International Journal of Engineering Applied Sciences and Technology, 2023
Vol. 8, Issue 01, ISSN No. 2455-2143, Pages 185-189
Published Online May 2023 in IJEAST (http://www.ijeast.com)

A REVIEW ON ARTIFICIAL INTELLIGENCE TECHNIQUES IN PREVENTING CYBER THREATS

Triveni Krishnappa
School of Computing and Digital Media Department of IT
London Metropolitan University, London, England, UK

Abstract— **Artificial intelligence advancements in the present day are proving to be the most effective method for preventing cyberattacks. Artificial intelligence (AI) is being used by experts as a protection against cyberattacks. This technology is being used by security analysts to spot abnormalities, which reduces time and reduces total company expenditures. With the proliferation of IoT and linked devices in today's digital world, cyber security professionals are constantly confronted with new difficulties. The expert needs all available tools to stop attacks, discover security problems, and respond to attacks. The greater standard of technology in today's environment is strongly correlated with the rise in cybersecurity risks. The digitalization of organizations makes it essential to focus on cybersecurity issues and ways to make them better. Using artificial intelligence in cybersecurity is essential to improve data protection because traditional computer algorithms may occasionally be inadequate to manage all cyber threats. A descriptive-analytical approach from previous research on the application of AI in cybersecurity is used. This paper aims to emphasise artificial intelligence and the concepts of cybersecurity that can be developed to improve the security of the data. Methods based on artificial intelligence can enhance the overall security operation of traditional security systems and give higher security against an increasing array of complicated cyber threats, when traditional security technologies may be incompetent or ineffective. In this study, we look at how human reasoning and artificial intelligence (AI) can be leveraged to improve cyber security. This study's primary goal is to showcase current developments in the use of AI approaches to defend against cyberattacks.**

Keywords— **Threats, Information Security, Cyber, Digital crimes, Cyber Attacks, Artificial Intelligence, Automation**

I. INTRODUCTION

Cyberattacks using AI are a new and developing trend. How this will impact cybercrime in the future is not yet apparent. Cybersecurity employs a variety of AI and machine learning approaches. The most popular ones are tactics that make use of AI to spot and keep an eye on criminal activity, identify online threats, and safeguard a company's networks. For example, a malware analyst can train an AI system to recognize dangerous files or locate compromised PCs using machine learning methods. The main issues that businesses face when integrating AI into cybersecurity are how to create and manage data that is accessible across many systems and how to structure data such that it is accessible for cognitive applications that can include human oversight. Today, AI is used in many different industries due to the diverse applications that are related with it. The impact of these applications has helped people have more interest in AI technology (Bibhu Dash, 2022). Grand View Research estimates the worldwide AI industry to be worth USD 93.5 billion in 2021, with a CAGR (compound annual growth rate) of 38.1% projected from 2022 to 2030. Lately, AI has been widely used in various fields, including cyber security (NICOLA CAPUANO, 2022).

In order to monitor and stop cyberattacks, a system must not only be able to recognise the attack but also fully comprehend it and communicate it to the user. Such as, Anomaly detection systems is common approaches that use ML (Machine Learning) or DL (Deep Learning) methods to simulate typical behaviours in a way that makes identifying suspicious deviations over the norm simple and data-driven. Data mining, pattern recognition, and event prediction can all be done with AI. It can also be used to spot cyberattacks and stop them before they begin. AI systems will soon be able to identify patterns that are not immediately obvious to humans, such as a potential cyberattack, by examining network traffic and evaluating whether various data packets are accessed in a strange way. While building a line of protection against hackers, artificial intelligence can be a valuable asset. AI is capable of identifying patterns and examining them regularly for any anomalies (Rakesh Kumar Saini, 2019).

II. RESEARCH METHODOLOGY

The methodology is the process of identifying different information by employing various instruments and strategies to collect data. To explore the function of artificial intelligence in cybersecurity, secondary data collecting is employed in this research paper. The secondary method of gathering data is the

most appropriate for this study because it draws on a variety of pre-existing sources, such as stored data from government and non-government organizations, records, articles from newspapers and other journals, and research scholars with relevant information about AI in cybersecurity. The secondary data collection approach is reliable as well as effective than the first. Given that the data is gathered quickly and from sources that already exist, it takes less time as well as resources to complete.

We have a clear understanding of artificial intelligence thanks to information gathered from numerous newspaper articles, academic studies, and other sources. We learn that artificial intelligence is engaged with the creation of a machine that can emulate human thought and behaviour. A wide variety of AI systems with different capabilities have been developed and used as a result of the ongoing performance advancements in software and hardware for computers (along with their declining costs) and methodologies like big data and cloud computing (SHERALI ZEADALLY, 2020). Artificial intelligence is quite helpful in handling various cybersecurity concerns when it comes to cybersecurity.

To stop destructive cyber attacks, security experts can now analyse network data using artificial intelligence to find vulnerabilities. According to research using alternative techniques of acquiring pre-existing data, artificial intelligence plays an important part in cybersecurity by safeguarding it from various threats.

III. LITERATURE REVIEW

Artificial intelligence is able to recognise different cyberattacks using a variety of web platforms and legitimate websites with high levels of security. to carry out penetration testing and uncover security gaps in the system as to be started by cyberattack hackers, using malware, ransomware, and many more tools (Gray, 2022). Due to this, websites with a high need for security rely on artificial intelligence as their main tool for identifying different cyberattacks. The website in control would also think like a hacker to stop a cyber assault. where it is necessary to use artificial intelligence to act like a hacker and attempt to crack security codes. In order to protect a website from hackers and cyberattacks, software techniques like the artificial intelligence-based Norm Shield Scorecard are used.

To make it harder for hackers to access their servers and other sensitive information kept in computers, artificial learning relies on cutting-edge technology such as deep learning, machine learning, natural language processing, etc. Artificial intelligence lessens the need for human intervention in cybersecurity issues. It is the responsibility of many cybersecurity experts to monitor the website's security. Professionals in the cybersecurity field find it challenging to work nonstop for extended periods of time without breaks, vacations, or holidays. While artificial intelligence is programmed to be able to deal with high-risk situations without worry, it can manage the same situations without pausing. Tele-monitoring systems for electronic health are now not as secure as they once were (Carmelo Ardito, n.d.). Artificial intelligence has had an effect on security since it enables experts to spot numerous network anomalies by examining user behaviour and studying patterns. To stop destructive assaults, security experts can now analyze network data using artificial intelligence to find flaws.

The intelligence and military sectors employ AI to pinpoint certain items in a picture or video. The capacity for AI to make autonomous decisions, such as how many individuals should perish based on an estimated crime rate, goes hand in hand with the potential for abuse. A 2019 study revealed that over 92% of Forex trading was carried out by AI and not by humans. AI is used to predict stock market disasters. Algorithms are presently used to conduct more than 60% of deals worth $10 million or more, and within the next four years, that percentage is anticipated to rise dramatically.

IV. CASE STUDY

A cyber security firm called Dark trace employs AI to find and address online threats. The Enterprise Immune System, the company's main product, utilizes algorithms based on machine learning to identify unusual network activity, such as insider threats and sophisticated persistent threats. In order to establish a baseline of typical activity, the system analyses data from network devices as well as other sources, including logs and user behaviour. Then, it employs machine learning algorithms to spot changes from that baseline that might portend a cyber threat (Darktrace, 2022).

The capacity of Darktrace's system to identify unique threats that might not have been noticed before is one of its main advantages. This is so that the system can gradually adapt to new dangers and learn from its environment. For instance, the system can identify a new malware variant's behaviour and identify it as a potential concern if it is brought into the network.

Organizations from a variety of industries, including the pharmaceutical, financial services, and government sectors, have employed Darktrace's solution. For instance, in 2017, a cyberattack was detected, and the National Health Service (NHS) of the UK employed Darktrace's method to respond. Thousands of NHS computers were impacted by the attack, which was eventually linked to the WannaCry ransomware, which interfered with patient care (Harris, 2018). The IT personnel was informed of the attack by Darktrace's system, which enabled them to react promptly and limit the damage.

The way cybersecurity is conceptualised and applied is evolving thanks to AI-powered technologies such as Darktrace's Enterprise Immune System. These systems can identify and respond to cyber-attacks within real-time, even when confronted with fresh and complex threats, by utilising algorithms that use machine learning and other AI techniques (Mitroff, 2018). AI-powered technologies will be more crucial for enterprises wanting to safeguard their data and networks as cyber-attacks continue to develop.

International Journal of Engineering Applied Sciences and Technology, 2023
Vol. 8, Issue 01, ISSN No. 2455-2143, Pages 185-189
Published Online May 2023 in IJEAST (http://www.ijeast.com)

V. DISCUSSION OF FINDINGS

Cognitive technologies are also being adopted by cybersecurity more and more in line with this trend. Cognitive technologies driven by AI are a crucial component of a comprehensive strategy for cybersecurity where the human element serves as the process's main guide. Cyber Vance emphasises the significance of evaluating cybersecurity strategy trends, particularly how firms may adopt new technology and defend against cyber-attacks, in its research, Cybersecurity Trends to Watch Out For in 2019. The other approach is the widespread application of classic military and military intelligence procedures, particularly so-called "kill chains," in cyber defence (ROUMEN TRIFONOV, 2017).

Professionals in the field of cybersecurity used to spend the majority of their time monitoring threats and constructing defences. The employment of AI technologies for nefarious purposes has increased the effect of possible cyber risks by enabling larger-scale and more potent attacks. In order to launch more potent attacks, cybercriminals have started to refine their methods by incorporating IoT hacking, malware, ransomware, and AI. As a result of the interconnection and intelligence of these attacks, everybody is put at danger (NEKTARIA KALOUDI, 2020). They are now more focused on evaluating and reducing risk, which enables them to steer clear of potentially harmful vulnerabilities. They no longer concentrate on monitoring dangers, but rather on reducing risks and determining probability. For individuals wishing to enter the field, these developments open up a completely new universe.

As technology advances daily, threats and attacks also do so, so in order to combat this assault, our security system must incorporate AI techniques (Amaan Anwar, 2017). Intelligent agents and Expert systems are two types of AI techniques that are used to identify and mitigate cyber threats.

– Expert Systems

Expert Systems are indeed a class of computer system that mimics human decision-making. A Knowledge Base as well as the Inference Engine are the two subsystems that make up knowledge-based systems (Dr. Sunil Bhutada, 2018). The knowledge base keeps the data and connects to the inference engine, which analyses the data and makes inferences to help in decision-making.

– Intelligent Agents

Software that operates in a setting that is not under external control is referred to as an intelligent agent. It has the capacity to adapt to changes in its environment and persistently work towards its objectives over time. An intelligent agent could be created to learn about all options and then choose the one that will best help it achieve its objective. It has the ability to spot behavioural patterns that could be signs of an impending attack.

VI. IMPLICATIONS

Despite breakthroughs in cyber security, cyber attacks are getting even more hazardous. Businesses employ behavioural analysis integrated with artificial intelligence to improve the threat hunting process. Artificial methods like UEBA can evaluate users' typical behaviour, as well as that of servers and endpoints, and detect user behaviour anomalies that can indicate a zero-day attack. The use of AI not only automates a work but also substantially boosts efficiency. As a result, attackers might consider such a delectable spread highly appealing (Abhilash Chakraborty, n.d.). This can assist businesses in defending against vulnerabilities that aren't even identified or fixed. Numerous crucial data centre operations, including temperature filters, backup power supplies, power usage, bandwidth consumption, and internal temperatures, can be monitored by artificial intelligence.

Artificial intelligence is able to recognise different cyberattacks using a variety of web platforms and legitimate websites with high levels of security. to perform penetration testing, find a hole in the system, and launch cyberattacks using malware, ransomware, and a variety of other tools. However, there are some restrictions on applying artificial intelligence in some kind of a cyber business, such as the cost of upkeep for resources such as computing memory, energy, and data. Yet not all tasks should be automated. Every stage of this procedure should be taken into consideration, including whether the investigation's current state has to be improved (A V Pilitsky, 2020). Security professionals must keep an eye out for numerous sets of malware, anomalies, and harmful programmes.

VII. RECOMMENDATIONS FOR FURTHER IMPROVEMENTS

Today's biggest threat to organisations including businesses, governments, and educational institutions is cybercrime. Data breaches in 2016 compromised more than 200 million personal details, including well-known ones at the Federal Bureau of Investigation and the Department of Homeland Security (Arockia Panimalar.S, 2018). Network security, which includes firewall, intrusion prevention system, antivirus programs, and encryption technologies, is the most popular line of defense against cyber threats. Although network security is beneficial, it is not a stand-alone solution. Neither system is 100% secure, experts believe, because attackers will always be able to take advantage of weaknesses. One element of a comprehensive cybersecurity plan is network security. Consequently, cloud security refers to securing data from hackers through cloud computing environments like Microsoft Azure or Amazon Web Services (AWS).

The goal of a security strategy is to lessen the effects of any security breaches. It consists of a number of tactics, policies, and procedures. It outlines actions to reduce risk from dangers including malware, data breaches, and cyberattacks. Firewalls increasingly rely on ANN and neural networks like deep Armor, which uses machine learning models to protect from

malware and zero-day exploits, as opposed to the rule-based engines used by anti-malware software (Kandala kalyana Srinivas, 2022). A cybersecurity strategy consists of the following elements: Risk assessment, which estimates overall likelihood that such an event will occur as well as the potential repercussions of the event, is one element of a cybersecurity plan. Various threats and weaknesses to a business will frequently be taken into account during a risk assessment. A Zero Trust Policy is one of many policies that is advantageous for companies looking to create more firm control over various facets of their digital security. It makes sure that businesses can control access to private data through taking into account available resources and past user behavior. The Zero Trust Policy enables the reduction of a risk of data breaches while upholding employee privacy. The zero-trust philosophy is advantageous to businesses, workers, and personal privacy. It assists people in creating a secure digital identity and opens doors for access when required. As far as traditional tactics are concerned, the following strategies were used to guard against cyber threats:

- Employing antivirus and firewall software:
- Making use of VPNs and secure browser add-ons
- Making use of strong passwords
- Making use of security updates and pathways

VIII. CONCLUSION

Artificial intelligence is improving both the security of businesses and individuals, but it is also giving the wrong people more control. We must make sure that Artificial Intelligence only works with humans who wear white hats if we want to grant it additional power in the near future for security considerations. Artificial intelligence is undoubtedly more powerful, intelligent, and quick than human intellect, but it needs human interaction to start. Therefore, businesses must put a lot of effort into finding and training AI experts who can collaborate with the machine to ensure the safety of their products. Mixing AI and the human intellect will undoubtedly aid in the fight against hackers. To conclude, artificial intelligence is starting to become more and more significant in how businesses protect its networks and sensitive data. As machine learning, artificial intelligence, and intelligent automation continue to advance, smart firms will be able to use newer, better, and more efficient solutions to stay one step ahead of hackers in the not-too-distant future.

IX. REFERENCE

[1]. Bibhu Dash, P. S. M. F., 2022. Threats and Opportunities with AI-based Cyber Security Intrusion Detection: A Review. International Journal of Software Engineering & Applications (IJSEA), Sep, 13(5), pp. 13-21.

[2]. NICOLA CAPUANO, G. F. V. L. C. S., 2022. Explainable Artificial Intelligence in CyberSecurity: A Survey. IEEE, 5 Sep, Volume 10, pp. 93575-93600.

[3]. Rakesh Kumar Saini, C. P. A. D., 2019. Current Trends in Information Technology A Survey on Artificial Intelligence Techniques for Cybersecurity. STM Journals, 9(3), pp. 5-13.

[4]. SHERALI ZEADALLY, E. A. Z. B. I. A. K., 2020. Harnessing Artificial Intelligence Capabilities to Improve Cybersecurity. IEEE, Jan, Volume 8, pp. 23817-23837.

[5]. Carmelo Ardito, T. D. N. E. D. S. D. L. A. P. a. F. V., n.d. An Artificial Intelligence Cyberattack Detection System to Improve Threat Reaction in e-Health. Italy, s.n.

[6]. ROUMEN TRIFONOV, S. M. R. Y. G. T. G. P., 2017. Artificial Intelligence Methods for Cyber Threats Intelligence. International Journal of Computers, Volume 2, pp. 132-135.

[7]. NEKTARIA KALOUDI, J. L., 2020. The AI-Based Cyber Threat Landscape: A Survey. ACM Computing Surveys, Feb, 53(1), pp. 20-34.

[8]. Amaan Anwar, S. I. H., 2017. Applying Artificial Intelligence Techniques to Prevent Cyber Assaults. International Journal of Computational Intelligence Researc, 13(5), pp. 883-889.

[9]. Dr. Sunil Bhutada, P. B., 2018. International Journal of Engineering Research in Computer Science and Engineering (IJERCSE). Applications of Artificial Intelligence in Cyber Security, Apr, 5(4), pp. 214-219.

[10]. Abhilash Chakraborty, A. B. a. A. K. K., n.d. Artificial Intelligence for Cybersecurity: Threats, Attacks and Mitigation. s.l.:National Institute of Technology.

[11]. A V Pilitsky, O. E. P. a. V. N. H., 2020. General approach to automating the process of responding to computer security incidents. Russia, s.n., pp. 1-5.

[12]. Kandala kalyana Srinivas, D. V. S., 2022. Artificial Intelligence Techniques for Prevention of Cyber Attacks and Detection of Security Threats. International Journal of Engineering Research and Applications, June, 12(6), pp. 37-44.

[13]. Arockia Panimalar.S, G. P. S. K., 2018. ARTIFICIAL INTELLIGENCE TECHNIQUES FOR CYBER SECURITY. 5(3), pp. 122-124.

[14]. Gray, C., 2022. cybermagazine. [Online] Available at: https://cybermagazine.com/cyber-security/five-ways-ai-can-be-used-to-prevent-cyber-attacks [Accessed Mar 2023].

[15]. Darktrace, 2022. Darktrace. [Online] Available at: https://darktrace.com/products [Accessed March 2023].

[16]. Harris, S., 2018. www.zdnet.com. [Online] Available at: https://www.zdnet.com/article/how-the-

nhs-used-ai-to-tackle-the-wannacry-ransomware-attack/ [Accessed Mar 2023].

[17]. Mitroff, 2018. wired.com. [Online] Available at: https://www.wired.com/story/darktrace-uses-ai-to-fight-cyber-attacks-before-they-even-start/[Accessed Mar 2023].