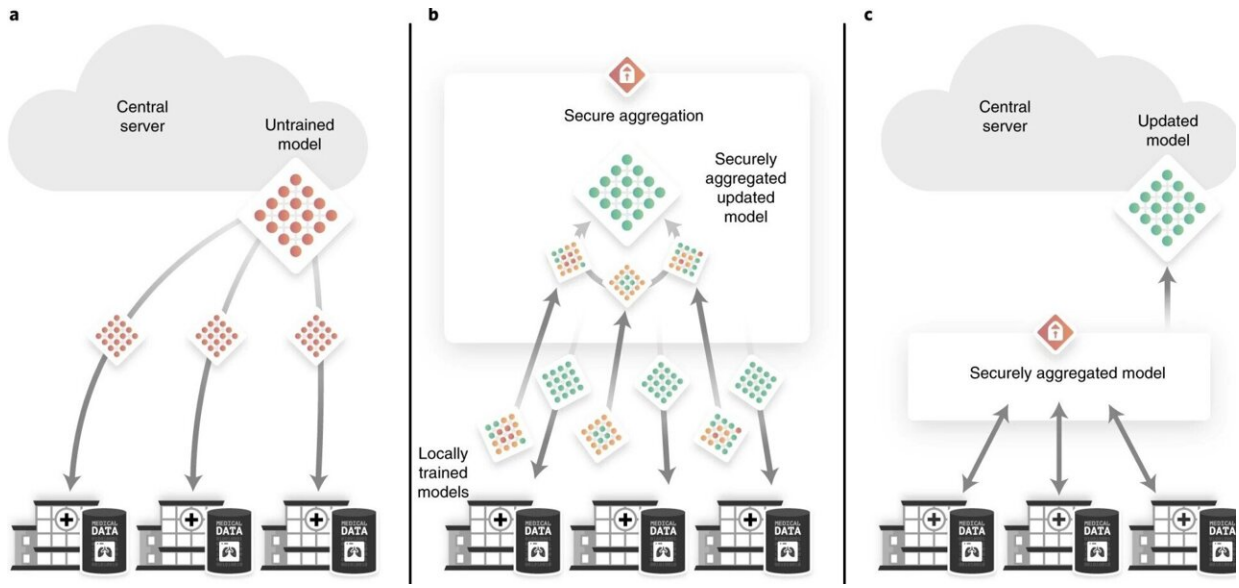
New AI technology protects privacy in healthcare settings

May 25 2021, by Caroline Brogan



Credit: Imperial College London

Researchers at TUM and Imperial have developed a technology that protects patients' personal data while training healthcare algorithms.

The technology has now been used for the first time in an algorithm that identifies pneumonia in X-ray images of children. The researchers found that their new privacy-protecting techniques showed comparable or better accuracy in diagnosing various pneumonias in children than existing algorithms might.

Artificially intelligent (AI) algorithms can support clinicians in diagnosing illnesses like cancers and sepsis. The effectiveness of these algorithms depends on the quantity and quality of the medical data used to train them, and patient data is often shared between clinics to maximize the data pool.

To protect these data, the material usually undergoes anonymisation and pseudonymisation, but the researchers say these safeguards have often proven inadequate in terms of protecting patients' health data.

To address this problem, an interdisciplinary team at the Technical University of Munich (TUM), Imperial College London, and the non-profit OpenMined developed a unique combination of AI-based diagnostic processes for radiological image data that safeguards data privacy.

In their paper, published in *Nature Machine Intelligence*, the team present a successful application: a deep learning algorithm that helps to classify pneumonia conditions in X-rays of children.

Co-author Professor Daniel Rueckert, of Imperial's Department of Computing and TUM, said: "Guaranteeing the privacy and security of healthcare data is crucial for the development and deployment of large-scale machine learning models."

Privacy protection

One way to protect patients' records is by keeping them at the site of collection rather than sharing them with other clinics. Currently, clinics share patient data by sending copies of databases to clinics where algorithms are being trained.

In this study, the researchers used federated learning, in which the deep

learning algorithm is shared instead of the data itself. The models were trained in the various hospitals using the local data and then returned to the authors—thus, the data owners did not have to share their data and retained complete control.

First author Georgios Kaissis of TUM and Imperial's Department of Computing said: "To keep patient data safe, it should never leave the clinic where it is collected."

To prevent identification of institutions where the algorithm was trained, the team applied another technique: secure aggregation. They combined the algorithms in encrypted form and only decrypted them after they were trained with the data of all participating institutions.

To prevent individual patient data from being filtered out of the data records, the researchers used a third technique when training the algorithm so that statistical correlations could be extracted from the data records, but not the contributions of individual persons.

Professor Rueckert said: "Our methods have been applied in other studies, but we are yet to see large-scale studies using real clinical data. Through the targeted development of technologies and the cooperation between specialists in informatics and radiology, we have successfully trained models that deliver precise results while meeting high standards of data protection and privacy."

Paving the way for digital medicine

The combination of the latest data protection processes will also facilitate cooperation between institutions, as the team showed in a previous paper published in 2020. Their privacy-preserving AI method could overcome ethical, legal and political obstacles—thus paving the way for widespread use of AI in healthcare, which could be enormously

important for research into rare diseases.

The scientists are convinced that by safeguarding the privacy of patients, their technology can make an important contribution to the advancement of digital medicine. Georgios added: "To train good AI algorithms, we need good data, and we can only obtain these data by properly protecting patient privacy. Our findings show that, with data protection, we can do much more for the advancement of knowledge than many people think."

"End-to-end privacy preserving deep learning on multi-institutional medical imaging," by Georgios Kaissis et al., was published 24 May 2021 in *Nature Machine Intelligence*.

More information: Georgios Kaissis et al, End-to-end privacy preserving deep learning on multi-institutional medical imaging, *Nature Machine Intelligence* (2021). DOI: 10.1038/s42256-021-00337-8

Provided by Imperial College London