European Spine Journal
https://doi.org/10.1007/s00586-024-08172-2

REVIEW ARTICLE

Preserving privacy in big data research: the role of federated learning in spine surgery

Hania Shahzad[1] · Cole Veliky[2] · Hai Le[3] · Sheeraz Qureshi[4] · Frank M. Phillips[5] · Yashar Javidan[3] · Safdar N. Khan[1]

Received: 27 November 2023 / Revised: 27 November 2023 / Accepted: 27 January 2024

Abstract

Purpose Integrating machine learning models into electronic medical record systems can greatly enhance decision-making, patient outcomes, and value-based care in healthcare systems. Challenges related to data accessibility, privacy, and sharing can impede the development and deployment of effective predictive models in spine surgery. Federated learning (FL) offers a decentralized approach to machine learning that allows local model training while preserving data privacy, making it well-suited for healthcare settings. Our objective was to describe federated learning solutions for enhanced predictive modeling in spine surgery.

Methods The authors reviewed the literature.

Results FL has promising applications in spine surgery, including telesurgery, AI-based prediction models, and medical image segmentation. Implementing FL requires careful consideration of infrastructure, data quality, and standardization, but it holds the potential to revolutionize orthopedic surgery while ensuring patient privacy and data control.

Conclusions Federated learning shows great promise in revolutionizing predictive modeling in spine surgery by addressing the challenges of data privacy, accessibility, and sharing. The applications of FL in telesurgery, AI-based predictive models, and medical image segmentation have demonstrated their potential to enhance patient outcomes and value-based care.

Keywords Machine learning · Federated learning · Spine surgery

Introduction

The integration of machine learning (ML) models into electronic medical record (EMR) systems has the potential to significantly improve healthcare outcomes and value-based care. ML models have proven effective in analyzing large datasets and providing valuable insights into various domains in spine surgery [1]. Notably, predictive modeling in spine surgery has revealed associations between Medicaid recipients, infections, pulmonary and neurological disorders, and insurance type, with higher rates of adverse events [2–4]. ML models have also demonstrated effectiveness in predicting sustained opioid use based on factors such as preoperative opioid use, antidepressant medication use, and insurance status [5–8]. Moreover, in cases of spinal metastases and epidural abscesses, ML has successfully identified age, laboratory parameters, and comorbidities as predictors of mortality, enhancing risk stratification and clinical decision-making in spine surgery [9–12]. In the context of spine surgery, predictive modeling has revealed associations between demographic factors, comorbidities, and adverse events.

The implementation of predictive modeling faces challenges in acquiring large and diverse databases necessary for training artificial intelligence (AI) models. Health data, subject to strict regulations due to its sensitivity, are challenging to obtain. Anonymization techniques, though employed, may not provide comprehensive protection of patient privacy as identifiable information can be reconstructed from imaging data. Additionally, the collection and curation of high-quality datasets demands significant time, effort, and expenses, limiting

✉ Safdar N. Khan
safkhan@ucdavis.edu

1 Department of Orthopaedics, UC Davis Medical Center, Sacramento, CA, USA

2 Ohio State College of Medicine, The Ohio State University, Columbus, OH, USA

3 UC Davis Medical Center, Sacramento, CA, USA

4 Hospital for Special Surgery, New York City, NY, USA

5 Rush University Medical Center, Chicago, IL, USA

Published online: 25 February 2024

their availability. Data collectors often retain control over their valuable data, hindering systematic sharing. These limitations concerning data accessibility and privacy pose obstacles to the development and deployment of effective predictive models in spine surgery.

Federated learning (FL), an ML concept, offers a solution to the challenges of data governance, privacy, and sharing in healthcare. It utilizes decentralized data collection to safeguard sensitive information. The approach allows local model training while only transferring model configurations, ensuring that data remain within the institution's secure boundaries. Initially proposed by Google for mobile devices, FL has found applications in various domains, such as autocorrect, where it learns speech patterns and common queries without personal data leaving the users' devices. Recent research has demonstrated that FL models achieve performance levels comparable to centrally hosted datasets, outperforming models trained on isolated single-institutional data [13].

This article aims to explore the concept of FL and review the literature concerning its potential applications, and the challenges of implementing it in orthopedic spine surgery.

Methods

The authors searched PubMed, Google Scholar, Embase, and popular media to ensure the novelty of this narrative review. Subsequently, these search engines were used to find papers pertaining to federated learning, federated learning in healthcare, federated learning in surgery, data privacy in federated learning, machine learning, machine learning in healthcare, and machine learning in orthopedics, telesurgery, and in spine surgery. Articles detailing concerns and impediments to the uptake of FL and ML in healthcare, as well as any future applications, were sought out. The authors did not adhere to a strict methodology in their search of the literature, with no strict inclusion or exclusion criteria for the subject material. This paper is meant to focus on FL and ML on the subject of spine surgery, an area that the authors believe represents many potential future applications for FL. The lack of attention thus far paid to this topic precludes a systematic search of the literature due to the absence of sufficient studies on it. The studies included were those that aided the authors in demonstrating a qualitative description of FL and bringing it from a more obscure position to a much larger audience in the orthopedic spine community.

Principles of federated learning

The usual ML model implements one central server that receives data from all data owners involved in collaboration and uses that data for model building and training [14]. This requires all data owners to send large quantities of raw data off-site to this central server. In FL, each data owner has a local ML model, which they train using their raw data, which develops an update that has been stripped of identifiable information. These updates are sent to the central server; the central server receives all the updates from each local ML model and compiles a weighted average from each local update [15]. This weighted average is an aggregate known as the consensus model or the global model, which serves as the latest update from the centralized server to the local models for future use. Each time the local models undergo on-site training, they send their updates to the centralized server, and the updates are combined to form the latest system-wide update, which is referred to as a federated round [15]. The principle of FL is to continue performing these federated rounds, improving the accuracy of the system at each iteration, without any sharing of sensitive information (Table 1).

Applications of federated learning in orthopedic surgery

Telesurgery, also known as remote surgery, has become popular in spine surgery for its cost-effectiveness and time-saving benefits. Surgical robotics for spine surgery, including da Vinci, SpineAssist, Renaissance, and Mazor X, have been approved for telesurgery in spine procedures. These robots offer improved visualization, precision, and accuracy, resulting in reduced hospital stays, decreased radiation exposure, and favorable learning curves [16]. Since they are digitally operated, they have the potential to be used to perform remote surgeries. However, these telesurgery systems are vulnerable to security and privacy attacks due to the use of traditional communication platforms. These attacks could include potentially redirecting surgical robot movement or manipulating feedback, which poses risks to patient safety and raises questions about ethical standards in medicine concerning risk-taking [17]. To enhance the security and confidentiality of patient health data, FL models can be utilized. This approach allows for the selective sharing of specific information while maintaining overall data privacy. In the FL paradigm, the collected data from sensors and actuators are transmitted to a privacy-enhancing layer. Data cleaning is performed on confidential patient data to address missing or imbalanced values, ensuring that only specific patients' health information is visible to external parties, thus enhancing security and trust. The FL paradigm involves local and global models, allowing the switch to a local model for training while processing data at the global model. This distribution of processing tasks avoids system overload and facilitates efficient communication between patients and doctors.

Table 1 Federated learning in spine surgery: summary table of applications, challenges, and solutions for enhanced predictive modeling

Applications	Challenges	Federated learning solutions
Telesurgery, including remote spine procedures with surgical robots	Vulnerability to security and privacy attacks through traditional communication platforms, risking patient safety and ethical concerns	Selective sharing of specific information while maintaining overall data privacy Privacy-enhancing layer for transmitted data from sensors and actuators Data cleaning to address missing or imbalanced values in confidential patient data Distribution of processing tasks between local and global models to avoid system overload and facilitate efficient communication
AI*-based predictive modeling in spine surgery to enhance accuracy in predicting various outcomes	Potential threats to data privacy when using AI in predictive modeling. Exploitation of vulnerabilities in data-sharing systems, risking control over critical systems and compromising patient privacy	Implementation of FL paradigms with secure aggregation to combine data securely without direct interaction Using Gaussian mechanism to add noise to individual data points to protect data details Ensuring the central server remains unaware of specific data being processed Enhancing privacy, security, and efficiency in collaboration between healthcare institutions
Autonomous segmenting in spine surgery to automatically identify and outline anatomical structures without manual intervention	Challenges in developing reliable and accurate models for segmenting vertebral bodies, including methods requiring manual intervention or providing rough segmentations, as well as limited data availability and GDPR* restrictions	Utilization of FL in training spine segmentation models at local institutions using patient MRI data Periodic submission of model configurations to a central server for aggregation into a global model Iterative process until satisfactory performance is achieved Improving accuracy of segmenting vertebral bodies while preserving patient privacy Advancing medical image analysis

*_AI_ artificial intelligence, _GDPR_ general data protection regulation

AI has emerged as a promising tool in enhancing predictive accuracy in spine surgery compared to traditional statistical modeling. A comprehensive review of the literature highlighted a wide range of studies that have utilized ML algorithms to predict various important outcomes in spine surgery, including patient-reported outcome measures (PROMs), complications, discharge disposition, length of hospital stay, readmission rates, mortality rates, and prolonged opioid use, among others [1]. These AI models can potentially improve with the availability of more data in the field of spine surgery [18]. However, several studies have highlighted potential threats to data privacy when using AI in predictive modeling. Hackers can exploit vulnerabilities in systems that share data with collaborators, enabling them to gain control over critical systems like wearable devices storing medical information and the decision-making processes of robots [18]. To address these concerns, FL paradigms employ secure aggregation, allowing different parties to combine their data securely without direct interaction. Furthermore, to enhance privacy, a method called the distributed Gaussian mechanism adds noise to each data point, protecting the details of the data. This also ensures that the central server remains unaware of specific data being processed. These proposed methods enhance privacy by leveraging FL paradigms. They provide a high level of security against advanced attacks using quantum computers, and they are also accurate and efficient [18]. This allows for a safe and secure collaboration between different healthcare institutions without compromising patient privacy, enhancing the performance of AI models [19].

Autonomous segmenting is the ability of a system or algorithm to automatically identify and separate specific objects or structures in an image or dataset without human intervention. In the context of spine surgery, it means that AI methods can accurately identify and outline anatomical structures without the need for manual input from surgeons or healthcare professionals. Despite previous investigations into spine MRI segmentation [20], further research is warranted due to the challenges posed by the repeatability of vertebral morphology, the variability in image acquisition parameters, and the anatomical differences between normal and pathological conditions [21]. However, there are two challenges in developing a reliable and accurate model for segmenting vertebral bodies: (1) Some methods require manual intervention and provide rough segmentations, while others offer fine segmentations but take more time and (2) limited data from a single medical institution and general data protection regulation (GDPR) restrictions hinder data transmission. To overcome this, researchers propose using FL. In this approach, each institution trains its spine segmentation model using its patient MRI data and periodically submits the model configurations to a central server. The server combines these contributions to create a global model, which is then distributed back to the institutions. This iterative process continues until the model achieves satisfactory performance. By leveraging FL, this method improves the accuracy of segmenting vertebral bodies while preserving patient privacy, advancing the field of medical image analysis [22].

In the context of spine surgery, FL models can be applied using data partitioning methods. Consider multiple hospitals or clinics specializing in different aspects of spine health, such as spinal surgery, physical therapy, and radiology, collaborating to develop a machine learning model for predicting surgical outcomes or assessing patient risk factors. Horizontal FL in spine surgery would involve hospitals sharing the same set of patient data (sample space) but having different features or attributes for each patient [23]. For instance, one hospital might provide surgical data, another might provide physical therapy records, and a third might provide radiological images. By collaboratively training a model on this horizontally partitioned data, insights could be gained into the relationships between surgical procedures, postoperative recovery, and diagnostic images. Vertical FL, on the other hand, would occur when different healthcare providers have access to the same set of features, but their patient datasets differ [23]. For example, multiple hospitals in different locations might have patient records with the same attributes, allowing for a collective analysis of the data to detect patterns or trends in spine health that might be specific to different geographic regions.

Additionally, federated transfer learning could be applied when a hospital and an implant company aim to jointly build a machine learning model to assess the outcomes of certain implants or osteobiologics. In this scenario, the implant or osteobiologics company could provide data related to its usage, while the hospital contributes patient outcome data. This collaborative effort would enable the development of a model that assesses the safety and efficacy of interventions in spine surgery while respecting the privacy and data ownership of each entity involved.

Challenges and limitations

Integrating medical datasets into public databases enables broader research but may result in the loss of data ownership for the collaborators involved. Successful model training relies on various factors, including data collection methods, data labeling, quality, bias, and standardization, which are challenges inherent to all predictive modeling methods [24]. However, granting more researchers and crowdfunding workers access to databases for data annotation can help address these issues. Implementing appropriate protocols such as well-designed studies, standardized data extraction, labeling, and annotation procedures,

accuracy assessments, quality management, and continuous updates is crucial to mitigating these challenges and addressing biases or failures. In this context, FL provides a viable solution to overcome limitations in data transfer between institutions.

Future directions

Federated learning in healthcare will see tremendous growth in the coming years. Models geared toward exploring complex relationships among various spinal conditions, procedures, and their outcomes (vertical FL), as well as those eliminating the need for a trusted server to enhance privacy preservation (decentralized FL), require further investigation to facilitate their implementation in future real-world FL projects [15]. Strategies to enhance privacy preservation in FL-based models also need improvement. The three most popular methods used for privacy preservation in FL are homomorphic encryption, secure multiparty computation, and differential privacy [25]. Homomorphic encryption acts as a protective layer, allowing encrypted patient data to be analyzed without exposing sensitive information. MPC provides a confidential platform for multiple healthcare institutions to collaborate, sharing only necessary data for research without revealing complete patient records. Differential privacy is a mechanism in which a small amount of random noise is added to any data to perturb its value. Among the three approaches, differential privacy is widely used in real-time applications due to its scalability and lower overhead compared to the other two.

Conclusion

Federated learning shows great promise in revolutionizing predictive modeling in spine surgery by addressing the challenges of data privacy, accessibility, and sharing. The applications of federated learning in telesurgery, AI-based predictive models, and medical image segmentation have demonstrated their potential to enhance patient outcomes and value-based care. However, careful consideration of infrastructure, data quality, and standardization is essential for successful implementation. Future research should focus on further optimizing federated learning approaches and promoting collaborations for the advancement of orthopedic spine surgery.

Funding No funding was received for this study.

Declarations

Conflict of interest The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

1. Malik AT, Khan SN (2019) Predictive modeling in spine surgery. Ann Transl Med 7:S173. https://doi.org/10.21037/atm.2019.07.99
2. Han SS, Azad TD, Suarez PA, Ratliff JK (2019) A machine learning approach for predictive models of adverse events following spine surgery. Spine J 19:1772–1781. https://doi.org/10.1016/j.spinee.2019.06.018
3. Goyal A, Ngufor C, Kerezoudis P, McCutcheon B, Storlie C, Bydon M (2019) Can machine learning algorithms accurately predict discharge to nonhome facility and early unplanned readmissions following spinal fusion? analysis of a national surgical registry. J Neurosurg Spine. https://doi.org/10.3171/2019.3.SPINE181367
4. Kim JS, Merrill RK, Arvind V, Kaji D, Pasik SD, Nwachukwu CC, Vargas L, Osman NS, Oermann EK, Caridi JM, Cho SK (2018) Examining the ability of artificial neural networks machine learning models to accurately predict complications following posterior lumbar spine fusion. Spine 43:853–860. https://doi.org/10.1097/BRS.0000000000002442
5. Martin BI, Turner JA, Mirza SK, Lee MJ, Comstock BA, Deyo RA (2009) Trends in health care expenditures, utilization, and health status among US adults with spine problems, 1997–2006. Spine 34:2077–2084. https://doi.org/10.1097/BRS.0b013e3181b1fad1
6. Kalakoti P, Hendrickson NR, Bedard NA, Pugely AJ (2018) Opioid utilization following lumbar arthrodesis: trends and factors associated with long-term use. Spine 43:1208–1216. https://doi.org/10.1097/BRS.0000000000002734
7. Karhade AV, Ogink PT, Thio QCBS, Cha TD, Gormley WB, Hershman SH, Smith TR, Mao J, Schoenfeld AJ, Bono CM, Schwad JH (2019) Development of machine learning algorithms for prediction of prolonged opioid prescription after surgery for lumbar disc herniation. Spine J 19:1764–1771. https://doi.org/10.1016/j.spinee.2019.06.002
8. Karhade AV, Ogink PT, Thio QCBS, Broekman MLD, Cha TD, Hershman SH, Mao J, Peul WC, Schoenfeld AJ, Bono CM, Schwab JH (2019) Machine learning for prediction of sustained opioid prescription after anterior cervical discectomy and fusion. Spine J 19:976–983. https://doi.org/10.1016/j.spinee.2019.01.009
9. Karhade AV, Shah AA, Bono CM, Ferrone ML, Nelson SB, Schoenfeld AJ, Harris MB, Schwab JH (2019) Development of machine learning algorithms for prediction of mortality in spinal epidural abscess. Spine J 19:1950–1959. https://doi.org/10.1016/j.spinee.2019.06.024
10. Shah AA, Karhade AV, Bono CM, Harris MB, Nelson SB, Schwab JH (2019) Development of a machine learning algorithm for prediction of failure of nonoperative management in spinal epidural abscess. Spine J 19:1657–1665. https://doi.org/10.1016/j.spinee.2019.04.022
11. Karhade AV, Thio Q, Ogink PT, Shah AA, Bono CM, Oh KS, Saylor PHJ, Schoenfeld AJ, Shin JH, Harris MB, Schwab JH (2019) Development of machine learning algorithms for prediction of 30-day mortality after surgery for spinal metastasis. Neurosurgery 85:E83–E91. https://doi.org/10.1093/neuros/nyy469
12. Karhade AV, Thio Q, Ogink PT, Bono CNM, Ferrone ML, Oh KS, Saylor PJ, Schoenfeld AJ, Shin JH, Harris MB, Schwab JH (2019) Predicting 90-day and 1-year mortality in spinal metastatic

disease: development and internal validation. Neurosurgery 85:E671–E681. https://doi.org/10.1093/neuros/nyz070
13. Lee GH, Park J, Kim J, Kim Y, Choi B, Park RW, Rhee SY, Shin S-Y (2023) Feasibility study of federated learning on the distributed research network of OMOP common data model. Healthc Inform Res 29:168–173. https://doi.org/10.4258/hir.2023.29.2.168
14. Sheller MJ, Reina GA, Edwards B, Martin J, Bakas S (2019) Multi-institutional deep learning modeling without sharing patient data: a feasibility study on brain tumor segmentation. Brainlesion 11383:92–104. https://doi.org/10.1007/978-3-030-11723-8_9
15. Narmadha K, Varalakshmi P (2022) Federated learning in healthcare: a privacy preserving approach. Stud Health Technol Inform 294:194–198. https://doi.org/10.3233/SHTI220436
16. Vadalà G, De Salvatore S, Ambrosio L, Russo F, Papalia R, Denaro V (2020) Robotic spine surgery and augmented reality systems: a state of the art. Neurospine 17:88–100. https://doi.org/10.14245/ns.2040060.030
17. Chaudjary S, Kakkar R, Gupta R, Tanwar S, Agrawal S, Sharma R (2022) Blockchain and federated learning-based security solutions for telesurgery system: a comprehensive review. Turk J Electr Eng Comput Sci 30(7):2446–2488. https://doi.org/10.55730/1300-0632.3950
18. Saravi B, Hassel F, Ülkümen S, Zink A, Shavlokhova V, Couillard-Despres S, Boeker M, Obid P, Lang GM (2022) Artificial intelligence-driven prediction modeling and decision making in spine surgery using hybrid machine learning models. J Pers Med 12:509. https://doi.org/10.3390/jpm12040509
19. Hao M, Li H, Luo X, Xu G, Yang H, Liu S (2020) Efficient and privacy-enhanced federated learning for industrial artificial intelligence. IEEE Trans Industr Inf 16:6532–6542. https://doi.org/10.1109/TII.2019.2945367
20. Darwish AA, Salem MAM, Hegazy D, Ebeid HM (2015). Vertebrae segmentation techniques for spinal medical images. In: 2015 IEEE seventh international conference on intelligent computing and information systems (ICICIS), Cairo, Egypt. https://doi.org/10.1109/IntelCIS.2015.7397206.
21. Rak M, Tönnies KD (2016) On computerized methods for spine analysis in MRI: a systematic review. Int J CARS 11:1445–1465. https://doi.org/10.1007/s11548-016-1350-2
22. Liu J, Liang X, Yang R, Luo Y, Lu H, Li L, Zhang S, Yanbg S (2022) Federated learning-based vertebral body segmentation. Eng Appl Artif Intell. https://doi.org/10.1016/j.engappai.2022.105451
23. Yang Q, Liu Y, Chen T, Tong Y (2019) Federated machine learning. ACM Trans Intell Syst Technol 10:1–19. https://doi.org/10.1145/3298981
24. Wang F, Casalino LP, Khullar D (2019) Deep learning in medicine-promise, progress, and challenges. JAMA Intern Med 179:293–294. https://doi.org/10.1001/jamainternmed.2018.7117
25. Wei K, Li J, Ding M, Ma C, Yang HH, Farokhi F, Jin S, Quek TQS, Poor HV (2020) Federated learning with differential privacy: algorithms and performance analysis. IEEE Trans Inf Forensics Secur 15:3454–3469. https://doi.org/10.1109/TIFS.2020.2988575