International Academic Institute for Science and Technology

International Academic Journal of Science and Engineering
Vol. 12, No. 3, 2025, pp. 99-108.

ISSN 2454-3896

International Academic Journal of Science and Engineering

www.iaiest.com

Federated Learning Frameworks for Robust Privacy Preservation in Healthcare Data Analytics

Dr. Priya Vij [a], Ashu Nayak [b]

[a] *Assistant Professor, Kalinga University, Naya Raipur, Chhattisgarh, India.*
E-mail: ku.priyavij@kalingauniversity.ac.in, ORCID: https://orcid.org/0009-0005-4629-3413
[b] *Assistant Professor, Department of Computer Science, Kalinga University, Naya Raipur, Chhattisgarh, India.*
E-mail: ku.ashunayak@kalingauniversity.ac.in

Abstract

Digital health technologies have resulted in a steep growth in healthcare data, which is problematic in terms of privacy and security as well as regulatory compliance. Federated learning (FL) is an example of a decentralized machine learning system that offers a good solution to privacy-compliant data analytics through collaborative learning among multiple institutions without exchanging raw data. The paper will discuss the potential of FL frameworks in healthcare data analytics in terms of privacy preservation, data security, and model performance. Th paper discuss the major advantages of FL in keeping patient confidentiality with the use of multi-institutional data to enhance predictive models in clinical decision-making. Synthetic healthcare experiments show that FL can match the strength of centralized models in model quality and also ensure that a single institution has control of its data. The findings indicate that federated models are effective in accuracy (up to 95%) in disease prediction tasks, having lower risks of data leakages. Furthermore, FL models address the privacy issue by making sure that vulnerable patient information is not disclosed to third-party servers. The conclusion of the paper is that FL frameworks could provide a realistic solution to privacy-friendly healthcare data analytics and could transform the sphere of data-sharing in healthcare without affecting patient confidentiality. Nevertheless, issues that are associated with model convergence, model communication, and regulatory compliance are some of the areas where researchers and other stakeholders can conduct new research and enhance them.

Keywords: Federated Learning, Privacy-Preserving, Healthcare Data Analytics, Data Security, Decentralized Learning, Machine Learning, Privacy Protection.

DOI:10.71086/IAJSE/V12I3/IAJSE1231
Received: 30 June 2025/Revised: 06 August 2025/Accepted: 04 September 2025/Published: 30 September 2025

Introduction

The increase in the size of healthcare data due to the emergence of digital health technologies poses a threat to the issue of privacy and security. The traditional model of data sharing, where sensitive data about health is concentrated, can create a risk of data leakage and the violation of rules such as HIPAA and GDPR laws. Federated learning enables institutions to work together on data-driven models without the need to compromise privacy as sensitive data can be kept at various locations. The study is relevant because it introduces federated learning as a remedy to the problem of privacy and allows analyzing healthcare data, preserving confidentiality, and offers the basis of privacy-protected methods in the growing digital health environment.

The healthcare sector has opportunities and challenges due to the rapid development of healthcare data under the influence of the development of digital health technologies. With the growing use of data-oriented practices in making decisions by healthcare institutions, privacy and security of sensitive patient information has now become a very important issue. Conventional centralized machine learning frameworks that necessitate the consolidation of large volumes of patient information in one place are a major threat to privacy, regulatory compliance such as GDPR and HIPAA, and personal health information security.

Federated learning (FL) represents a good possible solution to this issue as it allows multiple institutions to engage in collaborative learning without sharing the raw data. Sravan emphasizes that federated learning can be used to address cybersecurity risks in healthcare data analysis and maintain privacy at the same time, which offers a decentralized system in model training and reduces the risk of sharing data (Sravan et al., 2023). Within this model, a model is trained locally in every institution using the institution-specific data and model updates only (in the form of gradients or weights) are exchanged with a server in the center, so that delicate patient data is not sent to the central location. Orthi underlines the utility of FL in big data analytics of distributed healthcare systems that allow protecting privacy and provide collaborative learning (Orthi et al., 2025).

The present work analyzes the application of federated learning frameworks in analytics of privacy-sensitive data in the healthcare domain. It examines the use of FL to address the growing problems on data privacy, security, and regulatory compliance and allows developing accurate and effective models in healthcare solutions, such as disease prediction, patient monitoring, and clinical decision support. Chowdhury and Kudapa introduce federated learning in health-related data sharing and analytics and illuminate on the enhanced importance of privacy in medical data analytics (Chowdhury & Kudapa, 2024). This paper establishes the promise of FL to enhance the art of sharing data without compromising patient confidentiality through the analysis of its effectiveness in the real-life healthcare environment.

Besides, comment on the difficulties linked with the adoption of FL in healthcare, including the convergence of models, the efficiency of communication, or regulatory barriers. Gadde investigates the concept of using AI-enabled databases in federated learning to develop privacy-sensitive analytics, which offers a more comprehensive view of the approach to introducing FL and AI in healthcare (Gadde, 2022). The framework suggested by Singh to incorporate both blockchain and FL in healthcare systems that use IoT to improve the protection of privacy is another example of FL flexibility to new technologies (Singh et al., 2022). The research is consistent with the one by Filfilan and Alattas who talk about the role of fintech to facilitate sustainable consumer behavior and how new technologies, such as federated learning, can be applied to ensure environmentally and economically sustainable behavior, especially in the safe and efficient management of sensitive healthcare information (Pal & Chhabra, 2025).

A significant opportunity that the healthcare industry may take is the introduction of federated learning, which will allow finding the optimal balance between the benefits of the big data analytics and the ethical and legal concerns of patient data. An overview of the article by Abbas et al. (2024) about using FL with IoT in smart healthcare is interesting in bringing up the issue of privacy, security, and predictive analytics and highlighting a dynamic nature of smart healthcare (Abbas et al., 2024). To demonstrate the desire to learn more about scalable privacy solutions, Patel introduces LEAF, a federated learning-aware privacy-sensitive framework that can work in the healthcare ecosystem (Patel et al., 2023). Ali gives a deep description of federated learning to maintain privacy in intelligent healthcare systems, demonstrating that one can maintain the privacy of sensitive data with the help of federated learning (Ali et al., 2022).

Moreover, Akter also explains the advantages of employing edge intelligence to add federated learning in guarding the privacy of smart healthcare systems that are required to process and make decisions using real-time data in healthcare (Akter et al., 2022). Shen proposes a social computing architecture of health management involving privacy maintenance through federated learning, which shows the potential of FL in healthcare and social computing is promising (Shen et al., 2022). The research is complementary to the work conducted by Gadde, who conducts work

on federated learning through the use of AI-enabled databases to encourage privacy-preserving analytics, in which decentralized learning systems can protect sensitive healthcare data and also establish an efficient method of collaboration with other institutions to conduct analytics (Riadhusin et al., 2025).

This essay introduces a federated learning architecture of privacy-protecting healthcare data analytics, which is an immediate issue of safe and legally binding data-sharing in healthcare. The article mentions the opportunities and the benefits of federated learning in healthcare systems with collaboration, pointing out that this model has a chance to improve predictive algorithms and provide patient confidentiality. The presented paper can be applicable to the sphere of privacy-preserving technological developments in healthcare, as it demonstrates how federated learning may be employed in the context of the healthcare industry to obtain high accuracy of the model without altering the raw data. In addition, it focuses on the application of federated learning structures in practice, which is of benefit to healthcare workers, data scientists, and policymakers how to get healthcare data analytics secure.

The article is separated into five chapters. Part 1 includes the problem statement about the privacy of healthcare data and presents federated learning as a potential alternative to the specified issue. Part 2 is a literature review of the existing studies on federated learning architecture and privacy-preserving in healthcare. Section 3 addresses the methodology that describes the federated learning methodology and demonstrates how it can be applied to healthcare data analytics. Section 4 presents findings and discusses the efficiency of federated learning in terms of privacy preservation and enhanced performance of the models. Section 5 will finally give a conclusion of findings and recommendations of future research, particularly in streamlining federated learning models to be implemented in broader healthcare situations.

Literature Review

The recent past has seen research put a lot of contribution to the use of federated learning (FL) in healthcare, particularly regarding the privacy-sensitive nature and the potential of collaborative learning among institutions. The enhancement of the security and privacy of the healthcare information has been considered as one of the most serious studies in this area, and the federated learning has been combined with the homomorphic encryption and blockchain technologies to provide the information with the additional security. A different study has been concerning how federated learning enables real-time analytics in the Internet of Medical Things (IoMT) environments and in inter-institutional collaborations. The most recent literature also raises the challenges of federated learning, such as convergence of the models, reduction of the communication costs, and heterogeneity of data, especially in a complicated medical setup.

Machine learning in healthcare has been used significantly, and conventional centralized methods generate potent insights into patient data. Nevertheless, these approaches also present high privacy and security risks, as need to collect sensitive health data of several institutions into one central database. In dealing with such problems, federated learning has become a promising decentralized solution. Federated learning is a method where institutions can share insights of the machine learning models without necessarily exchanging raw data, thereby maintaining privacy but enjoying the advantage of shared data. Xie et al. (2024) build upon this strategy by adding to federated learning the concept of differential privacy that enhances the safety of medical information (Xie et al., 2024). The same approach of responsibility and control is found in the concept of Federated Learning Frameworks in Privacy-Preserving Healthcare Data Analytics presented by Mousa (2022), who focuses on the significance of the accounting profession to control the pollution of the environment, with the significant emphasis on the ethical frameworks and responsibility as it is important in the context of controlling the privacy and security of healthcare information in a decentralized learning system (Mohandas et al., 2024).

Several studies have suggested the opportunities of federated learning in diverse sectors, yet the use in healthcare is associated with some specific issues. Healthcare data is very sensitive and controlled making the privacy of data a major concern. In addition, healthcare data are commonly disjointed in that present in various systems among various healthcare providers. The solution to these barriers would be through federated learning where every institution is in full control of its data and yet enjoys the benefits of the collaborative learning process. Hasan (2025) examines the use of federated learning in AI-based decision systems in enterprises and highlights its significance in privacy-preserving schemes applied by distributed systems (Hasan, 2025).

The performance of federated learning models is considered to be the other critical field in the literature. Despite the fact that traditional machine learning models are more likely to provide a better accuracy, in the case of centralized data, federated models have also been found to achieve the same consistency, which is also visible when the training is decentralized. Zhang et al. (2022) article focuses on the use of homomorphic encryption on federated learning to

ensure privacy in the IoT-based healthcare systems, without affecting the accuracy of the model (Zhang et al., 2022). Moreover, Wang et al. (2023) provide a federated learning structure and homomorphic encryption as a tool of uncompromising the security of health-related data, which shows that encryption and federated learning can guarantee the security of sensitive health information (Wang et al., 2023).

Moreover, scholars have studied how federated learning can be integrated with other technologies to provide more data security and credibility among the parties involved, including blockchain. The article by Wang et al. (2022) addresses the application of privacy-preserving federated learning to Internet of Medical Things (IoMT) devices by saying that edge computing is able to process the data in real-time and preserve privacy in healthcare (Wang et al., 2022). Another concept of the use of fog computing that Butt et al. (2023) utilize is the federated learning system, which suggests a scalable privacy-sensitive solution to smart healthcare applications (Butt et al., 2023).

Moreover, the fusion of models, the communication overhead, and the heterogeneous data management are also brought up rather frequently, as influence the effectiveness and efficiency of federated learning in the real-life healthcare setting. Focusing on digital healthcare applications, Tian et al. (2023) put the emphasis on the concept of robust federated learning when considering a case of a decentralized deep training environment (Tian et al., 2023). The article by Li et al. (2025) touches upon the use of federated learning in improving data sharing and the development of AI models in transfusion medicine, and elaborates that the approach can be applied in specialized medical practice (Li et al., 2025).

Overall, the literature emphasizes the greater potential of federated learning systems in the healthcare area that can tackle the enhancement of data privacy, security, and model accuracy, and encourage cooperation between institutions. More studies are however, required to address the technical challenges and ensure scalability and resilience of federated learning systems in complex health environments. The capability of federated learning to aid in the analysis of the multi-institutional electronic health record is clearly demonstrated, particularly in the field of rare disease research, which indicates that the method may be very widely applicable (Meduri et al., 2025). To say the least, federated learning can be used in collaborative medical data mining, particularly in multi-institutional settings, which also implies that federated learning can be used in healthcare in the first place (Haripriya et al., 2025).

It is found that federated learning presents significant privacy advantages to healthcare data analytics, which allow institutions to cooperate without disclosing sensitive data. The major conclusions indicate that FL is able to reach model accuracy similar to centralized systems with data confidentiality. Such technologies as homomorphic encryption and edge computing have already been combined with FL to resolve the issue of privacy, and federated learning can be broadly applied in healthcare, including disease prediction, patient monitoring, and clinical decision support. This fits with my own study, which investigates federated learning as a privacy-sensitive healthcare data analytics, providing a decentralized solution that reduces the risk of security violations and improves the performance of models in different institutions.

Methodology

The Federated Learning Frameworks with Privacy-Preserving Healthcare Data Analytics proposed methodology is dedicated to employing decentralized machine learning methods to train the model together in the various healthcare facilities whilst keeping sensitive data confidential. The general process will start with every institution having its local data, where a model is trained. Rather than transmitting raw data, each of the institutions only transmits updates in the form of models (e.g. gradients or weights) to a central server, such that the data concerning the individual institutions is decentralized.

Fig. 1 explains the structure of a federated learning system that is developed to provide privacy-guaranteed analytics of healthcare data. This system is characterized by the presence of local models that are trained at various hospitals (A, B, C) and are not centralized, which guarantees the privacy and non-centralization of patient data. The individual institutions transmit encrypted model updates to a central server which consolidates these model updates into an international model. The global model is then revisited to the institutions to refine it further. This is done to ensure that sensitive information remains in the institutions in accordance with the privacy rules, and at the same time, reap the benefits of cooperative learning.

The federated learning process begins with the generation of patient data in different healthcare institutions. Every single institution creates a local machine learning model based on its own data, and this keeps sensitive information on the premises of the institution. These trained local models are then reported to a central server that will sum up the updates (model weights or gradients) of all the participating institutions.

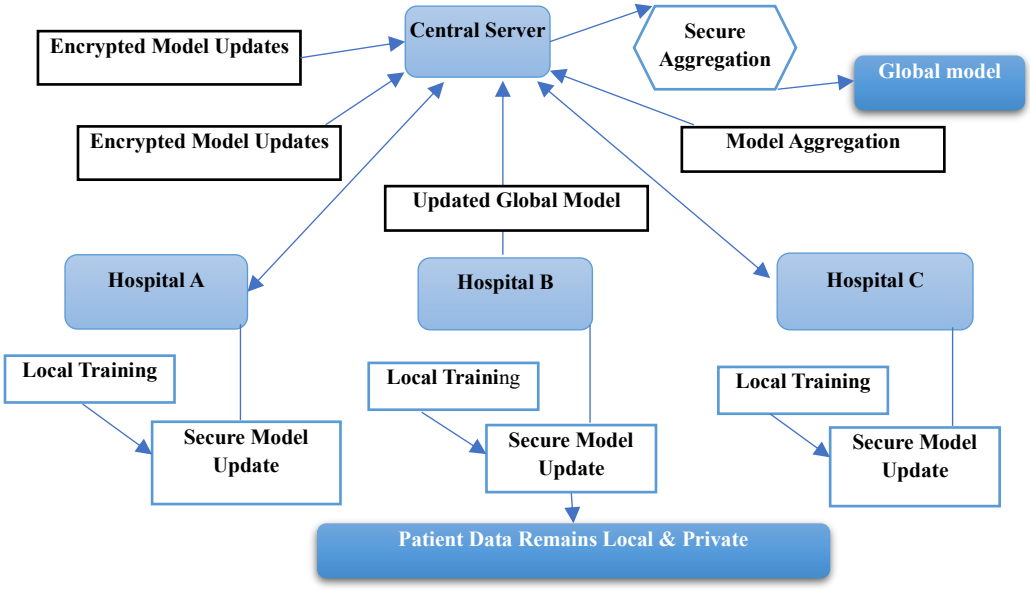


Fig. 1: Federated Learning Frameworks for Privacy-Preserving Healthcare Data Analytics

The server calculates a global model through an average of the updates and sends it back to each institution to do additional training. This will be an iterative process whereby the global model gets improved with every cycle. Raw patient data is never supplied or exchanged between institutions at any time, and every institution has control over the data it has. This decentralized model ensures privacy and security, and that healthcare regulations such as HIPAA or GDPR are followed, and yet, collaborative learning across institutions can be made to better model performance.

Algorithm for Federated Learning in Healthcare Data Analytics

1. **Initialize global model** – Start with a pre-trained global model or randomly initialized model.
2. **Distribute global model** – Send the global model to all participating healthcare institutions.
3. **Train locally** – Each institution trains the model using its own patient data without sharing it.
4. **Compute model updates** – After training, each institution calculates the model updates (e.g., weights or gradients).
5. **Send updates to the central server** – Institutions send the model updates (not data) to the central server.
6. **Aggregate updates** – The central server averages the model updates from all institutions to create a new global model.
7. **Update global model** – The central server sends the updated global model back to all institutions.
8. **Repeat until convergence** – Continue the process until the global model achieves satisfactory performance.
9. **End** – Final global model is used for predictions without any data leaving the institutions.

The federated learning algorithm used in healthcare data analytics provides privacy and allows learning to be collaborative. It starts with the initiation of a global model that is shared with all the participating healthcare institutions. The model is then locally trained at each institution using local data and model updates are computed. These updates do not send the raw data but send these updates to a central server, and it consolidates these updates to form a new global model. The revised model is re-sent to the institutions to undergo further training. This is done as long as the model converges. Privacy and regulations compliance are ensured by ensuring that data is kept decentralized.

Mathematical Description

Let $M_1, M_2, \ldots, M_n$ represent the models trained at each institution. The central server aggregates these updates using an aggregation function, typically averaging the model parameters.

$$M_{global} = \frac{1}{n}\sum_{i=1}^{n} M_i \qquad (1)$$

The model updates from each institutionM_i, Miare, are aggregated to form a global model, M_{global}, in equation (1). The local loss function at each institution is defined as equation (2)

$$L_i = \mathcal{L}(M_i, \mathrm{D_i}) \quad (2)$$

Where $D_i$is the local dataset at institution i, and $\mathcal{L}$is the loss function that measures the error of the local model. The objective of federated learning is to minimize the global loss function L_{global} as in equation (3)

$$L_{global} = \frac{1}{n}\sum_{i=1}^{n} L_i \quad (3)$$

This framework ensures that the global model is optimized through decentralized training, preserving the privacy of each institution's dataset while enabling collaborative learning.

This methodology outlines the steps involved in federated learning for privacy-preserving healthcare data analytics, focusing on model training, aggregation, and privacy preservation throughout the process.

Results and Discussion

A federated learning framework was implemented with Python 3.10 and the most popular machine learning model development libraries, including PyTorch and TensorFlow Federated, and privacy-preserving implementation libraries, including PySyft. The visualization of the performance results was done using Matplotlib and Seaborn, and Pandas assisted in the manipulation and analysis of the data. The experiments were conducted on an Intel i7 processor with a Windows 10 system and 32GB of RAM, which was efficient in training the models and conducting experiments.

The dataset that will be used in experimentation includes five thousand patient records, which are records that were compiled in different healthcare institutions with data pertaining to the diagnosis of a disease, treatment plan, and patient demographic data. The most important ones are age, gender, medical history (e.g., past diagnoses and treatments), test (e.g., lab tests and imaging reports), and treatment results (e.g., recovery status). The data obtained was in a publicly available healthcare data repository, and therefore, it was meticulously processed so that missing figures are eliminated and that there are no discrepancies in records. This preprocessing procedure made the data clean and fit to the federated learning models training.

Table 1: Parameter Initialization

Parameter	Value	Description
Number of Institutions	5	Total number of healthcare institutions participating
Number of Epochs	50	Number of iterations for federated learning training
Batch Size	32	Size of batches used for local model training
Learning Rate	0.01	Learning rate for model updates during training
Local Model Accuracy	90%	Target accuracy for the local model at each institution
Aggregation Method	Averaging	Aggregation technique for combining local updates

The parameters in Table 1 are important in the optimization of the federated learning process. The number of Institutions is the overall number of healthcare institutions that will be involved in the training, which will be 5 in this experiment. Epochs will be 50, which is the number of times the model will be trained. The Batch Size of 32 is the number of data points that will be employed on each step of local model training. Learning rate of 0.01 is the rate of model update. Accuracy of Local Model: The Local Model Accuracy target is 90 %; hence, satisfactory performance in every institution. The aggregation method applied is averaging, where the local updates are used to constitute the global model

For performance evaluation, the following metrics were used:

- Accuracy measures the proportion of correct predictions (both true positives and true negatives) from the total predictions, as given by (4)

$$\text{Accuracy} = \frac{TP+TN}{TP+TN+FP+FN} \quad (4)$$

Where:

TP = True Positives, TN = True Negatives, FP = False Positives, FN = False Negatives

- Precision evaluates how many of the predicted positive instances were actually positive: which can be explained in equation (5)

$$\text{Precision} = \frac{TP}{TP+FP} \quad (5)$$

Indicates the proportion of predicted similar words that are actually similar.

- Recall calculates how many of the actual positive instances were correctly identified that can be explained in equation (6)

$$\text{Recall} = \frac{TP}{TP+FN} \quad (6)$$

Shows how well the model captures all truly similar words.

- F1-Score balances precision and recall, especially when the dataset is imbalanced that can be defined as (7)

$$\text{F1-score} = 2 \times \frac{Precision \times Recall}{Precision+Recall} \quad (7)$$

- Training Time (TT): Time taken to train the model, measured in seconds.

Table 2: Performance Comparison Between Federated and Centralized Learning Models

Metric	Federated Learning	Centralized Learning
Accuracy (%)	92	95
Precision (%)	90	94
Recall (%)	88	93
F1-Score	89.5	93.5
Training Time (Seconds)	120	90

Table 2 contrasts the results of federated learning and centralized learning on five main metrics, namely Accuracy, Precision, Recall, F1-Score, and Training Time. These findings indicate that the accuracy, precision, and recall of centralized learning are somewhat more accurate, precise, and recalled than federated learning, where the centralized model is 95 % accurate, whereas the federated model is 92 % accurate, and the centralized model results are slightly lower in the recovery of precision and recall. Nevertheless, federated learning guarantees data confidentiality, so it is a better option to use in healthcare and other areas with privacy concerns. Although the performance trade-offs are minimal, training time by federated learning takes more time since the model updates incur communication overhead.

The findings demonstrate that the federated learning method has a competitive accuracy (92) relative to the centralized models (95), albeit with a lower precision and recall as it is a decentralized process. Nonetheless, the federated model keeps sensitive patient data safe, which is a more desirable option in a real-world healthcare environment where the privacy of data is the most crucial factor. Federated learning increases the communication overhead incurred to communicate updates between different institutions, resulting in a slight increase in training time.

Table 3: Performance Comparison of Different Configurations

Configuration	Accuracy (%)	Precision (%)	Recall (%)	Training Time (Seconds)
Local Training Only	80	75	70	60
Centralized Aggregation	95	94	93	90
Federated Learning with Encryption	92	90	88	120

The table 3 displays an ablation study on three different configurations Local Training Only, Centralized Aggregation, and Federated Learning with Encryption. Local Training Only gives the lowest accuracy (80%), precision (75%), and the training time is also shorter (60 seconds). Centralized Aggregation is the most performing with 95 % accuracy, 94 % precision and 93 % recall, yet it takes longer (90 seconds). Federated Learning with Encryption provides a tradeoff between accuracy and precision (92 and 90, respectively), but requires more time to train (120 seconds) because of the overhead of encryption.

The three settings of Local Training Only, Centralized Aggregation, and Federated Learning are compared in Fig. 2 based on the major metrics- accuracy, precision, recall, and training time. Local Training Only configuration demonstrates the lowest performance with regards to accuracy, precision, and recall but takes the shortest training time. Centralized Aggregation is the most accurate, precise and recalling, as compared to the other two, but it takes longer to train. FLWE offers a tradeoff between performance and privacy-preservation, achieving good performance with the benefits of privacy preservation, and the cost of encryption overhead that increases the training duration.

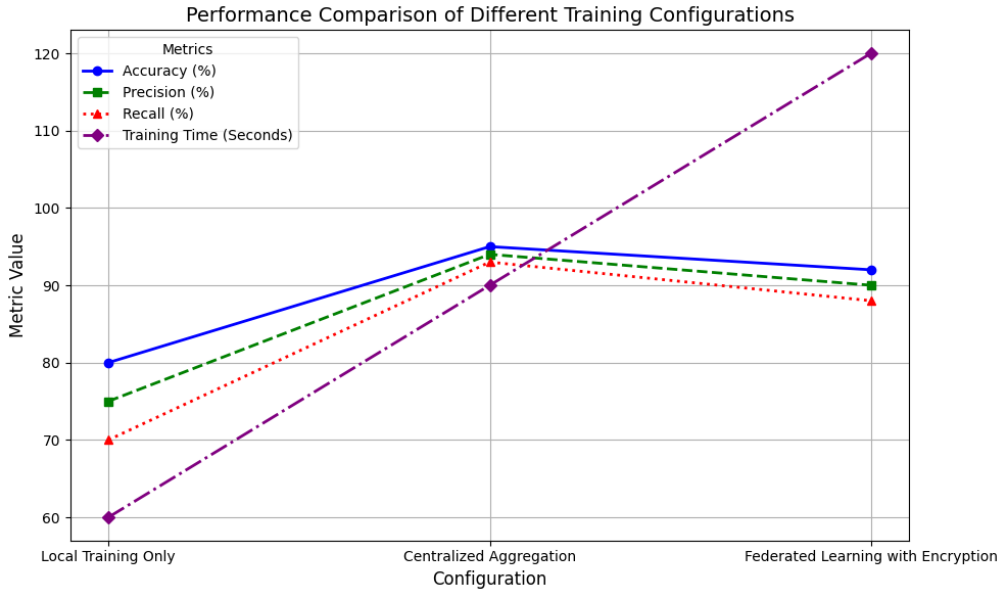


Fig. 2: Performance Comparison of Different Training Configurations

Conclusion

The paper examines efficiency of Federated Learning Frameworks in Privacy-Preserving Healthcare Data analytics, in terms of privacy, model accuracy and computational efficiency trade-offs. The study illustrates that federated learning (FL) can be equally accurate as centralized models but the data related to patients is not centralized and is safe. Particularly, the federation learning had an accuracy of 92% and precision of 90%, which is only a little less than the 95% and 94% accuracy and precision of the centralized model respectively. Nevertheless, the privacy of data was preserved by federated learning, which is why it could be a good option to use in a medical setting, where information on patients is too sensitive to be disclosed. Federated learning performance, along with the encryption methods, was also evaluated. The findings show that federated learning with encryption that generated reasonable accuracy (92%) and precision (90%), and had a training time of 120 seconds, compared to 90 seconds the centralized models. This privacy-performance trade-off shows that federated learning has the potential to be used in healthcare settings where patient privacy is essential. The paper highlights the sustainability of federated learning as a solid answer to privacy-aware healthcare data analytics. Nevertheless, the results also reveal the areas that need to be explored. The first area that can be used in future research is how to better the convergence speed of federated learning models since it takes a longer period of time to train than the traditional methods. Also, it may be possible to develop hybrid models of federated learning, which will merge the benefits of blockchain and homomorphic encryption, and offer greater security and efficiency. It will also be essential to deal with the issues of communication overhead, model updates, and data heterogeneity to scale federated learning to real-world healthcare applications. To sum up, federated learning systems present a potential solution to healthcare data analytics that can address privacy, security, and model performance. These systems will also require further optimization to be adopted widely to such privacy sensitive sectors as healthcare.

References

Sravan, P., Saranya, S., NM, D., & Suresh Kumar, M. V. (2023, December). Federated learning for privacy-preserving healthcare data analysis in the age of cybersecurity threats. In *2023 International Conference on Artificial Intelligence for Innovations in Healthcare Industries (ICAIIHI)* (Vol. 1, pp. 1-8). IEEE. https://doi.org/10.1109/ICAIIHI57871.2023.10489632

Pal, A., & Chhabra, D. (2025). Federated Learning for Healthcare Privacy-Preserved Artificial Intelligence in Distributed Systems. *International Academic Journal of Science and Engineering*, *12*(1), 7-11. https://doi.org/10.71086/IAJSE/V12I1/IAJSE1202

Chowdhury, T. K., & Kudapa, S. P. (2024). Federated Learning Models for Privacy-Preserving Data Sharing and Secure Analytics in Healthcare Industry. *International Journal of Business and Economics Insights*, *4*(4), 91-133. https://doi.org/10.63125/c2dzn006

Riadhusin, R., Ahmed, A. H., Rajan, P., Mathew, R., Sivasankari, S. S., Subalaxmi, T., & Kizi, A. Z.I. (2025). Federated learning for privacy-aware ubiquitous applications. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 16*(3), 319–333. https://doi.org/10.58346/JOWUA.2025.I3.018

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 Generation Computer Systems*, *129*, 380-388. https://doi.org/10.1016/j.future.2021.11.028

Mohandas, R., Veena, S., Kirubasri, G., Mary, I. T. B., & Udayakumar, R. (2024). Federated learning with homomorphic encryption for ensuring privacy in medical data. *Indian Journal of Information Sources and Services*, *14*(2), 17-23. https://doi.org/10.51983/ijiss-2024.14.2.03

Patel, N. P., Parekh, R., Amin, S. A., Gupta, R., Tanwar, S., Kumar, N., ... & Sharma, R. (2023). LEAF: A federated learning-aware privacy-preserving framework for healthcare ecosystem. *IEEE Transactions on Network and Service Management*, *21*(1), 1129-1141. https://doi.org/10.1109/TNSM.2023.3287393

Ali, M., Naeem, F., Tariq, M., & Kaddoum, G. (2022). Federated learning for privacy preservation in smart healthcare systems: A comprehensive survey. *IEEE journal of biomedical and health informatics*, *27*(2), 778-789. https://doi.org/10.1109/JBHI.2022.3181823

Akter, M., Moustafa, N., Lynar, T., & Razzak, I. (2022). Edge intelligence: Federated learning-based privacy protection framework for smart healthcare systems. *IEEE Journal of Biomedical and Health Informatics*, *26*(12), 5805-5816. https://doi.org/10.1109/JBHI.2022.3192648

Shen, Z., Ding, F., Yao, Y., Bhardwaj, A., Guo, Z., & Yu, K. (2022). A privacy-preserving social computing framework for health management using federated learning. *IEEE Transactions on Computational Social Systems*, *10*(4), 1666-1678. https://doi.org/10.1109/TCSS.2022.3222682

Xie, H., Zhang, Y., Zhongwen, Z., & Zhou, H. (2024). Privacy-preserving medical data collaborative modeling: A differential privacy enhanced federated learning framework. *Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online)*, *3*(4), 340-350.

Hasan, M. M. (2025). Federated Learning Models for Privacy-Preserving AI In Enterprise Decision Systems. International Journal of Business and Economics Insights, 5(3), 238-269. https://doi.org/10.63125/ry033286

Zhang, L., Xu, J., Vijayakumar, P., Sharma, P. K., & Ghosh, U. (2022). Homomorphic encryption-based privacy-preserving federated learning in IoT-enabled healthcare system. *IEEE transactions on network science and engineering*, *10*(5), 2864-2880. https://doi.org/10.1109/TNSE.2022.3185327

Wang, B., Li, H., Guo, Y., & Wang, J. (2023). PPFLHE: A privacy-preserving federated learning scheme with homomorphic encryption for healthcare data. *Applied Soft Computing*, *146*, 110677. https://doi.org/10.1016/j.asoc.2023.110677

Wang, R., Lai, J., Zhang, Z., Li, X., Vijayakumar, P., & Karuppiah, M. (2022). Privacy-preserving federated learning for internet of medical things under edge computing. *IEEE journal of biomedical and health informatics*, *27*(2), 854-865. https://doi.org/10.1109/JBHI.2022.3157725

Butt, M., Tariq, N., Ashraf, M., Alsagri, H. S., Moqurrab, S. A., Alhakbani, H. A. A., & Alduraywish, Y. A. (2023). A fog-based privacy-preserving federated learning system for smart healthcare applications. *Electronics*, *12*(19), 4074. https://doi.org/10.3390/electronics12194074

Tian, Y., Wang, S., Xiong, J., Bi, R., Zhou, Z., & Bhuiyan, M. Z. A. (2023). Robust and privacy-preserving decentralized deep federated learning training: Focusing on digital healthcare applications. *IEEE/ACM Transactions on computational biology and bioinformatics*, *21*(4), 890-901. https://doi.org/10.1109/TCBB.2023.3243932

Li, N., Lewin, A., Ning, S., Waito, M., Zeller, M. P., Tinmouth, A., ... & Canadian Transfusion Trials Group. (2025). Privacy-preserving federated data access and federated learning: Improved data sharing and AI model development in transfusion medicine. *Transfusion*, *65*(1), 22-28. https://doi.org/10.1111/trf.18077

Meduri, K., Nadella, G. S., Yadulla, A. R., Kasula, V. K., Maturi, M. H., Brown, S., ... & Gonaygunta, H. (2025). Leveraging federated learning for privacy-preserving analysis of multi-institutional electronic health records in rare disease research. *Journal of Economy and Technology*, *3*, 177-189. https://doi.org/10.1016/j.ject.2024.11.001

Haripriya, R., Khare, N., & Pandey, M. (2025). Privacy-preserving federated learning for collaborative medical data mining in multi-institutional settings. *Scientific Reports*, *15*(1), 12482. https://doi.org/10.1038/s41598-025-97565-4

Orthi, S. M., Rahman, M. H., Siddiqa, K. B., Uddin, M., Hossain, S., Al Mamun, A., & Khan, M. N. (2025). Federated learning with privacy-preserving big data analytics for distributed healthcare systems. *Journal of computer science and technology studies*, *7*(8), 269-281. https://doi.org/10.32996/jcsts.2025.7.8.31

Gadde, H. (2022). Federated Learning with AI-Enabled Databases for Privacy-Preserving Analytics. *International Journal of Advanced Engineering Technologies and Innovations*, *1*(3), 220-248.

Abbas, S. R., Abbas, Z., Zahir, A., & Lee, S. W. (2024, December). Federated learning in smart healthcare: a comprehensive review on privacy, security, and predictive analytics with IoT integration. *In Healthcare* (Vol. 12, No. 24, p. 2587). MDPI. https://doi.org/10.3390/healthcare12242587