Innovative Computing Review (ICR)
Volume 5 Issue 2, Spring 2025
ISSN$_{(P)}$: 2791-0024, ISSN$_{(E)}$: 2791-0032
Homepage: https://journals.umt.edu.pk/index.php/ICR

Check for updates

Article QR

Title:	**Privacy-preserving Federated Fog Distributed Database in Healthcare**
Author (s):	Seemab Firdous[1], Iman Nasir[2], and Maryam Tahir[3]
Affiliation (s):	Department of Information Technology, Faculty of Computing, University of Gujrat, Pakistan
DOI:	https://doi.org/10.32350/icr.52.05
History:	Received: June 21, 2025, Revised: July 24, 2025, Accepted: August 22, 2025, Published: December 29, 2025
Citation:	S. Firdous, I. Nasir, M. Tahir "Privacy-preserving Federated Fog Distributed Database in Healthcare," *Innov. Comput. Rev.*, vol. 5, no. 2, pp. 87-98, December. 2025, doi: https://doi.org/10.32350/icr.52.05.
Copyright:	© The Authors
Licensing:	This article is open access and is distributed under the terms of Creative Commons Attribution 4.0 International License
Conflict of Interest:	Author(s) declared no conflict of interest

A publication of
School of Systems and Technology
University of Management and Technology, Lahore, Pakistan

Privacy-preserving Federated Fog Distributed Database in Healthcare

Seemab Firdous[*1], Iman Nasir[2], and Maryam Tahir[3]

Department of Information Technology, Faculty of Computing, University of Gujrat, Pakistan

ABSTRACT The digital transformation of healthcare has increased the demand for analytical frameworks that can securely process the data. These frameworks address the rapidly growing volumes of medical data generated across interconnected hospitals and Internet of Medical Things (IoMT) ecosystems. Recent progress in distributed and privacy-preserving learning has reduced dependence on centralized storage of data. Most existing approaches are centralized in terms of model optimization. They pay little attention to underlying distributed data management issues in multi-institution healthcare environments. However, limited coordination between distributed healthcare data repositories often leads towards inconsistency, reduced reliability, and scalability. The final result negatively affects the reliability and scalability of collaborative healthcare analytics. In an effort to close this structural gap, the current study proposed the Federated Distributed Database System (FedDDBS). It is a coordinately designed hierarchical architecture consisting of robust database coordination as well as federated intelligence. The proposed approach enables healthcare institutions to perform local model training on protected medical data. It also ensures continuity and security of distributed data storage. Moreover, it deploys a pipeline of validation stages with multi-stage verification. Afterwards, it combines these verified updates. Experimental results proved that integrating the concepts of the DDBMS and Federated Learning (FL) enhanced data integrity and strengthened communication security. It also stabilized the model convergence without violating strict privacy provisions. In general, FedDDBS offers a scalable, high-assurance system for healthcare analytics. It delivers trustworthy intelligence within various medical facilities under the condition of adherence to privacy-preserving standards.

INDEX TERMS distributed databases, fog computing, federated learning, healthcare, internet of medical things

I. INTRODUCTION

In recent years, there has been a growing interest in privacy-preserving and distributed learning models for healthcare systems. These models maintain patient privacy and support collaborative intelligence. The digitization of healthcare has further complicated the need to specify analytical

frameworks. These frameworks can securely manage the medical-related data. The data is generated massively, increasing volumes across networked hospitals and IoMT networks.

FL has emerged as a key paradigm that enables collaborative intelligence without transferring raw patient records. Such transfers were recently required due to the presence of traditional data divisions [1]. Securing data protection at the network edge has become a significant challenge. This challenge arises when moving from hospital-centric services to patient-centered smart healthcare systems. The count of

*Corresponding Author: 24025956-005@uog.edu.pk

connected medical devices is expected to grow exponentially in the future [2].

Recent developments in distributed and privacy-preserving approaches have decreased the dependence on centralized repositories. Most of the existing approaches are left mostly optimizing the models [3]. Strict regulatory standards, such as HIPAA and GDPR restrict the offsite transfer of patient information. These strict privacy controls make the data utility and compliance complex to resolve [4].

FL reduces data sharing, it also adds to the problem of data quality, privacy attacks, and distributed infrastructure management. FL frameworks frequently do not possess powerful data administration technicalities. They need to prevent inference attacks or deal with the statistical non-homogeneity of varied datasets in hospitals [5].

Specifically, the absence of integrated DDBMS principles compromises data consistency, replication control, and interoperability. It delays the reliance of collaborative healthcare analytics on the scale and reliability.

A unified strategy, that integrates federated intelligence and distributed database infrastructure, is necessary. This approach supports privacy respecting and scalability healthcare analytics. The current study overcame this gap by presenting the FedDDBS, which combines FL with DDBMS-level transactional integrity to offer high-assurance next-generation healthcare data management. Major contributions of this research are as follows:

- An FedDDBS combining FL and distributed database transaction management for privacy-preserving healthcare analytics.
- Hierarchical architecture of Edge-Fog-Cloud provides data privacy, scalability, and consistency across various geography-located healthcare institutions.
- The introduction of Two-Phase Commit (2PC) Protocol for transactional atomicity and replication consistency across the distributed hospital databases.
- A fog-level multi-stage validation pipeline that integrates differential privacy, access control, and Z-score-based anomaly detection to eliminate invalid or malicious updates of the model.

II. RELATED WORK

In-depth studies have been conducted on privacy-preserving and distributed learning systems in healthcare systems. Fog-federation of FL to smart healthcare applications was an efficient approach in processing medical data near their origin and reducing the latency and data privacy risks. Their model demonstrated that decentralized model training at the hospital level may reduce risks posed by sharing the data first-hand [6].

Similarly, privacy-aware FL model applies a feature selection and local data sanitization in order to reinforce privacy-utility balance. The research of this nature is the basis of decentralized learning in medical settings. These studies primarily suggested privacy preservation and decentralized model training at the hospital level [7]. The concept of an Edge-IoMT framework that focused on fog nodes to processed data. In which group users controlled the context. This architecture is responsive and provides real-time healthcare analytics [8].

In contrast, a combined FL system was proposed that boosted secure patient

monitoring with a centralized system based on the concept of integrating IoMTs devices with the decentralized system. Their model demonstrated improved security and data integrity but required more effective mechanisms for managing distributed storage and standardization. They scaled FL to hierarchical Edge-Fog-IoMT in order to enhance responsiveness and security [9]. This issue was resolved by developing an adaptive aggregation approach that changed between Federated Averaging (FedAvg) and Federated Stochastic Gradient Descent (FedSGD) according to data divergence in real-time. New structures attempted to further address these two issues of heterogeneity and security [10].

DMFLNet, which is a decision-based chest X-ray classification framework. Although DMFLNet was a system in scheduling client involvement to save communication costs. It relies on a central server to make decisions, and that is a single point of failure. Although such solutions resolved the problem of heterogeneity of data and client involvement, they are based on centralization in coordination mechanisms [11]. In the field of security, Bi-LSTM autoencoder performs adaptive anomaly detection in IoMT. Although Fed Secure can catch the poisoning attacks with great efficacy, using deep learning (DL) models in detection causes the edge devices to start a great deal of computing power [12].

Additionally, recent surveys have concluded that although Blockchain enabled Federated Learning (BCFL) enhances security and trust, it still faces significant challenges related to latency and scalability due to blockchain transaction processing. Despite these limitations, the reviewed studies demonstrate that federated learning, hierarchical computing, and secure healthcare analytics have achieved substantial advancements. Most schemes revolve around model optimization and communication efficiency [13]-[14]. Statistical models are trained on the remote machines or isolated data centers, for instance a hospital or mobile phone, and the data is maintained locally [15].

Nevertheless, the authors of the reviewed studies state that training heterogeneous and large-scale networks introduces new challenges. These challenges have to be met with a radically original approach. Issues regarding distributed database management, for instance the issue of transactional atomicity, replication consistency, and coordinated commit protocols are hardly ever incorporated.

Consequently, the subject of data consistency and reliability is still problematic. These limitations highlight the need for a framework that jointly integrates FL with distributed data management to ensure privacy, consistency, and scalability in healthcare analytics.

III. PROPOSED ARCHITECTURE AND METHODOLOGY

The FedDDBS was designed as a hierarchical, privacy-sensitive system consisting of three layers that are interconnected, that is, Edge, Fog, and Cloud. This multi-layered design guaranteed safe cooperation of the healthcare institutions that are geographically dispersed. Furthermore, it also focused on the maintenance of patient confidentiality, interoperability between the heterogeneous environments, and ongoing and reliable FL. All layers have their own specific operations, which allow achieving effective model training, data exchange, anomaly detection, and world models optimization, as depicted in Figure 1.

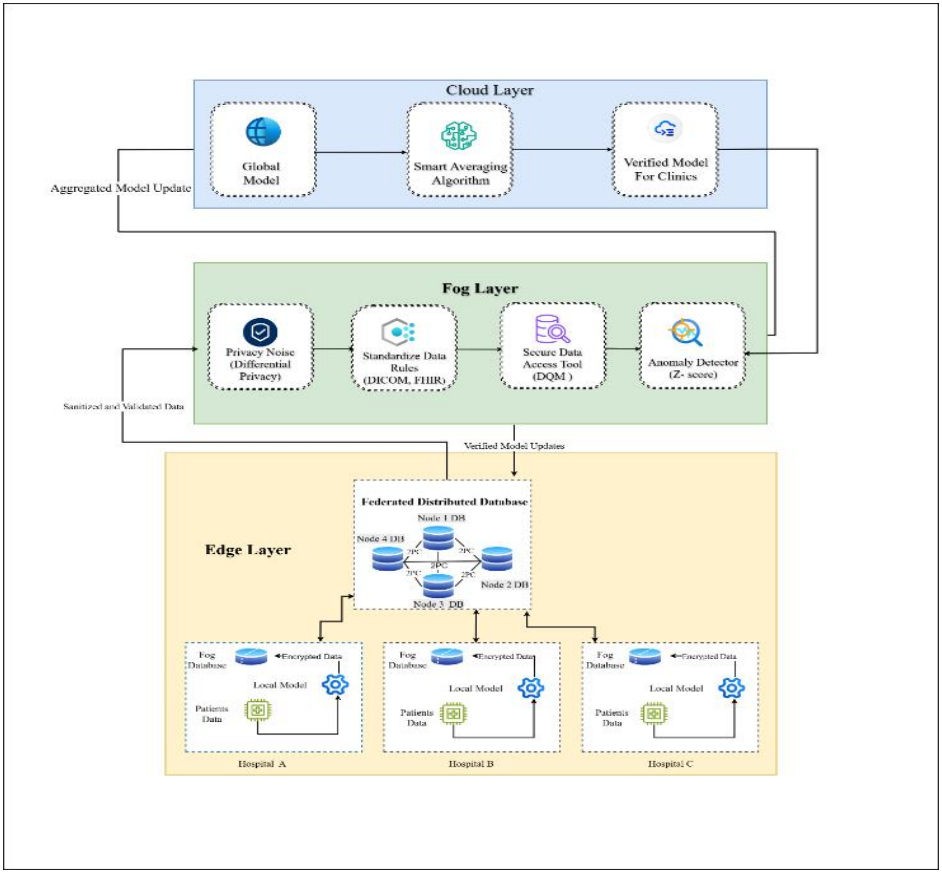

FIGURE 1. Proposed Federated Fog Distributed Database for Healthcare

A. EDGE LAYER

This layer operates in the safe zone of individual hospitals and takes care of local data storage, pre-processing, and model training. The patient data is gathered on the IoMT devices and Electronic Health Records (EHRs) and is safely stored in Fog DB which follows principles of DDBMS of replication, consistency, and encryption at rest. Each hospital maintains a local Fog Database instance at the Edge layer. The Edge Layer operates inside of the safe perimeter of the individual participating institutions (e.g., Hospital A, B, C). It manages all the local data, secures storage, and local model training.

1) LOCAL MODEL TRAINING

This part implements the principal method of decentralized training. In every hospital, the local model is trained on private patients' data with CNN-BiLSTM that identifies features and retrieves sequential dependencies. This might be helpful to enhance predictive modeling in healthcare systems. This ensures that confidential data never leaves out of the secure network of the institution. The local model is trained by minimizing the local loss function, as formulated in Equation Eq 1, following the standard local training objective described

in [16].

$$w_i^* = arg\ min_{w_i}\left[\frac{1}{|D_i|}\sum_{(x,y)\in D_i} L(f(x;w_i),y)\right] \quad (1)$$

The ensuing model changes are successfully stored and sent (Sent and Validated Data) to the Fog Layer over gRPC (gRPC Remote Procedure Calls) over mTLS (Mutual Tele Signature). It is a high-performance, modern data communication system. gRPC can be serialized data (has faster serialization than traditional JSON/REST), and mTLS (Mutual TLS) offered significant, bi-directional data authentication. It implies that the allocation of the Fog node and the hospital (Edge) should verify their identity to one another prior to any form of communication. This would guarantee complete encryption and safety of data during transmission against communicative eavesdropping.

2) LOCAL DATA MANAGEMENT (FOG DATABASE)

Next to training, the patients' data is managed locally in Fog Database. The purpose of this component is the persistence and security of the data. It implements cryptography protocols to generate encrypted data so that all sensitive patient information is encrypted safely in peace by the security system of the hospital. The selection of a system is based on a complex procedure involving consideration of multiple factors to guarantee an ideal solution for the issue that is chosen.

3) FEDERATED DISTRIBUTED DATABASES (FedDDBS)

This component represents the distributed FedDDBS. It works by connecting the individual Fog Databases all together in an effort to control consistency and integrity of data throughout the distributed nodes. Vendor-specific secure transport protocols, including Oracle Net Services, form the communication and data synchronization between these databases. In order to close the gap between the local storage and federated intelligence, the system uses the 2PC protocol. This guarantees that there is an atomically consistent update of the local Fog DB over the distributed network. This eliminates the split-brain data corruption that is inherent in the traditional FL configurations.

B. FOG LAYER

The Fog Layer is an important middle-ground pipeline, which facilitates the transition between distributed data management and FL. It is the regional DDBMS coordinator, in addition to being fed encrypted data in gRPC/mTLS, which coordinates distributed transaction logs to ensure global data consistency. The model updates are authenticated in the subsequent four phases:

1) PRIVACY-NOISE (DIFFERENTIAL PRIVACY)

Being the first part of the pipeline, it executes the Differential Privacy technique. Upon receiving model updates, the framework preserves privacy by injecting calibrated Gaussian noise, a statistical perturbation mechanism, according to the differential privacy formulation defined in Equation Eq2 [17]. This mathematical process makes it statistically impossible for an attacker to reverse-engineer the update to show any single patient's data.

$$\Delta\widetilde{w}_i = \Delta w_i + N(0,\sigma^2 I) \quad (2)$$

Here, the Gaussian noise term $N(0,\sigma^2 I)$ ensures that the contribution of any single record stays indistinguishable, claiming quantifiable privacy guarantees across

institutions.

2) STANDARDIZED DATA RULES

Following the above-mentioned details, the updates are transited by this module that conducts data standardizing tasks.

It implements universal model formats of healthcare data (including FHIR) to make metadata between heterogeneous systems of hospitals interoperable and consistent.

3) SECURE DATA ACCESS TOOL

The third component is a security check which performs secure access control. This tool also governs internal permissions and implements more granular access policies such that only authenticated and authorized processes have access to the data.

4) ANOMALY DETECTOR

Lastly, this component offers one of the principal security and integrity functionalities with the help of anomaly detection. It checks the updates against the Z-score statistical method (Eq 3). Statistical anomaly detection approach has been confirmed in [18]. If an update is a significant outlier (a high Z-score), it is flagged as anomalous potential sign of data corruption or a data poisoning attack—and is discarded.

$$z_i = \frac{\|\Delta\tilde{w}_i\| - \mu_{\Delta w}}{\sigma_{\Delta w}} \quad (3)$$

The data that successfully steps through all four stages is once again serialized and delivered in safe and efficient gRPC over mTLS protocol as the Aggregated Model Updates to Cloud Layer.

C. CLOUD LAYER

The Cloud Layer provides the integrator or the coordinator of the global model. The Aggregated Model Updates are delivered through the Fog Layer to it on its secure gRPC/mTLS endpoint, which ends the secure channel of the Fog.

1) GLOBAL MODEL AND SMART AVERAGING ALGORITHM

The Global Model is updated based on the received model, which is known as the Aggregated Model Updates. The main optimization engine is The Smart Averaging Algorithm. It uses Adaptive Federated Optimization technique to combine updates with different hospital nodes. This algorithm is intelligent in combining the efforts of all hospitals based on an adaptive aggregation mechanism, as shown in Eq 4, adaptive aggregation mechanism derived from [10].

$$\Delta W_{region} = \sum_{i=1}^{k} \beta_i \Delta\tilde{w}'_i \; where \; \sum_{i=1}^{k} \beta_i = 1 \quad (4)$$

The weights (β_i) are dynamically adjusted based on the reliability and performance metrics of each hospital node.

2) VERIFIED MODEL FOR CLINICS

The averaging process is governed by a global optimization rule, defined in Eq 5 global optimization process based on [19]. This uses adaptive learning rates to stabilize convergence in a heterogeneous (non-IID) environment.

$$W_{global}^{t+1} = Optimizer\left(W_{global}^{t}, \{\Delta W_{region}\}_{r=1}^{R}\right) \quad (5)$$

The end product of this entire process is the Verified Model of Clinics. This approved model is incorporated within the Continuous Learning Loop and is released to the hospitals involved so as to start the subsequent training cycle. According to this hierarchy, this distribution looks as follows:

- The Cloud sends the "Verified Model Updates" to the Fog Layer nodes that

receive the new model locally.

- The Fog nodes then inform their respective Edge Layer hospitals that a new model has been availed.
- The update is then effectively fetched by each hospital node via its regional Fog node, usually via a secure endpoint of a REST API (under HTTPS/TLS).

Such a hierarchical distribution is efficient, lessens the load on the central Cloud, and is superior in scaling. In the end, it creates a solid cyclical learning process, when the Cloud Layer further forces the Verified Model towards the Edge. This approach ensures that while the predictive intelligence grows globally, the underlying patient records remain locally locked and mathematically consistent, effectively solving reliability issues.

TABLE I

MATHEMATICAL NOTATIONS AND PARAMETERS

Symbol	Definition	Role in Architecture
$\boldsymbol{w_i}$	Local Model Weights	The trainable parameters of the CNN-BiLSTM at hospital.
$\boldsymbol{L}$	Local Loss Function	The function minimized during local training to reduce error.
$\boldsymbol{\Delta w_i}$	Weight Update	The calculated model update sent from Edge to Fog.
$\boldsymbol{\sigma^2}$	Noise Scale	The standard deviation of Gaussian noise added to privacy.
$\boldsymbol{z_i}$	Z-Score Metric	The statistical score used to detect anomalies ($z_i > 3$).
$\boldsymbol{\beta_i}$	Aggregation Weight	The reliability score assigned to each node during global averaging.
$\boldsymbol{W^t_{global}}$	Global Model Weights	The final aggregated model distributed back to clinics.

IV. EXPERIMENTAL SETUP AND IMPLEMENTATION

The application of the proposed FedDDBS framework is accomplished through the integration of distributed database elements, secured communication protocols, and the FL modules. This section provides the system set-up, parameter settings, and tool environment to verify the architectural workflow**.**

A. IMPLEMENTATION ENVIRONMENT

In order to illustrate the feasibility of the proposed FedDDBS architecture, the system prototype is developed based on a modular technology stack that is geared towards imposing distributed consistency and privacy. The implementation environment is subdivided into three main layers:

1) DEEP LEARNING (DL) ENGINE

The CNN-BiLSTM and the Global Aggregation algorithms had their architectural logic implemented in PyTorch (v1.13). This framework processes the dynamic graph of computation need in the adaptive federated optimization.

2) DISTRIBUTED DATABASE SYSTEM

The critical data management layer uses PostgreSQL (v14) instances that host as separate Edge nodes. The 2PC protocol is introduced into the application layer to solve the data consistency research gap at the higher layer to provide an atomicity of the transactions between these distributed nodes.

3) SECURE COMMUNICATION INTERFACE

The communication pipelines between the Edge, Fog, and Cloud Layers are constructed using gRPC with Protocol Buffers (Proto buff). This setup ensures low-latency serialization and strictly enforces mTLS (Mutual TLS) for encrypted, authenticated data streams.

4) STATISTICAL PROCESSING

The privacy-saving algorithms, namely Gaussian Noise injection Eq 2 and Z-Score Eq 3 validation, are coded in NumPy and SciPy in order to achieve accurate statistical calculation.

B. PROPOSED SYSTEM CONFIGURATION (PARAMETERS)

The framework is set with certain hyperparameters to guarantee reproducibility and provide a point of reference for future validation. As shown in Table II, choice of these values is informed by the existing literature standards on FL to ensure that the trade-off between data consistency and model utility is maximized.

C. VALIDATION STRATEGY

The implementation proposed is meant to be measured on two key performance indicators:

1) SYSTEM LATENCY

Estimating the time overhead that the 2PC Protocol is sustained at the redistribution phase in the model.

2) CONVERGENCE RATE

Training the global loss reduction rounds to ensure that the Z-Score validation at the Fog Layer does not have an adverse effect on the learning process. With the help of the industry-standard tools (Py Torch and PostgreSQL) and setup, the privacy-preserving parameters are provided in Table II .

This experimental setup is considered to strike a balance between the performance of the system and data safety. Such a modular setup confirms that the 2PC protocol is viable in a simulated setting and provides a strong, scalable basis of further application to physical Edge devices.

TABLE II

PROPOSED SYSTEM CONFIGURATION

Category	Parameter/Tool	Specification	Justification
Deep Learning	Framework	Py Torch 1.13	Manages dynamic computation graphs for FL.
	Model Architecture	CNN-BiLSTM	Optimized for sequential medical data feature extraction.
	Optimizer	Adam	Chosen for faster convergence on sparse gradients.
Database	Engine	PostgreSQL 14	Supports strict ACID compliance and serializable isolation.

Category	Parameter/Tool	Specification	Justification
	Consistency Protocol	2PC	Resolves the distributed consistency gap.
Security	Communication	gRPC over mTLS	Low latency, mutually authenticated secure channels.

V. CONCLUSION

This study discussed the critical need regarding the data management in the available FL models in healthcare. Although some previous researches have yielded efficiency in the application of computational aspects successfully; these have ignored the essential needs of data consistency and replication control that are required in enterprise-level medical systems. The current study addressed this gap by proposing FedDDBS, which is a new architecture that brings the privacy-preserving advantages of FL with the transactional integrity of DDBMS. By integrating the 2PC protocol at the Edge Layer and Z-Score anomaly detection at the Fog Layer, FedDDBS guarantees that global model intelligence can change without damaging the underlying data-synchronicity or transactional integrity. The scalability and interoperability constraints of conventional federated systems are effectively addressed by the proposed methodology, which offers a solid, high-assurance basis to IoMT.

A. FUTURE RESEARCH DIRECTIONS

Based on this architecture, future work would focus on the empirical testability of the framework in practice. The next steps would entail instant attempts to prove the scalability of the 2PC through simulation of a network of 50+ heterogeneous Edge nodes on parted datasets to measure the transaction latency at full load. Authors are also hopeful to deploy the prototype version of FedDDBS on the physical edge device, for instance the NVIDIA Jetson Nano, to measure the power consumption and inference of the model in a live IoMT scenario.

Author Contribution

Seemab Firdous: conceptualization, methodology, software, formal analysis, investigation, visualization, writing – original draft. **Iman Nasir:** methodology, software, validation, formal analysis, investigation, visualization, writing – review & editing. **Maryam Tahir:** conceptualization, resources, validation, writing – review & editing.

Conflict of Interest

The authors of the manuscript have no financial or non-financial conflict of interest in the subject matter or materials discussed in this manuscript.

Data Availability Statement

Data supporting the findings of this study will be made available by the corresponding author upon request.

Funding Details

No funding has been received for this research.

Generative AI Disclosure Statement

The authors did not use any type of generative artificial intelligence software for this research.

REFERENCES

[1] G. Yang et al., “Federated learning as a catalyst for digital healthcare innovations,” *Patterns*, vol. 5, no. 7, art. no. e101026, Jul. 2024, https://doi.org/10.1016/j.patter.2024.101026.

[2] M. Shafiq, J.-G. Choi, O. Cheikhrouhou, and H. Hamam, “Advances in IoMT for healthcare systems,” *Sensors*, vol. 24, no. 1, art. no. e10, Jan. 2024, https://doi.org/

10.3390/s24010010.

[3] M. Nasajpour et al., “Federated learning in smart healthcare: A survey of applications, challenges, and future directions,” *Electronics*, vol. 14, no. 9, art. no. e1750, May 2025, https://doi.org/10.3390/electronics14091750.

[4] R. Eden et al., “A scoping review of the governance of federated learning in healthcare,” *npj Digit. Med.*, vol. 8, no. 1, art. no. e427, Jul. 2025, https://doi.org/10.1038/s41746-025-01836-3.

[5] S. Pati et al., “Privacy preservation for federated learning in health care,” *Patterns*, vol. 5, no. 7, art. no. e100974, Jul. 2024, https://doi.org/10.1016/j.patter.2024.100974.

[6] M. Butt, N. Tariq, M. Ashraf, H. S. Alsagri, S. A. Moqurrab, H. A. A. Alhakbani, and Y. A. Alduraywish, “A fog-based privacy-preserving federated learning system for smart healthcare applications,” *Electronics*, vol. 12, no. 19, art. no. e4074, Oct. 2023, https://doi.org/10.3390/electronics12194074.

[7] T. U. Islam, R. Ghasemi, and N. Mohammed, "Privacy-preserving federated learning model for healthcare data," in *Proc. 2022 IEEE 12th Annu. Comput. Commun. Workshop Conf. (CCWC)*, Las Vegas, NV, USA, Jan. 26–29, 2022.

[8] S. Ghosh and S. K. Ghosh, “FEEL: Federated Learning framework for Elderly healthcare using Edge-IoMT,” *IEEE Trans. Comput. Social Syst.*, vol. 10, no. 4, pp. 1800–1809, Aug. 2023, https://doi.org/10.1109/TCSS.2022.3233300.

[9] B. Almogadwy and A. Alqarafi, “Fused federated learning framework for secure and decentralized patient monitoring in Healthcare 5.0 using IoMT,” *Sci. Rep.*, vol. 15, no. 1, art. no. 24263, Jul. 2025, https://doi.org/10.1038/s41598-025-06574-w.

[10] R. Haripriya, N. Khare, M. Pandey, and S. Biswas, “A privacy-enhanced framework for collaborative big data analysis in healthcare using adaptive federated learning aggregation,” *J. Big Data*, vol. 12, no. 1, art. no. 113, May 2025, https://doi.org/10.1186/s40537-025-01169-8.

[11] H. Malik, A. Naeem, R. A. Naqvi, and W.-K. Loh, “DMFL_Net: A federated learning-based framework for the classification of COVID-19 from multiple chest diseases using X-rays,” *Sensors*, vol. 23, no. 2, art. no. e743, Jan. 2023, https://doi.org/10.3390/s23020743.

[12] F. Alruwaili, S. P. Mohanty, and E. Kougianos, "FedSecure: A robust federated learning framework for adaptive anomaly detection and poisoning attack mitigation in IoMT," in *Proc. 1st IEEE Conf. Secure Trustworthy CyberInfrastructure IoT Microelectron. (SaTC)*, Fairborn, OH, USA, Feb. 25–27, 2025, https://doi.org/10.1109/SATC65530.2025.11137301.

[13] N. Nezhadsistani, N. S. Moayedian, and B. Stiller, “Blockchain-enabled federated learning in healthcare: Survey and state of the art,” *IEEE Access*, vol. 13, pp. 119922–119945, 2025, https://doi.org/10.1109/ACCESS.2025.3587345.

[14] Z. Ngoupayou Limbepe, K. Gai, and J. Yu, “Blockchain-based privacy-enhancing federated learning in smart healthcare: A survey,” *Blockchains*,

vol. 3, no. 1, art. no. 1, Jan. 2025, https://doi.org/10.3390/blockchains3010001.

[15] T. Li, A. K. Sahu, A. Talwalkar, and V. Smith, "Federated learning: Challenges, methods, and future directions," *IEEE Signal Process. Mag.*, vol. 37, no. 3, pp. 50–60, May 2020, https://doi.org/10.1109/MSP.2020.2975749.

[16] H. B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. Agüera y Arcas, "Communication-efficient learning of deep networks from decentralized data," in *Proc. 20th Int. Conf. Artif. Intell. Statist. (AISTATS)*, vol. 54, 2017, pp. 1273–1282.

[17] M. Abadi et al., "Deep learning with differential privacy," in *Proc. 2016 ACM SIGSAC Conf. Comput. Commun. Secur. (CCS)*, Vienna, Austria, 2016, pp. 308–318, https://doi.org/10.1145/2976749.2978318.

[18] T. Ohtani, R. Yamamoto, and S. Ohzahata, "IDAC: Federated learning-based intrusion detection using autonomously extracted anomalies in IoT," *Sensors*, vol. 24, no. 10, art. no. 3218, May 2024, https://doi.org/10.3390/s24103218.

[19] S. J. Reddi et al., "Adaptive federated optimization," in *Proc. 9th Int. Conf. Learn. Represent. (ICLR)*, Virtual Conf., May 3–7, 2021.