How Artificial Intelligence Is Changing Cyber Security Landscape and Preventing Cyber Attacks: A systematic review

Ishaq Azhar Mohammed

Data Scientist & Department of Information Technology

Dubai, UAE

Abstract*-The primary objective of this study is to assess the effect of artificial intelligence on the cybersecurity environment, particularly in the area of cyber-attack mitigation. The world is changing at a breakneck speed, and businesses that embrace technology have a bright future ahead of them [1]. Digitization has accelerated the pace of change in a variety of areas, including entertainment, new goods, and business [1]. The client receives what they want immediately since the service provider is armed with everything necessary to provide goods or services [1,2]. While the digital age offers many benefits and conveniences, it also has a few drawbacks. The danger of losing your private information is one of the most serious and damaging risks associated with it. Over the past decade, there have been many instances of identity theft, data breaches, and financial loss. Cyberattacks are often widespread, affecting people, government entities, and companies. Cybercriminals may now reach their targets from anywhere in the globe and at any time. The assault surface in contemporary business settings is enormous, and it is growing at a breakneck pace. This implies that evaluating and enhancing a business's cybersecurity posture requires more than human involvement [2,3]. Artificial intelligence is increasingly critical to information security since these technologies are capable of rapidly evaluating millions of data sets and identifying a broad range of cyber risks, ranging from malware attacks to suspicious behavior that may result in a phishing assault. This system is always evolving and improving, relying on previous and current events to identify new types of attacks that may occur today or tomorrow. In this paper, I will discuss the employment of artificial intelligence (AI) in cybersecurity (both positive and negative) in the business world.*

Keywords: *Artificial intelligence, cybersecurity, automation, cyberattacks, breach detection.*

I. INTRODUCTION

Not only has the usage of Artificial Intelligence (AI) revolutionized service delivery, but has strengthened cybersecurity. Globally, it is estimated that 15% of companies have used AI technological innovations [3]. However, technological adoption has both good and bad implications for companies. If your company does not implement rigorous security measures, hackers will use the same technologies that you use to protect yourself. As a result, you should never be complacent when it comes to technologically based security measures. Rather than that, you should upgrade your AI security solutions regularly to keep your company secure [3]. For instance, businesses must have distinct coded messages that may be read as a danger to the business by AI Technologies. Conducting a frequent cybersecurity risk assessment is one of the most secure ways to upgrade your AI system [3]. If a company is targeted, one should investigate the technique used by hackers to gain access to the institution's systems and write code to prevent similar behavior in their networks [5]. When an employee hits on a malicious link and infects a networked workstation, the infection may spread to other computers [5]. As a consequence, other network users must select whether or not to click on the malicious program. In comparison, when humans are removed from a business process, a virus that makes its way into an automated machine-to-machine network spreads considerably more quickly, thus magnifying the effect. As a result, cybersecurity has never been more critical than it is today. A cyberattack is a cybercriminal's effort to gain unauthorized access to, damage, or modify a target's network or computer [6]. It is deliberate, systematic, and planned to attack information systems and undermine their activities and organizations [6]. Even when the most robust preventive measures are in place, hackers will attempt to circumvent them. It is doubtful that cyber dangers will ever be fully eradicated since hackers are clever and persistent, always looking for new methods to penetrate a company's defenses. Automating dozens or hundreds of manual activities is becoming a fundamental requirement for many companies [6]. However, the same characteristics that make automation so successful also expose businesses to new dangers. The reason for this is that because AI enables businesses to remotely monitor computers and make them interact with one another, bad actors can take control of the emerging technologies and create havoc [7]. This paper will therefore discuss how AI works in addressing cybersecurity issues, specifically stopping possible attacks on a computer network: malicious code such as viruses and phishing emails used to mislead people.

II. PROBLEM STATEMENT

The main problem that this paper will solve is to examine how artificial intelligence can be used to resolve cyber-attack-related problems. Consider a malicious actor that employs AI to carry out their heinous acts. This individual may infiltrate a network and get data on a company's workers. The hacker may then persuade workers to disclose customer data or extort the business through a ransomware assault by utilizing AI to personalize messages and visuals (i.e., by displaying photos of known individuals) [8]. Although machine-to-machine interaction may eliminate the need for human involvement, IT professionals must reconsider how they grant authorization to their increasing number of computer systems [8]. Even if a machine receives an automated request to obtain data from another system (instead of a person), the first computer must be capable of rigorously authenticating the request. This presents a new issue for businesses whose information systems are mostly accessible by humans rather than other machines. It took years – and a slew of high-profile cyberattacks, government laws, and fines – for businesses to develop effective information technology security defenses [8,9,10]. They

have, however, mainly built their methods to prevent human-to-machine attacks—that is, to block the wicked but skilled hacker. Passwords have obvious flaws in today's age of widespread automation. They are susceptible to sharing and may therefore be used to get access to numerous systems. They are scribbled and shared.

III. LITERATURE REVIEW

A. Cybersecurity Landscape

The world's technological level is unquestionably increasing daily. Organizations are integrating technology into many aspects of their operations. While it may have many advantages for the business, it exposes it substantially to the dangerous realm of cyber criminals [10]. To guarantee the organization's continued security following technology adoption, companies must employ cybersecurity measures [10]. This entails developing comprehensive methods for safeguarding an organization's applications, networks, and technologies from cyberattacks. The cybersecurity landscape should include measures to protect the organization from crypto-jacking, data leaks, data phishing, ransomware, and Internet of Things threats (IoT). One should use experienced IT professionals and ethical hackers to guarantee that your AI security solution is impenetrable [10].

B. Relationship of Cybersecurity and Artificial Intelligence

Artificial intelligence is a key factor that determines computer decision-making. For instance, the computer may identify suspicious activity on the system and deny access until the appropriate authority authorizes it. These artificial intelligence methods make use of Machine Learning, in which IT experts build algorithms based on data collected over time [11]. The algorithm is built in such a manner that it is capable of identifying and distinguishing genuine access from fraudulent access. Machine Learning technology increases the predictability of attacks and abnormalities, thus enhancing an organization's security [11]. The precision and speed with which threats are identified are unmatched by humans. As a consequence, artificial intelligence and machine learning technologies can avert cyber-attacks that might cost your company millions. Nevertheless, businesses must continue to update security systems as hackers evolve in response to technological advancements.

C. Artificial Intelligence Operations

Artificial intelligence (AI) operations involve a framework designed up of a variety of computers that have been programmed to identify and prevent any suspicious activity in the networks [12]. The system is programmed in such a manner that it can identify dangers without human intervention. This independence reduces the possibility of compromise, which may result in unauthorized access to the organization's databases [12]. While the AI is mostly independent, it does allow for the incorporation of supervised instructions as necessary. This is important for classifying the organization's risks. For instance, the system may be instructed to categorize attacks like ransomware or malware based on their characteristics. Even so, the assessment will be categorical, assisting management in making critical choices about the AI system update [13].

D. Artificial Intelligence in Cybersecurity

There have been major technological advancements that have impacted cybersecurity. One of the main game changers in the area of cybersecurity is the development of tools and methods that are supplemented as a sub-group by artificial intelligence (AI) [13]. Artificial Intelligence (AI) is no longer simply a trendy term; it is now being utilized widely across a wide range of sectors. Customer support, healthcare, and robotics are just a few of the many areas where AI has accelerated progress [13]. Additionally, it is making a major contribution to the continuing combat against cybercrime. Here are a few ways AI is helping to improve cybersecurity.

Fig i: AI in cybersecurity

E. AI benefits in cybersecurity

AI has numerous benefits and uses in several domains, including cybersecurity. With rapidly changing cyber-attacks and the rapid increase of gadgets nowadays, AI can help keep cybercriminals alert, automate threat detection and react more efficiently than standard software and manual methods [14]. Here are some benefits and uses for cybersecurity use of AI:

1. Detecting New Threats

AI can be used to detect cyber risks and potentially harmful behavior. Because traditional software systems are unable of keeping up with the enormous volume of new viruses generated each week, this is an area where AI can truly help. Artificial intelligence algorithms are programmed to identify malware, perform pattern recognition and identify even the least complicated activities of a virus or ransomware assault before it infects a computer using complex algorithms. AI enables better predictive intelligence with natural language processing, which protects data itself by scrapping articles, news, and cyber danger research. This may provide information on new abnormalities, cyber-attacks, and preventive measures. And besides, cybercriminals are also changing with the times, so what is popular with them continually changes. Cybersecurity solutions based on AI can offer the newest information about global and industry-leading threats to better make key priority choices based not only on what will be used to exploit the systems but on what is most probably to be used to target the systems [14].

2. Battling Bots

Bots nowadays constitute a significant portion of internet traffic and may be problematic. From the taking of stolen credentials to the establishment of fake accounts and data theft, bills may be a serious threat. Automated attacks cannot be addressed with manual reactions alone. AI and machine learning assist to develop a comprehensive knowledge of website traffic and differentiate between acceptable bots (such as search engine crawlers), malicious bots, and people. AI helps us to evaluate a wide range of data and enables cybersecurity teams to adjust their approach to a changing environment. By examining behavioral patterns, companies will obtain answers to queries such as 'what looks like an average person trip' and 'what would be a potentially dangerous unusual experience? 'From here one can uncover the intention of their website visitors, get prepared and keep abreast of malicious bots.

3. Breach Risk Prediction

These AI solutions assist in creating accurate and comprehensive documentation of all connections, users, and apps with varying degrees of system access. Today, given the asset inventory and exposure to risk, Artificial intelligence systems can anticipate how and where

companies most likely are at risk so that they can prepare and assign resources to the most vulnerable regions. Prescriptive insights derived from artificial intelligence-based analysis help to design and enhance policies and procedures to strengthen corporate cyber resilience and security.

4. Better protection of endpoints

The number of remote-working devices is rapidly growing, and AI can help secure them all. Certainly, Antivirus and VPN solutions may assist to prevent cyber-attacks from distanced viruses, but frequently they operate based on signatures. To remain safe against the newest dangers, it is essential to stay informed on signature definitions. If virus definitions become out of date, whether as a result of the failure to upgrade the antivirus program or a lack of knowledge on the part of the software provider, this may be a source of worry. As a result, if a novel kind of malware attack is discovered, signature security may be unable to defend against it [15].

AI-driven endpoint security goes another step via a repetitive training procedure to create a standard of conduct for the endpoint. If anything, unusual happens, AI can alert a professional or even restore the system to a safe condition after a ransomware assault. This offers proactive threat prevention instead of relying on signature changes [15].

F. Authentication and Password Protection AI

Passwords have always been an extremely weak security control. And sometimes they are the sole obstacle between our accounts and cyber thieves. If we are honest with ourselves, the majority of us are very careless with our passwords - frequently that use the same one in several accounts, depending on the very same password for years, keeping a record of them in a draft text on our smartphone, and so on. However, although biometric authentication has been explored as a possible replacement for passwords, it is inconvenient and vulnerable to hacking. For instance, a facial recognition system may be vexing to use if it is unable to identify you due to a new haircut or hat. Attackers may potentially get around it by utilizing profile pictures from social media platforms such as Facebook or Instagram [16]. Developers use AI to improve biometric authentication and remove its flaws to make it a trustworthy system. One example is the facial recognition technology employed by Apple on its iPhone X smartphones. The system, called "Face ID," operates by analyzing the user's face characteristics through integrated infrared sensors and neural motors. Through pattern recognition, AI builds a comprehensive representation of the user's face. Apple says that using this technique, there is a one-in-a-million possibility of tricking the AI and getting your iPhone to open with a different facial recognition system [16]. The AI software design can also operate in various lighting situations and adjust for changes such as a new haircut, facial hair growth, or wearing a hat, among other things.

G. AI detection of phishing

Phishing is a popular cyber-attack technique in which cybercriminals attempt to distribute their malware through a phishing assault. Phishing emails are quite common; one in every 99 emails [16]. Luckily, artificial intelligence (AI) has the potential to play a major role in detecting and discouraging phishing cyber-attacks. AI is capable of detecting and tracking more than 10,000 active phishing sites, as well as reacting and remediating incidents considerably more quickly than humans. Additionally, AI-ML scans phishing threats from all over the globe, and its knowledge of phishing efforts is not geographically limited. AI makes it possible to distinguish rapidly between a phony and a genuine website.

H. Identification of vulnerability areas

This is a new application field in which human resources or developers analyze large quantities of code and automate weaknesses using machine learning before cyber attackers. It is very tough to manage all of these using human resources or conventional technologies. However, AI can deal with this far more easily. AI-ML-based systems are not waiting for the weakness of cybersecurity risks to be exploited [16,17]. Furthermore, such AI-based solutions actively monitor possible weaknesses incorporate information security, integrating various variables including talks of cybercriminals on the dark internet, the hacker's profile, the techniques utilized, etc. Sophisticated systems can evaluate these variables and utilize the knowledge to predict how and when the danger might reach susceptible objectives.

I. Fraud detection

By recognizing deviations and finding trends in the anticipated course of conduct, nefarious activities and transactions may be detected and stopped [17]. Data mining is one of the finest learning systems for selecting large quantities of event records. The use cases are not new, as you undoubtedly noticed since IT professionals do things for years. The main distinction is that in these instances artificial intelligence is utilized to make them safe and resilient. By expanding AI methods, companies can decrease the time it takes to detect and react to risks.

J. Strengthening intelligence on threats

The integration of artificial intelligence in threat intelligent systems helps to improve detection capability and cut down the number of attacks. Two critical components of cybersecurity are the development of security policies and the identification of an institution's network topology [17,18]. Generally, each of these tasks requires a significant amount of attention. However, we can utilize artificial intelligence to speed up these procedures, which it does by monitoring and understanding network traffic, and also by proposing security rules to administrators and users [18]. This not only saves time but also a significant amount of work and resources, which can be used in areas of technical growth and improvement.

K. Negative impacts of Artificial intelligence on cybersecurity

The aforementioned benefits represent only a tiny portion of AI's ability to improve cybersecurity. However, employing AI in this area has significant drawbacks. Building and maintaining an AI system will need much more resources and money. Additionally, since AI systems are educated programmed to capture and monitor large datasets, one will accumulate a large number of different units of malware codes, benign codes, and abnormalities. All these kinds of data are time-consuming and demand expenditures that most companies cannot afford [18]. AI systems may provide erroneous findings or false positives without enormous quantities of data and events. And incorrect data may potentially shoot back from untrustworthy sources. Hackers are very likely to artificial intelligence and then use it to extend their activities. One of the main worries is that cybercriminals may execute cyber operations on an enormous scale utilizing artificial intelligence [18]. The use of artificial intelligence to supplement the lack of human resources and reduce cybersecurity expenses is another significant topic to consider. Likewise, potential adversaries may take advantage of it in a similar manner. The resources and money required to plan, organize, and execute such cyberattacks will drop rapidly, resulting in a reduced return on investment for cyber attackers and a significant danger to national security. Furthermore, advances in artificial intelligence may pave the way for the emergence of new

kinds of cyber threats. Artificial intelligence can exploit a system's weakness quicker and more effectively than a human. Hackers may utilize AI to quickly cover intrusions that the victim may never realize have compromised their system or network.

IV. FUTURE IN THE UNITED STATES

As the digitalization of operations continues to increase, the role of artificial intelligence in solving cybersecurity issues in the United States is changing. Even though these ideas seem like something NASA might employ to transport astronauts to the moon, they may already be found in a wide variety of aspects of our everyday lives. The artificial intelligence that powers virtual assistants such as Siri and Alexa, as well as the machine learning that enables services such as Spotify to provide you with customized suggestions, are all made possible by artificial intelligence [19]. In recent times, cryptocurrency transactions have seen a significant increase in their appeal. These cryptocurrencies are based on blockchain technology, a cutting-edge technological method for securely storing decentralized transaction records. States are at various levels of cybersecurity modernization, and most are implementing multi-year technological maturation programs. For many organizations seeking to improve their security posture, the first approach is to get a better understanding of their existing vulnerabilities, blind spots, and attack surface vulnerabilities [20].

V. ECONOMIC BENEFITS

The economic advantages of artificial intelligence in tackling cybersecurity in the United States have been progressive and apparent over time. The benefit of artificial intelligence may not be predictable but rather may accumulate at an increasing rate over time. By 2030, artificial intelligence's contribution to the economy could become three or more times greater than it is during the past 5 years. AI deployment is expected to follow an S-curve pattern, with a sluggish start owing to the significant expenses and expenditure involved with developing and applying these technologies, followed by an acceleration spurred by the long-term impact of competition and improvements in complementing skills. Throughout the past few years, artificial intelligence (AI) technologies have been more common, changing the way we operate, play, and connect and the rest of the world. Increasingly, artificial intelligence (AI) is being embedded in the culture of corporate operations and is being extensively implemented across a myriad of different business applications [20]. The IT and telecoms industry is perhaps the most mature in regards to AI implementation, with the automobile sector close behind. As per a recent worldwide study that examined over 4,500 policymakers from various fields, 45% of big enterprises and 29% of small and medium-sized enterprises stated that they had embraced AI. While security breaches become more sophisticated, artificial intelligence (AI) will become more important in the cybersecurity business. Consequently, the global cybersecurity industry is predicted to increase in revenue by that year. The use of artificial intelligence (AI) is not without dangers, however, as more than 60% of businesses that have adopted AI consider cybersecurity threats created by AI to be the most significant [20]. Global robot exports grew by about 150% from 2010 and 2015. The growth of robot exports from the United States has been less more significant in terms of building the economy, rising by about 100% from 2010 to 2015. U.S economists are generally optimistic about the potential impact of artificial intelligence on economic development. The existing studies have shown a connection between innovation and economic growth. Several experts think that artificial intelligence (AI) and other types of sophisticated automation, such as robotics and sensors, may be viewed as a general-purpose technology (GPT) that will allow significant follow-on innovation, which would eventually lead to increased productivity.

VI. CONCLUSION

This study evaluated the impact of artificial intelligence on cybersecurity and the mitigation of cybersecurity threats. The findings suggest that technological developments have made it simpler for hackers to enhance their tactics, methods, and instruments to abuse people and organizations. While artificial intelligence is beneficial, it also has the potential to be harmful. Selecting technology wisely will enable businesses to avert a crisis. Artificial intelligence (AI) is quickly becoming a must-have tool for improving the effectiveness of information security organizations. Humans are no longer capable of adequately securing an enterprise-level attack surface, and artificial intelligence provides the much-needed monitoring and threat detection that can be utilized by security experts to reduce the likelihood of a breach and improve their organization's defense capabilities. Furthermore, artificial intelligence may assist in the discovery and prioritization of risks, the direction of incident response, and the identification of malware cyber-attacks before they occur. As a result, even with the possible drawbacks, artificial intelligence will aid to advance cybersecurity and assist businesses in developing a stronger overall security.

REFERENCES

[1] D. Cole, "Artificial intelligence and personal identity", Synthese, vol. 88, no. 3, pp. 399-417, 1991. Available: 10.1007/bf00413555.

[2] M. Stefik, "Artificial intelligence applications for business management", Artificial Intelligence, vol. 28, no. 3, pp. 345-348, 1986. Available: 10.1016/0004-3702(86)90055-x.

[3] G. Babu, N. Anandakuma and D. Muralidhar, "Countermeasures Against DPA Attacks on FPGA Implementation ofAES", Journal of Artificial Intelligence, vol. 5, no. 4, pp. 186-192, 2012.

[4] G. Qin, T. He and J. Chen, "Model of preventing URL attacks based on artificial immunity", Journal of Computer Applications, vol. 32, no. 5, pp. 1400-1403, 2013.

[5] N. Lee, "Artificial Intelligence and Data Mining," Counterterrorism and Cybersecurity, pp. 323–341, 2015.

[6] L. Shellberg, "A Cyber Chase in Cyber Space: How International Law Must Address the Threat of Cyber Attacks or Suffer the Consequences", SSRN Electronic Journal, 2013.

[7] H. R. Nemati, Information security and ethics: concepts, methodologies, tools, and applications. Hershey Pa.: Information Science Reference, 2008.

[8] T. Tagarev, "Intelligence, Crime and Cybersecurity", Information & Security: An International Journal, vol. 31, pp. 05-06, 2014.

[9] R. Winkels, Eleventh International Conference on Artificial Intelligence and Law: proceedings: June 4-8, 2007, Stanford Law School, Stanford, California. Place of publication not identified: ACM, 2007.

[10] D. Hutchison, M. Atiquzzaman, H.-H. Chen, T. Kanade, T.-hoon Kim, J. Kittler, J. M. Kleinberg, C. Lee, F. Mattern, J. C. Mitchell, M. Naor, O. Nierstrasz, C. P. Rangan, J. H. Park, B. Steffen, M. Sudan, D. Terzopoulos, D. Tygar, M. Y. Vardi, G. Weikum, and S.-S. Yeo, Advances in Information Security and Assurance. Berlin, Heidelberg: Springer Berlin Heidelberg.

[11] M. Zajko, "Canada's cyber security and the changing threat landscape", Critical Studies on Security, vol. 3, no. 2, pp. 147-161, 2015.

[12] R. Winkels, Eleventh International Conference on Artificial Intelligence and Law: proceedings: June 4-8, 2007, Stanford Law School, Stanford, California. Place of publication not identified: ACM, 2007.

[13] H. Bidgoli, Handbook of information security. Hoboken, NJ: John Wiley, 2006.

[14] H. Zhuge, "Semantic linking through spaces for cyber-physical-socio intelligence: A methodology", Artificial Intelligence, vol. 175, no. 5-6, pp. 988-1019, 2011.

[15] C. Blackwell and H. Zhu, Cyberpatterns: Unifying Design Patterns with Security and Attack Patterns, 2nd ed. Cham : Springer International Publishing, 2014.

[16] A. R. Dengel, K. Berns, T. M. Breuel, F. Bomarius, and T. R. Roth-Berghofer, KI 2008: advances in artificial intelligence 31st Annual

German Conference on AI, KI 2008, Kaiserslautern, Germany, September 23-26, 2008 ; proceedings. Berlin: Springer, 2008.

[17] D. Feng, D. Lin, and M. Yung, Information Security and Cryptology First SKLOIS Conference, CISC 2005, Beijing, China, December 15-17, 2005, Proceedings. Berlin: Springer, 2005.

[18] J. G. Siegel, The artificial intelligence handbook: business applications in accounting, banking, finance, management, marketing. Mason, OH: Thomson/South-Western, 2003.

[19] H. Zhuge, "Semantic linking through spaces for cyber-physical-socio intelligence: A methodology," Artificial Intelligence, vol. 175, no. 5-6, pp. 988–1019, 2011.

[20] J. R. Vacca, Computer and information security handbook. Waltham, MA, USA: Morgan Kaufmann Publishers, 2013.