Digital Health and Informatics Innovations for Sustainable Health Care Systems
J. Mantas et al. (Eds.)

doi:10.3233/SHTI240640

Methods and Algorithms of Ensuring Data Privacy in AI-Based Healthcare Systems and Technologies

Omar Farshad JEELANI [a,1], Makaire NJIE [a] and Viktoriia KORZHUK [a]
[a] *ITMO University, Russia*
ORCiD ID: Omar Farshad Jeelani https://orcid.org/0009-0006-5607-5265,
Makaire Njie https://orcid.org/0009-0004-5699-0346,
Viktoriia Korzhuk https://orcid.org/0000-0002-0240-9067

Abstract. This project seeks to devise novel algorithms and techniques leveraged in healthcare to guarantee data privacy in AI-powered systems. To bolster its credibility, the study review presents various modern approaches and technologies used to preserve data privacy of healthcare data. The project conducted an empirical study of the current development in healthcare regarding AI privacy protection to compile a steadfast literature on the subject.

Keywords. Data Privacy, Artificial Intelligence (AI), Healthcare AI, Data Sharing, Healthcare Organizations (HCOs)

1. Introduction

Artificial Intelligence (AI) has been introduced into healthcare to enable personalized treatments and investigations through algorithms. Various types of health data are stored and processed using such technologies as machine learning, deep learning, computer vision, and natural language processing. [1,2].

1.1 Importance of data privacy and security in AI-driven healthcare systems

AI-driven healthcare systems prioritize the protection of clients' confidentiality and their related information as well as ensuring consent is obtained prior to any activity involving a patient's personal data the information being handled with impartiality.

2. Background

Healthcare AI has made progress in medical imaging, decision support, virtual assistants, and drug research. The absence of privacy regulations has resulted in data breaches that affected public trust impeding sustainable development of AI in healthcare. [3,4]

[1] Corresponding Author: Omar Farshad Jeelani; E-mail: omar@itmo.ru.

3. Materials and Methods

The study compares global data privacy regulations by looking at differences across different countries before examining how these laws are formulated. Various measures for protecting healthcare data privacy were reviewed.

4. Results

GDPR HIPAA Laws on the Digital Personal Data Protection Bill were some examples mentioned. Some of federated learning models encoded with cryptographic techniques like differential privacy were designed to protect user privacy better than previous methods used during training an algorithm using a centralized dataset.

5. Discussion

In the field of healthcare AI, it is very important that there are strong data protection measures and legal frameworks in place to ensure patient data is safe. In fact, there must be regulations designed by authorities to fill the gaps from legislation already in existence, and enhance data confidentiality [1-4].

6. Conclusions

Various AI innovations are vital to maintaining privacy in healthcare data. Patients' information security can be enhanced using such methods as federated learning, cryptographic techniques or differential privacy thereby complying with the laws on safeguarding data privacy across borders.

In conclusion, this summary highlights the importance of AI in healthcare data protection and confidentiality urging for stringent precautions to shield confidential patient details against evolving landscape of healthcare involving artificial intelligence.

References

[1] Jumper J, Evans R, Pritzel A, Green T, Figurnov M, Ronneberger O, Tunyasuvunakool K, Bates R, Žídek A, Potapenko A, Bridgland A. Highly accurate protein structure prediction with AlphaFold. Nature. 2021 Aug;596(7873):583-9.

[2] Vemuri N, Thaneeru N, Tatikonda VM. AI-Optimized DevOps for Streamlined Cloud CI/CD. International Journal of Innovative Science and Research Technology. 2024;9(7):10-5281.

[3] Rasheed K, Qayyum A, Ghaly M, Al-Fuqaha A, Razi A, Qadir J. Explainable, trustworthy, and ethical machine learning for healthcare: A survey. Computers in Biology and Medicine. 2022 Oct 1;149:106043.

[4] Akgün M, Pfeifer N, Kohlbacher O. Efficient privacy-preserving whole-genome variant queries. Bioinformatics. 2022 Apr 15;38(8):2202-10.