IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 9, September 2022

DOI: 10.17148/IJARCCE.2022.11912

The Impact and Limitations of Artificial Intelligence in Cybersecurity: A Literature Review

Meraj Farheen Ansari[1], Bibhu Dash[2], Pawankumar Sharma[3], Nikhitha Yathiraju[4]

School of Computer and Information Sciences, University of the Cumberlands, Williamsburg, KY [1,2,3,4]

Abstract: Artificial intelligence is opening up new avenues for value generation in enterprises, industries, communities, and society as a whole. Technology has been researched to be relevant in many aspects of the world. This factor has made it to be included mainly in different businesses and industries. The applications of AI are endless to discuss. The research below examines the applications of artificial intelligence (AI) in cybersecurity. Cybersecurity has also been a growing concept in the technological industry. Many companies have included information technology in their businesses. This factor has required companies and organizations to demand more security measures. The attempt to protect the available data and information has resulted in the growth of cybersecurity, and AI has been seen to influence cybersecurity heavily on a large scale. This factor has made machine learning to be significantly induced in recent technologies supporting cybersecurity. The research paper performs a literature review and examines the overall impacts of artificial intelligence on cybersecurity.

Keywords: Cybersecurity, AI, Cyber threats, Vulnerability, Data Privacy, AI value creation**.**

I. INTRODUCTION

Artificial intelligence was developed in the 20th century. This development resulted from trying to create a structure that would not require the help of a human brain. The discovery led to more research being conducted on the matter [1]. More people have tried to create intelligent systems and robots. The developments all attempted to include an object that mimics human behavior and acts without significant impact on humans. The research was also included in mathematics, where several mathematicians tried to develop formulas to help with the aspect. Organizations poured much money to ensure these research studies were successful. The entire history of AI showcases the growth that the technology has come. AI platforms assist enterprises in the development, management, and deployment of machine learning and deep learning models at scale. Decreasing software development tasks such as data management and deployment make AI technology more accessible and economical [2]. With the increase in cyber risks, artificial intelligence (AI) is increasingly widely employed to monitor and restrict cybercrime.

II. BACKGROUND

The development of computers and processing units ensured that the growth of AI was to continue incredibly. Looking at the graph above, it is clear that people were finding the use of the technology [3]. Other people have seen the potential of AI since its early years. Algorithms were developed and continued to grow with the generations of computers. Countries were now in competition over who would set the technology first. This aspect led to the factor of the technology extensively growing. As shown above, the end of the 20th century saw a remarkable rise in AI technology [4]. During this period, the true power of AI and its significance had been noticed. The continued research ensured that more applications were being discovered for the technology. Below Fig.1 shows an AI life cycle in detail.

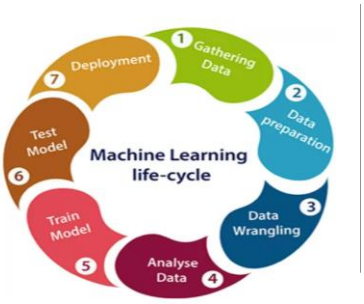

Fig.1 Graphical life-cycle of AI [5]

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 9, September 2022

DOI: 10.17148/IJARCCE.2022.11912

Looking at the situation today, it is clear that artificial intelligence has dramatically grown. Over the years, vast amounts of information have been collected to provide correct analysis and predictions [6]. These attributes have greatly influenced the applications of AI in different industries and organizations. Technology has dramatically benefited initiatives such as banking, marketing, and entertainment. Modeling human actions and reactions has shown fruitful when done by computers. Robots mimicking human behavior have also been developed. Personal assistant applications and devices have also been on the rise based on artificial intelligence technology. Key examples of such devices include Alexa and Siri. Applications such as Google assistant have also proven efficient in helping people. Below fig.2 showcases some of the applications of AI. The figure below showcases the overall impact of AI on different technologies.

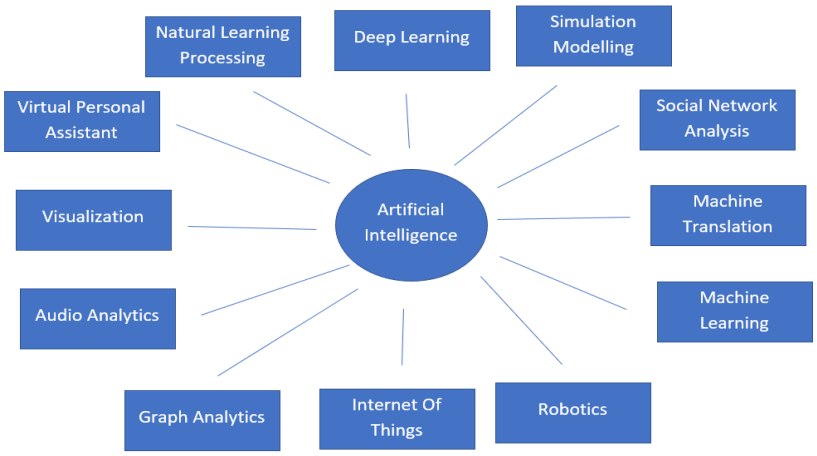

Fig 2. Possible Applications of Artificial Intelligence.

As mentioned above, artificial intelligence has many applications in different sectors and industries. One of the sectors that have continued to benefit from artificial intelligence has been cyber security. This has resulted in specific impacts that are discussed in the study below. The aspect has resulted in different challenges and benefits, which are discussed below. Cyber security is the aspect of protecting computers and other devices from attacks. Most of these attacks are over the Internet [7, 8]. Based on these attacks, organizations always lose many resources. Stevens [9] showcases those cyber-attacks will become the new forms of terrorism attacks on countries. Recent developments in the technological universe have shown that businesses and companies could be destroyed based on a single attack. Trappe and Straub [10] define cyber security as protecting computers from attacks that could be performed through the Internet. Organizations need to include strategies that will ensure the protection of their information. Competitors may attack an organization to gain an advantage against the company. These factors all require the aspects of cyber security. Confidential and private information always requires more measures to ensure people cannot access this information. This factor ensures that people and organizations have been made safer.

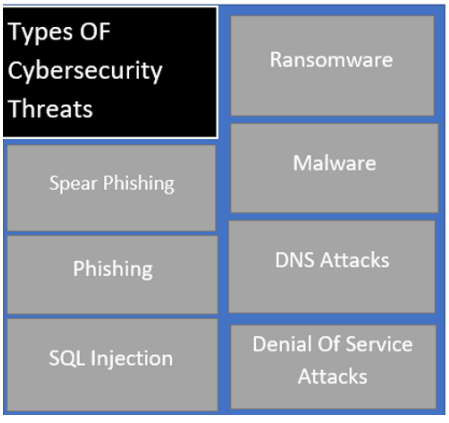

Fig.3: Types of Cybersecurity Threats

Cyber security, in general, has been divided into different sections. The essential parts and units in cybersecurity ensure privacy and security by companies and individuals [11]. These categories include application, network, information, and

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 9, September 2022
DOI: 10.17148/IJARCCE.2022.11912

operational security. Achieving these factors ensures that all the benefits of cybersecurity have been experienced. This factor thus allows for business continuity and development. Fig.3, showcased below, explains the types of threats affecting cybersecurity. Based on the discussions above, it is clear that individuals must protect their information. There are a few ways through which this is achieved. The different methods are being improved daily. Artificial intelligence is one of the applications of AI to ensure more security. Stoianov and Ivanov [12] detailed that significant data advantages result from the recent successes of artificial intelligence in cybersecurity. The threats available are avoided using machine learning technology. This factor has included more security on the company's data and information. Based on this factor, artificial intelligence has enormously impacted cybersecurity. Below are other impacts as a result of artificial intelligence on cyber security.

III. IMPACT OF AI ON CYBERSECURITY

Different impacts result from including AI technology worldwide. The effects resulting from the technology are both positive and negative. Technology has showcased massive development in different industries [13]. All industries have, however, benefited from the impact it has had on cybersecurity. Perols and Murthy [14] showcase that artificial intelligence has influenced businesses and companies. However, the overall implications of artificial intelligence on cybersecurity are both positive and negative. Attacks on companies have proven to become more and more dangerous. Attackers have neem found to increase their knowledge to find weaknesses in cybersecurity technologies. The automation resulting from machine learning algorithms has ensured that attackers cannot use the same ways to attack systems with artificial intelligence. The technology has showcased that machine learning algorithms are better at providing security than humans. Integrating artificial intelligence into cybersecurity ensures that errors are avoided. This factor is among the different benefits of AI on cybersecurity discussed below.

The different artificial intelligence technologies have all obtained different roles in ensuring cyber security [15, 16]. The technologies are continuing research to ensure maximum efficiency in avoiding attacks. As mentioned above, other organizations across the world have information that they need confidential. The technologies have to ensure that nobody can access this information. The future has also been seen to incorporate artificial intelligence on a larger scale. This factor will mean artificial intelligence will be highly developed to ensure maximum security in organizations. Having systems that could protect themselves and detect any attempt is one of the visions of most companies. The aspect of security is a dream that researchers and IT companies are fighting to achieve. The first key attribute of artificial intelligence being significantly embedded in systems is learning from their experiences. This is one of the essential characteristics of AI in general. It has been proven that systems could learn from the different aspects that have made the technology highly relevant in cybersecurity. AI has been regarded as t come and rescue technology in cybersecurity [17]. Learning from experiences is an attribute of artificial intelligence algorithms where systems can learn from factors that have happened before [18]. The algorithms have been used in cyber security technologies and algorithms to ensure that a mistake cannot happen again. Attacks are thus embedded in a system where the artificial intelligence algorithm will detect and learn from the attack.

AI technology is one of the most sophisticated technologies in the modern world. Technology has perfected everything the machine works and wishes to achieve. Man has an insatiable need to create gadgets that can conduct flawless computations and carry out activities without constraints. AI technology is one of man's best works, even beyond most of our understanding. Every organization implementing the technology guarantees they have improved their services and efficiency [19]. AI technology has also contributed to ensuring that it has helped reduce the cybercrimes we experience, as this is one of the challenges in the world today [18]. AI technology has confirmed that these activities are detected and dealt with. AI technology has ensured faster detection of malfunctioning in the system as their monitoring stills are much greater than those of man [19]. This aspect dramatically impacts ensuring that there are no crimes or penetration into the system by unauthorized individuals [17]. And therefore, technology has contributed to having excellent technological security in the world today. Real-time traffic monitoring allows AI technology to identify any activity without the correct measurements or protocols and act on the actions [3]. Upon placing the move, the system must ensure it has worked on the matter [18]. This factor allows the technology to deal with the situation before it's too late. The system will be safe and not corrupt at this stage, helping the organization better its security protocols and protect its data and information.

In data security measures and protocols, AI technology has been one of the best technologies in ensuring that they have improved them. Data is critical to business organizations, so it needs to be secured [20]. With the help of multiple data encryption protocols, the system can facilitate great encryption and guarantee the security of the data involved. The great protocol significantly impacts the technology in the cybersecurity sector of technology [21].

AI technology has also resulted in unemployment in some cyber security posts it replaced. The computer has better efficiency in whatever it does makes it a priority for individuals with skills in the field [10]. The introduction affected the

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 9, September 2022

DOI: 10.17148/IJARCCE.2022.11912

employment of cybersecurity specialists as they had less contribution to an organization since the AI technology has done it all well and efficiently. It also resulted in the organization reducing the system's maintenance and check-up rate. How AI technology secures the security protocols is incredibly efficient compared to where an individual does it. Organizations with this technology are guaranteed to secure their data as the technology in their system ensures greater efficiency as it continues to understand its system and operations.

Mengidis et al. [22] also state that including artificial intelligence learning systems in cybersecurity helps prevent attacks in a system. The learning-based system learns from the attackers' actions ad adjusts to protect the information. This factor makes it impossible for attackers to gain access to the data. Having a system that keeps adjusting and learning is one of the attributes that has made the technology very efficient. AI has been able to avoid cyber-attacks using the approaches discussed below. The different techniques ensure the efficiency of AI in cybersecurity.

A. **Signature Based Techniques**

The subsequent impact of AI on cybersecurity is through signature-based techniques. Understanding signature codes has been a critical attribute of AI technology in cybersecurity. The method involves AI detecting cyberattacks and malware through the available codes [29]. These codes in the malware or attacks are detected using an AI algorithm [21]. Matching the signature from recent attacks or a database thus gives the cyber security team an advantage in stopping the attack. The signatures must be compared quickly to detect the attack. The type of attack being understood thus provides the time and resources required to stop the attack [30]. Before AI technology impacted cybersecurity, these detections would be conducted a lot of time, leading to massive failures and losses.

The database mentioned above, where malware signatures are stored, is called the blacklist. The system detects the attack by comparing the available signatures in the blacklists to the known signature caught in the attack. The signatures are sometimes referred to as the patterns present in the attack, and this could be said to be another form of machine-based learning [31]. Although the method has proven very efficient over the years, it has been seen to be useless in the case of a new attack. The technique fails since the database has no record of the attack. The technology, however, has been seen to be very efficient and stopped many attacks over the years. The above technique has been seen to be evaded using specific techniques. A key example is how attackers have understood the different ways of avoiding attacks by altering their patterns. Hackers understand the aspects susceptible to AI and change these values completely [10]. Changing their patterns ensures they can access the data and information before they are detected. As mentioned above, the technique has shown huge impacts on cybersecurity. Research shows that most attacks have been stopped and avoided using the method. Below fig.4 shows applications of AI in cybersecurity.

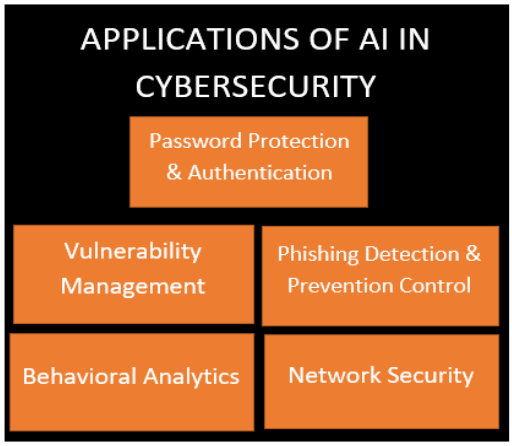

Fig. 4 Application of AI in Cybersecurity

B. **Machine Learning Approach**

As mentioned above, machine-based learning has dramatically influenced cybersecurity. Mengidis et al. [22] discovered that humans always make mistakes when analyzing data or information. A considerable advantage of AI technology is that they are system. The system has the advantage of avoiding errors or missing details of attacks. Using AI to analyze logs and network packets has ensured that attacks are quickly detected [11]. The AI technology detects systems, analyses the available records, and detects logs included in the system. This factor ensures that system administrators can change the information accessed to avoid further loss. This factor has led to the analogy that AI closely replaces human analysts

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 9, September 2022
DOI: 10.17148/IJARCCE.2022.11912

The main advantage of AI in cybersecurity is the attribute of being able to analyze enormous data. Extensive data is always tiring to investigate, being a human analyst. This attribute was significantly changed after the information of AI technology. AI can analyze large pieces of information and not make an error. Human analysts are also efficient in detection since they can operate AI technology [23]. The efforts between the systems and analysts ensure that all the data available has been analyzed and compared. This factor has proven efficient in stopping attacks. Before preventing attacks and protecting the available data, malware identification is always the first step. Classification and clustering are thus great attributes of machine learning systems. They compare the available information and how it should be in the logs. This factor provides detection if there are errors in the system. The regular records are compared to the current ones to identify the infected logs. After an attack has been detected, necessary steps are taken to ensure the attack has been stopped. Clustering involves grouping the available records or information from the system and detecting anomalies. Both of these techniques used in machine learning have proven effective since it is impossible for humans.

C. Network Intrusion Detection

Network attacks are one of cyber security's most used forms of aggression. The raids are conducted through the networks that the organizations or companies use. It is always important to detect attacks through networks. This factor gives the system the advantage of stopping the attack from the web. Through AI, this attribute has been made very easy. Network firewalls being embedded with AI technology have also been found to be very efficient. Accessing the network has been made very hard without the proper authorization. Stopping attacks from the web is the first step in protecting the information available. This approach has thus been very efficient in preventing future attacks. The above guidelines are also embedded in the networks to ensure maximum security. The main key attribute and advantage of network intrusion detection systems are that they have five elements that support the full security of such networks. The first key element is how AI systems acquire large sums of information from the network. This factor can be achieved through the AI system's ability to analyze large amounts of data [23]. All the factors help ensure the security of the network has been completed. Stopping an attack from the network gives the organization a higher chance of protecting the information. All the way a network may be compromised is avoided using the AI techniques available.

The above discussions showcase that AI has influenced cyber security on a large scale. The way mentioned above is from an impact of artificial intelligence on cyber security at a network level. The systems are taught the different forms of avoiding any possible attack to ensure the network is uncompromised [24]. This factor of artificial intelligence learning also played a massive part in ensuring network security [25]. This factor and many others have increased the benefits of artificial intelligence to AI impacting cybersecurity.

D. Vulnerability Management

Vulnerability management is the attribute of artificial intelligence machines managing the possible vulnerabilities that organizations may have in their systems. Research showcases that in 2019, around 20,362 vulnerabilities were reported. There was an 18% increase compared to 2018 [24]. This factor showcases that organizations are continuing to experience threats daily. The management of these vulnerabilities is becoming exhausting for the personnel present. This factor required the inclusion of AI systems to manage recorded exposures. This factor has made it hard for hackers to gain access to systems. Vulnerability management is thus one of the benefits resulting from the impact of AI on cyber security. According to IBM research on AI in cybersecurity market dynamics that considers all disclosed vulnerabilities, spending on cyberspace globally is increasing despite the COVID-19 pandemic (see Table 1) [26].

Table I Artificial Intelligence Valuation in Cybersecurity market prediction

Market	Artificial Intelligence in Cybersecurity Market
Market size 2018	USD 9.8 Billion
Market size 2021	USD 14.9 Billion
Market size 2025	USD 36.6 Billion
Market size 2030	USD 133.8 Billion

Most hackers used to exploit the slow reaction of the available vulnerability management. Artificial intelligent systems managing the vulnerability database ensure that attack attempts are re4ported in real-time, thus ensuring safer systems [27]. Another critical aspect is how machine learning algorithms detect user account anomalies [23]. This factor ensures that the systems are protected if a user in the system proves to be a threat. The aspect of vulnerability management by AI systems has provided servers are safer, and information stored in these machines is safer.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 9, September 2022

DOI: 10.17148/IJARCCE.2022.11912

E. **Data Centers Security**

Cyber security involves the protection of data from any attacks. The use of AI, as mentioned above, has ensured that these ways are more efficient and secure. Data centers are one of the most critical aspects that require cybersecurity [28]. The main advantage of AI has been found to ensure that processes included in these centers have been automated. Power consumption, bandwidth usage, and temperatures are vital aspects significantly controlled in data centers. Since humans sometimes make errors, using AI to manage such canters ensures maximum efficiency.

Another critical factor in data centers is that the cost of hardware maintenance is always observed when using AI systems to manage the entire center. The data centers always require protection from environmental factors since they hold essential information for the customers or organizations [28]. Based on this factor, it is always necessary for AI to ensure that machines are safe. Over the years, more companies and organizations have included AI systems in their data centers for more security and efficiency [23]. This factor showcases the impact of AI on cyber security. Although Artificial intelligence is beneficial in cybersecurity, there are other limitations resulting from AI in cyber security.

IV. LIMITATION OF AI IN CYBERSECURITY

From Charles Darwin's theory about Man's devolution, we can learn that man has always tried to ensure that they have perfected how nature treats them. The ability to change what nature offers to favor their activities and survival has always been the objective of humanity in ensuring that they have a better environment to stay in. Getting to the industrial stage of the human revolution, we can see that they have contributed to ensuring that they extensively utilize the knowledge of machinery that will help them in their day-to-day activities [32]. The idea of physics knowledge and how to use and advance machinery helped humanity entirely replace the animals allowing them in their activities. With the help of the machinery, there were able to ensure that they have improved their product and efficiency in their work. A man comes to learn that machinery is better than humans. Therefore, the goal was to entirely replan making with a machine to have more excellent production and avoid any inconvenience brought by human actions. And by developing the machinery, they could get to the computer technology we have today.

Computer technology has become one of the most widely used technologies today, resulting in many essential elements in life being supported by technology. Therefore, some standards must be implemented in the technology to ensure that the efficiency and the security of the services offered are of concern [32]. The technology is entitled to financial institutions and other sectors that hold essential information about our lives. Also, the technology contains information about our organization, which other organizations can use to create a competitive advantage. Considering how vital information is to the current world, computer technicians and developers must ensure that they have included all the security protocols to ensure the security of the data involved in the system. Computer scientists had to develop a way of ensuring data security; therefore, they had to encrypt their data before sending it [33]. The encrypting protocol will ensure that if the data falls to the wrong people, they will still be unable to use it. One must have the decryption code to decode the data involved, making it difficult to use [34]. Data encryption generation continued, so people understood the principles used in the process. The below fig.5 explains how data encryption and business process barriers are the huddles to use AI in all organizational challenges, including cyber threats to generate value.

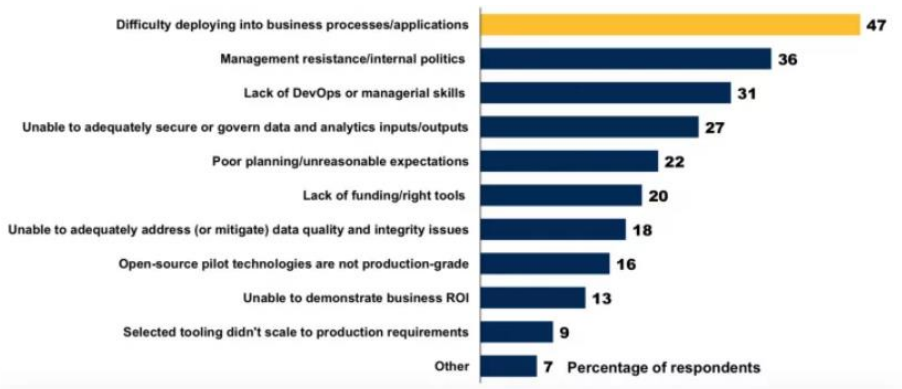

Fig. 5 Barriers to implementing AI against cyber threats on delivering business value [5]

People learning and understanding the process resulted in another challenge catered for [35]. People learning the protocols used by the encryption systems and programs made it easy to reverse engineer the process. The ability to obtain the data being transmitted by having the protocol of identifying the encryption key significantly puts the entire process of securing

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 9, September 2022
DOI: 10.17148/IJARCCE.2022.11912

data in a hot soup [35]. Computer scientists had to develop more complicated protocols and methods for encrypting data and ensuring it operates correctly. The ultimate goal of securing the data is achieved. With the idea that machines are better than humans in everything they have been programmed to do, it is logical to say that they will be best at ensuring their security [36]. This results in introducing Artificial Intelligence technology that ensures the machine's security is excellent. There is no instance where the information can get unintended [22]. The AI system works to ensure that they have assigned all the protocols they are programmed to follow to guarantee the security of the data involved.

The AI feeds into different protocols of data encryption and uses other methods. It can generate a more complex way to solve or encrypt the data. With these different data encryption protocols, the system can ensure that it is difficult enough to ensure that nobody can decode the data involved in the transaction. AI has served networking companies and other organizations efficiently as data security is more advanced and guaranteed. However, considering that man created the technology, they have faults even though they were designed to reprogram and develop themselves in case of any responsibility. The fact that man created the program gives him a chance to study it and reverse engineer the process involved, thereby putting the security problem at risk of getting into the wrong hands [35]. As an individual, has indeed created the AI technology involved in data security.

One of the most significant limitations of AI is that it is just a computer code programmed to ensure that they have followed the protocols and developed themselves in case of anything. This instance may sound okay as they can develop themselves in case of anything. However, the system is entirely programmed; therefore, anybody can take control of them, and they can be manipulated and used as a weapon. Few lines of code are required to be edited, and then the long work hours may be turned into a weapon that will be used against itself. Therefore, with the appropriate ability and knowledge, AI technology can be used as a weapon that will be used to destroy what it was made to protect. This factor is one of AI's most significant limitations to cyber security [26]. Developers and computer scientists should consider this as they understand the capability of AI technology.

AI systems can also be trained to detect cyber threats and malicious malware, thus making them more effective in cyber security. The increasing number of cyber security attacks has led to AI adoption in cybersecurity. The entire process is to ensure that there is efficiency and accuracy. However, AI is limited and cannot replace humans since it is only instructed to perform a specific task. At times, it cannot detect virtually indistinguishable threats and hence gets into trouble since it looks like the actual message. AI may also find it difficult to detect threats due to evolving cyber threats. Viruses and malware improve at any given time, and so should the AI system need an improvement for efficiency. Also, the practice of cybersecurity is many compared to cybercriminals, who tend to acquire more information on hacking. Therefore, cybercriminals can create a better threat that artificial intelligence would not detect easily [9]. Although AI saves time for the security team, it also requires human experts for creativity, thus making work easier for them. The limitation calls for the developers to ensure they have equipped the technology with multiple capabilities to handle any crime resulting from their restraints.

On the other hand, we can identify that AI technology is not entirely being used to protect data and ensure data security. We can also have the AI technology that is developed to have it generate and create computer viruses. The complexity included in the technology makes it difficult for an individual to compete with the machine, leading to the bridging of data. With as many powers generated in the AI-generated codes, which are used to develop a computer virus, it makes it entirely possible for it to be super easy to corrupt a database and manipulate data in it. This is another limitation that is essentially not to AI technology as a watchdog of cybercrime but as a participant in cybercrime. This limitation showcases another massive impact of AI in cybersecurity. The complexity of the technology is a limitation of AI technology as not everyone in society knows technology. There is also the fact that it is not a simple task to understand the different models involved in the technology. Technology being so challenging to use and implement to the total capacity can give criminals a chance to get the system as we cannot operate the approach to the maximum capability. The technology requires much information about its operation, which many individuals do not have. Therefore, organizations are still at risk as they cannot get the system to operate to its best.

Also, because we have complexity in the system, we understand that the technology will cost a lot [34]. Therefore, the cost of implementing the technology is much more expensive. Therefore, not all organizations in the world will be able to access the technology and ensure the security of the data. Therefore, the cost of the technology is also a limitation to the implementation [38, 39]. Even though the organization's information is essential to any organization, the cost of implementing AI technology is much higher, limiting the number of individuals who will use the technology for the safety of their data and information. The system's cost results in few members and organizations using the technology, making it hard to appreciate the technology's ability.

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 9, September 2022
DOI: 10.17148/IJARCCE.2022.11912

V. CONCLUSION

There are many impacts resulting from AI technology in different industries. These impacts include both the benefits and limitations of this technology. Looking at the discussion above, it is clear that AI has proven more beneficial to cyber security than its limitations. Artificial intelligence is still growing, and more research is being done on the technology. This factor showcases huge advancements underway in the technology—the approaches used to ensure cybersecurity support. The procedures showcase the technological impact of the technology on cybersecurity measures. The above research also focuses on some limitations of AI impacting cyber security. The limits showcase how people have managed to use AI for their gains. This factor has led to constraints in cybersecurity. Researchers and innovators should work to ensure that the limitations discussed above have been avoided. Systems should be made more secure through the use of AI systems. Increasing cybersecurity measures will ensure that attackers cannot exploit organizations. This factor will ensure more growth and development of organizations and companies. Based on the research above, the conclusion is that artificial intelligence has dramatically impacted cyber security.

ACKNOWLEDGMENT

We are thankful to our advisor Dr. Azad Ali from the University of the Cumberlands, for all his support and guidance in writing this review paper on cyber security. Also, thanks to him for reviewing it before our submission.

REFERENCES

[1] Blake, C. (2020). Artificial Intelligence and Advances. Advances In Machine Learning & Artificial Intelligence, 1(1). https://doi.org/10.33140/amlai.01.01.03
[2] Dash, B., & Sharma, P. (2022). Role of artificial intelligence in smart cities for information gathering and dissemination (a review). Academic Journal of Research and Scientific Publishing, 4(39), 58–75. https://doi.org/10.52132/ajrsp.e.2022.39.4
[3] Chen, Z., & Liu, B. (2016). Lifelong Machine Learning. Synthesis Lectures On Artificial Intelligence And Machine Learning, 10(3), 1-145. https://doi.org/10.2200/s00737ed1v01y201610aim033
[4] Vorobeychik, Y., & Kantarcioglu, M. (2018). Adversarial Machine Learning. Synthesis Lectures On Artificial Intelligence And Machine Learning, 12(3), 1-169. https://doi.org/10.2200/s00861ed1v01y201806aim039
[5] Dilmegani, C. (2022, September 12). AI platforms: Guide to ML Life Cycle Support Tools. AIMultiple. Retrieved September 26, 2022, from https://research.aimultiple.com/ai-platform/
[6] Chen, Z., & Liu, B. (2018). Lifelong Machine Learning, Second Edition. Synthesis Lectures On Artificial Intelligence And Machine Learning, 12(3), 1-207. https://doi.org/10.2200/s00832ed1v01y201802aim037
[7] Heldah, C. (2021). How Artificial Intelligence (AI) is Transforming Cybersecurity. Plug and Play Tech Center. Retrieved 1 September 2021, from https://www.plugandplaytechcenter.com/resources/how-artificial-intelligence-transforming-cybersecurity/.
[8] Ansari, M. F., Sharma, P. K., & Dash, B. (2022). Prevention of phishing attacks using AI-based Cybersecurity Awareness Training. International Journal of Smart Sensor and Adhoc Network., 61–72. https://doi.org/10.47893/ijssan.2022.1221
[9] Stevens, T. (2020). Knowledge in the grey zone: AI and cybersecurity. Digital War, 1(1-3), 164-170. https://doi.org/10.1057/s42984-020-00007-w
[10] Trappe, W., & Straub, J. (2018). Cybersecurity: A New Open Access Journal. Cybersecurity, 1(1), 1. https://doi.org/10.3390/cybersecurity1010001

[11] Catherine. (2021). Artificial Intelligence in Cyber Security - Impacts & Advancements. Intellipaat Blog. Retrieved 1 September 2021, from https://intellipaat.com/blog/artificial-intelligence-in-cyber-security/.
[12] Stoianov, N., & Ivanov, A. (2020). Public Key Generation Principles Impact Cybersecurity. Information & Security: An International Journal, 47(2), 249-260. https://doi.org/10.11610/isij.4717
[13] Vlassis, N. (2007). A Concise Introduction to Multiagent Systems and Distributed Artificial Intelligence. Synthesis Lectures On Artificial Intelligence And Machine Learning, 1(1), 1-71. https://doi.org/10.2200/s00091ed1v01y200705aim002

[14] Perols, R., & Murthy, U. (2018). The Impact of Cybersecurity Risk Management Examinations and Cybersecurity Incidents on Investor Perceptions. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3112872
[15] Hamilton, W. (2020). Graph Representation Learning. Synthesis Lectures On Artificial Intelligence And Machine Learning, 14(3), 1-159. https://doi.org/10.2200/s01045ed1v01y202009aim046

DOI: 10.17148/IJARCCE.2022.11912

[16] Sharma, P., Dash, B., & Ansari, M. F. (2022). Anti-phishing techniques – a review of Cyber Defense Mechanisms. IJARCCE, 11(7). https://doi.org/10.17148/ijarcce.2022.11728

[17] Szepesvári, C. (2015). Algorithms for Reinforcement Learning. Synthesis Lectures On Artificial Intelligence And Machine Learning, 4(1), 1-103. https://doi.org/10.2200/s00268ed1v01y201005aim009

[18] Hassanien, A., Haqiq, A., Tonellato, P., Bellatreche, L., Goundar, S., & Azar, A. et al. Proceedings of the International Conference on Artificial Intelligence and Computer Vision (AICV2021).

[19] Puthal, D., & Mohanty, S. (2021). Cybersecurity Issues in AI. IEEE Consumer Electronics Magazine, 10(4), 33-35. https://doi.org/10.1109/mce.2021.3066828

[20] Keen, E. (2021). The benefits and limitations of AI in cybersecurity - Help Net Security. Help Net Security. Retrieved 1 September 2021, from https://www.helpnetsecurity.com/2018/12/20/ai-cybersecurity-benefits-limitations/.

[21] Raedt, L., Kersting, K., Natarajan, S., & Poole, D. (2016). Statistical Relational Artificial Intelligence: Logic, Probability, and Computation. Synthesis Lectures On Artificial Intelligence And Machine Learning, 10(2), 1-189. https://doi.org/10.2200/s00692ed1v01y201601aim032

[22] Mengidis, N., Tsikrika, T., Vrochidis, S., & Kompatsiaris, I. (2019). Blockchain and AI for the Next Generation Energy Grids: Cybersecurity Challenges and Opportunities. Information & Security: An International Journal, 43(1), 21-33. https://doi.org/10.11610/isij.4302

[23] Daily, J., & Gardiner, B. (2018). Cybersecurity Considerations for Heavy Vehicle Event Data Recorders. SAE International Journal Of Transportation Cybersecurity And Privacy, 1(2), 113-143. https://doi.org/10.4271/11-01-02-0006

[24] Vostoupal, J. (2021). The Cybersecurity Qualifications as the Prerequisite for the Cybersecurity Certification of Entities. Jusletter-IT, (27-Mai-2021). https://doi.org/10.38023/2029e2f5-bd30-4757-aef5-01b27ae61962

[25] Vermesan, O., & Bacquest, J. Next Generation Internet of Things.

[26] Johnson, R. (2022, July 18). Artificial Intelligence in cybersecurity market size to reach USD 133.8 billion by 2030 driven by growing number of cyber attacks. Yahoo! Finance. Retrieved September 26, 2022, from https://finance.yahoo.com/news/artificial-intelligence-cybersecurity-market-size-070000706.html

[27] Rada, R. (2014). Artificial intelligence. Artificial Intelligence, 28(1), 119-121. https://doi.org/10.1016/0004-3702(86)90034-2

[28] Kravets, V. (2019). Comparative Analysis of the Cybersecurity Indices and Their Applications. Theoretical And Applied Cybersecurity, 1(1). https://doi.org/10.20535/tacs.2664-29132019.1.169090

[29] Chung, S. (2021). AI-Based CYBERSECURITY: Benefits and Limitations. 1-2. https://doi.org/10.22471/ai.2021.6.1.18

[30] Computer.org. (2021). The Impact of AI on Cybersecurity | IEEE Computer Society. Computer.org. Retrieved 1 September 2021, from https://www.computer.org/publications/tech-news/trends/the-impact-of-ai-on-cybersecurity/.

[31] Creese, S., Dutton, W., Esteve-Gonzalez, P., & Shillair, R. (2020). Cybersecurity Capacity Building: Cross-National Benefits and International Divides. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3658350

[32] Raghavan, V., Venkat N. Gudivada, & Venu Govindaraju. (2016). Cognitive Computing: Theory and Applications. Elsevier Science.

[33] Here, P., Look, E., & Data, B. (2021). Impact of AI-Driven Cybersecurity in Fighting Data-Driven Cyberattacks. SmartData Collective. Retrieved 1 September 2021, from https://www.smartdatacollective.com/how-ai-driven-cybersecurity-drastically-impacts-our-lives/.

[34] upGrad. (2021). Artificial Intelligence in Cyber Security: Role, Impact, Applications & List of Companies | upGrad blog. upGrad blog. Retrieved 1 September 2021, from https://www.upgrad.com/blog/artificial-intelligence-in-cyber-security/.

[35] John, N. (2021). The Impact of AI and Machine Learning on CyberSecurity. Globaltechcouncil.org. Retrieved 1 September 2021, from https://www.globaltechcouncil.org/cyber-security/the-impact-of-ai-and-machine-learning-on-cybersecurity/.

[36] Dubber, M., Pasquale, F., & Das, S. (2020). The Oxford Handbook of Ethics of AI. Oxford University Press, Incorporated.

[37] Thomas, B. (2021). Artificial Intelligence in Cyber Security: Role, Impact, Applications & List of Companies | upGrad blog. upGrad blog. Retrieved 1 September 2021, from https://www.upgrad.com/blog/artificial-intelligence-in-cyber-security/.

[38] Xia, L. (2019). Learning and Decision-Making from Rank Data. Synthesis Lectures On Artificial Intelligence And Machine Learning, 13(1), 1-159. https://doi.org/10.2200/s00876ed1v01y201810aim040

[39] Dash, B., Ansari, M. F., Sharma, P., & Ali, A. (2022). Threats and Opportunities with AI-based Cyber Security Intrusion Detection: A Review. International Journal of Software Engineering & Applications, 13(5), 13–21. https://doi.org/10.5121/ijsea.2022.13502

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 9, September 2022

DOI: 10.17148/IJARCCE.2022.11912

BIOGRAPHY

Bibbu Dash is a data Architect in a Fortune 100 financial organization in Madison, WI. He completed his Ph.D. in Information Technology from the University of the Cumberlands, Kentucky. Bibhu has also completed his Master of Engineering in Electronics and Communication Engg. and MBA from Illinois State University, Normal, IL. Bibhu's research interests include AI, Cloud Computing, Big Data, and Blockchain technologies.

Meraj Farheen Ansari completed her Ph.D. (IT) from the Graduate School of Information Technology, University of the Cumberlands. She also completed her MBA with a Specialization in Management Information Systems from Concordia University, Milwaukee, WI, USA. Her research interests include cybersecurity awareness, eliminating Cyber Threats, & ML. Her current research involves making organizational employees aware of cyber security threats using AI awareness programs. Currently, she is a Cyber Security Analyst at Northern Trust Bank, Chicago, IL.

Pawankumar Sharma is a Senior Product Manager for Walmart in San Bruno, California. He is currently on his Ph.D. in Information Technology at the University of the Cumberlands, Kentucky. Pawankumar completed his Master of Science in Management Information Systems from the University of Nebraska at Omaha in 2015. He also holds another Master of Science in Information Systems Security from the University of the Cumber lands, Kentucky, and graduated in 2020. His research interests are cyber security, Artificial Intelligence, Cloud Computing, Neural Networks, Information Systems, Big Data Analytics, and Intrusion Detection and Prevention.

Nikhitha Yathiraju completed her Ph.D. (IT) from the Graduate School of Information Technology, University of the Cumberlands. She also completed her Master's in computer sciences from Silicon Valley university, USA in 2016. She works as a Lead QA automation engineer and a teaching assistant at Silicon Valley university. Her research interests include cybersecurity awareness, Cloud technologies, IoT, AI & ML.

