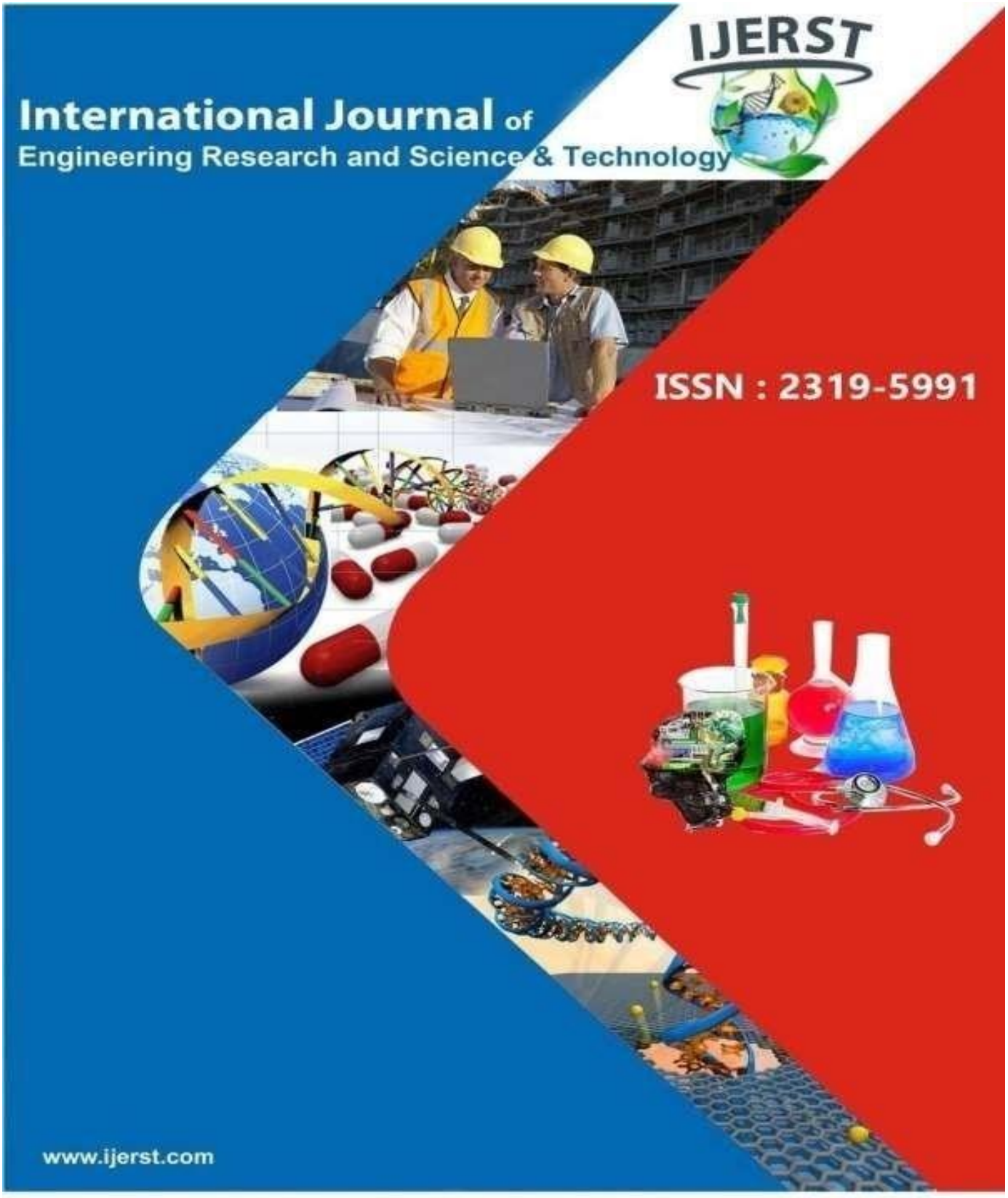

Harnessing Artificial Intelligence to Combat Cyber Threats

Ms. ZAHOORA ABID, Mr. MOHAMMED SADDAM HUSSAIN, Mrs. TAHERA ABID
Department of Information technology
Nawab Shah Alam Khan College of Engineering and Technology (NSAKCET

Vol. 20, Issue 3, 2024 https://doi.org/10.62643/ijerst.2024.v20. i3.pp366-375

Abstract. Humans are woefully unequipped to handle the sheer volume and complexity of data needed to keep cyberspace safe. However, it is challenging to construct technologies and software with conventional fixed implementations (hardwired decision-making logic) that adequately protect against security risks. Machine learning and other forms of artificial intelligence can handle this problem. This study assesses the potential for increasing defensive mechanisms and gives a brief review of artificial intelligence (AI) implementations of different cybersecurity employing artificial technologies. Reviewing existing AI software for cybersecurity leads us to believe that useful applications currently exist. To begin, neural networks are used for the purpose of protecting the perimeter and several other sectors of cybersecurity. However, it was obvious that using AI technologies was the most effective way to tackle some cybersecurity concerns. For example, logical decision assistance is a question in cybersecurity that has no clear solution, and thorough knowledge is crucial in strategic decision making.

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

1. Introduction

With the exponential growth in complexity of cyber-arms and malware over the last two years, it is evident that only intelligent technologies can aid in the defence against such sophisticated cyber weapons. Regarding the following instance of "On 15 January 2009, Conficker corrupted "Ultramar" the computer network of the French Navy," Consequently, the service has been placed under quarantine, and planes at several airbases have been compelled to land due to the inability to modify their flight itineraries [1]. The UK Ministry of Defence has acknowledged that some of its critical equipment and computers were contaminated. Sheffield hospitals have verified infections to over 800 computers, and the virus has spread into government offices and Navy Star/N* desk divisions. The Bundeswehr, the combined military forces of the Federal Republic of Germany, breached more than 100 of its computers, according to a report from 2 February 2009. For three days in January 2010, the Greater Manchester Police Information Network took preventative measures by disconnecting the Police Central Database. Employees were required to coordinate with certain groups in order to conduct routine vehicle and person searches [2]. Network Centric Warfare (NCW) increases the likelihood of cyber events, making changes to cyber defences an absolute need. Innovative offensive strategies, such as the completely automated responses to network assaults, integrated crisis management, and the dynamic building of protective perimeters, would greatly benefit from the use of AI approaches and knowledge-intensive tools [3].

For what reasons has the importance of smart applications grown so rapidly in cyberwarfare? If you examine the cyber room closely, you will see the following answer. Firstly, AI is necessary for the rapid reaction to events on the Internet. To understand and make sense of cyberspace activity, a large amount of data must be handled rapidly. People will not be able to achieve success in terms of operation speed and data volume without significant technological advancements. However, new threats arise all the time, making it difficult to construct computers with typical, fixed algorithms (hardwired decision-making logic) that can effectively fight against cyberattacks. This is a platform for intelligent automation [4].

Section two of this study delves into the scientific and technological domains that have adopted AI. We shall examine the well-established AI implementations of cyber defence in Chapter 3, which is grouped into AI approaches. In the fourth part, we'll look at some of the potential outcomes and present some new smart gadgets.

2. Research Methodology

To get an all-round impression of the junction between cybersecurity and AI, we used four databases:

Vol. 20, Issue 3, 2024 https://doi.org/10.62643/ijerst.2024.v20. i3.pp366-375

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. The search results which we got were limited only to the papers published in the last four years, as the determination of this paper is to bring out the newest trends of AI in cybersecurity. Last, the findings were categorized by the number of certifications. Besides those documents were selected, which had more than five citations. On the other side, newly published research papers that had less than five citations/references but innovative methods/approaches were also selected. The resources which meet the succeeding [6] requirements were subsequently accepted:

- Papers with titles belonging to subjects outside the scope of this research paper.
- Technical Reports, Patent Documents, Books, citations.
- Papers that had not been published in English.

In the 3rd step, we inspected the conclusions besides the abstracts for filtering the pertinent information. This step helped the authors to find if the confidential papers coordinated the topic to find the junction between cybersecurity and AI. Accordingly, those papers were chosen which had the most relevant data and met our objective. The methodology followed was an extensive literature review to analyze the gaps. This study latches the gap by bringing together the effect of multiple areas, AI usage in the Security domain, methods implemented, and methods that were put forth. It is used to develop an overall architecture for future research in this specific domain [7].

3. AI in depth

Artificial intelligence (AI) has been around for almost as long as computers (also known as initial system intelligence) as a field of study magazine. It has long been "on the horizon" in the field of artificial intelligence that machines may one day out-think humans in terms of intelligence. Problematically, the time period is becoming longer by the second. For instance, we saw several robots play really well at chess and solve quite difficult issues [8]. In the early stages of the computing, the chess game was seen as a challenge to the brain. Even though computer chess was all the rage in the 1970s, it seemed like an insurmountable task to create a system that could beat the world champion. Still, this transpired more rapidly than expected. Advances in computing power and the creation of effective search algorithms are the three main causes. Besides games like chess (for more on this, see the "Check" section below), it has a well-structured skill set that contains every conceivable piece of chess knowledge. Since the so-called tiny AI was just concerned with abstract concepts, the chess problem was essentially resolved. Improving a certain AI's ability to translate across languages is another example [9]. Natural Language Processing was supposed to get some early attention in the 1960s, particularly after N. Chomski's work in computational linguistics. Despite early indications of success from certain unusual projects like Google's AI linguistics, it hasn't happened yet. This involves AI being able to learn and master every facet of human life and function normally in response. Artificial intelligence (AI) is a branch of human intelligence that aims to build smarter machines that can do tasks that humans aren't very good at, like solving complex problems or making good decisions based on a large amount of data [10]. Here we take a straight shot, address the most recent developments in AI, and suggest using specific AI techniques to cyber defence problems (IOS Press, n.d.).

4. The Role of AI in Cyber Security

4.1 Is AI the future of cybersecurity?

Vol. 20, Issue 3, 2024 https://doi.org/10.62643/ijerst.2024.v20. i3.pp366-375

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. 03.09.2019 search Implemented Neural Structured Learning (NSL), an open- source 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].

AI is what brought us speech recognition apps (assume Siri), a search app from Google, and facial recognition tools from Facebook. Many manufacturers of payment cards often use AI to aid investment banks in stopping trillions of dollars in recorded fraud. But what about the application of their Information Security?

Is artificial intelligence a benefit or a challenge to digital security in the business? On the one hand, modern information management infrastructure is valuable because it facilitates the evaluation, study, and understanding of cybercrime by safety practitioners. It strengthens the digital management strategies companies utilize to counter cybercrime and helping in keeping businesses and customers secure. Artificial intelligence, on the other hand, may be very resource-intensive [16]. That might not be possible in any implementation. In fact, it may also serve as a formidable armament in the computer offenders' arsenal that leverages technology to improve and intensify cyber-attacks.

The debate around artificial intelligence was nothing special in terms of information security. Information is, after all, at the very heart of cyber safety trends. But what better way to analyze the information than using computer systems that can think in nanoseconds and then perform tasks that would take people considerably longer?

AI is rapidly a field of emphasis inside the computer safety community. We will analyze advancements in security tools for AI and how the technology impacts institutions, cybercriminals, and consumers alike. Let's work it all out. Why automated information protection protocols better improve internet security? Whether you're like multiple increasing companies, you have a variety of security

Vol. 20, Issue 3, 2024 https://doi.org/10.62643/ijerst.2024.v20. i3.pp366-375

layers in place boundary, network, edge, device, and computer storage. [17] For e.g., you might have firewall rules for hardware or software in addition to network security systems that track besides determining which linked devices are authorized and avoid others. If hackers make these protections past, the antivirus and malicious solutions will be up to them. Then they could face IDS / IPS solutions, etc.

Yet what will happen as cybercrime overtakes certain protections? When the security of knowledge depends entirely on human-based surveillance capacities, then you are in trouble. After that, cybercrime isn't necessarily pursuing a fixed timetable and shouldn't suit your susceptibility to cyber protection either. You need to be able to detect, identify and respond instantly to the threats 24/7/365. Irrespective of holidays, hours off work, even whether workers are simply unavailable, IT departments ought to be up to the job and ready to react promptly [18]. Artificial intelligence-powered information protection systems were designed to operate around the clock, shielding you. Infractions of a second, Artificial Intelligence may respond to cyber threats, which would require many minutes, hours, days, months, or even years to recognize by human beings.

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

It's not anything that can be achieved immediately that incorporates artificial intelligence technologies successfully with the current information defence networks. As you can expect, it requires time for preparing, instruction, and preparations to ensure that the programs and staff will utilize it to their greatest gain [20]. Allerin CEO and founder Naveen Joshi shares in an article for Forbes that there are numerous ways AI systems can ensure the sustainability of cybersecurity operations. Some of those features include:

- Developing precise, biometric password-based log-in technique/s
- Detection of risks and suspicious activity by predictive analysis
- Improved thinking and interpretation by way of natural speech recognition
- Securing identification and connection by a requirement

After you've incorporated AI into your information defense systems, your information intelligence experts and other IT management staff would need to learn how to do it efficiently. Which demands time, as well as planning. Be vigilant not to fail to invest with the organization's human aspect. Lots of big position players now use AI as part of their products and services if you reach around the industry. Examples of companies currently implementing artificial intelligence cybersecurity technologies involve major market pioneers such as [21]: Palo Alto Networks, Crowd Strike, Check Point, Fortinet, Log Rhythm, Fire Eye, Sophos Symantec, etc. Though there are many advantages of using artificial intelligence in knowledge security, there are risks to keep in mind too. One of the big difficulties in

Vol. 20, Issue 3, 2024 https://doi.org/10.62643/ijerst.2024.v20. i3.pp366-375

applying AI in information defense is that it appears to take more time and funds than traditional non-AI computer protection solutions.

That's partly because AI frameworks-based information protection technologies — besides those aren't cheap. As such, several businesses – particularly small and medium-sized organizations – have historically become prohibitively costly. Though, there are new SaaS (Security-as-a-service) technologies available that make AI cyber defence technologies more cost-efficient for business. So, let's all be honest, it's much easier to opt for viable information defence measures than facing the penalties, delays, and other expenses involved with violent cyber assaults.

4.4 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.

4.5 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. Offerings that we have

After a review of the articles on AI technologies on cybersecurity, we may infer that there are already multiple important features in this field. Firstly, they are used in perimeter shooting neural networks. [28] On the other hand, it is obviously only because AI approaches were used that even more cybersecurity problems could be overcome efficiently. In decision making, comprehensive information use is needed, and sound decision assistance is one of the cyber security's unresolved problems. In the artificially intelligent sector, a broad variety of approaches has been established for the resolution of complicated situations, which involve human intelligence [24]. Most of these strategies have attained a mature phase where specific algorithms based on these approaches are available. Several methods are even so prominent that they are no longer considered as a part of artificial intelligence. They are now a part of certain applications, such as data mining algorithms, which emerge from AI's learning subfield. In a short survey, you will not be able to attempt to include a more or less comprehensive overview of all practicable AI approaches. We have also divided approaches and architectures into multiple categories: artificial neural, expert systems, smart agents, quest, computer education, data gathering, and constraint resolution. Here we define the following groups and refer to the use of respective cyber protection approaches. We do not cover machine vision, robotics, and comprehension of natural languages that we find in particular AI applications. Robots and machine views undoubtedly have amazing military capabilities, but nothing unique to cybersecurity has been observed there [25].

Vol. 20, Issue 3, 2024 https://doi.org/10.62643/ijerst.2024.v20. i3.pp366-375

5.1 Neural Nets

Network Neural has had a long background starting with Frank Rosenblatt's discovery of the perceptron in 1957 an artificial neural network that is one of the most common neural network components. Already a limited combination of perceptions will study and resolve fascinating issues.

Yet, a huge proportion of neural networks could be made of neural networks. Neural networks thus include a parallel distributed learning and decision-making capability [26]. The operating frequency is their most defining characteristic. These are ideal for identification of learning patterns, grouping, a compilation of threat responses, ((4) Use of Artificial Intelligence Techniques / Applications in Cyber Defence, n.d.), etc. They may be applied in applications or electronics. Intrusion detection techniques avoidance is also applicable to neural networks. Plans were created in DoS detection, software worm identification, spam filtering, zombie identification, analysis of malware, and forensic science.

The fast mobility, whether implemented in hardware or used in graphical chipsets, causes the prominence of deep learning in computer security. The innovation of neural nets is new: cognitive nets of third-generation – rocketing machine learning that more effectively imitate artificial neurons and which offer greater possibilities for application. The use of FPGAs (field gate arrays) is a great way to rapidly build and adapt neural networks to changes in risks. They provide interesting possibilities.

5.2 Expert Systems

The most commonly deployed AI methods are certainly specialist programs. An expert program is a technology to seek solutions to problems raised either by a customer or a certain technology in a certain technology area. This may be used specifically in decision-making assistance, for example, with medical care, banking, or virtual worlds. There are various optimization techniques for solving complicated problems size from tiny analytical medical diagnoses to highly advanced hybrid systems. A scheme of expertise comprises a knowledge base that contains the specialist analysis of a specific application area [27]. In advisement to the knowledge base, this contains a deduction engine that offers solutions based on that understanding. Vacant understanding and motor of implication are commonly referred to as a current plastic understanding must be filled before it is used. The artificial intelligence shell must be endorsed by knowledge base software and can be lengthened by interactive query programs and with other programs which can be used in skilled hybrid engines. The advancement of a specialist system means, first, that the artificial intelligence shell should be selected and adapted, and, second, that erudite knowledge is gathered and the learning's supplied. The second step is far longer and much more complex than the first step. The development of intelligent machines has many

methods. In general, a device contains an artificial intelligence shell and has usability to add understanding to the repository of information.

There are several types of representations in expert systems, and the most general is stabilizers interpretation. Artificial intelligence may provide additional functionalities for simulation and so on, etc. Nevertheless, the importance of a master system primarily relies on the consistency of data in the skill set of the master system and not so much on the on-premises nature of the delineation of expertise. For security preparation, the instance of a cyber security device specialist is one. This skilled system enables substantially the collection and instruction of security initiatives to optimize the use of scarce resources. Initial stuff on the deployment of professional detection techniques is underway.

5.3 Intelligent Agents

Computational intelligence software components with some smart-action features which make themselves special: proactive, ACL, reactive (capabilities to make and act certain decisions). Intelligent agents are software applications. They may have the capacity to prepare, organize and evaluate. There is indeed a notion of software agents in the software development community in which they are seen as artifacts that at least proactively use the networking language of an agent. Differentiating agents and subjects, subjects can be passive and have no communication to comprehend (though they embrace strictly delineated syntax messages).

Vol. 20, Issue 3, 2024 https://doi.org/10.62643/ijerst.2024.v20. i3.pp366-375

Intelligent agents were used to protecting DDoS, and simulations were described where it is possible to effectively protect cooperation agents from the attacks of DDoS. When all regulatory and contractual problems have been addressed, a 'cyber police force' composed of mobile smart officers would, in practice, be feasible. This would include technology to enable mobility and connectivity of cyber personnel, which must be inaccessible to opponents. Cooperation with ISPs is important. However, if further experience can be used to direct the search, it can greatly enhance the efficacy of the quest. Almost every smart system has some type of quest, and its quality is often important for its overall performance.

5.4 Search

A broad variety of search techniques is created that takes detailed focus on specific search problems into consideration. Although numerous search techniques in AI were established and are commonly used in many applications, they are rarely used as using AI. Of one, the search is embedded in the application stack and is not seen as an AI function. In this sense, dynamic analysis programming is used primarily to address optimal security concerns. Check on besides- or trees, αβ-index, minimal check-in addition stochastic index is commonly used in the applications of gamers and is useful in network security decision-making. Originally designed for software chess, the αβ-search algorithm is an adaptation of a common assistance principle "divide and conquer" in the resolution of problems and, in particular, in decisions where two opponents chose their absolute best move. This uses minimum expected gain and cumulative potential loss figures. Perhaps you can disregard a vast range of options and speed up the quest considerably.

5.5 Learning

Learning strengthens the information structure through the extension, reorganization, or enhancement of the knowledge base. It is one of the most important artificial intelligence topics being studied intensively. Calculative approaches for gaining new ideas, new abilities, and innovative ways to coordinate current knowledge require computer learning. Learning challenges range widely from basic parametric learning, which means knowing the meaning of such quantities, to complex types of abstract teaching, such as concept learning, grammar learning, usability, and behavioural teaching.

AI offers both monitored (learning with a teacher) and unattended learning forms. The above is particularly helpful where vast volumes of data are present. In addition, this is popular in cybersecurity, where massive logs can be obtained. Initially, data mining was derived from uncontrolled AI learning. Uncontrolled learning may be a function of self-organized neural networks,

in general. Parallel neural networks are used for output in parallel hardware with a distinctive class in learning techniques. These methodologies of learning are defined by an evolutionary algorithm and neural networks. For instance, genetic analytics, in addition to fuzzy logic, was used in mentioned threat detection methods.

6. 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 decision- making 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

Vol. 20, Issue 3, 2024 https://doi.org/10.62643/ijerst.2024.v20. i3.pp366-375

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

Sophisticated cybersecurity solutions are essential in a world where cyber threats and malevolent intelligence are growing at an exponential pace. Furthermore, DDoS avoidance experience has shown that, with effective tactics, large-scale attacks may be securely prevented with minimum resources. Reviewing the literature on artificial neural networks reveals that these fields have produced the AI results that are most applicable to cybersecurity in general. The use of neural networks in cybersecurity is ongoing. Sophisticated cyber-security methods are still terribly required in several domains where neural networks weren't the best technology. Assistance with decisions, situational awareness, and information control are all examples of such domains. Expert machine development is the most intriguing part of this situation.

Unfortunately, it is impossible to predict how quickly general-purpose AI will develop; yet, criminals may take use of any available technology. Nobody sees this coming. Further, stateof-the-art technology in data comprehension, analysis, and management, especially in the field of machine learning, will greatly enhance cybersecurity capabilities of systems.

References

[1] The First Use of AI Methods and Tools for Cyber Defence (n.d.). The research article "Use of Artificial Intelligence Techniques Applications in Cyber Defence" was retrieved on August 14, 2020, from https://www.researchgate.net/publication/333477899. This information is sourced from Ahmad et al. (2009). Use of a neural network for the purpose of detecting denial-of-service attacks. Page numbers 229–234 from the 2009 SIN conference on information and network security.
Doi: 10.1325/10.1145/1626195.1626252.

[2]In 2006, Bai, Wu, Wang, Yang, and Qiu published a study. An innovative approach for intrusion detection that uses principal component analysis and multi-layer self-organising maps. Volume 3973 of the Lecture Notes in Computer Science (including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) has pages 255–260. This citation is available at: https://doi.org/10.1007/11760191_37.

[3]In 2012, Bitter, North, Elizondo, and Watson published a study. An overview of neural networks and its use to detecting intrusions in networks. Chapters 5–24 of Studies in Computational Intelligence, volume 394, page. Here is the link to the article: https://doi.org/10.1007/978-3-642-25237-2_2.

Vol. 20, Issue 3, 2024 https://doi.org/10.62643/ijerst.2024.v20. i3.pp366-375

[4]This is a reference to Carrillo (2012). In the pedagogical connection with the student, can technology take the role of the teacher? The article may be found in Procedia - Social and Behavioural Sciences, volume 46, pages 5646–5655, and the DOI is 10.1016/j.sbspro.2012.06.490.

[5]In 2009, Chang, Lai, and Kouh published a study. Using a query-based sampling filter for signal processing, we can detect network intrusions. The article was published in 2009 and may be accessed at https://doi.org/10.1155/2009/735283 in the Eurasip Journal on Advancesin Signal Processing.

[6]A study conducted by Chatzigiannakis, Androulidakis, and Maglaris in 2004 was cited as . We present a security agent-based distributed intrusion detection prototype. University Association for HP OpenView, June 2014.

[7]The authors of this work are Chmielewski, Wilkos, and Wilkos (2010). Constructing a semantic service-based multi-agent environment for use by military decision-support technologies. Articles 173–182 from the 6070 LNAI (PART 1) Computer Science Lecture Notes (Including Subseries AI and Bioinformatics Lecture Notes). The publication's DOI is 10.1007/978-3-642-13480-7_19.

[8]According to a 2007 study by Corral et al., Llull, Herrera, Management, Ignasi, and Llull, the authors of this work are [9]. New developments in hybrid intelligent systems {— } Workshop on Hybrid AI Systems, Second International Conference (HAIS'07). June 2014, number 44/2008. Doi: 10.1007/978-3-540-74972-1.

[9]In 2009, Eyeereisl and Aickelin published a paper. Page number: 1-30 in S Elf-O Rganising M Aps. August.

Ghosh, A. K., Michael, C., & Schatz, M. (2000) written in 2000. A learning-based intrusion detection system that operates in real-time. Proceedings of the 1907 Fall Lectures on Computer Science (With Supplemental Lectures on Artificial Intelligence and Bioinformatics): 93–109. Find it at this URL: https://doi.org/10.1007/3-540-399453_7.

[10]In 2012, Hosseini, R., Qanadli, S. D., Barman, S., Mazinani, M., Ellis, T., and Dehmeshki, J. published their work. Using a gaussian interval type-2 fuzzy membership function application to a lung CAD classification system, an automated method for learning and tweaking is shown. (224-234). In: IEEE Transactions on Fuzzy Systems, Volume 20, Issue 2. Please find the following link: https://doi.org/10.1109/TFUZZ.2011.2172616.

[11] Source: iOS Press. "Algorithms and Architectures of Artificial Intelligence" by Ios Press, retrieved August 14, 2020.

[12]Published by Kotenko and Ulanov in 2007. Simulation of adaptive cooperative defence against internet threats using a multi-agent framework. The 4476th volume of the Lecture Notes in Artificial Intelligence and Bioinformatics series, which includes Computer Science Lecture Notes, is numbered 212-228. This is the link to the article: https://doi.org/10.1007/978-3-540-72839-9_18..

Vol. 20, Issue 3, 2024 https://doi.org/10.62643/ijerst.2024.v20. i3.pp366-375

[13] In a 2010 study, Kotenko, Konovalov, and Shorov analysed the data. Agend-based Modelling and Simulation of Botnets and Botnet Defence. Pages 21–44 of the Conference on Cyber Conflict. see this link: http://ccdcoe.org/229.html.

[14]A study conducted by Kotkas, Penjam, Kalja, and Tyugu (2013) was cited as [16]. A proposal for software technology based on models. Presented at the 2013 MODELSWARD Conference on Model-Driven Engineering and Software Development, the proceedings include pages 312-315.
The link to the article is https://doi.org/10.5220/0004348203120315".

[15]In 2009, Pachghare, Kulkarni, and Nikam published a study. Intrusion detection system employing self organising maps. Volume 4, Issue 12, Pages 11–16, 2009 International Conference on Intelligent Agent and Multi-Agent Systems (IAMA 2009). The link to the article is https://doi.org/10.1109/IAMA.2009.5228074?.

[16]In a 2017 study, Pathi and Anand found [18]. Data Mining for Cyber Defence. In: International Journal of Computer Science and Engineering, Volume 5, Issue 12, Pages 317-318.