguishing proof and association by a prerequisite

Once you've integrated AI into your information defenses, your IT pros and managers need to figure out how to do it effectively. This takes time and planning, so make sure you don't miss out on investing in the organization's human side. A lot of big players in the industry are already using AI in their products and services. Some of the biggest names in the market include [21], [2], [3], [4], [5], [6], [7], [8], [9], [10], [11], [12] and [13]. There are lots of benefits to using AI in knowledge security, but there are also risks. One of the biggest challenges is that it seems to require more time and money than regular non-AI computer protection.

AI frameworks-based info protection technologies aren't cheap, which is why some businesses, especially SMEs, have found them too expensive. But there are some new SaaS technologies that can make AI cyber defence more cost-effective for businesses. So, it's a lot easier to choose the right info protection measures than dealing with the fines, delays, and costs of a major cyber attack.

4.5 Fixing the Vulnerabilities Caused by AI Cybersecurity Tools

The use of AI in information security is creating new problems for physical security. It's important to use AI to detect and stop malware, but cyber criminals can use AI tools to advance their attacks. This is partly because access to advanced AI technologies, like machine learning, is getting cheaper as the cost of creating and using them goes down. This means that cyber criminals can build more advanced malicious apps faster and cheaper. The mix of variables makes it easier for cyber criminals to get their way.

4.6 Adversary AI: How Hackers Use Artificial Intelligence to Manipulate Various Organizations

Information security, including AI, is in danger from something called "adversarial AI," which is a term used for bad reasons to describe the use of AI. According to Accenture, it's when a machine learning algorithm misinterprets inputs into a framework and responds in a way that benefits the attacker. Basically, it's when the AI program's neural networks are tricked into mistaking or pretending to be artifacts because of changed inputs.

Without the right safeguards or precautions, cyber security implementations could be almost limitless. Fortunately, cybersecurity researchers are aware of the risks and are taking steps to protect themselves. An article in IBM's Security Intelligence blog says they're building protections and making models to test AI weaknesses. Plus, IBM's labs in Dublin are really on the cutting edge and have created the AI index.

V. OFFERINGS THAT WE HAVE

Following a review of articles on AI technologies related to cybersecurity, it can be concluded that there are already a number of significant characteristics in this field. The most prominent of these characteristics is the use of perimeter shooting neural networks [28]. However, it is clear that even more cybersecurity issues could be effectively resolved if AI approaches were employed. Decisions need to be made using comprehensive information, and proper decision support is one of the most persistent issues in cyber security. In the AI sector, a wide range of approaches have been developed for the resolution of complex situations that involve human intelligence. The majority of these strategies have reached a mature stage where specific algorithms are available based on these approaches. Some methods are even so important that they are not considered as part of artificial intelligence, but are instead incorporated into certain applications. In the course of a brief survey, it will not be possible to provide a comprehensive overview of all feasible AI approaches.

In addition, we have categorised approaches and architectures into a variety of categories, including Artificial Neural, Expert Systems, Smart Agents, Quest, Computer Education, Data Collection, and Constraint Resolution. The following groups have been defined and the use of appropriate cyber protection approaches has been discussed. Machine Vision, Robotics, and the comprehension of natural languages found in AI applications have not been discussed. Although robots and machine views have impressive military applications, they have not been discussed in the context of cybersecurity [25].

5.1 Neural Nets

The field of Network Neural has a long history, beginning with the 1957 discovery of a perceptron, a type of artificial neural network component. Initially, a small number of perceptions were used to investigate and solve complex problems. However, a large number of neural networks have been created from neural networks, which include the ability to simultaneously learn and make decisions. The operating frequency of a neural network is its most defining feature. These networks are suitable for identifying learning patterns, groupings, compilating threat responses, and so on. They can be used in applications or electronic devices. Additionally, neural networks can be used to detect DoS, identify software worms, filter spam, identify zombies, analyse malware, and perform forensic science. Neural networks can also be used to avoid intrusions.

Deep learning has become increasingly prominent in computer security due to its rapid mobility, whether in hardware or graphical chipsets. Neural nets have seen a new development in the form of cognitive nets of the third generation, which are capable of mimicking artificial neurons more effectively and offer a wider range of applications. The utilization of field gate arrays (FPAs) is an effective way to quickly construct and adjust neural networks to alterations in risks, offering a range of potential applications.

5.2 Expert Systems

Artificial Intelligence (AI) methods are typically implemented through specialist programs, which are technologies designed to address issues posed by customers or a particular technology in a particular field of technology. These programs may be used to assist decision-making, such as in medical care or banking, or in virtual worlds. Optimization techniques for solving complex problems of varying sizes are available, ranging from small-scale analytical medical diagnostics to more sophisticated hybrid systems. An expertise program is a knowledge base containing the expertise of a particular application area.

In order to provide solutions based on an understanding, a deduction engine must be included in the knowledge base. This is known as a "current plastic understanding" and must be filled in before it can be used. Additionally, knowledge base software can be used to extend the capabilities of the AI shell, as well as other programs that can be employed in more advanced hybrid engines. As technology advances, the Artificial Intelligence shell must be chosen and adjusted, and the learning must be gathered and supplied. This second step is much more intricate than the first. Intelligent machines can be developed in a variety of ways. Generally, a device has an AI shell and is capable of adding understanding to the data repository.

There is a wide range of representations in expert systems, with the most common being stabilizers interpretation. Artificial intelligence can be employed to augment these representations, such as through simulation. Nevertheless, the most significant component of the master system is consistency in the data within its skill set, as opposed to the on-site nature of the defined expertise. An example of such a skilled system would be, for security preparation purposes, the "Cyber Security Device Specialist". This skilled system can be used to collect and train security initiatives in order to make the most of scarce resources. Currently, work is being conducted to implement professional detection techniques in this area.

5.3 Intelligent Agents

Computational intelligence software components In the software development world, there is a concept of software agents, which are software applications that are capable of making and acting on certain decisions. This concept is known as "software agents" and can be distinguished from "subjects" who are passive and do not communicate (although they accept strictly defined syntax messages).

The use of intelligent agents has proven to be effective in mitigating DDoS attacks. Additional experience can further enhance the efficiency of the search process. Cooperation with internet service providers is also essential. As soon as regulatory and contractual matters are settled, a mobile intelligent officer force could be envisaged, which would incorporate technology that would enable mobility and connectivity of cyber personnel but would be unavailable to adversaries. Ultimately, the quality of the search process is often a determining factor in the performance of any intelligent system.

5.4 Search

A wide range of search algorithms are developed that pay close attention to particular search problems. While many search algorithms in AI have been developed and are widely used in various applications, they rarely serve as using AI functions. First, the search function is built into the application stack, and is not considered an AI function in this sense. Dynamic analysis programming is mainly used to solve optimal security problems.

Check on besides-or trees, check on trees, check on a minimum check-in-plus-index, check-in-minus-stochastic index are widely used in the games of gamers and are useful for network security decisions.

The algorithm of the “αβ-search” was originally developed for software chess. It is based on the common assistance principle “divide-and-conquer” in solving problems and, more specifically, when two opponents choose the absolute best move, this algorithm takes into account the minimum expected gain (MEG) and the cumulative potential loss (CPL) figures. Maybe you can ignore a huge number of options and significantly speed up your quest.

5.5 Learning

Learning improves the structure of information by expanding, reorganizing, or improving the existing knowledge base. This is among the most important areas of artificial intelligence that are being studied closely. Calculative techniques for learning new concepts, new skills, and new ways to coordinate existing knowledge need computer learning. The learning challenges range from simple parametric learning (knowing the meaning of quantities) to more complex abstract learning, like concept learning, grammatical learning, usability learning, and behavioural learning.

AI provides both monitored learning (learning with teacher) and non-monitored learning forms. This is especially useful where there is a large amount of data. For example, in cybersecurity, there are massive logs that can be extracted.

Data mining was originally derived from unmanaged AI learning. In general, unmanaged learning may be the result of self-organizing neural networks. In parallel hardware, parallel neural networks provide a distinct class of learning techniques. For example, genetic analytics combined with fuzzy logic was used in threat detection methods mentioned above.

VI. CHALLENGES

When considering future research, development, and implementation of an AI approach to cybersecurity, it is important to distinguish between immediate objectives and long-term perspectives. Several AI approaches can be implemented on cybersecurity in a short period of time, and urgent cybersecurity issues necessitate more intelligent solutions than those currently being implemented. These immediate applications have already been discussed. The introduction of entirely new concepts of context-sensitive information processing and future decision-making can only be accomplished through automated information management. Net Central Warfare (NCW) knowledge management is a highly complex technology domain. Rapid evaluation of the situation is essential for leaders and policy makers to have full control at every stage of the chain of command. This review outlines the central and decentralised information model of modern Bundeswehr command and control.

It may be that the Narrow AI should not be relied upon for at least a few decades. Some may be tempted to believe that the AI's primary objective – artificial cognition creation (AGI) can be achieved in the middle of the twentieth century. In 2008, the first meeting on AGI was held at the University of Memphis. The Singularity Institute (SIAI), established in 2000, has warned investigators that there may be a risk of an increase in the rate of intelligence growth on machines, which can progress to the Singularity, a technical advancement of intelligence that is more intelligent than an individual. Many developments are commonly cited as a path forward, with Artificial Intelligence being the most commonly discussed. However, there are many other developments that can lead to intelligent intelligence, provided that they meet a certain level of complexity.

VII. CONCLUSION

In a rapidly increasing number of malicious actors and cyber threats, it is essential to have a comprehensive cybersecurity strategy in place. Experience with DDoS prevention has demonstrated that security can be achieved with minimal resources when smart approaches are employed. According to publications reviews, studies into AI offer the most pertinent findings for cybersecurity. The implementation of neural networks is still in need of attention in many areas where neural networks are not the most suitable technologies.

These fields include decision making, situational awareness, and information control. Expert machine development is the most interesting area to focus on in this situation. Although the speed of general artificial intelligence cannot be predicted, it is likely that criminals will take advantage of any form of AI that is available. Furthermore, the most recent technology in understanding, interpreting, and managing information, particularly computer learning, could significantly enhance the cybersecurity capabilities of systems.

REFERENCES

[1] Smart technology / applications in cyber security. (n.d.). Retrieved August 14, 2020, from https://www.researchgate.net/publication/333477899_Use_of_Artificial_Intelligence_Techniques_Applications_in_Cyber_Defense.

[2] Ahmad, I., Abdullah, A. B. and Alghamdi, A. S. (2009). We apply artificial neural networks to detect DOS attacks. SINand#039;09 - Proceedings of the Second International Conference on Information and Network Security, 229–234. https://doi.org/10.1145/1626195.1626252.

[3] Bai, J., Wu, Y., Wang, G., Yang, S.X. and Qiu, W. (2006). A new recognition model based on multiple self-organizing maps and key component analysis. Computer Science Class Notes (including Artificial Intelligence subsections, Class Notes, and Bioinformatics Class Notes), 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. Research in Computer Science, 394, 5-24. https://doi.org/10.1007/978-3-642-25237-2_2.

IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

Impact Factor: 7.53

Volume 4, Issue 3, March 2024

[5] Carrillo, F.A.G. (2012). Can technology replace teachers in educational relationships with students? Procedia - Theory and social behavior, 46, 5646-5655. https://doi.org/10.1016/j.sbspro.2012.06.490.

[6] Chang, R.I., Lai, L. Bin and Kouh, J.S. (2009). Network intrusion detection using signal processing using query-based pattern filters. Eurasip Journal on Advances in Signal Processing, 2009. https://doi.org/10.1155/2009/735283.

[7] Chatzigiannakis, V., Androulidakis, G. and Maglaris, B. (2004). An example of distributed intrusion detection using security agents. HP OpenView University Association, June 2014.

[8] Chmielewski, M., Wilkos, M., & Wilkos, K. (2010). Building a Multi-Enterprise Environment for Military Decision Support Tools Using Semantic Services. Computer Science Class Notes (Including Artificial Intelligence Subseries Class Notes and Bioinformatics Class Notes), 6070 LNAI (PART 1), 173-182. https://doi.org/10.1007/978-3-642-134807_19.

[9] Corral, G., Llull, U. R., Herrera, A. F., Administrado, H., Ignasi, S. me Llull, U. R. (2007). Innovations in Hybrid Intelligent Systems {--} Articles of the II International Workshop on Hybrid Artificial Intelligence Systems (HAISand#039;07). 44/2008 (Pipiri 2014). https://doi.org/10.1007/978-3-540-74972-1.

[10] Feyerisl, J. and Aickelin, U. (2009). S Elf - Management M Aps. 1.-30. Akuhata.

[11] Ghosh, A.K., Michael, C., e Schatz, M. (2000). An intruder detection system based on the characteristics of the project. Informatics class notes (including the subseries of Artificial Intelligence Lecture Notes and Bioinformatics Lecture Notes), 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. and Dehmeshki, J. (2012). An automated approach to learning and refining type 2 Gaussian phase membership functions for pulmonary CAD classification systems. IEEE Transactions on Fuzzy Systems, 20(2), 224–234. https://doi.org/10.1109/TFUZZ.2011.2172616.

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

[14] Kotenko, I. and Ulanov, A. (2007). A multi-agency framework for benchmarking adaptive defense performance against cyberattacks. Computer Science Class Notes (Including Artificial Intelligence Class Notes Subseries and Bioinformatics Class Notes), 4476 LNAI, 212-228. https://doi.org/10.1007/978-3-540-72839-9_18.

[15] Kotenko, I. V, Konovalov, A., and Shorov, A. (2010). Client modeling and botnet modeling and botnet protection. In The Internet War Forum (pp. 21-44). http://ccdcoe.org/229.html.