


A federated learning approach for smart healthcare systems

Ayushi Mishra¹  · Subhajyoti Saha¹ · Saroj Mishra² ·
Priyanka Bagade¹

Received: 24 December 2022 / Accepted: 7 March 2023 / Published online: 11 April 2023
© CSI Publications 2023

Abstract With periodic technology advancements and pandemic-like situations, remote patient health monitoring has increased significantly. The Internet of Things (IoT) devices, including wearables, sensors, and actuators deployed on the human body, detect and regulate physiological data. These systems can establish a trigger mechanism in the event of a possible health incident. Health monitoring using IoT devices generates a large amount of data. Several Machine Learning (ML) strategies have been utilized to analyze the collected data and derive precise predictions. The confidentiality of patient data is one of the essential requirements of these systems. It has been discovered that malicious coordination of ML algorithms might result in a massive attack surface, providing cyber-criminals with an accessible platform. Considering these requirements for using IoT systems for health monitoring, Federated Learning (FL) can solve data privacy challenges by training ML models locally on IoT devices without any data transfer to the cloud. FL facilitates information sharing among all IoT devices installed in hospitals through collaborative ML model training. This article will examine the significance of embedding FL into IoT-enabled smart hospitals and

future guidelines for accomplishing this. This article discusses identifying rare diseases and critical care, resolving the problem of insufficient patient health data to train ML models, and preserving patient privacy.

Keywords Internet of things · Healthcare systems · Smart hospitals · Federated learning · Machine learning

1 Introduction

The Medical Internet of Things (MIoT) is crucial component for enabling the Industry 4.0 revolution across healthcare industry. MIoT connects large number of medical devices to the internet. The rapid growth of medical IoT has transformed the healthcare system through the use of sensors and smart medical systems [1]. The inadequacies in our present healthcare systems have been highlighted by a number of natural disasters, including the COVID-19 pandemic. IoT and data analysis using machine learning (ML) methods can considerably increase the cost-effectiveness, accessibility, and resilience of our healthcare system by converting some of the conventional physical healthcare methods to their online remote equivalents, such as remote patient health monitoring [2]. ML in healthcare would augment physicians in making critical decisions quickly. However, ML approaches are data-hungry. An approach to machine learning (ML) training that protects data privacy is essential given the significance of protecting patient health data. The use of FL in smart healthcare can solve the problem of limited healthcare data availability, especially for rare diseases, and patient data privacy during training by collaborating the ML model training among various hospitals.

A healthcare organization consists of several patient health records that vary from hospital to hospital. Electronic

✉ Ayushi Mishra
ayushim@cse.iitk.ac.in
Subhajyoti Saha
subhajyoti@cse.iitk.ac.in
Saroj Mishra
skmishra@iitk.ac.in
Priyanka Bagade
pbagade@cse.iitk.ac.in

¹ Department of Computer Science and Engineering, Indian Institute of Technology, Kanpur, India

² Gangwal School of Medical Science and Technology, Kanpur, India

medical records generated during clinical practices are captured at various points throughout the hospital, beginning at the registration desk and continuing until the patient is discharged. However, these records of different kinds, like medical imaging, are stored in hospital servers not accessible to stakeholders outside a particular hospital/ healthcare provider institution to adhere to the privacy and security regulations of a particular country. However, the disease spectrum varies worldwide; for example, medical students or lecturers in the western countries do not observe tropical diseases as well as different symptoms for the same diseases across various parts of the world. In this situation, FL technology holds great significance in cross training physicians on various diseases while ensuring the security and privacy of patient records, as the records do not move outside a hospital server. Clinical training and therapeutic aspects can be taught to trainees, and management skills can be imparted. Personalized FL [3] can jointly train distributed ML models from the knowledge of the data across all the different geographical locations, still producing personalized models specific to each geographical location simultaneously.

In 1976, philosophy professor Patrik Hill proposed the term FL to form a Federated Learning Community (FLC) for bringing people from different research universities to learn together [4]. McMahan et al. [5]. used the term FL for the first time in 2017 to preserve patient data privacy by training the ML model in a distributed fashion.

Figure 1 describes a general privacy-preserving FL framework. Multiple clients in FL receive a global model with weight parameters from the server. The clients then train their models from local data using various stochastic optimization methods (for example, stochastic gradient descent [6]) and send the trained model to the server. The server then aggregates these weights in order to learn a global model. Consequently, the global model acquires all

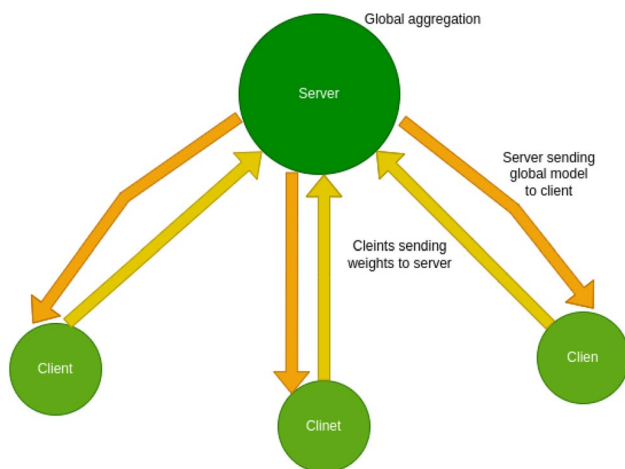


Fig. 1 Federated learning framework

the local clients' knowledge without even accessing their local datasets [5]

FL can reduce the computational budget required to train a high-quality global model due to the resource-constrained IoT devices by distributing the workload and training it in parallel [7]. Because FL training occurs on edge devices, it can accelerate the inference step where network bandwidth is limited. FL can also reduce bandwidth requirements by transferring only weights rather than data. Data breaches are prevented because each edge server performs local computing, ensuring privacy.

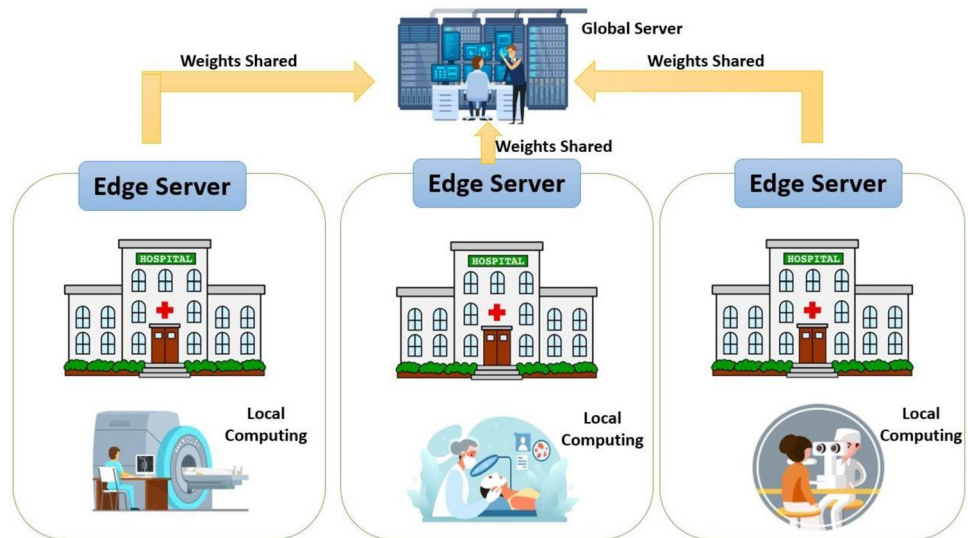
This paper discusses the importance of FL in healthcare systems, how it can solve several disease detection problems, and how it can ensure patient health-related data privacy. The remainder of the paper is structured as follows: The overview of FL in healthcare is described in Sect. 2. Sect. 3 discusses the current state of FL in IoT-based healthcare applications. Sect. 4 describes the difficulties encountered by FL-based ML models. Following that, future work is discussed in Sect. 5. Finally, Sect. 6 concludes the paper.

2 System model for FL in healthcare

Figure 2 illustrates a generic framework for FL in IoT-enabled healthcare systems. The IoT-enabled medical devices collect the data on the respective edge servers of each hospital. Afterward, local computation of the model is done on the edge servers that provide the optimal weights. Each server's optimal weights are then sent to the global server, which aggregates all the weights and trains and evaluates the model. This way, weights are shared in parallel from all the hospitals to the centralized server. The training of the FL model can be used for classification and detection approaches. For example, hospitals that contain the patient's ECG measurements can have several classes depending on the heart-beat measurements. Few patients have an average heart rate, while others can have catastrophic heart diseases like arrhythmia and ventricular tachycardia. To distinguish between normal and diseased patients, local computing at each client can be trained for the classification task. Later, the local weights can be aggregated on the global server for final evaluation.

According to the Health Insurance Portability and Accountability Act (HIPAA) [8], patient safety is essential when applying any ML algorithms. The FL approach can ensure patient privacy and secure patient health records (PHI). During the transmission of health data, the data gets transmitted from medical devices to the cloud and is susceptible to cyber-attacks like spoofing, information disclosure, denial of service (DoS), and privilege escalation attacks. The first crucial aspect of using FL in healthcare is preventing

Fig. 2 A Federated learning system model in healthcare



data sharing with the gateway or a cloud server. This way, the safety of the patient data is also ensured.

3 Related work

The FL model for IoT-enabled healthcare delivery provided several solutions for interconnected IoT devices’ diverse, low-power, and distributed nature. The earlier research discusses the architecture of federated learning, system problems, and a method for protecting privacy [9]. With the advancement of wearables and sensor technologies, enormous data is now evolving, which is essential to be trained using different ML algorithms. Syreen et al. [9] proposed several classification and clustering techniques for FL-enabled IoT systems. The resource-constraint nature of IoT makes these devices share data with edge nodes using different communication protocols, which are prone to cyber-attacks. To address this, Nguyen et al. [10] address the extensive range of FL applications in IoT services, including data sharing, attack detection, and IoT privacy and security. Similarly, Alam et al. [11] emphasize the importance of robust FL classifiers that aid in the non-disclosure of

information, resulting in highly secure privacy rules. The industry 4.0 revolution has upgraded the healthcare system by incorporating AI into edge devices to enable training. FL can facilitate the connectivity of various industrial internet of things (IIoT) devices at the gateway while maintaining patient confidentiality. However, the previously stated study demonstrates future uses of FL in numerous technological sectors. These papers focus primarily on the role of FL and the challenges it can confront in all application domains.

Recently, the FL concept is becoming increasingly prevalent in clinical care. Table 1 describes different FL healthcare applications implemented until to-day. With the growth of IoT devices that offer affordable healthcare monitoring, the FL method can expedite the detection of diseases based on the patient’s physiological characteristics. Elayan et al. [12, 13] offer a deep federated learning system that utilizes transfer learning to detect skin disorders. The authors evaluated their results using the evaluation metrics of precision (the number of optimistic predictions), recall (the number of correctly classified accurate predictions), and the F1 score (the weighted average of precision and recall). The FL model increases the area under the curve, a classifier’s

Table 1 Federated learning applications in healthcare

Papers	Physiological Parameters	FL Algorithms	Evaluation	Privacy
Elayan et al. [17]	Diseased and Normal skin	Deep FL	AUC=0.97	No
Li et al.[19]	Alzheimer’s disease	Classification Model	Acc=81.9%	No
Brisimi et al. [20]	Cardiac Events	Binary Supervised		No
Stephanie et al. [16]	Colon and Breast Cancer	Ensemble FedAvg	Acc > 80%	No
Zhang et al. [22]	Skin Lesion	Classification Model	Acc = 76.9%	Yes
Khoa et al.[23]	Human Activities	Encode Deep CNN		yes
Lian et al. [24]	Covid-19 CT Scans	Classical FL and ML		Yes
Castillo et al. [27]	Diabetes Monitoring	IL and FL	Acc=97.87%	Yes

ability to distinguish between classes, to 0.97. The higher the value, the better the performance. The author, however, did not resolve the issue of limited data availability. Singh et al. [14] offer a blockchain-based distributed FL architecture for IoT-enabled medical devices. This research aims to train machine learning models at various IoT device locations without transmitting patient data to the cloud.

The early diagnosis of certain fatal diseases is crucial. Li et al. [14] proposed an ADDetector, a detector for Alzheimer's disease. The author introduces three layers to privacy: users, clients, and gateway. A classification model with a differential privacy mechanism was designed to protect model aggregation between clients and, clouds. The accuracy of their ADDetector is 81.9%. Brisimi et al. [15]. suggest a binary supervised learning system to predict hospitalizations of cardiac events through distributed algorithms. Without explicitly exchanging raw data, the study aims to enable diverse data holders to interact and converge on a shared predictive model. Blanquer et al. [16]. propose a hardware-enhanced architecture for encrypting sensitive data in memory and on discs that can only be accessed within trusted execution contexts. The use of federated clouds enables the collection of resources needed for high performance and security.

Securing local models from violating the user's privacy is also crucial. The current locally trained models are exposed to adversaries such as inversion and membership inference attacks. Stephanie et al. [17]. present a blockchain-based heterogeneous model to learn from healthcare institutions collaboratively. Each hospital owned an edge server where data collected from the medical devices were trained. The trained model is verified and stored in a private blockchain. The author took two datasets: Colon Pathology and Breast Cancer. The model used for training purposes is centralized FL, FedAvg, TEE-based FL, and Ensemble-Fed Avg. All algorithms gave an accuracy of more than 80%.

Zhang et al. [18]. used cryptographic primitives, including masks and homomorphic encryption, to protect the local models. Private medical data can be attacked using a model reconstruction attack. Along with data protection, the author analyzed the communication and computation costs. The model was trained on HAM1000 medical dataset for skin lesion classification. The maximum accuracy obtained was around 76.9%.

Khoa et al. [19]. uses Encode Depth Convolutional Network as both server and client for recognizing human activity. They compared their approach with LSTM and CNN in the FL setting. A DEEP-FEL model was proposed by Lian et al. [20]. This method teaches medical centers their local model and aggregates the sub-model by maximizing the topological ring structure. Sub-global model information was transmitted using differential privacy. The model was evaluated using FL and ML techniques on COVID-19

CT scan images. An estimation and classification model for a diabetes-monitoring healthcare system was proposed by Castillo et al. [21]. The estimation model forecasts the glucose level in the patient, while the classification model detects the anomalous points in patient data. The authors implemented the FL and independent learning (IL) approach with a recall rate of 98.69% and 97.87%, respectively.

The current state of research describes the significance of FL in IoT-enabled healthcare systems. The authors discussed numerous applications of FL in healthcare domains in the literature survey. With the progress of this healthcare field, several limitations like data heterogeneity, loss of essential data, and modification of model weights need to be addressed, as discussed in Sect. 4, for making these FL-deployed healthcare systems robust.

4 Challenges in FL for IoT-enabled healthcare systems

FL for the healthcare system can be proved to be the most influential future contributions to the medical industry. However, with current FL approaches, there are several limitations:

- **Data heterogeneity:** Healthcare organizations contain diverse information. When training a local model on edge devices, the differential weights shared by all the local servers will have a significant disparity, leading to inefficient model prediction. Because of heterogeneous patient metadata, obtaining essential data comparable to other edge devices from hospitals can take time and effort.
- **Heterogeneous healthcare systems:** Most healthcare organizations train models with varying processing capabilities during local computing on edge servers. Consequently, the GPU and hospital processing unit are essential for local training. With hospitals with less computing power, the local model may be less efficient, and the shared weights from these hospitals may contribute less to the central server's global aggregation.
- **Loss of important healthcare data:** During the sharing of weight from local clients to the global server, packets with the most significant contribution to the model prediction may be dropped during the communication. As a result, if the FL was trained on critical illness detection applications, data packet loss during communication can cause severe concerns about patient health and medicine.
- **Modifications with the model weights:** The exchanged weights during FL are vulnerable to cyber-attacks. Any adversary can use reverse engineering to discover the shared weight's attributes and modify them maliciously. Even if the data is not shared, it is essential to safeguard the model weights.

- **Single server problem:** Until now, most FL approaches in healthcare applications utilize a single server for global weights aggregation and training. However, relying on a single server cannot be trustworthy. A single point of failure may result in the complete failure of critical infrastructure like health-care. Privacy issues are still present on the server. A cyber-attack can ever occur on the server, directly affecting the final model weights and resulting in a considerable loss for hospitals. Therefore, distributed systems or backup can help overcome these challenges and prepare them for fault tolerance.
- **Trade off between noise and accuracy:** As the client's model weights can be reverse-engineered to extract meaningful information about the client's knowledge, differential privacy can make the weight update more robust. However, adding noise to the model parameters will temper the knowledge contained in the parameters, which would eventually decrease the accuracy of the aggregated global model. Thus, there exists a trade-off between adding noise and the final accuracy of the model.

5 Future work

FL sees a tremendous expansion. It is possible to extend it further by following the paths of study.

- **Detection of malicious weights at the client level:** Malicious clients have previously been identified at the server level during aggregation [22, 23]. However, determining the specific corrupted weights at the client level has yet to be investigated.
- **Energy efficient communication:** Several research papers have investigated more efficient methods of communicating client weights to the server. Transferring only the top few percentages of weights as opposed to all weights is known as sparsification of weight. This significantly reduces communication expenses. However, the proof of convergence of such communication-efficient federated learning frameworks needs to get investigated. [24].
- **Statistical data heterogeneity:** The signs and symptoms of a disease can vary significantly across time and space. Thus, it is necessary to design federated aggregation algorithms that can capture healthcare data's temporal and spatial variations and efficiently learn from data spanning a large geographical area and time.
- **Resource constrained training:** Medical devices are made to be used in a hospital or clinic. However, they need more computing power to train the
- **ML algorithms, which need considerable data to learn.** This problem can be fixed by looking into FL training for IoT devices with limited resources [25]. Neural architec-

ture search can be used to find the best model size based on resources available, and FL can be used to train those models. [26]

- **Novel communication scheme:** Federated learning approaches can be divided into synchronous and asynchronous (bounded delay) approaches. This Federated learning training approach is practical when the clients are only dedicated to the task of federated learning. However, real-world clients are only sometimes available for training, e.g., mobile phones on low batteries, etc. Thus, a device-centric training approach is highly needed for the Federated learning training [27–29].
- **Necessity of training medical professionals:** In the current scenarios, FL training is only performed to train ML models to improve patient health. However, medical professionals are not comfortable using these technologies. Thus, training medical professionals on how to use these technologies are necessary. They also need to be trained in the abilities of these ML algorithms so that the problems can be communicated better with the technical persons to solve the problems in the healthcare domain efficiently. [30, 31]

6 Conclusion

FL is a novel AI methodology that has generated attention for developing scalable and secure smart healthcare applications. The use of FL in various health-care settings is analyzed in this article. We discussed diverse reasoning and how and why it could be used in smart healthcare. After that, there was a discussion about new FL ideas that, if implemented, would make federated intelligent healthcare work better. Then, critical FL applications in innovative health-care were carefully looked at and defined. Some of these were federated EHR management, federated remote patient health monitoring, and medical image diagnosis and, illness detection. Last, we discussed some intriguing difficulties and the future of FL-smart healthcare.

References

1. Hu, Fang, Dan Xie, and Shaowu Shen (2013): On the application of the internet of things in the field of medical and health care. 2013 IEEE International conference on green computing and communications and IEEE Intt Things and IEEE Cyber, Physical Social Comput. IEEE
2. Beam AL, Kohane IS (2018) Big data and machine learning in health care. *JAMA* 319(13):1317–1318
3. Tan, AZ, et al. (2022): Towards personalized federated learning. *IEEE Transactions on Neural Netw Learn Syst*
4. Hill, Patrick (1985): The Rationale for Learning Communities and Learning Community Models

5. McMahan, Brendan, Eider Moore, Daniel Ramage, Seth Hampson, and Blaise Aguera y Arcas. (2017): Communication-efficient learning of deep networks from decentralized data. In: *Artificial intelligence and statistics*, 1273–1282. PMLR, <https://ui.adsabs.harvard.edu/abs/2016arXiv160205629B/abstract>
6. Amari S-I (1993) Backpropagation and stochastic gradient descent method. *Neurocomputing* 5(4–5):185–196
7. Imteaj, Ahmed, et al. (2023): Federated learning for resource-constrained IoT devices: panoramas and state of the art. *Fed Transf Learn* :7–27
8. Nosowsky R, Giordano TJ (2006) The Health Insurance Portability and Accountability Act of 1996 (HIPAA) privacy rule: implications for clinical research. *Annu Rev Med* 57:575–590
9. Banabilah S, Aloqaily M, Alsayed E, Malik N, Jarar-weh. Y (2022) Federated learning review: fundamentals, enabling technologies, and future applications. *Inf Process Manage* 59(6):103061
10. Nguyen DC, Ding M, Pathirana PN, Seneviratne A, Li J, Vincent Poor H (2021) Federated learning for internet of things: a comprehensive survey. *IEEE Commun Surv Tutori* 23(3):1622–1658
11. Alam T, Gupta R (2022) Federated learning and its role in the privacy preservation of IoT devices. *Future Int* 14(9):246
12. Elayan, Haya, Moayad Aloqaily, and Mohsen Guizani. (2021): Deep federated learning for IoT-based decentralized healthcare systems. In *2021 International Wireless Communications and Mobile Computing (IWCMC)*, 105–109. IEEE
13. Elayan H, Aloqaily M, Guizani M (2021) Sustainability of healthcare data analysis IoT-based systems using deep federated learning. *IEEE Int Things J* 9(10):7338–7346
14. Singh S, Rathore S, Alfarraj O, Tolba A, Yoon B (2022) A framework for privacy-preservation of IoT healthcare data using Federated Learning and blockchain technology. *Future Gener Comput Syst* 129:380–388
15. Brisimi TS, Chen R, Mela T, Olshevsky A, Paschalidis IC, Shi W (2018) Federated learning of predictive models from federated electronic health records. *Int J Med Inf* 112:59–67
16. Blanquer I, Brasileiro F, Brito A, Calatrava A, Carvalho A, Fetzer C, Silva F (2020) Federated and secure cloud services for building medical image classifiers on an intercontinental infrastructure. *Future Gener Comput Syst* 110:119–134
17. Stephanie, Veronika, Ibrahim Khalil, Mohammed Atiquzzaman, and Xun Yi. (2022): Trustworthy privacy-preserving hierarchical ensemble and federated learning in healthcare 4.0 with blockchain. *IEEE Transac Ind Inf*
18. Zhang, Li, Jianbo Xu, Pandi Vijayakumar, Pradip Kumar Sharma, and Uttam Ghosh. (2022): Homomorphic encryption-based privacy-preserving federated learning in IoT-enabled healthcare system." *IEEE Transac Netw Sci Eng*
19. Khoa, Tran Anh, Do-Van Nguyen, Minh-Son Dao, and Koji Zettsu. (2021): Fed xData: a federated learning framework for enabling contextual health monitoring in a cloud-edge network. In *2021 IEEE International Conference on Big Data (Big Data)*, pp 4979–4988. IEEE
20. Lian, Zhuotao, Qinglin Yang, Weizheng Wang, Qingkui Zeng, Mamoun Alazab, Hong Zhao, and Chunhua Su. (2022): DEEP-FEL: decentralized, efficient and privacy-enhanced federated edge learning for healthcare cyber physical systems. *IEEE Transac Netw Sci Eng*
21. Astillo PV, Duguma DG, Park H, Kim J, Kim B, You I (2022) Federated intelligence of anomaly detection agent in IoTMD-enabled diabetes management control system. *Future Gener Comput Syst* 128:395–405
22. Li, Suyi, et al. (2020): Learning to detect malicious clients for robust federated learning. *arXiv preprint arXiv:2002.00211*
23. Zhang, Zaixi, et al. (2022): FLDetector: Defending federated learning against model poisoning attacks via detecting malicious clients. *Proceedings of the 28th ACM SIGKDD Conference on Knowledge Discovery and Data Mining*
24. Yuan, Binhang, Song Ge, and Wenhui Xing (2020): A federated learning framework for healthcare IoT devices. *arXiv preprint arXiv:2005.05083*
25. Zhu H, Zhang H, Jin Y (2021) From federated learning to federated neural architecture search: a survey". *Complex Intell Syst* 7(2):639–657
26. Imteaj, Ahmed, et al. (2023) Federated Learning for Resource-Constrained IoT Devices: Panoramas and State of the Art." *Fed Transf Learn*: 7–27
27. Li T et al (2020) Federated learning: Challenges, methods, and future directions". *IEEE Signal Process Mag* 37(3):50–60
28. Rehak, Dan, Philip Dodds, and Larry Lannom (2005): A model and infrastructure for federated learning content repositories. *Interoperability of web-based educational systems workshop*. 143.
29. Jensen PB, Jensen LJ, Brunak S (2012) Mining electronic health records: towards better research applications and clinical care. *Nat Rev Genet* 13(6):395–405
30. Mukherjee, Rajat, and Howard Jaffe: System and method for dynamic context-sensitive federated search of multiple information repositories. U.S. Patent Application No. 10/743,196
31. Author F (2016) Article title *Journal* 2(5):99–110

Springer Nature or its licensor (e.g. a society or other partner) holds exclusive rights to this article under a publishing agreement with the author(s) or other rightsholder(s); author self-archiving of the accepted manuscript version of this article is solely governed by the terms of such publishing agreement and applicable law.