Opportunities and Risks in the Use of Artificial Intelligence Models in Healthcare

Aurelian Buzdugan, Gheorghe Capatana, Artur Buzdugan

Abstract

The advancements in artificial intelligence are triggering discussions on transforming many processes in the industry, society or economy, including the healthcare sector. The new capabilities offered by emerging technologies applied in healthcare help deliver more accurate and efficient diagnoses and treatment options. Artificial intelligence models can be used for various purposes in healthcare, from functions such as personal assistant, up to analyzing data and providing recommendations for tasks such as medical imaging analysis, drug development, disease identification, and emergency support. Furthermore, artificial intelligence models can support research actions, to speed up the development of certain cures or medicines. They can also assist in detecting high-risk conditions in patients, discovering and researching new drugs and medicines, and developing new treatment plans. However, these digital technologies come with cybersecurity risks, both due to the underlying technical systems, such as computers used, up to the risks or issues in the models themselves, which can lead to questions on the accuracy of the recommendations and solutions provided by the models, or data breaches and cyber-attacks. Such incidents can lead to serious consequences, including compromised data privacy and safety. This paper presents some potential use cases of the AI model in the healthcare industry. In addition, several cyber security recommendations are offered to ensure that the adoption and use of such emerging tools minimize potential cyber risks.

6th International Conference on Nanotechnologies and Biomedical Engineering
Proceedings of ICNBME-2023, September 20–23, 2023, Chisinau, Moldova
Volume 2: Biomedical Engineering and New Technologies for Diagnosis, Treatment, and Rehabilitation

Keywords: cybersecurity, artificial intelligence, artificial intelligence models, healthcare

References

1. Oxford English Dictionary. https://www.oed.com/viewdictionaryentry/Entry/271625

2. ChatGPT. https://openai.com/blog/chatgpt

3. Kwo, L.: Contributed: Top 10 Use Cases for AI in Healthcare. https://www.mobihealthnews.com/news/contributed-top-10-use-cases-ai-healthcare

4. Buzdugan,A.: Integration of cyber security in healthcare equipment. In: Tiginyanu, I., Sontea, V., Railean, S. (eds.) ICNBME 2019. IP, vol. 77, pp. 681–684. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-31866-6_120

5. Mirsky, Y., et al.: CT-GAN: Malicious Tampering of 3D Medical Imagery Using Deep Learning (2019). https://www.researchgate.net/publication/330357848_CT-GAN_Malicious_Tampering_of_3D_Medical_Imagery_using_Deep_Learning

6. The IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems. https://standards.ieee.org/industry-connections/ec/autonomous-systems/

7. Directive on Automated Decision-Making. https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32592EUAIAct

8. EU AI Act. https://artificialintelligenceact.eu/the-act/

9. Bohr, A., Memarzadeh, K.: The rise of artificial intelligence in healthcare applications. Artif. Intell. Healthc. 25–60 (2020). https://doi.org/10.1016/B978-0-12-818438-7.00002-2

10. Healthcare Cybersecurity Challenges, Maryville University. https://online.maryville.edu/blog/healthcare-cybersecurity/

11. Sobieszek, A., Price, T.: Playing games with AIs: the limits of GPT-3 and similar large language models. Minds Mach. **32**(2), 341–364 (2022)