

Building Trust in Medical Use of Artificial Intelligence – The Swarm Learning Principle

Joachim L. Schultze ^{a,b,c}

^aSystems Medicine, Deutsches Zentrum für Neurodegenerative Erkrankungen (DZNE), Bonn, Germany; ^bPRECISE Platform for Single Cell Genomics and Epigenomics, Deutsches Zentrum für Neurodegenerative Erkrankungen (DZNE) and University of Bonn, Bonn, Germany; ^cGenomics & Immunoregulation, sLife and Medical Sciences (LIMES) Institute, University of Bonn, Bonn, Germany

ABSTRACT

An avalanche of medical data is starting to be build up. With the digitalisation of medicine and novel approaches such as the omics technologies, we are conquering ever bigger data spaces to be used to describe pathophysiology of diseases, define biomarkers for diagnostic purposes or identify novel drug targets. Utilising this growing lake of medical data will only be possible, if we make use of machine learning, in particular artificial intelligence (AI)-based algorithms. While the technological developments and chances of the data and information sciences are enormous, the use of AI in medicine also bears challenges and many of the current information technologies (IT) do not follow established medical traditions of mentoring, learning together, sharing insights, while preserving patient's data privacy by patient physician privilege. Other challenges to the medical sector are demands from the scientific community such as "Open Science", "Open Data", "Open Access" principles. A major question to be solved is how to guide technological developments in the IT sector to serve well-established medical traditions and processes, yet allow medicine to benefit from the many advantages of state-of-the-art IT. Here, I provide the Swarm Learning (SL) principle as a conceptual framework designed to foster medical standards, processes and traditions. A major difference to current IT solutions is the inherent property of SL to appreciate and acknowledge existing regulations in medicine that have been proven beneficial for patients and medical personal alike for centuries.

ARTICLE HISTORY

Received 10 January 2022
Revised 19 December 2022
Accepted 20 December 2022

KEYWORDS



Swarm learning; artificial intelligence; machine learning; medical tests; diagnostics; companion diagnostics

Introduction

In 2019, Rajkomar and colleagues started an article in the New England Journal of Medicine by describing the history of a melanoma patient as it could occur nowadays everywhere in the world, before they introduce their view on machine learning in medicine [1]. They end their article with the same case, but in a future scenario that is based on a very efficient use of medical data and AI solutions. The changes required to get from today's limitations and delays in diagnostics and therapy to their future vision are huge and include complete access to all medical data in the world, the integration of different data sources in different institutions, and the development and use of computer-assisted diagnosis and therapy suggestions. In this ideal world, different institutions have to work hand-in-hand in a digital form and computer-based models must be established that can provide insights from the ever-increasing medical data space [2]. While the necessary organisational changes due to digitalisation are likely to occur at every institution, it requires more thought about

how computer-assisted systems will be efficiently developed, also considering today's legal frameworks. For example, European regulations such as the General Data Protection Regulation (GDPR), which protects data privacy, are not only valid within the member states of the European Union but worldwide and they have a significant impact on how we actually develop AI for medicine [3,4].

At the same time, the ever-increasing avalanche of medical data ranging from clinical data to imaging data, but also conquering new data spaces such as the omics data, requires methods that allow to look at these data in a concerted fashion. Considering the strictly decentralised production of medical data requires further thoughts about data logistics. What is the most sustainable and environmentally protective way forward to store and compute medical data? Certainly not by data duplication and significant moving of data, particularly, when it comes to large primary data in medicine. As a consequence, concepts suggesting centralisation of data that are mainly produced in

CONTACT Joachim L. Schultze  joachim.schultze@dzne.de  Systems Medicine, Deutsches Zentrum für Neurodegenerative Erkrankungen (DZNE), Bonn, Germany

© 2023 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group.

This is an Open Access article distributed under the terms of the Creative Commons Attribution-NonCommercial License (<http://creativecommons.org/licenses/by-nc/4.0/>), which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited.

a decentralised fashion do not really seem to be sustainable.

Another important aspect during the transformation process from today's daily practice to what has been envisioned by Rajkomar and others is the role of AI and the physicians [1]. There is no doubt anymore that we need AI to make sense of the enormous data at our disposal, because it will be critical for physicians to base their decision-making process on state-of-the-art knowledge and information [5]. Such information can only be extracted from these large data with the help of AI [6]. Whether it might have even legal implications in the future, if physicians make decisions without utilising AI-based knowledge and information, requires further research. But even if not considering legal issues, it is every physician's duty to treat patients to the best of one's own knowledge, and if basically every medical data in the world would be somehow accessible, available and interpretable by AI, there would be no way around the use of AI-based diagnostics and therapy decision-making.

In this perspective, I intend to develop a conceptual framework that could unite medical concepts with very long tradition with technical developments from the IT sector as a prerequisite for building the cornerstones that are required to build the scenarios that have been laid out before [1].

AI – Structural Aspects, from Local to Swarm

AI applications require large enough data to train models with sufficient robustness [7] and appropriate algorithms [8]. If sufficient data are available, AI models can be trained locally. However, since medicine is inherently decentralised and medical data are usually stored and handled at the production sites (for example, imaging data at a regional hospital), the locally available data for any kind of medical problem are usually insufficient for optimally training AI-based models [1,9].

Similar to other areas with large data, a technical solution to this problem was proposed by the IT sector, namely the centralisation of data from different places [10] often referred to as cloud storage and cloud computation. Initially, the concept was intriguing, since it solved the technical problems concerning the lack of sufficiently large data for AI applications. Once data – generated in a decentralised fashion – were moved towards a central storage, much more data would be available to train AI models. However, data centralisation comes with disadvantages. These include data duplication and increase of storage space needed, increased data traffic as well as increasing concerns

about security, data privacy and confidentiality, and even data ownership. Moreover, it can lead to data monopolies, if sufficiently large amounts of data in any given domain are now stored centrally under the control of a single entity [7]. Furthermore, data duplication and data trafficking increase the carbon footprint and are not an environmentally friendly and sustainable IT solution [11].

As the disadvantages started to outweigh the initial advantages, alternative solutions were sought. A concept that was put forward by several of the major players in big data computation was called federated learning. In this setting, the data are indeed kept locally thereby reducing data duplication and data traffic [7,12]. Federated learning also addressed concerns recently raised for central computing models, such as confidentiality issues [13]. However, the concept of federated learning still requires a central entity handling the model parameters and thereby still concentrating power centrally. Moreover, since parameters are handled centrally, federated learning systems usually have a star-shaped architecture which clearly decreases fault tolerance. While federated learning addresses many important disadvantages of central and local AI solutions and is therefore a major area of research and development, it still harbours disadvantages that require further attention, particularly in medicine.

Before introducing the technical solution addressing most if not all disadvantages of local, central and federated learning models, let me conceptualise the requirements the medical domain would have for the technical solution providing AI to the highest standards. Such solution 1) would have to keep large medical data locally, completely decentralised and with the data owner to ensure that local data privacy regulations apply. 2) It would guarantee that raw data are not exchanged or stored on central cloud solutions and as a consequence also reduce data traffic. 3) It would provide a data infrastructure that provide the highest level of data security, confidentiality and privacy. 4) It would enable secure, fair and transparent onboarding of new members. 5) It would dismiss any central custodian as in federated learning to avoid any data or analysis monopoly. 6) All members of such a network would follow rules and regulations agreed on before any AI is started, such rules would be regulated by smart electronic contracts in a democratic fashion and with equal right for all members. 7) Lastly, the solution would have to protect the AI models from any attacks.

Based on these requirements, and in cooperation with a commercial IT provider (Hewlett Partner Enterprise, HPE), we have developed a technical

solution that can fulfil these criteria and together we tested the technical solution in medical use cases including chest x-rays as an example for commonly generated clinical data as well as blood transcriptomes, a very rich data space that we envision to become a very important data space for future medical applications. This solution was termed Swarm Learning as the idea of this AI concept is equality among participating partners as it is observed for members in a natural occurring swarm. We hypothesised that such structure would overcome most of the shortcomings of today's solutions, it would perfectly fit to the inherently decentral data structures in medicine and it would accommodate data security and privacy regulations as they apply to medical data. Swarm Learning builds on decentralised hardware infrastructure at the institutions where the data are generated, it contains standardised AI engines in container format that are easily to be installed on existing hardware infrastructures, it harbours a so-called permissioned blockchain, which is required for the smart electronic contract, the onboarding of members and during the dynamic process of electing leaders among the swarm members during the learning processes for each learning round. To ensure these processes to work seamlessly, Swarm Learning contains a special Swarm Learning library (SLL). Collectively, Swarm Learning is built around the concept to maximise trust and transparency in the development and application of AI-solutions for major medical questions.

How Can Swarm Learning Be Applied to Medical Research?

To test, whether the Swarm Learning concept is truly applicable to medicine, we defined several use cases and determined the performance of Swarm Learning in comparison to local and central AI models [14]. Starting with a large blood transcriptome dataset with more than 12,000 patient samples, we could clearly demonstrate that AI models trained in a Swarm Learning setting outperformed local models and where at par with central models, which would already strongly argue against further development of central models [14]. Furthermore, simulating different forms of bias, Swarm Learning could even outperform central models. To extend these promising results, we then went ahead and connected blood transcriptome data from patients with tuberculosis by Swarm Learning and clearly illustrated that the classifiers for tuberculosis or latent tuberculosis derived by Swarm Learning always outperformed local models and performed even better than central models. With these two use cases in mind

we asked, whether it would be even possible to identify patients with COVID-19 disease based on blood transcriptomes in a Swarm setting. One could imagine for the future that hospitals would be already connected via Swarm Learning technology and as soon as a hospital would experience a new infectious disease, parameters measured in the clinic could be locally assessed for a specific signature for the new disease and as soon as the next hospitals would experience similar cases, the swarm of jointly learning hospitals would grow continuously improving the identification of patients with the new infectious disease. By cooperating with several large hospitals in Germany, we simulated exactly such a scenario and could successfully demonstrate that Swarm Learning always outperformed individual members (local learning) and that the results became better and better with every new Swarm member entering the learning process [14].

With these use cases, we contributed the basic principles of how Swarm Learning can now be adapted to any medical data space and organisational setting. For example, a network of hospitals, for example all German university hospitals could be connected via Swarm Learning to develop novel biomarker or biomarker signature-based diagnostics. Indeed, in context of the Network University Medicine (NUM) in Germany as a response to the COVID-19 pandemic, we are currently evaluating, whether immune data from COVID-19 patients can be analysed in a much more efficient way, if forces between different hospitals are joined (Schultze, unpublished results). Another scenario could be the collaboration between large cancer centres across Europe. Yet another example would be data analysis within large European research consortia. Instead of moving all data to central data repositories with all its legal obligations, the data producer could keep their data locally and Swarm Learning could be used to develop AI-based algorithms based on novel biomarker signatures from high-resolution data.

The Way Forward

Certainly, it now will be important to showcase further examples of how Swarm Learning could be utilised in medicine to develop better diagnostics – AI-based diagnostics. Very recently, a group at the RWTH Aachen University has utilised the openly available Swarm Learning software and asked whether Swarm Learning could improve cancer histopathology [15]. It was demonstrated using multi-centric data of gigapixel histopathology images derived from over 5000 patients that AI models trained using Swarm Learning

predicted BRAF mutational status and microsatellite instability (MSI) directly from haematoxylin and eosin (H&E)-stained pathology slides of colorectal cancer (CRC). This is an independent illustration how powerful and how fast Swarm Learning can be applied to important diagnostic areas in medicine without the need of data sharing. The authors agree with us that Swarm Learning can be used to train distributed AI models for any histopathology image analysis tasks. Additional examples need to illustrate the value of Swarm Learning. Based on these positive early experience, it will be necessary to develop professional services that make it seamless to establish Swarm Learning nodes across a large number of institutions, and hospitals allowing this technology to be applied to daily medical work.

Even More Opportunities, from “Open Data” to “Open Insights”

There is another important area that needs further attention. Current developments in research mandate “Open Science”, “Open Data”, “Open Access” concepts, when it comes to medical data. The motivation and the idea behind this concept are rather simple. The more people can have access to the ever larger data produced, the better is the utilisation of existing data and the more we will learn from such data. As a side effect, cost-effectiveness of data production could be dramatically improved. While very appealing, this concept comes with a significant drawback, because it is often very difficult to sometimes even impossible to comply with data privacy regulations and it does not meet patient-physician privilege, the most important constituent of the physician–patient relationship. While sharing insights has always been a major part of medicine since the ancient times, sharing data from patients was always highly restricted, often even prohibited. There are very good reasons for this and only because today's technical solutions cannot really comply with these requirements is not a good argument to jeopardise the physician-patient relationship. However, with technological solutions such as Swarm Learning, there is a way out of the dilemma. “Open Science” can still be achieved, if one exchanges “Open Data” with “Open Insights”. And “Open Access” only needs to be newly interpreted as “Open Access to insights” instead to data. In fact, Swarm Learning is exactly supporting this shift. Instead of sharing data, Swarm Learning enables to share the insights from learning on the privately and locally held data. At least for medicine, I therefore strongly advocate to replace the current concept “Open Science”, “Open Data”, “Open Access”

with the new concept of “Open Science” by “Open Access to Insights”. Since data privacy is not only an issue in medicine but also in other areas, this concept might even be more widely applicable.

Summary and Outlook

In conclusion, Swarm Learning is a new concept that could democratise the use of AI by allowing everybody with a certain type of data to contribute to joined efforts to build AI-solutions with the highest quality particularly due to a largely increased data space within swarms of equal partners. The concept is not restricted to medicine, but it can be envisioned that many areas with highly private and valuable data will benefit. For example, Swarm Learning could foster Smart City concepts, security in Smart Energy Grids, joined learning in AI-based industry machines or in autonomous driving, to name only a few. For medicine, Swarm Learning could lead to democratisation and much broader participation of many physicians and medical institutions, when it comes to novel AI-based solutions to enable precision medicine approaches. As live-long learning is mandatory for physicians themselves, Swarm Learning could also enable such continuous learning for AI-solutions. Swarm Learning will make these processes very transparent, which will further support better medical diagnostics and therapies.

Disclosure Statement

The author has nothing to declare.

ORCID

Joachim L. Schultze  <http://orcid.org/0000-0003-2812-9853>

References

- [1] Rajkomar A, Dean J, Kohane I. Machine learning in medicine. *N Engl J Med.* 2019;380(14):1347–1358.
- [2] Stephens ZD, Lee SY, Faghri F, et al. Big data: astronomical or genomics? *PLoS Biol.* 2015;13(7):e1002195.
- [3] McCall B. What does the GDPR mean for the medical community? *Lancet.* 2018;391(10127):1249–1250.
- [4] Sovrano F, Vitali F, Palmirani M (2020). Modelling GDPR-compliant explanations for trustworthy AI. In *Electronic government and the information systems perspective: 9th international conference, EGOVIS 2020, Bratislava, Slovakia, Cham: Springer International Publishing*, September 14–17, 2020, pp. 219–233.
- [5] Obermeyer Z, Emanuel EJ. Predicting the future - big data, machine learning, and clinical medicine. *N Engl J Med.* 2016;375(13):1216–1219.

- [6] Rajewsky N, Almouzni G, Gorski SA, et al. LifeTime and improving European healthcare through cell-based interceptive medicine. *Nature*. 2020;587(7834):377–386.
- [7] Kaissis GA, Makowski MR, Rückert D, et al. Secure, privacy-preserving and federated machine learning in medical imaging. *Nat Mach Intell*. 2020;2(6):305–311.
- [8] LeCun Y, Bengio Y, Hinton G. Deep learning. *Nature*. 2015;521(7553):436–444.
- [9] Savage N. Machine learning: calculating disease. *Nature*. 2017;550:S115–S117.
- [10] Ping P, Hermjakob H, Polson JS, et al. Biomedical informatics on the cloud: a treasure hunt for advancing cardiovascular medicine. *Circ Res*. 2018;122(9):1290–1301.
- [11] Jones N. How to stop data centres from gobbling up the world's electricity. *Nature*. 2018;561(7722):163–166.
- [12] Konečný J, McMahan HB, Yu FX. Federated learning: strategies for improving communication efficiency . 2016. Accessed 30 December 2022. <https://arxiv.org/abs/1610.05492>. doi:10.48550/arXiv.1610.05492.
- [13] Shokri R, Shmatikov V (2015). Privacy-preserving deep learning. In 2015 53rd Annual Allerton Conference on Communication, Control, and Computing (Allerton) 29. September to 2. October, 2015. Allerton, (IEEE, 53,pp. 909–910. <https://ieeexplore.ieee.org/document/7447103>. doi:10.1109/ALLERTON.2015.7447103
- [14] Warnat-Herresthal S, Schultze H, Shastry KL, et al. Swarm Learning for decentralized and confidential clinical machine learning. *Nature*. 2021;594(7862):265–270.
- [15] Saldanha OL, Quirke P, West NP. Swarm learning for decentralized artificial intelligence in cancer histopathology *Nat Med*. 2021;28:1232–1239. doi:10.1038/s41591-022-01768-5. <https://www.nature.com/articles/s41591-022-01768-5>