The Contribution of Federated Learning to AI Development

Shijia Huang *, Su Diao , Huayu Zhao , Lidong Xu

Posted Date: 5 July 2024

doi: 10.20944/preprints202407.0551.v1

Keywords: Federation Learning; Privacy; Edge Artificial Intelligence; Medical Artificial Intelligence

Article

The Contribution of Federated Learning to Ai Development

Shijia Huang [1], Su Diao [2], Huayu Zhao [3] and Lidong Xu [4]

[1] Applied Science, Columbia University,New York, 1002 and USA
[2] Industrial & Systems Engineering, Auburn University, Auburn, Alabama, The United States,36849
[3] Electrical Automation Design, Beijing Shougang International Engineering Technology ,Co., Ltd, 100043, China
[4] Graziadio Business School, Pepperdine University, 24255 Pacific Coast Hwy, Malibu, CA 90263
* Correspondence: m24296170@gmail.com

Abstract: With the widespread application of artificial intelligence technology in various industries, users' attention to privacy and data security has increased significantly. Federated learning, as a new technology paradigm combining privacy-enhanced computing and artificial intelligence, resolves the contradiction between data security and open sharing. This paper presents the benefits of federated learning in terms of privacy, real-time processing, model robustness, compliance and cross-industry applications. At the same time, when combined with Edge AI technology, federated learning promotes the decentralisation of intelligent systems, improving data privacy protection and model accuracy. This paper also discusses the application cases of federated learning in the medical field, through local data processing and model training, effectively protecting user privacy, realizing medical data sharing and model optimization, and promoting the development of artificial intelligence.

Keywords: federation learning; privacy; edge artificial intelligence; medical artificial intelligence

1. Introduction

As artificial intelligence (AI) technologies are increasingly applied across various industries, concerns about user privacy and data security have grown significantly. Users are particularly worried about whether their private information is being used without permission for commercial or other purposes, and even being misused. The implementation of relevant laws and regulations has led to significant penalties for many internet and financial institutions due to user data breaches. Concurrently, national policies emphasize the need to explore and establish secure standards for the circulation of data elements. This indicates that in a regulatory tightening environment, organizations are becoming more cautious about data collection, circulation, and application. Simultaneously, there is a continuous push towards the open sharing of data elements.

Federated learning, a new technological paradigm that combines privacy-enhancing computation with artificial intelligence, emerges as a crucial solution to the conflict between data security and open sharing. In federated learning, clients can use local data on their devices to train models and then upload encrypted model parameters. These parameters are aggregated to update and optimize the prediction model without exposing individual data points. Wang et al. 's research focuses on the detection and classification of AI-generated text based on BERT deep learning algorithms. They propose a novel method for efficient recognition and classification of AI-generated text by using BERT model for deep learning feature extraction and classification of generated text. The results show that the proposed method exhibits high accuracy and efficiency in text detection and classification tasks, and provides an effective solution to the challenge of text generation by artificial intelligence.

 doi:10.20944/preprints202407.0551.v1

This method ensures that data privacy is maintained while enabling collaborative model improvement. As a result, federated learning addresses the dual needs for data security and open data sharing, significantly contributing to the advancement of AI development.

2. Related Work

Edge AI and Federated Learning are two revolutionary technologies that together drive the decentralization of intelligent systems and the advancement of data privacy. The combination of edge AI and federated learning provides a powerful synergy that enables smart devices not only to do real-time data processing locally, but also to continuously optimize their intelligent algorithms through collaborative learning while protecting privacy. The combination of these two technologies has created unprecedented opportunities and challenges for various industries.

(1) Federated Learning

Federated Learning is an innovative machine learning technique that protects user privacy by training algorithms distributed across multiple devices without the need to share data.

Data Privacy and security: One of the core strengths of Federated Learning is enhanced data privacy. Since the data does not leave its original device, only model updates (not the original data) are sent to the central server for aggregation, thus greatly reducing the risk of data breaches or unauthorized access.

Real-time and bandwidth efficiency: In federated learning, data is processed on local devices and there is no need to transfer large amounts of data to the cloud or a central server. This not only reduces communication costs and latency, but also increases processing speed so that decisions can be made more quickly and in real time.

Robustness and generalization of models: Because federated learning can be performed on a wide variety of devices and data sets, it allows the model to learn more diverse data features, which helps to improve the model's generalization and robustness.An article authored by Wang, Hao et al delves into the realm of detecting and classifying AI-generated text through the utilization of BERT deep learning algorithms. BERT, standing for Bidirectional Encoder Representations from Transformers, stands as a state-of-the-art model in the domain of natural language processing, boasting exceptional semantic understanding and representation capabilities. The primary objective of their research is to tackle the prevalent issue of identifying and categorizing AI-generated text, spurred by the escalating dissemination of misinformation and objectionable content.

Through fine-tuning and optimizing the BERT algorithm, the research team has engineered an efficient system for text detection and classification. This system exhibits the ability to accurately discern and differentiate AI-generated text amidst diverse textual data. The outcomes of their experiments underscore the system's commendable performance in the realm of detecting and categorizing AI-generated text. This technological advancement holds significant promise in offering crucial support in addressing challenges pertaining to information security and content audit.

Compliance and adaptability: Federal learning supports data processing and model training in compliance with regional regulations and policies, especially in regions with strict data protection laws, such as the EU's GDPR.

Applications across verticals: Applications of federated learning span multiple industries, including healthcare, financial services, smart manufacturing, agriculture, and more. In these areas, federated learning not only improves operational efficiency, but also enhances the quality of service by optimizing the decision-making process.

Collaboration and shared intelligence: Without directly sharing data, different organizations can work together to train more powerful and intelligent models. This collaborative approach fosters knowledge sharing and innovation while protecting the data privacy of all parties.

(2) Edge AI (Edge AI)

 doi:10.20944/preprints202407.0551.v1

The synergy of Edge AI and Federated Learning is one of the major innovations in modern technology, which together drive the decentralization of intelligent systems and the protection of data privacy.

The combination of real-time intelligent decision making and privacy protection: Edge AI devices can perform real-time data processing and initial model training locally, and through federated learning, these devices can jointly optimize and update the global AI model without sharing specific data.

Enhanced data security and model accuracy: The structure of federated learning ensures data privacy, while the real-time processing capabilities of edge AI improve model responsiveness and accuracy.

- Expansion of cross-industry applications: This combination of technologies is widely used in healthcare, smart agriculture, autonomous vehicles and many other fields, improving operational efficiency and optimizing decision-making processes.

In healthcare, for example, wearables use edge AI to monitor a patient's health status in real time and conduct preliminary analysis, and federated learning allows these devices to jointly optimize disease diagnosis models without sharing patient-specific data. In smart agriculture, agricultural drones use edge AI to analyze crop health in real time, while federal learning enables agricultural cooperatives in different regions to work together to train and optimize crop management models.

3. Applications of Federated Learning in Artificial Intelligence

In federated learning, there is usually a central server and multiple clients. The central server coordinates the training process and does not touch the client's data. The client is responsible for training the model on local data and sending the trained parameter updates or gradient information to the central server. Once the update information is collected by the central server, it is aggregated and then a global model update is generated and distributed to all clients. The client then applies these updates to its own model for the next round of training.

1. Application of federated learning to medical models

Data privacy protection: Medical data often contains sensitive information such as a patient's personal identity and health records. Federated learning ensures data privacy and security through local data processing and model training.

Data sharing, Federal learning allows multiple healthcare organizations to share not the raw data, but the results of model training, without disclosing their respective data, thereby improving the generalization and accuracy of the model.

By integrating data from different medical institutions, Federated Learning is able to train more robust and accurate medical models, which are important for the diagnosis, treatment and prevention of disease.

Federated learning aims to solve the problem of data protection and data silos by allowing the sharing of data to train the model under the premise of ensuring security and privacy. Through these methods, federated learning can realize the sharing of data and the training of the model without sharing the original data, thus promoting the development of artificial intelligence while protecting the privacy of users.

2. The application of federated learning to medical imaging

In medical AI, the most valuable information that can bring to the model is usually the medical image. At present, the medical imaging methods used in clinic mainly include ultrasound, X-ray, computed tomography, nuclear magnetic resonance and so on. Current medical image datasets typically include only a few hundred pieces of relevant data, which can be trained in deep learning models through methods such as data augmentation, but can face conditions such as inadequate coverage when used as a real-world medical diagnosis.

Pulmonary nodules refer to thunder stars or irregular lesions less than or equal to 3cm in the lung, with imaging manifestations of increased density shadows. Pulmonary nodules with different density have different malignant probabilities. According to the density of nodules, pulmonary

 doi:10.20944/preprints202407.0551.v1

nodules are divided into three categories: solid nodules, partially solid nodules and ground glass nodules.

The pathogenesis of pulmonary nodules is also affected by a variety of factors, including benign and malignant, malignant early hidden, if not early intervention, its rapid course of disease, strong malignancy, poor prognosis, correct judgment of benign and malignant is conducive to correct treatment.

3. Case Study

The goal of this case is to identify the probability of a given user having a malignant lung nodule from a CT dataset of the user's lungs. The model is divided into two parts, the decibel is the lung nodule detection model and the classification model.

Lung nodule detection model: Aiming at the recognition problem of 3D medical images, a 3D convolutional neural network was designed to detect the location of lung nodule. The whole network structure is mainly composed of convolutional layer, residual structure and deconvolution layer. The model will output images of candidate lung nodule regions.

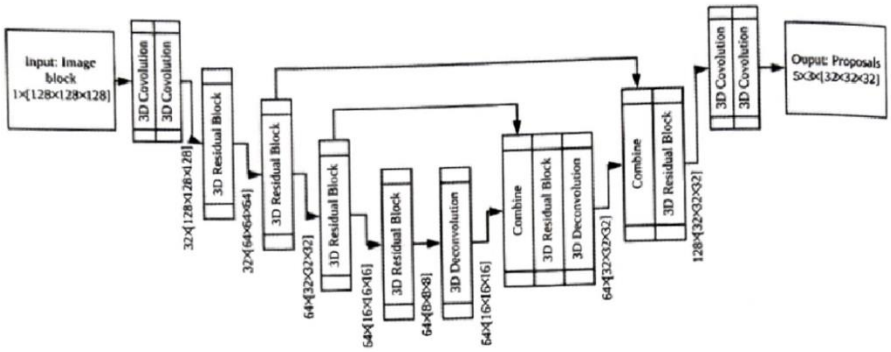

Figure 1. Composition of federated learning residual structure and deconvolution layer.

Classification model: After obtaining the candidate lung nodule region, the next step is to determine whether the current user has a benign or malignant lung nodule. To this end, the images of the top 5 candidate nodule regions obtained from each user's CT images were first re-introduced into the lung nodule detection model, and the output of the last convolutional layer was taken as the feature representation of each candidate region and brought into the fully connected layer to obtain the probability of malignant lung nodules, as shown in the figure:

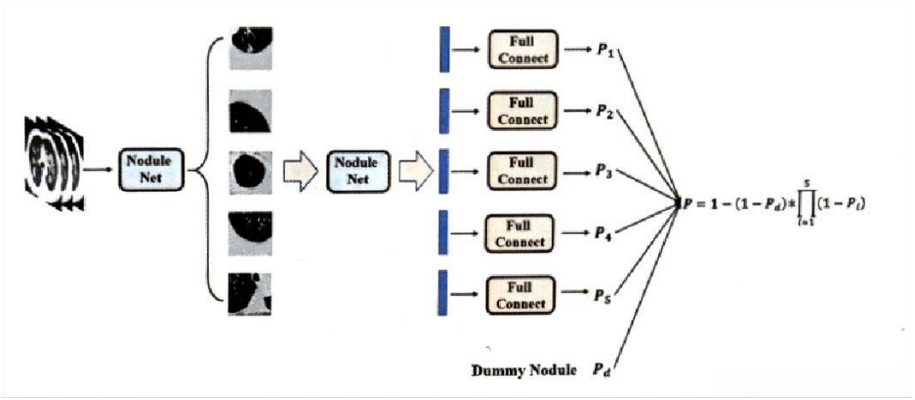

Figure 2. Effects of federated learning in medical imaging.

The biggest challenge of medical artificial intelligence is that the data between medical institutions can not be interoperable, and the amount of data in any hospital (or data center) is limited, forming a lot of "data islands", large and small. We can use the federal learning technology to learn the model without data leaving the data center, and provide a privacy and secure computing environment for the medical field in the case of or close to the data concentration, so that all parties

 doi:10.20944/preprints202407.0551.v1

can improve system efficiency and expand the application of medical artificial intelligence under the premise of protecting user privacy and information security.

4. Conclusions

With the rapid development of artificial intelligence technology, federated learning as an innovative data processing and model training method provides an effective way to resolve the contradiction between data security and open sharing. By protecting user privacy, enabling real-time processing, and improving model robustness and compliance, federated learning breathes new life into the development of intelligence across industries. At the same time, when combined with edge AI technology, federated learning promotes the decentralisation of intelligent systems, making an important contribution to protecting privacy and improving model accuracy. In the medical field, the application of federated learning provides viable solutions for secure medical data sharing and model optimisation, promoting the development of medical artificial intelligence and bringing more hope and opportunities for human health.

In conclusion, federated learning is particularly important in the current context of data security and open sharing. By protecting data privacy, enabling the decentralisation of intelligent systems, and facilitating collaboration between institutions, federated learning provides a viable solution for the sustainable development of AI. With the continuous development of technology and the expansion of application scenarios, federated learning will play an increasingly important role in various fields and make a greater contribution to the progress of artificial intelligence technology and the development of society.

References

1. Wang, Hao, Jianwei Li, and Zhengyu Li. "AI-Generated Text Detection and Classification Based on BERT Deep Learning Algorithm." arXiv preprint arXiv:2405.16422 (2024).
2. Wang, Hao, Jianwei Li, and Zhengyu Li. "AI-Generated Text Detection and Classification Based on BERT Deep Learning Algorithm." arXiv preprint arXiv:2405.16422 (2024).
3. Yang, Jing, et al. "Optimizing diabetic retinopathy detection with inception-V4 and dynamic version of snow leopard optimization algorithm." *Biomedical Signal Processing and Control* 96 (2024): 106501.
4. Lai, Songning, et al. "FTS: A Framework to Find a Faithful TimeSieve." *arXiv preprint arXiv:2405.19647* (2024).
5. Liang, Hao, et al. "Progression in immunotherapy for advanced prostate cancer." *Frontiers in Oncology* 13 (2023): 1126752.
6. Hu, Liyong, et al. "Laparoscopic pyelotomy combined with ultrasonic lithotripsy via a nephroscope for the treatment of complex renal stones." *Urolithiasis* 52.1 (2024): 22.
7. Chen, Jiexiao. "School Reforms for Low-Income Students Under Conflict Theory." *Journal of Advanced Research in Education* 3.3 (2024): 36-44.
8. Li, Bohang, et al. "A Feature Extraction Method for Daily-periodic Time Series Based on AETA Electromagnetic Disturbance Data." *Proceedings of the 2019 4th International Conference on Mathematics and Artificial Intelligence*. 2019.
9. Zhou, C., Zhao, Y., Cao, J., Shen, Y., Gao, J., Cui, X., ... & Liu, H. (2024). Optimizing Search Advertising Strategies: Integrating Reinforcement Learning with Generalized Second-Price Auctions for Enhanced Ad Ranking and Bidding. *arXiv preprint arXiv:2405.13381*.
10. Liang, Hao, et al. "Development and validation of a predictive model for the diagnosis of bladder tumors using narrow band imaging." *Journal of Cancer Research and Clinical Oncology*149.17 (2023): 15867-15877.
11. Wantlin, K., Wu, C., Huang, S. C., Banerjee, O., Dadabhoy, F., Mehta, V. V., ... & Rajpurkar, P. (2023). Benchmd: A benchmark for modality-agnostic learning on medical images and sensors. *arXiv preprint arXiv:2304.08486*.
12. Liu, Y., Yang, H., & Wu, C. (2023). Unveiling patterns: A study on semi-supervised classification of strip surface defects. *IEEE Access*, *11*, 119933-119946.
13. Restrepo, David, et al. "DF-DM: A foundational process model for multimodal data fusion in the artificial intelligence era." *Research Square* (2024).
14. Shovestul, Bridget, et al. "Social affective forecasting and social anhedonia in schizophrenia-spectrum disorders: a daily diary study." *Schizophrenia* 8.1 (2022): 97.

15. Du, Yanfei, et al. "Diagnostic value of routine Ultrasonography combined with ultrasound Elastography for papillary thyroid Microcarcinoma: A protocol for systematic review and meta-analysis." *Medicine* 100.4 (2021): e23905.
16. Restrepo, David, et al. "Multimodal Deep Learning for Low-Resource Settings: A Vector Embedding Alignment Approach for Healthcare Applications." *medRxiv* (2024): 2024-06.
17. Wu, Chenwei, et al. "De-identification and Obfuscation of Gender Attributes from Retinal Scans." *Workshop on Clinical Image-Based Procedures*. Cham: Springer Nature Switzerland, 2023.
18. Nakayama, L. F., Choi, J., Cui, H., Gilkes, E. G., Wu, C., Yang, X., ... & Celi, L. A. (2023). Pixel Snow and Differential Privacy in Retinal fundus photos de-identification. *Investigative Ophthalmology & Visual Science*, *64*(8), 2399-2399.
19. Cajas, S. A., Restrepo, D., Moukheiber, D., Kuo, K. T., Wu, C., Chicangana, D. S. G., ... & Celi, L. A. A Multi-Modal Satellite Imagery Dataset for Public Health Analysis in Colombia.
20. Zhang, Y., Abdullah, S., Ullah, I., & Ghani, F. (2024). A new approach to neural network via double hierarchy linguistic information: Application in robot selection. Engineering Applications of Artificial Intelligence, 129, 107581.
21. Tianqi, Y. (2022). Integrated models for rocking of offshore wind turbine structures. American Journal of Interdisciplinary Research in Engineering and Sciences, 9(1), 13-24.
22. Ma, H. (2021, January). Research on promotion of lower limb movement function recovery after stroke by using lower limb rehabilitation robot in combination with constant velocity muscle strength training. In 2021 7th international symposium on mechatronics and industrial informatics (ISMII) (pp. 70-73). IEEE.
23. Sun, Y., Cui, Y., Hu, J., & Jia, W. (2018). Relation classification using coarse and fine-grained networks with SDP supervised key words selection. In Knowledge Science, Engineering and Management: 11th International Conference, KSEM 2018, Changchun, China, August 17–19, 2018, Proceedings, Part I 11 (pp. 514-522). Springer International Publishing.
24. Sun, Y. (2024). TransTARec: Time-Adaptive Translating Embedding Model for Next POI Recommendation. arXiv preprint arXiv:2404.07096.
25. Sha, X. (2024). Time Series Stock Price Forecasting Based on Genetic Algorithm (GA)-Long Short-Term Memory Network (LSTM) Optimization. arXiv preprint arXiv:2405.03151.
26. Huang, C., Bandyopadhyay, A., Fan, W., Miller, A., & Gilbertson-White, S. (2023). Mental toll on working women during the COVID-19 pandemic: An exploratory study using Reddit data. PloS one, 18(1), e0280049.
27. Srivastava, S., Huang, C., Fan, W., & Yao, Z. (2023). Instance Needs More Care: Rewriting Prompts for Instances Yields Better Zero-Shot Performance. arXiv preprint arXiv:2310.02107.
28. Rosner, B., Tamimi, R. M., Kraft, P., Gao, C., Mu, Y., Scott, C., ... & Colditz, G. A. (2021). Simplified breast risk tool integrating questionnaire risk factors, mammographic density, and polygenic risk score: development and validation. Cancer Epidemiology, Biomarkers & Prevention, 30(4), 600-607.
29. Yu, D., Xie, Y., An, W., Li, Z., & Yao, Y. (2023, December). Joint Coordinate Regression and Association For Multi-Person Pose Estimation, A Pure Neural Network Approach. In Proceedings of the 5th ACM International Conference on Multimedia in Asia (pp. 1-8).
30. Sha, X. (2024). Research on financial fraud algorithm based on federal learning and big data technology. arXiv preprint arXiv:2405.03992.
31. Sarkis, R. A., Goksen, Y., Mu, Y., Rosner, B., & Lee, J. W. (2018). Cognitive and fatigue side effects of anti-epileptic drugs: an analysis of phase III add-on trials. Journal of neurology, 265(9), 2137-2142.
32. Rosner, B., Tamimi, R. M., Kraft, P., Gao, C., Mu, Y., Scott, C., ... & Colditz, G. A. (2021). Simplified breast risk tool integrating questionnaire risk factors, mammographic density, and polygenic risk score: development and validation. Cancer Epidemiology, Biomarkers & Prevention, 30(4), 600-607.