



International Journal of Research Publication and Reviews

Journal Homepage: www.ijrpr.com ISSN 2582-7421

Federated Learning for Privacy-Reversing Healthcare Challenges, Applications and Future Directions

Rishi Awasthi¹, Vanshika Singh², Mrs. Richa Pandey³

^{1,2} School of Computer of Applications, Babu Banarasi Das University, Lucknow, India

³ Assistant Professor, School of Computer Applications, Babu Banarasi Das University, Lucknow, India

rishiawasthi43@gmail.com, vanshikasingh56666@gmail.com, pandeyricha1606@bbdu.ac.in

ABSTRACT—

In the today's digital age, healthcare organizations are collecting vast amounts of highly sensitive data, such as patient records, diagnostic reports, and medical images. Traditionally, machine learning models required all of the data to be collected and stored in one centralized location. This presented several challenges concerning the confidentiality and security of the data. Federated Learning (FL) provides another way to use ML. Under FL, each organization keeps its own data on its premises. Rather than sharing the actual patient data, each organization shares only the updated version of the model. In this paper, we review several studies concerning FL applications within the field of healthcare. The studies we selected focus on medical imaging, smart healthcare, data protection, security, data heterogeneity, communication efficiency, scalability and interoperability. The studies demonstrate that FL enables organizations to collaborate and train models using their collective knowledge base without having to share the underlying data.

However, there are several challenges and problems preventing wide-scale implementation of FL in real-world scenarios. Some of these include: heterogeneity among different datasets used for training models, communication requirements for FL, potential security risks associated with FL systems, limits to how large an FL system can grow, and interoperability issues between various healthcare systems. Based upon our review of the relevant studies, we identify a major gap in the current body of literature regarding FL applications in healthcare. The conceptual model we developed is also intended to provide a logical structure for incorporating all of the previously discussed limitations.

While this conceptual model is based on prior research (and therefore, not yet empirically proven), experimental studies will need to validate its effectiveness in order to make it usable in future research.

Index Terms—Federated learning, healthcare, privacy preservation, medical imaging, data heterogeneity, security, scalability, interoperability.

I. Introduction

Healthcare organizations have a huge amount of patient information in their possession - including patient demographics, medical history, test results, imaging studies and treatment records. Due to the very nature of this type of data makes it extremely sensitive as it relates directly back to individual patients.

Therefore, the data must be protected with extreme care. When an organization stores, shares or uses this type of information they must implement strict privacy and security procedures.

However, healthcare data also has the potential to drive machine learning systems which could help identify early symptoms of disease, analyze images and assist physicians in making better clinical decisions. Conventionally, hospitals/clinics share their data to a single location for analysis. Sharing raw patient data among different organizations creates significant privacy challenges and creates difficulty for them to work together effectively.

Federated Learning (FL) provides a different option. Instead of sending patient data to a centralized server, organizations keep their data at home, develop a local model, send the updated model parameters to a centralized server, which then combines all of the model parameters from each organization to create a new global model.

Therefore, several organizations can work collaboratively to create models while never having to share their patients' personal health information [1], [2]. Although organizations keep their data in-house, there are still concerns regarding the security and privacy of the patient data. Model parameter updates may provide clues as to what type of patient data was used to train the models, and communications between devices and servers require protection. Additionally, healthcare organizations often have varying data types, computational resources, network speeds and internal system capabilities

1

[1] – [5]. The variability among healthcare organizations impacts how FL operates in the real world. As such, this paper will address both of these areas in an attempt to identify the true-world challenges and opportunities of applying FL to healthcare.

II. Problem Statement

Patient data collected by healthcare organizations is generally highly personal and thus difficult to transmit. With conventional machine learning techniques, all patient data would need to be transmitted to a single central server. Transmission of patient data to a central server would pose potential problems regarding both privacy and security. FL resolves these problems by enabling each organization to train a model on its own local computer system, and then transmit only the updates to that model (rather than transmitting all patient records).

While FL does help with protecting patient data, there are still some major obstacles to implementing FL within the medical community. Different hospitals and/or clinics will have varying amounts of data. Also, the types and/or quality of that data may also vary.

Additionally, the devices that are being used to perform the training may vary greatly in terms of how fast they run and/or how well they operate.

Finally, the network connectivity that exists between the various sites where models are being trained may either be too slow or too unreliable.

Model updates may create risk in terms of leaking information regarding the data that was used in training the model. The use of more devices creates greater network usage; and as the number of institutions in the network grows, managing and scaling the network will be increasingly difficult. Many different kinds of software, as well as several common formats are used by most healthcare systems. These factors create a situation that makes it less probable for healthcare providers to cooperate with each other. The primary focus of this research project was: How could FL assist healthcare providers in collaborating on Machine Learning tasks, while maintaining the privacy of patient data, and dealing with issues such as Security, Differences in Data, Network Efficiency, Number of Collaborators and Technology Compatibility?

III. Research Objectives

The objectives of this study are to:

1. Evaluate how FL is utilized in health care applications.
2. Study different ways to protect privacy using machine learning techniques within the context of healthcare
3. Review how FL has been applied in both health care and medical imaging
4. Determine challenges associated with heterogeneous data sources, communications, security, and scalability
5. Evaluate the potential for interoperability between various healthcare organizations and their respective information systems.
6. Identify research gaps and future directions identified through the selected literature

IV. Background

A. Federated Learning

Federated learning has many participants working toward improving a common model. The participants do not send their data to a single location; instead, each participant trains a part of the model using their own device and sends updates back. The most common way that these model updates are combined is by taking the weighted average of all of the update vectors.

$$W_{global} = \sum_{k=1 \dots K} (n_k / n) W_k$$

where W_k denotes the model parameters from participant k , n_k is the number of data samples held by participant k , and n is the total number of samples across all K participants. The way updates are combined can differ between FL systems.

B. Healthcare Data Privacy

Health care data may include both identifying information (i.e. who you are) and health-related information. FL assists in the protection of this data by allowing the data to remain at its location rather than being sent to a single site. Nevertheless, the messages and updates that occur between participants in a FL network can include sensitive information or put participant's information at risk. To ensure that FL is secure and maintains participant's privacy, it will be necessary to use techniques like differential privacy, secure aggregation and encryption [1], [2].

V. Methodology

This study utilizes an empirical literature-based methodology to evaluate implementation of FL within the health care sector. The study on FL's advantages, limitations it faces, successes and failures it has accomplished, as well as areas needing additional investigation, was conducted through

1

evaluating several previous studies that investigated FL. The structure of the analysis of these studies was based upon common themes appearing in the literature:

- FL applications in healthcare.
- Privacy-preserving techniques.
- Medical imaging and healthcare analytics.
- Data heterogeneity and non-IID data.
- Security and privacy challenges.
- Communication efficiency.
- Scalability.
- Interoperability.

The studies were evaluated based upon these commonalities to allow for the identification of challenges and opportunities for continued study. A gap in the current knowledge base regarding this topic has been identified and a conceptual model of how to address that gap has been created. There was no real-time patient data used within an actual healthcare setting when conducting any of the experimental studies.

VI. Federated Learning Architecture for Healthcare

Fig. 1 illustrates how Federated Learning (FL) will work in the context of Healthcare Institutions. In FL, each Institution will maintain control over their Patients' Data and Train Models at the Local level. Each Institution will Send Model Updates to a Central Aggregation Server that will Collect All the Updates from Each Institution and Forward a Global Model to All of the Participating Institutions

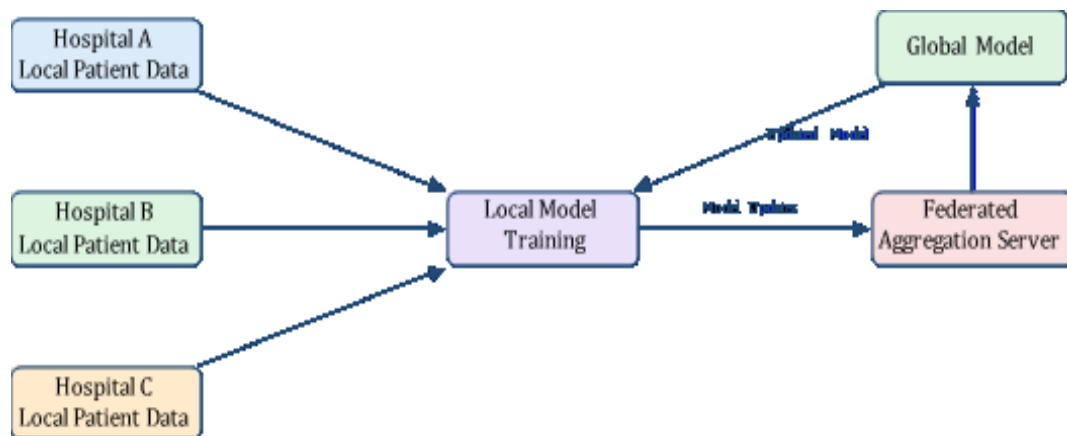


Fig. 1. Conceptual architecture of Federated Learning for collaborative healthcare.

VII. Literature Review

The literature reviewed has been chosen to cover related topics of FL within health care such as medical imaging, intelligent/smart healthcare, privacy protection, security, heterogeneity of data, efficient communication, scalability and interoperability.

A. Medical Imaging and Privacy-Preserving Learning

The study by Sandhu et al. (2018) [1], provided an examination of various ways that FL has been utilized in research using image based methods, along with an explanation of how distributed learning could be used to enable researchers to conduct collaborative studies without having to provide each other with access to sensitive or private patient image data. The studies' emphasis on privacy, security, and other data related concerns in the area of medical imaging are particularly significant.

B. Smart Healthcare and IoT Integration in Healthcare

Abbas et al. (2018) examined the use of FL in the health care industry; specifically, how FL is used with IoT (Internet of Things) devices, wearable technologies, remotely monitored medical equipment, and predictive analytics. The authors also identify potential security concerns, heterogeneous data, scalability issues, and interoperability concerns. Additionally, they provide examples of privacy-preserving techniques, including differential privacy and secure multi-party computing.

C. Challenges in Smart Healthcare

1

Nasajpour et al. [3] conducted a survey of FL applications and challenges within the field of healthcare. The authors included in their review examples of smart device-based applications; disease prediction models; and medical image analysis, along with identifying ongoing research issues related to security; communication cost; and heterogeneity of healthcare data.

D. Healthcare Data Sharing

Dhade and Shirke (4) provided an overview of FL in health care and addressed how this type of collaborative learning may be relevant in cases where it is not possible to directly share sensitive medical information. The authors identified privacy, data ownership, and secure collaborations as major themes.

E. Multi-Institutional Medical Data Mining

In addition to these studies, Haripriya et al. [5] researched private-preserving FL for medical data mining within multi-institute environments. The researchers evaluated the use of image datasets (such as tuberculosis chest X-ray images, brain tumor MRI scans and diabetic retinopathy images) and evaluated aggregation methods for different types of heterogeneous data. The reviewed research indicates that FL is currently under investigation across a wide range of applications in health care; however, to deploy FL in practice, it is necessary to simultaneously address issues related to privacy, security, heterogeneity of data, communication, scalability, and interoperability [1]–[5].

VIII. Comparative Analysis of Selected Studies

The studies reviewed here look at FL using different healthcare perspectives (e.g., medical imaging, smart healthcare, etc.). Table I compares the studies based upon their focus, how they are applied in healthcare and what are some of the main issues.

TABLE I

COMPARATIVE ANALYSIS OF SELECTED STUDIES

Study	Main Focus	Application	Major Challenges
Sandhu et al. [1]	Medical imaging FL	Medical imaging	Privacy, security
Abbas et al. [2]	Smart healthcare FL	IoT, wearables, predictive analytics	Security, Heterogeneity, scalability, interoperability, security
Nasajpour et al. [3]	FL Applications and Challenges	Smart healthcare; imaging	Security, communication, Heterogeneity, Communication, security
Dhade and Shirke [4]	Healthcare FL review	Collaborative healthcare learning	Privacy
Haripriya et al. [5]	Privacy-preserving FL	Medical image classification	Privacy, heterogeneity, aggregation

IX. Research Gap

The reviewed research indicates that FL is an essential tool in health care applications. The issues discussed in the literature are closely related and can't be resolved with just addressing privacy concerns. Issues such as differences in data sets, large amounts of communications required by the system, increasing size of the system, and no compatibility among health care technology, all require explicit attention to resolve them.

Healthcare organizations have different types of patient populations, amounts of data collected, types of devices used to provide care, and information systems operated. These differences can affect how the responsibilities of training are distributed among them. If you are constantly updating your models, you will be adding to the communication burden, and with each new participant there is an increased need for coordination and additional resources. The differences in data format and technology used by healthcare providers can also create a barrier for collaboration between their respective systems. Therefore, this paper emphasizes the necessity of developing a conceptual healthcare Federated Learning (FL) model based upon treating privacy, security, data heterogeneity, effective communication, scalability, and system interoperability as interdependent needs.

X. Major Challenges in Healthcare Federated Learning**A. Data Heterogeneity**

Data used in healthcare may be very different across various organizations. Differences in patient populations, use of different kinds of medical equipment, variations in clinical practice patterns or local health factors all contribute to this variability. These differences can lead to challenges when training a global model with data from multiple sources and may ultimately result in reduced performance of the model in actual application [2], [3], [5].

B. Privacy and Security

1

Although all the raw data used in this process remains on site, there still exists risks associated with both the privacy and security of that data. The model update messages transmitted to the central server may include sensitive details regarding your organization's business operations; additionally, there is a risk of hacking or other forms of attack occurring at some point in time during the transmission of these messages (i.e., data breaches, unauthorized access, etc.).

Therefore, it is imperative to implement strong protective safeguards for the purpose of preserving the security of your organization's data and ensuring its accuracy.

C. Communication Efficiency

In FL, institutions regularly communicate their model updates with each other through the use of a centralized server. When there are numerous institutions involved in a FL network, model updates can produce large amounts of network traffic. The frequent exchanges of model updates among institutions within FL networks contribute to additional communication costs and slow down the training process, particularly when bandwidth is limited [3].

D. Scalability

A health care FL system could potentially expand to hundreds of hospitals and clinics, possibly even thousands of devices. The more participants there are in a health care FL system, the higher the need will be for computing power, transfer of information (data), and communication among all parties involved. This type of system should be able to continue functioning at its current rate of speed and/or accuracy as it expands [2].

E. Interoperability

Healthcare organizations are using different computer software programs and data formats and hardware devices. Many healthcare organizations still utilize old legacy systems; however, many have started using newer, modern technologies. The use of various software programs and data formats and hardware devices makes sharing data or models difficult[2].

F. Computational and Resource Requirements

When creating a learning system, it is important to consider the differences in computing power, storage capacity and/or network speed that exist among institutions.

For example, some institutions may have very powerful computers (servers) while others will be struggling to maintain adequate equipment. If the design process does not account for these differences, then the smaller institutions could fall behind or be excluded from using the new learning system [2], [3].

XI. Proposed Conceptual Framework

Based upon the thematic analysis of the literature reviewed in this paper, we propose a Privacy-Preserving Collaborative Healthcare Learning Framework. Within this framework, each participating institution maintains control over their respective patient data; however, all participating institutions will conduct their own local model training.

Additionally, each participating institution will transmit their trained model updates to an aggregation server. After receiving all of the update messages from the various institutions, the aggregation server will combine these updates into a single "global" model.

Finally, the aggregation server will send the newly developed global model back to each of the participating institutions. Figure 2 illustrates the primary interconnecting challenge areas that the proposed framework addresses. Figure 3 illustrates the proposed framework itself.

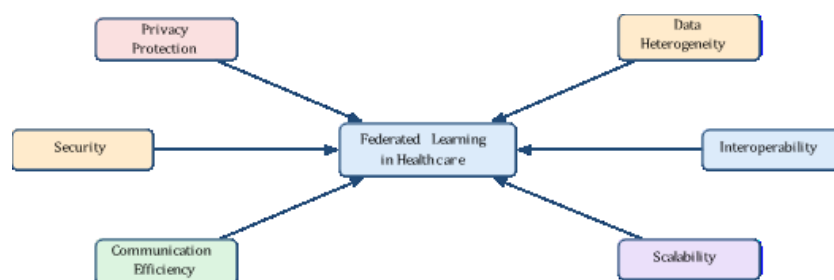


Fig. 2. Major interconnected challenges in healthcare Federated Learning.

1

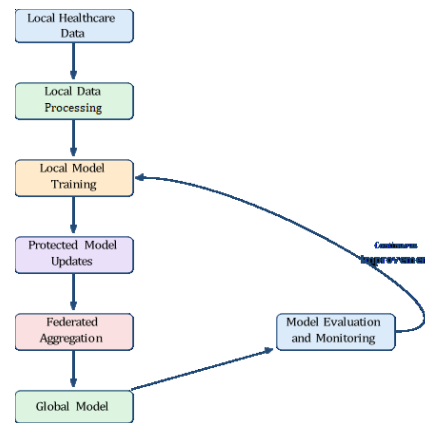


Fig. 3. Proposed conceptual framework for privacy-preserving collaborative healthcare learning.

The privacy and security protections, the heterogeneity of data, the efficiency of communications, the ability to scale and the interoperability of all the different systems used to collect and use information about a patient's health are considered as inter-related needs and not as individual parts of the Internet of Things (IoT) that would be used to monitor a patient's health.

XII. Findings from the Literature

As demonstrated through the literature review conducted for this research project, FL can facilitate collaborative machine learning within the field of medicine by allowing multiple users/sites to collaboratively build models based upon data from those users/sites, while avoiding the need to transfer or share their own patient-related data to a single centralized location [1]-[5]. Data collected at different medical facilities may differ due to differences in demographics of the patients being treated at each facility; variations in distribution of patient-related data across the different medical facilities; differences in the type of equipment used to collect/process patient-related data; and the geographic location of the medical facility. A common issue that occurs with repeat communication is that every time there is a repeat communication, each participant site sends model updates during the training process. Repeatedly sending model updates puts additional pressure on the network infrastructure and computational resources of all participating sites. Privacy/security issues will remain regardless of whether the initial data remains local. Issues will arise when sending model updates themselves and/or in the means of sending model updates between participating sites [1]-[3]. The literature also indicates that scalability and interoperability are necessary for FL to be implemented practically.

Additionally, differences in systems, data format, and technology can hinder communication between participating sites [2], [3].

XIII. Discussion

The use of Federated Learning (FL) to build models based on patient data could create a way to build models with the ability to learn in healthcare organizations where there are serious restrictions about how patient data is shared. Studies have illustrated how FL can be applied in the fields of healthcare analytics, medical image processing, smart healthcare, and collaborative learning.

The implementation of FL on decentralized systems may lead to some technical difficulties in the development process of FL. Data collection from patients varies greatly, so this variation could affect the way FL trains its models. As well, the amount of time FL systems communicate with each other during training processes (i.e., when they exchange model updates) can be an additional source of cost due to increased use of network resources and computing power [2], [3].

While FL reduces the need for transferring large quantities of raw patient data, it is important to protect model updates and the methods in which these updates are transmitted. Depending upon the type of FL system being used, it may be required to utilize different types of privacy-preserving/security tools [1], [2].

Additionally, in order to successfully implement FL within a healthcare system there must be an understanding as to how it may be expanded into every aspect of that system. In particular, this means that FL should be compatible with each of the multiple information systems being utilized by the many different organizations who are participating in its utilization.

XIV. Limitations

The basis of this study was a review of previous studies.

Therefore, the findings of this study are limited in two ways: the amount of previous research that was reviewed, and the quality of the previous research. The model developed in this study is conceptual. As a result, it has not yet been implemented in practice and should not be viewed as a feasible solution to the problems that exist within healthcare systems until it is put into use in real-life healthcare settings.

1

Additionally, this study did not collect any primary data from healthcare organizations. Future research can address this limitation by using the model to develop and test a model (e.g., determine if the model effectively protects patient privacy; determines if the model meets the communication needs of healthcare professionals; determines if the model can support future growth; determines if the model can integrate with current models; determines if the model accurately predicts outcomes when used with real-world data).

XV. Future Scope

- Develop a method for securely aggregating models in federated learning (FL) and identify techniques to handle malicious or untrustworthy clients.
- Develop an approach for dealing with non-identically distributed data in healthcare FL.
- Investigate methods to decrease the amount of communication required for exchanging model updates in FL.
- Design scalable architectures that will allow many healthcare institutions and devices to be involved with FL while maintaining good performance.
- Develop methods to increase the compatibility of various healthcare information systems, data formats, and technology.
- Evaluate the results of applying learning methods to real-world or realistic healthcare data sets from multiple institutions.
- Investigate methods to make FL more understandable and reliable within healthcare settings where transparency is important.
- Explainable and trustworthy FL: study methods that make FL more explainable and trustworthy in healthcare environments where transparency matters.

XVI. Conclusion

FL provides a method of distributed collaboration for machine learning with healthcare-related problems in which there are restrictions on directly sharing patient information. As indicated by the reviewed literature, FL is currently being applied to several areas including medical image analysis, smart health care, health care analytics, and multi-institutional learning [1]–[5].

However, the development of an effective FL-based application is dependent upon much more than merely keeping data localized; rather, the design of the application will be influenced by differences in data characteristics, privacy and security concerns, efficient communication methods, scalability issues, available computing resources, and interoperability. The conceptual model developed here provides a basis for future research by bringing together these factors. Since this model has not been tested empirically, future research should assess it within actual multi-institution healthcare environments utilizing relevant datasets.

References

- [1] S. S. Sandhu, H. T. Gorji, P. Tavakolian, K. Tavakolian, and A. Akhbardeh, "Medical imaging applications of federated learning," *Diagnostics*, vol. 13, no. 19, p. 3140, 2023, doi: 10.3390/diagnostics13193140.
- [2] S. R. Abbas, Z. Abbas, A. Zahir, and S. W. Lee, "Federated learning in smart healthcare: A comprehensive review on privacy, security, and predictive analytics with IoT integration," *Healthcare*, vol. 12, no. 24, p. 2587, 2024, doi: 10.3390/healthcare12242587.
- [3] M. Nasajpour, S. Pouriyeh, R. M. Parizi, M. Han, F. Mosaiyebzadeh, L. Liu, Y. Xie, and D. M. Batista, "Federated learning in smart healthcare: A survey of applications, challenges, and future directions," *Electronics*, vol. 14, no. 9, p. 1750, 2025, doi: 10.3390/electronics14091750.
- [4] P. Dhade and P. Shirke, "Federated learning for healthcare: A comprehensive review," *Eng. Proc.*, vol. 59, no. 1, p. 230, 2024, doi: 10.3390/engproc2023059230.
- [5] R. Haripriya, N. Khare, and M. Pandey, "Privacy-preserving federated learning for collaborative medical data mining in multi-institutional settings," [venue, volume, pages, year, and DOI missing: the source reference list was cut off here — please complete].