International Journal of Scientific Research in Science and Technology
Print ISSN: 2395-6011 | Online ISSN: 2395-602X (www.ijsrst.com)
doi : https://doi.org/10.32628/IJSRST218675

Artificial Intelligence in Cyber Security - A Review

Jenis Nilkanth Welukar, Gagan Prashant Bajoria
Computer Science and Engineering, Jawaharlal Darda Institute of Engineering and Technology Yavatmal, Yavatmal, Maharashtra, India

Article Info
Volume 8, Issue 6
Page Number : 488-491
Publication Issue
November-December-2021
Article History
Accepted : 15 Dec 2021
Published : 30 Dec 2021

ABSTRACT

In this paper we are going to discuss how Artificial Intelligence (AI) can be used to address cyber security issues and cyber-threats. Cyber security is a vast growing field since the last decade. So the number of applications as well as the number of threats are rising continuously. This paper discuss the uses of Artificial Intelligence in cyber security and also shed some light on the disadvantages.

Keywords: Artificial Intelligence, Cyber Security, Cyber-threats, Block chain.

I. INTRODUCTION

The day to day raising and progressing cyber security threat facing global businesses can be reduced by the integration of Artificial Intelligence into cyber security systems. Machine learning and Artificial Intelligence (AI) are being connected more extensively crosswise over industries and applications than any other time in recent memory as computing power, storage capacities and data collection increase. This vast measure of information can't be dealt with by people progressively. With machine learning and AI, that peak of data could be carved down in fraction of time, which helps the enterprise to identify and recover from the security threat. [1]

II. ROLE OF ARTIFICIAL INTELLIGENCE IN CYBER SECURITY

A. Artificial Intelligence:

Artificial Intelligence is a way of making a computer, a computer-controlled robot, or a software think intelligently, in the similar manner the intelligent humans think. AI is accomplished by studying how human brain thinks, and how humans learn, decide, and work while trying to solve a problem, and then using the outcomes of this study as a basis of developing intelligent software and systems. Intelligence is commonly considered as the ability to collect knowledge and reason about knowledge to solve complex problems. In the near future intelligent machines will replace human capabilities in many areas. Artificial Intelligence is the study and developments of intelligent machines and software that can reason, learn, gather knowledge, communicate, manipulate and perceive the objects.

John McCarthy coined the term in 1956 as branch of computer science concerned with making computers behave like humans. It is the study of the computation that makes it possible to perceive reason and act. Artificial Intelligence is different from psychology because it emphasis on computation and is different from computer science because of its emphasis on perception, reasoning and action. It makes machines smarter and more useful. [2]

B. **The emergence of AI in cyber security:**

Machine learning and Artificial Intelligence (AI) are being connected more comprehensively crosswise over enterprises and applications than any other time in recent memory as registering power, information accumulation and capacity abilities increment. This tremendous trove of information is 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 off human security "partners." They are cautioned when an activity is required, yet in addition can invest their energy taking a shot at more inventive, productive undertakings.

A helpful relationship is to consider the best security proficient in your association. In the event that 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, in the event that 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. [3]

C. **Where Can Artificial Intelligence Be Used in Cyber security?**

The use of Artificial Intelligence (AI) is already being used to, or is being actively explored for, some of the following areas in cyber security 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, you are assisting in training the AI to detect spam in the future. 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. 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 the identical queries on a site in a single attack. This may include unsuccessful login attempts (a botnet brute force password attack), networks 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.

These are just a handful of the areas in which Artificial Intelligence has been used for cyber security. There are currently a large number of research articles that provide compelling data in support of Artificial Intelligence's effectiveness in the field of

cyber security. 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. [4]

D. **Benefits of AI in Cyber Security:**

A review on the advantages of Artificial Intelligence in the field of cyber security reveals that institutions that implemented AI in cyber security realize significant benefits. This is evident as ROI of two out of three organizations increased on cyber security tools. For example, Siemens AG, leader of Global electrification, automation, and digitalization used Amazon Web Services (AWS) to create AI based, high speed, self-controlled, and extremely elastic platform for its Siemens Cyber Defense Center (CDC). The AI deployed was able to estimate 60,000 potential assaults per unit time. As a result of the AI deployed, this capability was managed with a team consisting of less than dozen members without any negative impact on system performance. Employing AI in cyber security permit institutions to comprehend and reapply prior threat patterns in identification of novel threats. This results to preservation of time and effort in identifying and investigating incidents, and remediate threats. About 64% of administrators reveal that AI cut down the cost to identify and react to breaches. Fast response is essential in evading cyber-attacks. Cost reduction for organizations is within an average of 12%. AI offers opportunities for cyber security largely because the cyber security landscape is rapidly moving from identification, manual response and mitigation towards automated mitigation. AI can identify novel and complex modifications in attack extensibility. [5]

E. **Disadvantages of AI in Cyber Security:**

1) Cost effectiveness: Sometimes the cost of using AI services exceeds the limit, so everyone is not able to take its advantages.
2) Cyber threats: Your data and privacy now a days is too vulnerable to attacks by hackers. They can easily track your location and hack your private data if preventive measures are not taken.
3) Machine gaining control over humans: It's the oldest concern over AI. This concern has been depicted in many movies books before. Steps must be taken to prevent this from happening.
4) Loss of jobs: Artificial Intelligence is considered as a threat as some studies are predicting that a big slice of the workforce is going to lose their jobs and replaced by Artificial Intelligence applications and machinery.
5) Not everyone is familiar with AI: Not everyone wants to work with new modern-day technologies and is willing to understand it.

F. **Future Aspects:**

As businesses grow more conscious of the cyber-threats they face, all sources agree that cyber security 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. Block chain technology has the greatest potential net benefit in the United States of America (the 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. The use of Block chain may assist businesses from the 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 crypto currencies, as well as the promotion of digital payments by cross-border and remittances are intended to assist reduce fraud and identity theft. [4]

III. CONCLUSION

So in this paper we saw the importance of Artificial Intelligence in cyber security and the various problems that come along with it and how they can be minimized. Though there are some drawbacks, but still Artificial Intelligence plays a significant role in cyber security. For overcoming the drawbacks, Artificial Intelligence will assist to advance cyber security.

IV. REFERENCES

[1] Arockia Panimalar.S, Giri Pai.U, Salman Khan.K, "ARTIFICIAL INTELLIGENCE TECHNIQUES FOR CYBER SECURITY", International Research Journal of Engineering and Technology (IRJET), Volume: 05 Issue: 03 | Mar-2018, e-ISSN: 2395-0056, p-ISSN: 2395-0072.

[2] Rajneesh Kumar, "Artificial Intelligence : A Path to Innovation", International Journal of Scientific Research in Science and Technology (IJSRST), 2017 IJSRST | Volume 3 | Issue 1 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X.

[3] Jagadeeshwar Podishetti and Kadapala Anjaiah, "Role of Artificial Intelligence in Cyber Security", International Journal of Research in Advanced Computer Science Engineering, Volume No:3, Issue No:3 (August-2017), ISSN No : 2454-423X (Online).

[4] Ishaq Azhar Mohammed, "ARTIFICIAL INTELLIGENCE FOR CYBERSECURITY: A SYSTEMATIC MAPPING OF LITERATURE", INTERNATIONAL JOURNAL OF INNOVATIONS IN ENGINEERING RESEARCH AND TECHNOLOGY [IJIERT], VOLUME 7, ISSUE 9, Sep.-2020, ISSN: 2394-3696.

[5] Shidawa Baba Atiku, Achi Unimke Aaron, Goteng Kuwunidi Job, Fatima Shittu and Ismail Zahraddeen Yakubu, "Survey On The Applications Of Artificial Intelligence In Cyber Security", INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH VOLUME 9, ISSUE 10, OCTOBER 2020, ISSN 2277-8616.

Cite this article as :

Jenis Nilkanth Welukar, Gagan Prashant Bajoria, "Artificial Intelligence in Cyber Security - A Review", International Journal of Scientific Research in Science and Technology (IJSRST), Online ISSN : 2395-602X, Print ISSN : 2395-6011, Volume 8 Issue 6, pp. 488-491, November-December 2021. Available at doi : https://doi.org/10.32628/IJSRST218675
Journal URL : https://ijsrst.com/IJSRST218675