PROFITABLE USES OF ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING TO SECURE OUR DATA

Nikitha Merilena Jonnada

University of the Cumberlands, Williamsburg, Kentucky, USA

ABSTRACT

The author used this paper to discuss the techniques, strategies, and concepts of artificial intelligence and machine learning to learn their uses in providing security and other essential features. The author also discusses the advantages, drawbacks, or limitations of using artificial intelligence and machine learning. Any technology or development comes with certain advantages and limitations. This scenario applies to artificial intelligence and machine learning. By emphasizing the importance of artificial intelligence and machine learning, the author attempts to educate the users and readers about the significant concepts within the study, as this could help many users and organizations to identify the critical factors about these concepts.

KEYWORDS

Artificial Intelligence, Machine Learning, Virus, Security, Malware, Data.

1. INTRODUCTION

Artificial intelligence and machine learning are the two significant concepts many organizations have been trying to adapt to lately. Many organizations are implementing artificial intelligence and machine learning on their websites, mobile applications, and other processes and interfaces to join different organizations using those technologies. Many banking, healthcare, retail, and other organizations use artificial intelligence and machine learning. Every action that happens, like a robot, is developed using artificial intelligence and machine learning. These concepts have also been taken advantage of in the job profiles. Many students also prefer learning artificial intelligence and machine learning to save their jobs from being lost to robots.

2. RESEARCH QUESTIONS

- Can we rely on artificial intelligence to provide security to the systems?
- Can machine learning help the users with security?

3. ARTIFICIAL INTELLIGENCE (AI)

Artificial Intelligence is a technique where the human mind is studied and replicated to an extent into a computer-based device called a robot. Humans develop robots and their actions to help them perform particular tasks or, in a way, replace humans to perform specific tasks. Many organizations have been using Artificial Intelligence lately to enhance their user experience. Nowadays, everyone is addicted to going digital in everything they do. Even though artificial intelligence comes with certain advantages and limitations, many organizations still want to change their interfaces to artificial intelligence standards to make the navigation on their website

easy. With Artificial Intelligence, users can get their frequently asked questions answered in minutes, even when there is no available customer representative to answer their questions. Google also uses artificial intelligence when returning search results. In Las Vegas, a building called the Sphere uses artificial intelligence and machine learning techniques to create a user interaction experience that attracts visitors. Many organizations are also using artificial intelligence to enhance their customer and user experience, to act as immediate support, and to automate their internal processes to cut down on work burdens. Artificial intelligence could replace humans as soon as scientists and developers study human behavior and incorporate those features and behaviors into robots to act as their assistants. This approach comes with more security concerns than expected, as it is unsafe to depend entirely on machines as an intruder can try to corrupt them. But it would be different with humans as no scientist or a developer could alter a human brain. Artificial intelligence works with code and can be easily hacked, overwritten, and misused [2].

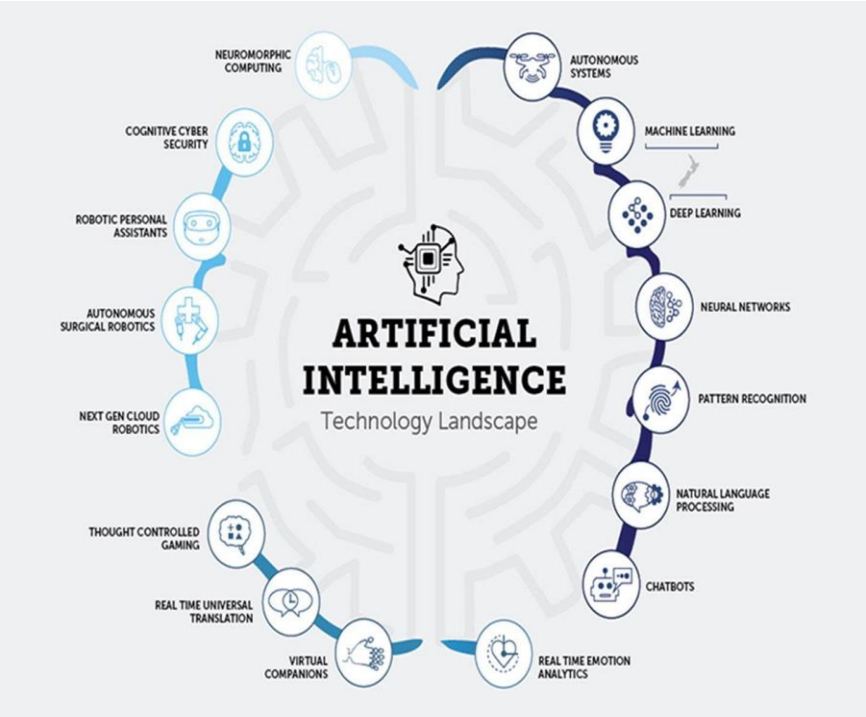

Figure 1. Artificial Intelligence

4. ARTIFICIAL INTELLIGENCE FOR SECURITY

In terms of security, artificial intelligence can enhance and improve threat detection. We can use artificial intelligence within cybersecurity. Organizations can use Artificial Intelligence to detect intruders, viruses, and malware entering the network. By automating specific processes, We can use artificial intelligence to our advantage with continuous monitoring techniques. Many individuals and organizations can also use artificial intelligence (AI) to provide enhanced realtime tracking. We can adjust the camera viewpoint in any way we like so that they can detect and notify based on their setting set using Artificial Intelligence. With artificial intelligence, we can also automate updates without missing deadlines to complete updating specific applications [6].

4.1. Advantages of Using Artificial Intelligence

- Many organizations are using AI Bots to help them
- Provide a better user interaction experience.
- Enhance customer experience.
- Provide relevant search suggestions and results.
- Provide an improved decision-making experience.
- Detect any intruder and malware activities.
- Provide an option to auto-update their processes.

4.2. Disadvantages of Using Artificial Intelligence

- The cost of implementing Artificial Intelligence is high.
- Security could always be a concern.
- The machines can expose sensitive data and could be at risk.
- Human requirements might decrease.
- Humans could lose their jobs.
- Artificial Intelligence cannot be creative.
- Artificial Intelligence can only follow what gets written in the code or what instructions it receives.
- It could be easily hacked and misused.

5. MACHINE LEARNING (ML)

Machine Learning is derived and developed as an extension to artificial intelligence. Machine Learning teaches and guides a machine on how to work and perform. Machine Learning learns and adapts from the data provided. This process does not need a code like artificial intelligence. Machine Learning is an advanced version that uses data patterns to provide a better experience to its users. The performance of Machine Learning depends on the amount of data it has access to. The performance is high if it has access to large amounts of data. The performance is low if fed with smaller amounts of data [4].

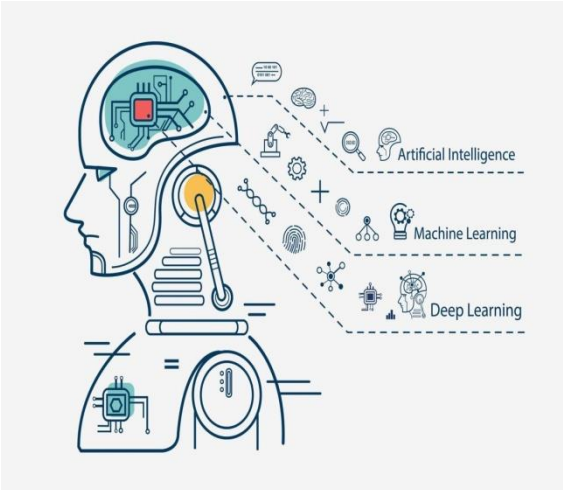

Figure 2. Machine Learning

6. MACHINE LEARNING FOR SECURITY

Security organizations can use machine learning to detect and report malware attacks based on the data fed to them. This method can help organizations realize when there is a virus attack within their systems. Even when the data is encrypted, machine learning can help detect the malware in the data without having to decrypt it to find it. It also allows its users to provide faster and enhanced data analysis to stay alert. When the humans and machines using the machine learning concepts get compared, the system can filter data faster using machine learning concepts than humans. This approach could come with its drawbacks. A machine can make errors compared to humans [5].

6.1. Advantages of Machine Learning

- We can automate the processes.
- We can automate the repeating tasks by setting a date and time.
- Improve customer experience.
- Help with better assisting the users by using the advanced technology.
- Scalability.

6.2. Disadvantages of Machine Learning

- Machine Learning depends on the data.
- Without the data, machine learning uses are limited.
- High costs.
- The process could be too complex.
- Security issues could be high.
- Humans could lose their jobs.

7. NEEDED ENHANCEMENTS IN THE FUTURE

Artificial intelligence and machine learning concepts must be developed and enhanced mainly within security. Even today, with advanced technology, artificial intelligence and machine learning still need to fill the void of providing complete protection to their users and organizations. Data is always at risk. Putting that data in the hands of robots that run with artificial intelligence and machine learning is extremely risky as humans create and develop robots using the concepts of artificial intelligence and machine learning. These robots act the way humans design them. If organizations use artificial intelligence and machine learning to achieve security, it is advantageous for information security analysts to use these concepts for their benefit.

8. CONCLUSION

Artificial intelligence and machine learning could provide us a better future, but both concepts have limitations. Many organizations prefer artificial intelligence and machine learning to automate their processes and provide users with a more effortless and better experience. However, organizations must be aware that when using artificial intelligence and machine learning, they must continuously monitor their activities so that their code and data are not corrupt. If corrupted data gets fed, it could cause significant issues, as implementing artificial intelligence and machine learning is costly. When something goes wrong, the organizations

would incur substantial losses to cover the costs incurred by the artificial intelligence and machine learning wrongdoings.

REFERENCES

[1] Berente, N., Gu, B., Recker, J., & Santhanam, R. (2021). Managing Artificial Intelligence. 1-5.
[2] Zhang, Z., Hamadi, H. A., Damiani, E., Yeun, C. Y., & Taher, F. (2022). Explainable Artificial Intelligence Applications in Cyber Security: State-of-the-Art in Research. 93104 - 93139.
[3] What is machine learning (ML)? (2024).
[4] Xue, M., Yuan, C., Wu, H., Zhang, Y., & Liu, W. (2020). Machine Learning Security: Threats, Countermeasures, and Evaluations. 74720 - 74742.
[5] Artificial Intelligence. (2023).
[6] Machine Learning. (2024).

AUTHOR

Nikitha Merilena Jonnada is a PhD degree holder. She earned her PhD in Information Technology (Information Security Emphasis) from the University of the Cumberlands in 2024. The author continues her research with a security emphasis and is expanding her research into artificial intelligence and machine learning to develop security measures using the latest technology standards.