



ARTIFICIAL INTELLIGENCE & ITS SECURITY

Anjana Dass

Under Graduate Sri Krishna Arts and Science College Coimbatore-641041

ARTICLE INFO

Article History:

Received 24th January, 2020

Received in revised form 19th

February, 2020

Accepted 25th March, 2020

Published online 28th April, 2020

ABSTRACT

Artificial Intelligence is the study on how to make computers to do things where at the moment people do better. The primary goal of Artificial Intelligence is to improve its behavior so it would be called as intelligent. Where there are tremendous advancements in security, the experts of cyber security do face lots of issues day by day. There are lot of breaches and security attacks daily that makes it difficult for the humans to handle alone. The problems regarding in cyber security can be solved by Artificial Intelligence. In this paper, it gives an overview about Artificial Intelligence and its security issues.

Key words:

Artificial Intelligence, Applications, Security.

Copyright©2020 Anjana Dass. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

INTRODUCTION

Artificial Intelligence has been used widely in academics and in industry area. AI brings out both opportunities and challenges for upcoming applications. On the other hand, AI protects privacy in challenging situations, improving the start of security solutions.

Using Artificial Intelligence in security systems reduces the increasing threats of cyber security which are faced by many. The cybersecurity arena faces vital challenges in the form of hacking attacks that harm all kinds of organizations and creates damage over billions of dollars in business.

Scientists described some short research goals to see how AI impacts the prudence, the laws and beliefs that are involved with AI and how to minimize the risks of AI security. The scientists have proposed to continue improving function while decreasing the possible security risks that come with the emerging technologies.

Artificial Intelligence

The term Artificial Intelligence (AI) was first composed by John McCarthy in 1956. AI can be studied as a science that has been developed for seeking to find the realization of knowledge for the intelligent machines, or science giving out techniques to take care of compound issues. It is the ability of a computer-controlled robot to perform tasks that are combined with the intelligent beings. This term is constantly applied to be equipped with the creative processes, uniqueness of humans, like the ability to reason, to discover meaning, or learn from the past experiences.

***Corresponding author: Anjana Dass**

Under Graduate Sri Krishna Arts and Science College Coimbatore-641041

On the other hand, some programs have earned the conduct levels of human experts and professionals in performing certain tasks, so that artificial intelligence is found in applications as medical diagnosis, computer search engines, and voice recognitions. From SIRI to self-driving cars, artificial intelligence is advancing swiftly. AI makes it possible for machines to learn from human experience, adjust to newer methods and perform human tasks. By using these technologies, computers can be trained to achieve specific tasks by managing large amounts of data and observing patterns in the data.

Countless techniques have been founded in the AI field for taking care of issues which are difficult that require keen observation from the human frame of reference. Some of these strategies have achieved a stage of development where the algorithms that are found to be exact exist do depend on these techniques. Artificial Intelligence in cyber security is essential because it improves on how security experts analyze and understand cybercrime globally. It complements the cyber security technologies that companies use to repel cybercriminals and keeping organizations and their customers safe from security breach.

Advantages

The advantages of Artificial intelligence applications are enormous and can reform any professional region,

1. Making faster decisions: Using Artificial intelligence, decisions can be taken in a very faster manner like playing a chess game, it is nearly impossible to beat CPU because of A.I. behind that game.
2. Usage in daily applications: In today's era, A.I. is used in many applications just like Apple's Siri, Google's

OK Google. Using these applications can communicate with our device using our voice which makes our work easy.

1. 3.No Emotions: The absence of emotions makes the machines to think in a logical manner avoiding distractions by making right decisions where humans emotions are combined with moods that affect human efficiency.
3. Error Reduction: The advantage of using Artificial Intelligence is that, it helps us in correcting errors and increasing the chance of higher accuracy with a degree of greater precision.
4. Medical Applications: It helps the patient to know about the different side effects in medicines and behaves as personal digital care. Artificial surgery simulator is the great introduction part of the AI.

Disadvantages

The Disadvantages of AI are as follows,

1. Loss of Jobs: Artificial intelligence will replace millions of jobs that are engaged by humans. The growth of AI in self-driving cars is alarming to displace millions of jobs all around the world.
2. Expensive: Artificial intelligence has cost billions of dollars in its development so far to the governments and private organizations.
3. Loss of skills: AI will not just take away people's job, it will lead to the loss of their relevant skills.

Artificial Intelligence Security

Having machines do intelligent things on their own without having human guidance is known as artificial intelligence. AI security involves AI to identify and stop cyber threats and breaches with intervention of less humans is needed with security approaches. More advanced applications of AI security can simply identify the good or bad behavior by inspecting vast amounts of information that could indicate suspicious behavior. AI security behaves in a manner that is similar to the most capable human analyst.

In addition to the growing talent of AI, it is clear that the current security analysts often struggle to find the time to detect new threats in the internet. AI shows the greatest potential for fraud and malware detection, assigning many logins attempts on networks. Supervised and unsupervised machine learning algorithms are verifying to be active in identifying likely breaches in online transaction activity.

How ai Reduces the Threats of Cyber Security?

To develop in the new era, operation security needs the risks to reduce that are posed by AI and make the most of the opportunities AI offers.

Some organizations will have their business models entirely relied on AI technology. Such systems and the information that supports them have essential vulnerabilities and are at risk from both accidental threats. Taking steps to secure the internal AI systems and fight against the external AI-enabled threats will become essentially important in reducing information risk to the businesses. Organizations must be ready to find themselves to defend in order to cope up with the scale and elegance of AI-enabled cyber-attacks. AI tools and techniques can be used in defend the criminals, hackers and state-sponsored groups. AI can update security databases by analyzing logs from various sources, artificial intelligence can detect when new threats are inevitable. The focus of AI is to point out the bugs and security flaws. For example, machine learning can be used to detect a security flaw when an unwanted data has been sent from an application. It cannot only detect when a system has a flaw, but automatically prevent those flaws from being oppressed.

CONCLUSION

Artificial intelligence has made so many things to be presumed impossible years ago, to be possible today. It is transforming industries and impacting on our daily lives. We can use AI in different ways for the benefit of cyber security. There are many more greater techniques forthcoming in AI. We should therefore adopt into this change and by embracing AI and moving there is no doubt that it going to play a major and a positive role in the future of mankind.

References

1. Artificial Intelligence -The Wikipedia
2. Artificial Intelligence Techniques for Cyber Security- (Arockia Panimalar), (Giri Pai), (Salman Khan).
3. Advantages and Disadvantages of Artificial Intelligence-Sunil Kumar.
4. Advantages of Artificial Intelligence- Educba.
5. Advantages and disadvantages of AI- The crazy programmer.
6. Artificial Intelligence Security- Hashedout.
7. Charts That Will Change Your Perspective of AI in Security- Louis Columbus.
8. Special Issue on Cyber Security and AI- (Seong Oun Hwang), (Taekyoung Kwon), (Wei-Chuen Yau), (DaeHun Nyang).
9. AI Security – Awake.
10. Artificial Intelligence tool penetration in business adoption, challenges and fears – (Stephan Schlogl), (Claudia Postulka).

How to cite this article:

Anjana Dass (2020) ' Artificial Intelligence & Its Security', *International Journal of Current Advanced Research*, 09(04), pp. 21925-21926. DOI: <http://dx.doi.org/10.24327/ijcar.2020.21926.4317>
