International Journal of Scientific Research in Science, Engineering and Technology

Print ISSN - 2395-1990
Online ISSN : 2394-4099

OPEN ACCESS

Available Online at : www.ijsrset.com
doi : https://doi.org/10.32628/IJSRSET241118

The Future of Artificial Intelligence in Cyber Security -A Review

Miss. Tanmayi Ajay Dubey*[1], Mr. Chinmay R. Sambhe[2], Miss. Aboli Sanjay Gujar[3]

*[1] UG Student, Department of CSE, Jawaharlal Darda Institute of Engineering & Technology, Yavatmal, Maharashtra, India

[2] UG Student, Department of Mechatronics Engineering, Technical University of Applied Science, Wurzburg-Schweinfurt, Germany

[3] UG Student, Department of CSE, Jawaharlal Darda Institute of Engineering & Technology, Yavatmal, Maharashtra, India

ARTICLEINFO

Article History :

Accepted: 02 Jan 2024
Published: 22 Jan 2024

Publication Issue :

Volume 11, Issue 1
January-February-2024

Page Number :

111-117

ABSTRACT

Cyber Security has emerged as a key worry in the digital age & the last ten years, the field of Cyber Security has expanded significantly. whereas the importance of Artificial Intelligence (AI) is also increasing day by day, So the use of AI to handle Cyber Security concerns and dangers will be covered in this Paper.

Keywords: Artificial Intelligence, Cyber Security, AI Benefits, Drawbacks of AI, Future of AI.

I. INTRODUCTION

Cybersecurity and Artificial Intelligence are two revolutionary technologies in the current era. AI is the simulation of human intelligence processes by machines, especially computer systems whereas Cyber Security refers to the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, damage, or unauthorized access According to the definition provided by Myriam Dunn Cavelty.

The integration of AI into cyber security systems can help to reduce the ever-increasing and evolving cyber security threats that global enterprises face. Cyber security is just a moral practice that aims to make our computers safer and protected from such hackers. AI in cyber security offers insights that support companies in comprehending issues. These revelations can speed up reaction times and help companies stick to security best practices [1]. As we know "cybersecurity refers to the set of activities and measures, technical and non-technical, intended to protect the 'real geography' of cyberspace but also devices, software, and the information they contain communicated, from all possible threats". Cybersecurity has become one of the most important issues in cyberspace so, Traditional cybersecurity methods work based on response to an attack and rely on the static control of security devices.

For instance, in case of network intrusion attacks, security systems monitor nodes according to a pre-defined set of rules. These methods wait to be notified that an attack has occurred. However, with the increasing number of cyberattacks, the traditional approach is no longer useful. One example of the inadequacy of traditional cybersecurity methods is the hack of Equifax in 2017, causing a significant risk to sensitive information by exposing data for as many as 143 million customers [2].

During 2014-2015, computer security experts had to respond to a great number of cybercrimes involving Blue Cross / Blue Shield, Anthem, Target, and Home Depot, among others. Attackers hack government and private computer systems by taking advantage of loopholes and malfunctions in security systems or exploiting the vulnerabilities within IT infrastructures. Therefore, the traditional passive defense approaches are insufficient nowadays [3]. The only way to protect data in the unstable world of today—where cyberattacks occur frequently and are always changing—is to employ aggressive cyber methods. As a result, the new strategy must stop attacks before they start rather than wait to learn about them after they've already happened.

Fig.1 How AI is Changing the Cyber Security Landscape [4].

II. ROLE OF Artificial Intelligence:

Artificial intelligence is the process of making a computer, software, or robot under computer control think intelligently and similarly to how intelligent humans think. The method of creating artificial intelligence (AI) involves first understanding how the human brain functions and how people learn, make decisions and collaborate to solve problems. The results from this study are then used to create intelligent software and systems. Most people define intelligence as having the capacity to learn new things and use that information to think to solve challenging situations. In several fields, intelligent machines will soon surpass human skills. The study and creation of intelligent hardware and software that can reason, learn, acquire information, communicate, manipulate, and see objects is referred to as artificial intelligence.

John McCarthy coined the term in 1956 as the branch of computer science concerned with making computers behave like humans. It is the study of computation that makes it possible to perceive reason and act. Artificial Intelligence is different from psychology because it emphasizes computation and is different from computer science because of its emphasis on perception, reasoning, and action. It makes machines smarter and more useful [5].

III. EMERGENCE OF ARTIFICIAL INTELLIGENCE IN CYBERSECURITY

Machine learning and Artificial Intelligence (AI) are being connected more comprehensively crosswise over enterprises and applications than at any other time in recent memory as registering power, information accumulation, and capacity abilities increment. This tremendous trove of information is a significant grub for AI, which can process and examine everything caught to see new patterns and subtle elements. For cyber security, this implies new endeavors and shortcomings can rapidly be recognized and investigated to help moderate further assaults. It can take a portion of the weight of human security "partners." They are cautioned when an activity is required, yet in addition can invest their energy in taking a shot at more inventive, productive undertakings [6]. A helpful relationship is to consider the best security proficient in your association. If you

utilize this star representative to prepare your machine learning and Artificial Intelligence programs, the AI will be as shrewd as your star worker. Presently, if you set aside the opportunity to prepare your machine learning and Artificial Intelligence programs with your 10 best representatives, the result will be an answer that is as savvy as your 10 best workers set up together. Furthermore, AI never takes a wiped-out day [7].

IV. WHERE CAN ARTIFICIAL INTELLIGENCE BE USED IN CYBERSECURITY?

The use of artificial intelligence (AI) is already being used to or is being actively explored for, some of the following areas in cybersecurity solutions: To identify and prevent undesirable spam and fraudulent emails, Gmail makes use of artificial intelligence (AI). Gmail's artificial intelligence was taught by the millions of current Gmail users - every time users click an email message or not spam, they are assisting in training the AI to detect spam in the future [8]. As a result, artificial intelligence has progressed to the point where it can identify even the most subtle spam emails that attempt to pass unnoticed as “frequent” emails. • Fraud detection: An artificial intelligence-based fraud detection system that employs algorithms based on expected consumer habits to identify fraudulent transactions through MasterCard deployed Decision Intelligence [9]. It examines the customer's normal purchasing patterns, the seller, the location of the transaction, and many other complex algorithms to determine if a purchase is unusual. • Botnet Detection: A very complicated area, botnet detection is usually based on pattern recognition and timing analysis of proxy servers. Since botnets are usually managed by a master script of instructions, a wide-scale botnet assault will usually include a large number of "users" all making identical queries on a site in a single attack. This may include unsuccessful login attempts (a botnet brute force password attack), network vulnerability scans, and other breaches. It is very difficult to explain the incredibly complicated function that artificial intelligence plays in botnet identification in just a few words, but here is a fantastic study article on the subject that does a great job [10]. These are just a handful of the areas in which artificial intelligence has been used for cybersecurity. There are currently a large number of research articles that provide compelling data in support of artificial intelligence's effectiveness in the field of cybersecurity. According to the majority of study studies, the success rate for identifying cyber assaults is between 85 and 99 percent. One artificial intelligence development firm, Dark Trace, claims to have a 99 percent success rate and already has thousands of clients across the world [11].

V. BENEFITS OF ARTIFICIAL INTELLIGENCE IN CYBERSECURITY

We may use AI for cyber defense in several ways. In the future, we will have the cleverest systems than such processes. Indeed, attackers can use Artificial Intelligence for attacks as well. The recent developments in knowledge comprehension outline and coping up with what is advanced in machine learning would enhance the digital security capability of the systems that can be used. The description of the various approaches dealt with in this paper appears in the diagram below.

AI TECHNIQUES	ADVANTAGES
Expert Systems	• Decision Support. • Intrusion Detection. • Knowledge Base. • Inference.
Neutral Nets	• Insltrusion detection and prevention system. • High speed of operation. • DoS detection. • Forensive Investigation.
Intelligent Agents	• Proactive. • Agent Communication

	Language. • Reactive. • Mobility. • Protection Against DdoS.

Table1: Advantages of AI Techniques

This research was applied using the methods of literature and previous reviews of empirical and descriptive research. "The findings revealed the possibility of utilising techniques of machine learning, deep learning, and data mining for cybersecurity purposes in three major areas: identification of intrusions, examination of malware, and detection of spam. Every day, malware technologies are developed and today, data mining algorithms can detect and classify malware". To detect and classify malware, however, it is critical to develop new data mining algorithms to be fast and scalable [12].

VI. THE DRAWBACKS OF ARTIFICIAL INTELLIGENCE IN CYBERSECURITY

The benefits mentioned above represent just a tiny portion of AI's potential for enhancing cybersecurity. However, like with everything, there are certain drawbacks to using artificial intelligence in this area. Organizations would need much more resources and financial expenditures to develop and sustain an artificial intelligence system [13]. Furthermore, since AI systems are taught using data sets, you will need to collect a large number of different sets of malware codes, non-malicious codes, and anomalies to train your system. Acquisition of all of these data sets is time-consuming and necessitates expenditures that are beyond the financial means of most businesses. AI systems may provide inaccurate findings and/or false positives if they do not have access to large amounts of data and events. Furthermore, obtaining incorrect information from untrustworthy sources may have negative consequences [14]. The fact that hackers may utilize artificial intelligence to evaluate their software and conduct increasingly sophisticated assaults is another significant drawback, which takes us to the following issue.

FUTURE ASPECTS AND SCOPE

Researchers predict that by 2020, artificial intelligence technologies will be implemented in almost all new software products and services, which will inevitably bring a sea change the way we work, live and do business. Though AI is in its infancy, it has shown to the world its infinite potential in performing task efficiently and accurately in an array of industries from manufacturing, retail, education to healthcare and cyber security. As always, a coin has two faces. AI is no exception. People have shown their worries for destructive use of AI. A report from The Guardian warns "As AI capabilities become more powerful and widespread, we expect the growing use of AI systems to lead to the expansion of existing threats, the introduction of new threats and a change to the typical character of threats,". Fortunately, the discussion on AI still ends up with bright face of AI. No doubt, if AI is implemented and trained with proper care, it can improve cyber security in many ways. It can protect against the cyber-attacks in real time with lesser resources. As cyber threats are constantly evolving, data is bursting new patterns that are hard to capture and analyze for human analyst can be crunched down by a machine learning technique in seconds. Equipped with power of deep analysis provided by Machine learning, Human analysts can focus on interpretin FUTURE ASPECTS AND SCOPE Researchers predict that by 2020, artificial intelligence technologies will be implemented in almost all new software products and services, which will inevitably bring a sea change the way we work, live and do business. Though AI is in its infancy, it has shown to the world its infinite potential in performing task efficiently and accurately in an array of industries from manufacturing, retail, education to healthcare and cyber security. As always, a coin has two faces. AI is no exception. People have

shown their worries for destructive use of AI. A report from The Guardian warns “As AI capabilities become more powerful and widespread, we expect the growing use of AI systems to lead to the expansion of existing threats, the introduction of new threats and a change to the typical character of threats,”. Fortunately, the discussion on AI still ends up with bright face of AI. No doubt, if AI is implemented and trained with proper care, it can improve cyber security in many ways. It can protect against the cyber-attacks in real time with lesser resources. As cyber threats are constantly evolving, data is bursting new patterns that are hard to capture and analyze for human analyst can be crunched down by a machine learning technique in seconds. Equipped with power of deep analysis provided by Machine learning, Human analysts can focus on interpretin FUTURE ASPECTS AND SCOPE Researchers predict that by 2020, artificial intelligence technologies will be implemented in almost all new software products and services, which will inevitably bring a sea change the way we work, live and do business. Though AI is in its infancy, it has shown to the world its infinite potential in performing task efficiently and accurately in an array of industries from manufacturing, retail, education to healthcare and cyber security. As always, a coin has two faces. AI is no exception. People have shown their worries for destructive use of AI. A report from The Guardian warns “As AI capabilities become more powerful and widespread, we expect the growing use of AI systems to lead to the expansion of existing threats, the introduction of new threats and a change to the typical character of threats,”. Fortunately, the discussion on AI still ends up with bright face of AI. No doubt, if AI is implemented and trained with proper care, it can improve cyber security in many ways. It can protect against the cyber-attacks in real time with lesser resources. As cyber threats are constantly evolving, data is bursting new patterns that are hard to capture and analyze for human analyst can be crunched down by a machine learning technique in seconds. Equipped with power of deep analysis provided by Machine learning, Human analysts can focus on interpretin FUTURE ASPECTS AND SCOPE Researchers predict that by 2020, artificial intelligence technologies will be implemented in almost all new software products and services, which will inevitably bring a sea change the way we work, live and do business. Though AI is in its infancy, it has shown to the world its infinite potential in performing task efficiently and accurately in an array of industries from manufacturing, retail, education to healthcare and cyber security. As always, a coin has two faces. AI is no exception. People have shown their worries for destructive use of AI. A report from The Guardian warns “As AI capabilities become more powerful and widespread, we expect the growing use of AI systems to lead to the expansion of existing threats, the introduction of new threats and a change to the typical character of threats,”. Fortunately, the discussion on AI still ends up with bright face of AI. No doubt, if AI is implemented and trained with proper care, it can improve cyber security in many ways. It can protect against the cyber-attacks in real time with lesser resources. As cyber threats are constantly evolving, data is bursting new patterns that are hard to capture and analyze for human analyst can be crunched down by a machine learning technique in seconds. Equipped with power of deep analysis provided by Machine learning, Human analysts can focus on interpre

VII.FUTURE ASPECTS OF ARTIFICIAL INTELLIGENCE IN CYBERSECURITY

Researchers predict that by 2020, artificial intelligence technologies will be implemented in almost all new software products and services, which will inevitably bring a sea change in the way we work, live, and do business. Though AI is in its infancy, it has shown to the world its infinite potential in performing tasks efficiently and accurately in an array of industries from manufacturing, retail, and education to healthcare and cyber security. As always, a coin has two faces. AI is no exception. People have shown their

worries about the destructive use of AI. A report from The Guardian warns "As AI capabilities become more powerful and widespread, we expect the growing use of AI systems to lead to the expansion of existing threats, the introduction of new threats and a change to the typical character of threats,". Fortunately, the discussion on AI still ends up with the bright face of AI. No doubt, if AI is implemented and trained with proper care, it can improve cyber security in many ways. It can protect against cyber-attacks in real time with fewer resources. As cyber threats are constantly evolving, data is bursting new patterns that are hard to capture and analyze for human analysts can be crunched down by a machine learning technique in seconds. Equipped with the power of deep analysis provided by Machine learning, Human analysts can focus on interpreting the results and devising novel techniques for fighting criminals proactively. Therefore, using Deep learning and machine learning in defense systems will surely take cyber security to a new level of intelligence [15].

.

VIII. BUSINESS GROWTH SCOPE OF ARTIFICIAL INTELLIGENCE IN CYBERSECURITY

As businesses grow more conscious of the cyber threats they face, all sources agree that cybersecurity expenditure will increase in the next years. For instance, the Technology Industry Association (TIA) predicts that US expenditure will exceed $63.5 billion, or 0.35 percent of GDP, in 3 years. Gartner Inc. predicts that worldwide spending will expand by 8.2 percent between 2014 and 2015. Blockchain technology has the greatest potential net benefit in the United States of America (US $407 billion). The biggest economic opportunity (US$962 billion) is in product inventory management, also known as provenance, which has become a new focus for many businesses' supply chains [16]. The use of Blockchain may assist businesses from heavy industry, like mining, to fashion brands, in response to increasing attention by the public and investors about sustainable and ethical procurement. Banking and financial institutions, such as the usage of digital cryptocurrencies, as well as the promotion of digital payments by cross-border and remittances are intended to assist reduce fraud and identity theft. The use of blockchain in negotiations and dispute settlement (worth US$73 billion) as well as consumer interaction (worth US$54 billion), which includes the use of blockchain in loyalty programs, further expands blockchain's capabilities into a far broader variety of public and private sector industries [17].

IX. CONCLUSION

Stronger and more sophisticated cybersecurity measures are required as cybercrimes grow in complexity. This will enable defense systems to make judgments in real-time and successfully respond to complex attacks. Researchers and practitioners must be aware of current cyber-security techniques to support this. Particularly the application of artificial intelligence to the combat of cybercrimes.

Therefore, the significance of artificial intelligence in cyber security, as well as the many issues that arise and how to prevent them, are covered in this paper. Even with its shortcomings, artificial intelligence is still a big part of cyber security. Artificial Intelligence will help advance cyber security to overcome the limitations.

X. REFERENCES

[1] Nadide Beyza Dokur, "Artificial Intelligence (AI) Applications in Cyber Security", January 2023, pp. 01-03.

[2] Katanosh Morovat and Brajendra Panda, "A Survey of Artificial Intelligence in Cyber Security", November 2020, pp. 01-02.

[3] McAfee Labs Report, March 2016, pp. 04-05.

[4] Graham Foss, "How AI is Changing the Cyber Security Landscape", May 2023.

[5] Rajneesh Kumar, "Artificial Intelligence: A Path to Innovation", 2017, pp. 05-06.

[6] Jenis Nilkanth Welukar and Gagan Prashant Bajoria, “Artificial Intelligence in Cyber Security - A Review”, December 2021, pp. 02-03.
[7] Jagadeeshwar Podishetti and Kadapala Anjaiah, “Role of Artificial Intelligence in Cyber Security”, August 2017, pp. 04-05.
[8] C. Bitter, D. Elizondo, and T. Watson, "Application of artificial neural networks and related techniques to intrusion detection", 2010, pp. 02-03.
[9] P. Andrews and J. Timmis, “Diversity and Artificial Immune Systems: Incorporating a Diversity Operator into aiNet”, 2005, pp. 04-05.
[10] S. Forrest, A. Perelson, L. Allen, and R. Cherukuri, “Self-nonself Discrimination in a Computer”, 1994, pp. 04-05.
[11] Ishaq Azhar Mohammed, “Artificial Intelligence for Cybersecurity: A Systematic Mapping of Literature”, September 2020, pp. 174-175.
[12] Dr. K. Ramasubramanian, Dr Lendale Venkateswarlu and, Sneha Yerram, “Applications and Techniques of of Artificial Intelligence in Cyber Security”, 2021, pp. 338-339
[13] S. Hofmeyr and S. Forrest, “Immunity by Design: An Artificial Immune System", “In Proceedings of the Genetic and Evolutionary Computation Conference, vol. 2, 1999, pp. 1289-1296.
[14] S. Hofmeyr and S. Forrest, “Architecture for an Artificial Immune System, Journal of Evolutionary Computation”, December 2000.
[15] Kirti Raj Bhatele, Harsh Shrivastava and, Neha Kumari “The Role of Artificial Intelligence in Cyber Security”, January 2019, pp 21-22.
[16] H. Hou and G. Dozier, “Immunity-based Intrusion Detection System Design, Vulerability Analysis, and GENERTIA's Genetic Arms Race”, 2005, pp. 952-956
[17] 20.J. Zhan and L. Thomas, “Phishing Detection using Stochastic Learning-based Weak Estimators”, April 2011.

Cite this article as :

Miss. Tanmayi Ajay Dubey, Mr. Chinmay R. Sambhe, Miss. Aboli Sanjay Gujar, "The Future of Artificial Intelligence in Cyber Security A Review ", International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Online ISSN : 2394-4099, Print ISSN : 2395-1990, Volume 11 Issue 1, pp. 111-117, January-February 2024. Available at doi : https://doi.org/10.32628/IJSRSET241118
Journal URL : https://ijsrset.com/IJSRSET241118