Diyala Journal of Engineering Sciences

Journal homepage: https://djes.info/index.php/djes

ISSN: 1999-8716 (Print); 2616-6909 (Online)

# Balancing Privacy and Performance: Federated Learning with Differential Privacy for Real-Time, Resilient Healthcare AI

Md Mahfuzur Rahman[1], Mst Sumya Yeasmin[2], Lamia Kabir[3], Tarek Abedin[4], Md. Helal Uddin[4], Monowar Mahmud[4], Atiqur Rahman[5], Mohammad Nur-E-Alam[4,6], and Md. Rokonuzzaman[7*]

[1]Department of Computer and Information Science, Southern Arkansas University, Arkansas, USA
[2]Department of Pharmaceutical Sciences, Faculty of Pharmacy, University of Cyberjaya, 63000, Cyberjaya, Malaysia
[3]Popular Medical College, Dhanmondi, 1205, Dhaka, Bangladesh
[4]Institute of Sustainable Energy, Universiti Tenaga Nasional (The Energy University), Jalan Ikram-Uniten, Kajang, 43000, Selangor, Malaysia.
[5]Department of computer science and engineering, Chittagong Independent University, 12 Jamal Khan Rd, Chattogram, Bangladesh
[6]Centre for Promotion of Research, Graphic Era (Deemed to be University), Clement Town, Dehradun, India
[7]Interdisciplinary Research Center for Sustainable Energy Systems (IRC-SES), King Fahd University of Petroleum and Minerals (KFUPM), Dhahran 31261, Saudi Arabia

**ARTICLE INFO**

***Article history:***
Received June 12, 2025
Revised August 03, 2025
Accepted August 07, 2025
Available online September 01, 2025

***Keywords:***
Federated Learning
Machine Learning
Decentralized Systems
Health care
Differential Privacy
Privacy-Preserving

**ABSTRACT**

The escalating dependence on artificial intelligence (AI) within the healthcare sector presents significant challenges pertaining to data privacy, regulatory adherence, and the pragmatic implementation of predictive models. This review meticulously examines the amalgamation of Federated Learning (FL) and Differential Privacy (DP) as a prospective framework to mitigate these issues within decentralized healthcare infrastructures. We conduct a comprehensive analysis of extant FL-DP frameworks, concentrating on their capacity to safeguard privacy, uphold performance standards, and function efficiently in real-time clinical settings. The review encompasses architectural advancements, edge computing methodologies, adaptive privacy budgets, and the contributions of blockchain and the Internet of Medical Things (IoMT) in facilitating secure data interchange. Comparative assessments and case studies are synthesized to evaluate model precision, scalability, and conformity with regulatory mandates. Notwithstanding significant advancements, we delineate critical deficiencies, including ethical dilemmas, algorithmic equity, data disparity, and obstacles to deployment. Our contributions consist of a benchmarking framework, the delineation of unresolved research inquiries, and actionable insights for the formulation of secure, just, and scalable FL-DP systems within the healthcare domain. This paper delineates a strategic framework for prospective research and the execution of privacy-preserving AI within clinical practice. The outcomes highlight significant potential for real-world clinical implementation, fostering enhanced patient care, supporting regulatory compliance, and enabling scalable, privacy-preserving AI adoption across diverse healthcare environments.

## 1. Introduction

The incorporation of artificial intelligence (AI) into healthcare frameworks is markedly reshaping the domain of medical diagnostics, prognosis, and tailored treatment by utilizing extensive arrays of multimodal patient information [1,2]. AI tools in healthcare, including radiology, genomics, wearable health devices, and electronic health records (EHR), are producing large datasets that can be leveraged through deep learning to create predictive models for early disease identification, clinical decision support, and

[*] Corresponding author.
E-mail address: md.rokonuzzaman@kfupm.edu.sa (M.R.)

DOI: 10.24237/djes.2025.18301

epidemic prediction [3,4]. Nonetheless, the conventional centralized machine learning (ML) systems, which require collating data into a unified repository, raise significant privacy and security issues, especially under strict healthcare laws like Health Insurance Portability and Accountability Act (HIPAA) and the General Data Protection Regulation (GDPR) [5-7]. In 2023, a prominent healthcare provider faced a $6 million penalty for violating HIPAA by compromising patient data due to weak encryption and unauthorized access, illustrating the legal repercussions of non-compliance in today's digital environment [8]. Likewise, in the European Union, a technology firm incurred a €40 million fine under GDPR for improperly managing medical data processed by AI systems without adequate consent or anonymization [9]. The implementations of FL-DP are intentionally structured to adhere to pivotal healthcare regulations: DP aligns with the de-identification mandates set forth by the HIPAA and the principles of data minimization as delineated by the GDPR, whereas federated architectures naturally comply with the HL7 FHIR guidelines by facilitating decentralized and interoperable data exchange. These alignments with regulatory frameworks serve to bolster the legal and ethical legitimacy of FL-DP systems within clinical environments [10]. These systems are unfeasible in decentralized healthcare settings, such as multi-hospital networks, rural clinics, or wearable IoT infrastructures, due to logistical and legal hurdles related to inter-institutional data sharing [11]. To address these challenges, innovative methodologies such as federated learning and differential privacy are emerging as effective solutions, facilitating the development of artificial intelligence models without compromising the confidentiality of patient information. Moreover, the ethical and regulatory complexities associated with artificial intelligence applications necessitate a multidisciplinary approach that involves healthcare professionals, AI developers, ethicists, and legislators to ensure the establishment of robust, privacy-preserving AI frameworks within the healthcare sector [12]. As AI progresses, its effective integration with healthcare systems presents significant potential to transform medical practice, boost diagnostic precision, streamline clinical processes, and ultimately enhance patient outcomes [13].

In the medical field, FL has become a revolutionary method that facilitates cooperative model training from multiple data sources while ensuring the protection of data confidentiality and privacy. This distributed approach enables various parties, such as hospitals and research institutions, to create machine learning models without revealing raw data, thereby addressing privacy concerns associated with centralized data collection [14]. A healthcare FL system is shown in Figure 1, where localized models are generated using patient data (e.g., chest X-rays, ECGs, and medical histories) from many institutions. Then, while maintaining the confidentiality of sensitive data, these local models are sent to a central server for synthesis into a comprehensive model. In the lower section, the FL process is described: (1) local models are submitted, (2) the models are aggregated at the server, and (3) the global model is redistributed to local entities. Within the healthcare sector, FL has been effectively applied for applications like classifying COVID-19 chest X-rays and segmenting brain tumours, achieving performance metrics comparable to centralized systems with only a minor drop in accuracy, as indicated by research from NVIDIA Clara across multiple hospitals [15,16]. FL is still vulnerable to privacy issues, though, as model modifications might unintentionally expose private data to inference or reconstruction attacks [17]. Differential Privacy (DP), which offers mathematical assurances that no one record significantly affects the model's parameters, is incorporated into FL to reduce these dangers. By providing a configurable privacy budget (ε), DP techniques like noise injection and gradient clipping enable developers to balance model effectiveness and privacy [18]. However, attaining stronger privacy assurances frequently leads to decreased model accuracy, fueling ongoing research into ideal privacy-utility compromises. By merging encryption techniques with secure multi-party computation (SMPC), we enhance privacy safeguards and ensure adherence to regulations such as GDPR and HIPAA [19]. In addition, FL systems that utilize distributed database architectures and fog computing address issues like data variability and communication overhead, leading to better scalability and efficiency in healthcare settings [20]. A significant advancement toward safer, more effective, and equitable healthcare solutions, FL encourages collaborative intelligence while maintaining the confidentiality of patient information.

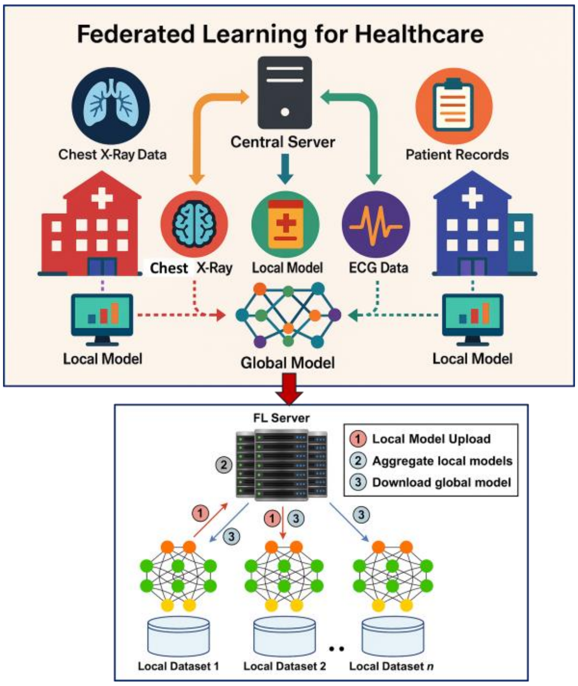


**Figure 1.** A FL framework for medical applications. Describes the structure of FL in healthcare, in which many companies collaborate to construct machine learning models on dispersed patient data, protecting privacy while boosting model precision through coupled local updates.

The integration of FL and DP in real-time healthcare predictive analytics presents an exciting yet intricate challenge. The urgency for instant analytics in healthcare, driven by applications such as sepsis prediction in intensive care units and arrhythmia detection through wearables, necessitates models that can operate efficiently in rapid, latency-sensitive environments. Real-time performance is often defined by latency limits that are unique to the field—particularly, a response time of under 1 second for alerts in ICUs and a range of 2–3 seconds for responses in telemedicine. Past implementations, like FLARE-Health, have demonstrated inference latency as low as 800 milliseconds, highlighting the potential of such systems in latency-critical healthcare scenarios. These established limits act as practical standards for evaluating the responsiveness of future FLDP-IoMT systems [21]. By adopting a decentralized method for machine learning, federated learning addresses privacy and compliance issues by enabling various healthcare organizations to collaborate on training models without sharing sensitive patient information [22]. Integrating FL with DP in these situations presents various challenges, such as delays in communication, non-IID data distributions, and limitations on edge resources [23,24]. By processing data closer to its source, reducing latency and communication constraints, edge computing, when combined with FL, can help mitigate these issues. Emerging strategies for choosing clients and adjusting differential privacy budgets offer promising ways to strike a balance between privacy and the accuracy of models, making sure that only the most relevant data is used for training while adhering to privacy regulations. But there are still issues that need to be addressed, such as guaranteeing model correctness in various healthcare contexts and handling moral dilemmas with data privacy and algorithmic biases [25]. To enhance the scalability and acceptance of secure, smart healthcare AI solutions, upcoming research needs to focus on advancing these technologies, embedding them within existing healthcare frameworks, and promoting interdisciplinary partnerships. By addressing these challenges, Federated Learning and Differential Privacy combined could revolutionize predictive analytics in the healthcare sector, enabling prompt interventions and improved patient results while ensuring privacy and security are upheld [27].

This study addresses significant gaps in the existing literature by combining FL with DP to provide a viable and scalable approach for privacy-focused, real-time healthcare AI systems. While previous research has concentrated on either FL or DP in healthcare environments, there aren't many comprehensive frameworks that tackle privacy and performance in decentralized environments, particularly when real-time demands are involved. Additionally, current literature frequently neglects the technical challenges of ensuring privacy while managing non-independent and identically distributed (non-IID) data across various healthcare organizations. This paper advances the field by introducing a strong integration of FL and DP, bolstered by adaptive privacy strategies and edge computing, thus ensuring compliance with regulations such as HIPAA and GDPR while improving model robustness in dynamic and latency-sensitive healthcare settings. Moreover, it emphasizes the role of blockchain-supported Internet of Medical Things (IoMT) for secure and transparent data sharing, an aspect largely overlooked in earlier research on federated healthcare systems. Here are the contributions of the paper:

- Presents a unified FL-DP model for scalable, privacy-focused healthcare AI.

- Incorporates adjustable privacy budgets to optimize privacy and model efficiency in decentralized frameworks.

- Boosts model efficiency and scalability by merging edge computing with IoMT in healthcare applications.

- Utilizes blockchain for secure and transparent data sharing among healthcare organizations and IoT devices.

The document is organized as follows: Section 2 introduces essential concepts and terminology related to Federated Learning and Differential Privacy. Section 3 examines current studies on FL and DP applications within healthcare. Section 4 explores the combination of FL and DP, emphasizing its use in real-time healthcare predictive analytics. Section 5 outlines the proposed framework, highlighting its structure and technical execution. Section 6 discusses the challenges, unresolved research issues, and possible solutions in FL-DP-enabled healthcare systems. Lastly, Section 7 wraps up the paper and considers future research avenues.

## 2. Foundations and Key Concepts

Federated Learning represents a decentralized paradigm of machine learning that facilitates collaborative model training among multiple clients, such as healthcare institutions or devices, without necessitating the exchange of their raw data; this characteristic serves to uphold privacy while simultaneously mitigating data transmission expenses [28,29]. The procedure encompasses three fundamental phases: the dissemination of the global model to the clients, the execution of local training at each client, and the integration of the local updates to enhance the global model [30]. A typical FL round involves three steps: (1) global model distribution; (2) local training on each client; and (3) aggregation of local updates. The most common aggregation algorithm is Federated Averaging (FedAvg) (Figure 2), where the global model parameters at round t+1 are calculated as [31].

$$\theta^{(t+1)} = \sum_{i=1}^{N} \frac{n_i}{n} \theta_i^{(t)}$$

Where,

- $\theta_i^{(t)}$ is the model trained locally on client i at round t,
- $n_i$ is the number of data samples at client i,
- $n = \sum_{i=1}^{N} n_i$ is the total number of samples across all N clients.

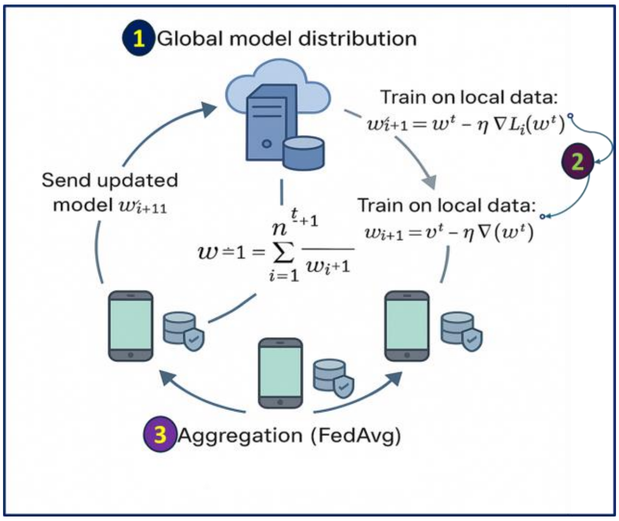

1 Global model distribution
Train on local data:
$w_{i+1}^{t} = w^t - \eta \nabla L_i(w^t)$
2
Send updated model $w_{i+11}$
Train on local data:
$w_{i+1} = v^t - \eta \nabla (w^t)$
$w \doteq 1 = \sum_{i=1}^{n} \frac{t+1}{w_{i+1}}$
3 Aggregation (FedAvg)

**Figure 2.** Federated learning round workflow with FedAvg aggregation.

FL has exhibited nearly centralized accuracy within practical healthcare contexts, but in isolation, it does not comprehensively mitigate the risk of privacy violations. The model's gradients or weights disseminated throughout the training process may still be susceptible to adversarial techniques such as model inversion or membership inference attacks. In response to this concern, DP is integrated to furnish formalized privacy assurances. DP guarantees that the contribution of any individual data point to the model's output is effectively negligible [32]. A randomized mechanism M satisfies ϵ-differential privacy if, for all neighboring datasets D and D′ (differing in one record), and for any output subset S ⊆ Range(M), the following condition holds:

$$P_r\ [\mathrm{M(D)\epsilon S}] \leq e^{\epsilon}.P_r[M(D')\epsilon S]$$

Where:

- ϵ (epsilon) is the privacy budget, quantifying the degree of privacy: smaller values indicate stronger privacy.
- The privacy loss grows with multiple training rounds, necessitating privacy accounting techniques.

In real-time predictive analytics, the applications encompass early warning systems for sepsis within Intensive Care Units (ICU), real-time arrhythmia detection through wearable technology, and surveillance dashboards for epidemic outbreaks. Real-time systems are necessitated to confront a multitude of distinctive challenges: asynchronous updates from various clients, devices operating under resource constraints, and non-independent and identically distributed (non-IID) data distributions across diverse populations. For instance, data collected from Intensive Care Units in two separate hospitals may exhibit considerable variation in terms of demographic composition, measurement frequencies, and definitions of labels [26]. The integration of FL, DP, and real-time analytics necessitates a cohesive architectural framework that effectively balances the principles of security, responsiveness, and scalability. A conventional system comprises local training modules equipped with integrated DP mechanisms, routinely scheduled global aggregations, and on-device inference engines. Open-source frameworks such as PySyft, Flower, and FATE provide modular implementations of FL and DP, thereby enhancing the feasibility of deployment within practical healthcare settings [33]. .

## 3. Federated Learning in Healthcare

Federated Learning, Differential Privacy, and real-time predictive analytics persist in transforming secure artificial intelligence applications within the healthcare domain. Figure 3 represents the FL-DP, illustrating the interactions between clients and servers, privacy layers, and the incorporation of IoMT and blockchain technologies [34]. It showcases the collection of data from IoMT sensors, its transfer to a central server through APIs, and the utilization of blockchain for secure data exchanges. The diagram highlights the pathway of encrypted data and the off-chain database used for monitoring patients and facilitating healthcare interactions. In healthcare Federated Learning, DP maintains data confidentiality by incorporating noise into model updates. Key DP methods consist of Laplace DP, which adds noise relative to data sensitivity and ε, Gaussian DP, ideal for multi-query and high-dimensional datasets, and Rényi DP, which offers enhanced privacy assurances in multi-round aggregation scenarios. The privacy budget (ε) regulates the noise intensity; lower ε values enhance privacy but impair model accuracy. Adjusting ε is based on data sensitivity and model needs. Generally, adaptive privacy budgets are employed, modifying ε to balance privacy and accuracy while complying with regulations such as HIPAA and GDPR [35].

Current approaches merging FL and Reinforcement Learning (RL) in IoT and Edge Cloud Networks are being increasingly utilized in healthcare systems to improve data privacy, real-time performance, and efficiency [36]. Federated Learning is effectively employed to facilitate decentralized model training on sensitive healthcare data, preserving privacy while enabling multi-site collaboration. The

Adaptive Federated Reinforcement Learning System (AFRLS) has been suggested in multiple studies to enhance scheduling and offloading tasks, reducing delays and energy usage in fog and cloud networks. Edge computing is vital for local data processing, lowering communication overhead, and ensuring prompt responsiveness [37]. Furthermore, blockchain technology has been incorporated into various frameworks to guarantee secure and transparent data exchange, tackling the privacy and security issues associated with distributed healthcare applications [38]. As these frameworks progress, contemporary developments unveil progressive methodologies that tackle previously unresolved issues such as cross-silo collaboration, dynamic modeling of patient data, and adherence to regulatory standards in decentralized infrastructures. This section systematically examines innovative contributions spanning from 2017 to 2025, with a focus on cutting-edge techniques and insights that have not been previously explored.

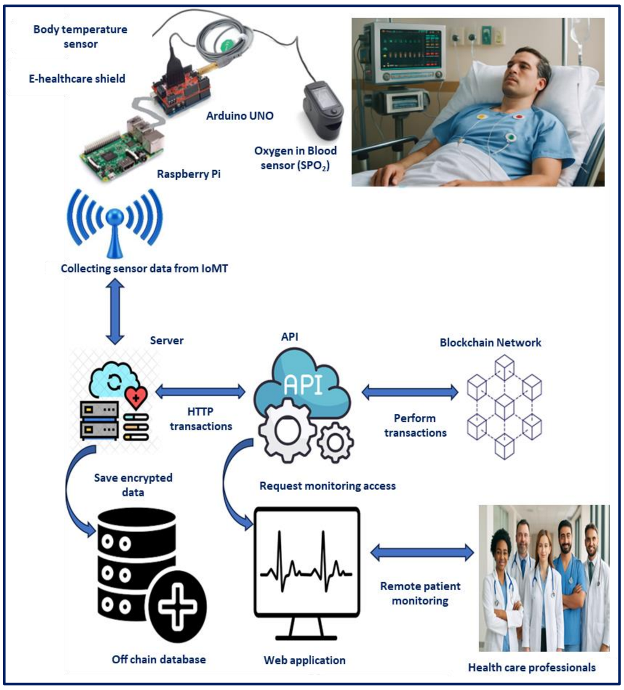


**Figure 3.** Diagrammatic overview of the FL-DP pipeline illustrating client-server interactions, privacy layers, and integration with IoMT or blockchain layers for better clarity. Reprinted from S. B. Othman [34].

FL's use in the healthcare industry has significantly expanded as a result of recent advancements, particularly in novel and real-time clinical settings. Based on previous research, Table 1 compares and contrasts centralized, federated, and FL-DP systems to emphasize trade-offs in privacy, performance, scalability, and regulatory alignment. One notable example of this is the 2023 study on diabetic retinopathy diagnosis using smartphone-based fundus images, which achieved an AUC of 91.8% without requiring raw data sharing by using domain adaptation to reduce inter-hospital imaging disparities [39]. This approach is in line with FL's broad potential to improve diagnostic accuracy while protecting patient privacy, which has been highlighted in studies focusing on collaborative medical imaging diagnostics across many institutions [40]. Similarly, in smart ICU environments revealed a 12% enhancement in patient stability metrics was revealed, thereby illustrating the adaptability of FL in dynamic clinical settings [18]. The incorporation of FL within healthcare not only mitigates privacy issues but also promotes the creation of robust and generalizable models across a spectrum of healthcare environments, as demonstrated by its deployment in under-resourced areas for diabetic retinopathy diagnosis [41,42]. The integration of DP/FL paradigms has emerged as a significant area of scholarly inquiry, especially in the realm of medical applications where the sensitivity of data is of utmost importance. Figure 4 timeline diagram showing the introduction of key frameworks and breakthroughs (e.g., FL in 2016, DP-FedAvg in 2017, PATE in 2018, Flower in 2020, async FL in ICU use-cases by 2021–2023). The research conducted on hierarchical differential privacy serves as a prime illustration of the utilization of contextual aware privacy budgets, successfully attaining high accuracy in federated oncology models while adhering to rigorous privacy constraints for populations classified as high-risk. DP-enhanced federated transfer learning framework for the classification of pediatric diseases, achieving over 87% accuracy despite challenges posed by dataset imbalances and complying with HIPAA-level privacy regulations [43]. The challenge of balancing privacy and model performance is a recurring theme, with various studies proposing innovative solutions. To maximize privacy protection without sacrificing accuracy, Liang and Chen's architecture, for example, uses adaptive privacy budgeting and dynamic threshold clipping [35]. The development of federated edge-AI infrastructures has also led to an evolution in real-time analytics. For instance, the FLARE-Health project (2023–2025) integrated wearable sensor data with hospital electronic medical records (EMR) to implement hybrid federated models for cardiovascular event prediction across rural clinics. This initiative merges information from wearable devices and electronic medical records, achieving an average F1-score of 88.3% along with a prediction latency of under 800 milliseconds. These findings have been validated across five different countries. By implementing adaptive update scheduling and prioritizing clients, these systems establish a benchmark for scalable and robust federated learning systems in environments with limited resources, ensuring they remain resilient amidst unpredictable network conditions [44]. The FedEDFA methodology, which combines FL with a meta-heuristic optimization algorithm to increase system resilience and achieve a prediction accuracy of 98.3% [45], demonstrates how federated learning with Internet of Medical Things (IoMT) devices is crucial for protecting data privacy while guaranteeing accurate disease predictions. Even in situations without centralized data dissemination, Table 2 shows that FL achieves improved diagnostic efficacy across a wide range of healthcare applications. A maximum Dice Similarity Coefficient (DSC) of 89.85% was attained by segmenting brain tumors using the U-Net architecture on the BraTS dataset, and the model's generalizability was further improved by applying data augmentation approaches. In the context of COVID-19 detection, FL frameworks that leverage residual networks and self-supervised learning methodologies attained accuracies exceeding 93%, with one investigation incorporating homomorphic encryption alongside Bootstrap Your Own Latent (BYOL) to achieve an impressive accuracy of 97.19%, all while ensuring the protection of user privacy. The effectiveness of differential privacy techniques, including PATE ($\varepsilon < 1$) and DP-FedAvg ($\varepsilon \approx 5$), to preserve patient anonymity with minimal utility deterioration was validated by their impressive performance levels (88–90% accuracy). These findings substantiate that the amalgamation of FL with privacy-preserving methodologies, including differential privacy and encryption, constitutes a robust, secure, and scalable paradigm for contemporary healthcare artificial intelligence. The approaches and materials employed in framing IoT-enhanced ICU care for remote and critical patient monitoring are outlined in this section. This encompasses a discussion of the IoT devices and sensors utilized, the procedures for data communication and examination, the plan and execution of the deep learning model, as well as the framework proposed for the study.

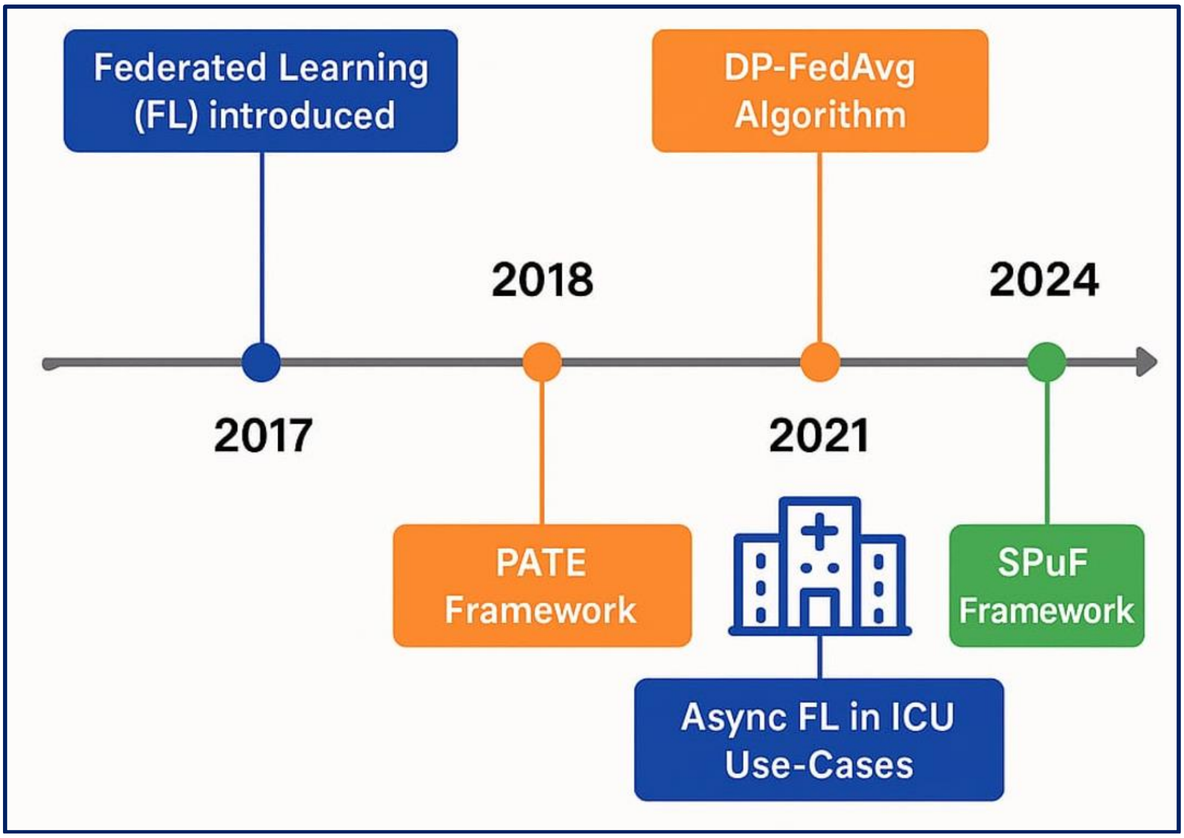


**Figure 4.** Evolution of FL + DP in Healthcare Research2016–2024).

**Table 1.** Comparative summary of centralized, decentralized, and FL-DP approaches in healthcare AI.

| Approach | Privacy Protection | Model Accuracy | Scalability | Compliance (HIPAA/GDPR) | Typical Use Cases |
|---|---|---|---|---|---|
| **Centralized ML** [46] | Low (requires raw data sharing) | High | Limited (single server) | Often non-compliant | Hospital-level diagnostics |
| **FL** [47] | Medium (no raw data sharing) | ~90–95% of centralized | Moderate to high | Better compliance potential | Multi-hospital collaboration |
| **FL + DP** [48] | High (formal privacy guarantees) | Slight drop (~5–15%) | High with edge computing | Strong (ε-based guarantees) | ICU monitoring, remote diagnostics |

The investigations presented in Table 1 elucidate the manner in which FL-DP cater to a variety of healthcare objectives. The segmentation of brain tumors based on the BraTS dataset prioritized cross-institutional learning while ensuring minimal degradation in accuracy, whereas the classification of COVID-19 underscored the necessity for rapid convergence alongside the preservation of patient privacy in diagnostic processes. The prediction of patient readmissions utilizing the MIMIC-III database illustrated that substantial privacy protections (ε ≈ 5) can be attained while concurrently achieving accuracy levels exceeding 90%, thereby facilitating practical implementation in real-world settings. Collectively, these results signify progress in the domains of generalizability, operational efficiency, and the ethical stewardship of data.

**Table 2**. Comparative summary of FL and DP applications in healthcare across various tasks and performance outcomes.

| Ref | Healthcare Task | Privacy Method | Dataset | Architecture | Performance Outcome | Key Contributions |
|---|---|---|---|---|---|---|
| [49] | Brain tumor segmentation | - | BraTS | U-Net | 89.85 % of centralized DSC | Cross-institutional FL viability |
| [50] | Brain tumor segmentation | - | BraTS | U-Net | 52.6% (dice scores of 0.858 for whole, 0.775 for core and 0.647 for enhancing tumor) | Preventing overfitting through data augmentation |
| [51] | COVID-19 X-ray classification | - | COVID-19 Chest X-ray Database | Residual networks | 93.9%, 92.1%, 92.8% and 94.7% | Reducing the convergence time of the global model by about 30 minutes |
| [52] | COVID-19 classification from lung CT scans | - | Three hospitals | Self-supervised learning | 97.19%, a precision of 97.43%, and a recall of 98.18% | Privacy-preserving FL-SSL framework with high diagnostic accuracy |
| [53] | Medical image classification | PATE (ε < 1) | Private dataset | linear regression (second-order methods) | 88% accuracy | Strong DP with acceptable utility |
| [54] | Hospital readmission prediction | DP-FedAvg (ε ≈ 5) | MIMIC-III | DP-FedAvg method | >90% accuracy | Balanced privacy-utility trade-off |

## 4. Differential Privacy in Federated Deep Learning

In federated healthcare systems, the incorporation of differential privacy is imperative for the protection of patient-level data throughout decentralized model training, thereby addressing both ethical considerations and legal requirements such as those delineated in HIPAA and GDPR. Federated Learning fundamentally bolsters privacy by retaining data on local devices; however, it remains vulnerable to privacy infringements via model gradients, which necessitates the implementation of DP to furnish formal privacy assurances by ensuring minimal influence on model output resultant from the inclusion or exclusion of any individual’s data [33].

The trade-off between privacy and utility in FL using DP becomes clear when modifying the privacy budget (ε). For instance, setting ε to 1.0 allows a model to reach 90% accuracy (high utility) but offers limited privacy protection. Lowering ε to 0.5 achieves moderate privacy while accuracy drops to 85% and decreasing ε further to 0.1 enhances privacy but reduces the model's accuracy to 75%. This flexible strategy, where ε is modified according to data sensitivity and privacy needs, strikes a balance between data security and model effectiveness, ensuring adherence to privacy laws like HIPAA and GDPR without greatly sacrificing predictive accuracy [35,55]. Case studies indicate that the precision of models fluctuates in accordance with the privacy budget (ε): DP-FedAvg applied to MIMIC-III sustained an accuracy exceeding 90% at ε approximately equal to 5, whereas an ε value of 0.1 in imaging tasks resulted in a reduction of accuracy by as much as 15% [56]. In the field of genomics, the implementation of Gaussian Differential Privacy achieved an accuracy rate of 88.5% at ε equal to 1.0. These findings underscore the critical significance of calibrating ε to achieve an equilibrium between privacy and utility in healthcare applications [57].

DP can be operationalized through either Central Differential Privacy (CDP) or Local Differential Privacy (LDP). CDP introduces noise at the aggregation server, which proves effective when a trusted server is available, whereas LDP perturbs data prior to transmission, thereby offering enhanced security, even though at the cost of performance [17]. The utilization of noise mechanisms such as Laplace and Gaussian noise is essential, with Gaussian noise being particularly advantageous for deep learning under (ε, δ)-DP, especially within healthcare contexts where model precision is paramount [58,59]. Gradient clipping is a prevalent technique employed to constrain each client's contribution before the addition of noise, and privacy accounting methodologies such as the Moments Accountant or Rényi DP are utilized to oversee cumulative privacy loss [60]. Recent innovations have proposed novel DP mechanisms, including the dissemination of random seeds among clients to generate perturbations, thereby permitting clients to mitigate noise impacts and restore the original global model, thus upholding privacy without sacrificing performance. Furthermore, adaptive differential privacy strategies have been devised to optimize the noise scale and allocate privacy budgets, thereby enhancing privacy management while preserving model accuracy, as evidenced in medical imaging applications [61]. These methodologies underline the persistent endeavors to reconcile privacy with utility in federated healthcare systems, ensuring adherence to regulatory frameworks while facilitating effective collaborative model training [62].

Survey articles pertaining to DP serve to condense the diverse methodologies, optimal practices, and prospective avenues for further investigation that are requisite. Table 3 presents the principal applications of FL-DP within the healthcare sector. While centralized models attain optimal accuracy levels, they are deficient in terms of privacy considerations and adherence to regulatory standards. Conversely, FL-DP frameworks establish a harmonious equilibrium by providing formalized privacy assurances and decentralized scalability, although this may result in a marginal decline in performance metrics. This examination highlights the significant practical implications of FL-DP in the context of real-world healthcare applications, wherein the dual concerns of data sensitivity and interoperability are of utmost importance. It encompasses a variety of fields including ophthalmology, psychiatry, genomics, radiology, and intensive care, each utilizing privacy-preserving techniques that incorporate Gaussian or Laplace noise. Nevertheless, additional scholarly inquiry is essential to comprehensively grasp the compromises linked with particular applications, such as the extent of utility degradation that may occur at specified levels of privacy. In the year 2022, a federated model designed for the detection of diabetic retinopathy, employing Gaussian DP with the parameters ε = 4 and δ = 1e-5, accomplished a remarkable accuracy of 90.1% whilst preserving a negligible loss of utility [63]. In genomic analysis, the use of DP with an epsilon value of 1.0 has demonstrated an accuracy of 88.5%, effectively balancing the trade-off between data utility and privacy protection [64]. The application of adaptive ε-scaling methods in predicting ICU readmissions from multimodal EHR data, achieving a recall of 92.3% while dynamically tuning noise levels [65].

**Table 3.** Recent advancements and applications of federated deep learning with differential privacy in healthcare, focusing on performance outcomes and privacy-preserving techniques.

| **Ref** | **Task** | **Application Domain** | **Privacy Mechanism** | **Noise Type** | **Dataset Type** | **Performance Outcome** | **Remark** |
|---|---|---|---|---|---|---|---|
| [66] | Diabetic retinopathy screening | Ophthalmology | Gaussian DP (ε = 4) | Gaussian | Retinal images | 90.1% accuracy | Low utility loss with visual imaging |
| [67] | Mental health outcome prediction | Psychiatry | Laplace DP (ε = 1.2) | Laplace | Clinical notes | 86.4% AUC | Retained performance under moderate privacy |
| [68] | Rare disease genomic analysis | Genomics | Gaussian DP (ε = 1.0) | Gaussian | Gene sequences | 88.5% accuracy | Strong DP with minimal data leakage |
| [69] | COVID-19 chest X-ray classification | Radiology | Local DP (ε = 1.0) | Gaussian | Public imaging dataset | 88.7% precision | Enabled real-time FL across hospitals |
| [70] | ICU readmission prediction | Intensive Care | Adaptive ε-scaling | Gaussian/ Laplace | Multimodal EHR | 92.3% recall | Dynamic privacy tuning by data modality |

## 5. Real Time Monitoring Rule-based IoT Sensor Node

Remote patient monitoring utilizes IoMT technology and blockchain frameworks to facilitate the acquisition of real-time health data while ensuring the provision of secure and transparent medical services. The IoT/blockchain framework provides improved security and transparency in real-time monitoring, it encounters multiple limitations, especially concerning scalability. To ensure a robust integration of edge computing and blockchain technologies within IoMT-based healthcare systems, it is imperative to rigorously assess their practical performance across critical parameters. Essential metrics such as latency, energy consumption, and security throughput must be systematically evaluated to substantiate the efficacy of these technologies in real-time, resource-constrained environments. The incorporation of such evaluations not only corroborates their practical viability but also yields actionable insights for the optimization of deployment architectures in clinical applications [71]. As the quantity of connected devices rises, the data volume can overwhelm both network and storage resources. Moreover, the decentralized aspect of blockchain may result in increased transaction costs and delayed processing times, potentially affecting real-time performance in extensive deployments. These issues necessitate continual optimization of blockchain protocols and network infrastructure to maintain effective data management and system scalability in evolving healthcare settings [72,73]. In [74], a remote patient monitoring system that utilizes IoT nodes and blockchain technology to aggregate and secure real-time health information, particularly in the context of critical care. The IoT nodes, which are integrated with a Raspberry Pi [75] (a Linux-based platform featuring a 40-pin GPIO), are outfitted with sensors for blood glucose (BG), body temperature (BT), and blood pressure (BP). Blood glucose levels are assessed using a glucose strip connected via an OPA2134 operational amplifier, body temperature is recorded utilizing a calibrated DS18B20 digital sensor, and blood pressure is monitored through an MPS20N0040D-D MEMS pressure sensor, which is subsequently amplified by an LM358 operational amplifier. The system documents sensor outputs in the units of mg/dL (for BG), °C (for BT), and mmHg (for BP), which are subsequently transmitted to a blockchain network to enhance transparency and foster trust. In order to elucidate the amalgamation of blockchain technology and rule-based artificial intelligence within remote healthcare systems, we draw upon the architectural framework delineated by V. Puri et al. [54], which is illustrated in Figure 5. Figure 5a represents a three-tiered rule -based smart contract is implemented to oversee device authentication, categorize health conditions in accordance with established thresholds (BG <140 mg/dL, BT 36.1–37.2°C [76], BP <120/80 mmHg), and identify invalid, missing, or zero sensor readings.

The clinic node functions as a facilitator between healthcare institutions and Internet of Things (IoT) nodes, thereby streamlining the processes of patient registration and the synchronization of medical data through blockchain technology to promote trust and transparency [77-79]. Conventional systems encounter obstacles such as fragmented patient records, redundant laboratory tests, insufficient secure data sharing, and suboptimal management of health records. The incorporation of blockchain technology mitigates these challenges by permitting clinics to access and amend patient histories via a distributed ledger. Within this investigation, clinic nodes establish connections with hospital nodes to obtain personal health records (PHR), react to notifications from remote IoT sensor nodes, and provide timely medical assistance. A rule-based artificial intelligence smart contract regulates the operations of clinic nodes (Figure 5b), encompassing three fundamental functions: (1) authentication through the utilization of device ID (Did), public key (Pb), contract address, and Application Binary Interface (ABI); (2) acquisition of patient records by transmitting patient ID (Pid) and Pb to the blockchain; and (3) modification of medical data by submitting Pid, Pb, and updated information, with contract address and ABI verification ensuring secure interactions.

Hospitals bear the responsibility of overseeing patient care and delivering services during both critical emergencies and routine visits; however, they frequently hesitate to disseminate medical data with other entities owing to concerns related to trust, privacy, and transparency. This deficiency in data interchange can result in delays in essential treatment, particularly in emergencies where access to a patient's medical history is crucial. Given that patients generally exhibit a preference for visiting clinics rather than hospitals, robust synchronization between these two entities is imperative. To mitigate these issues, the application of blockchain technology is proposed to facilitate trust, transparency, and the secure exchange of medical data. In the present study, a rule-based artificial intelligence smart contract (Figure 5c) is implemented at the hospital node, encompassing four primary functions: (1) Create Pid – the hospital transmits patient information (e.g., name, address, contact details) along with the smart contract address and ABI; should this information not correspond to existing records, a new Patient ID (Pid) is established; (2) Create Did – an IoT device is registered by submitting unique identifiers (e.g., MAC address, manufacturer, sensor information); if the device is not previously registered, a Device ID (Did) is generated; (3) Update patient/device data – subsequent to Pid verification, updated information regarding the patient or device is submitted and acknowledged; (4) Final data upload – following Pid validation, new or amended patient data is uploaded to the blockchain, accompanied by confirmation of successful storage.

While this examination amalgamates architectural and theoretical advancements, empirical confirmation continues to be an essential subsequent measure. In order to direct forthcoming inquiries and enhance replicability, we advocate for a benchmarking framework aimed at assessing FL-DP-IoMT systems within practical healthcare contexts. Table 4 delineates appropriate datasets, critical evaluation metrics, and experimental design factors for prospective implementations.

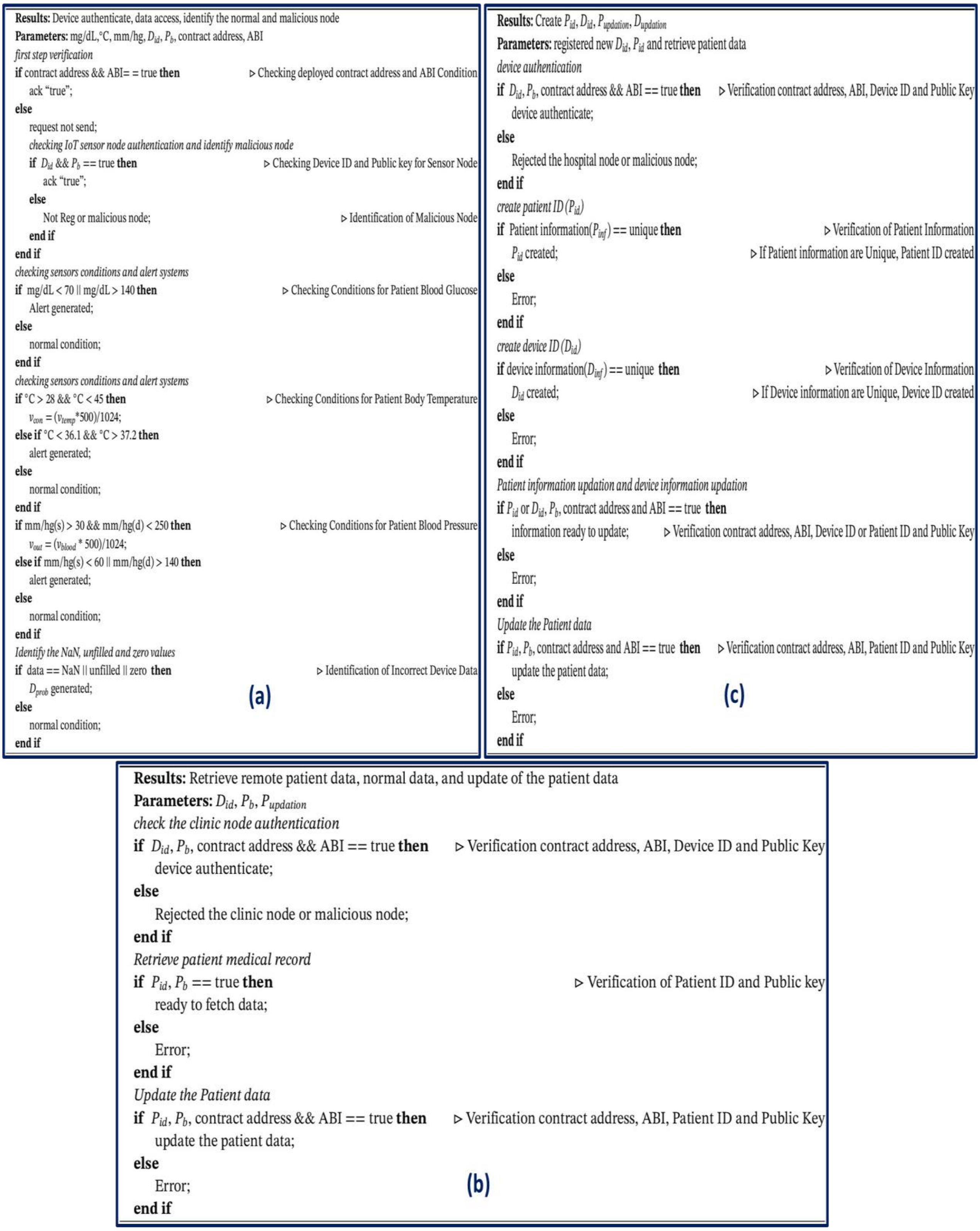
**Table 4.** Recommended experimental benchmarking framework for future FL-DP-IOMT healthcare studies.

| Component | Recommendation |
|---|---|
| **Datasets** | MIMIC-III (ICU readmission), BraTS (brain tumor segmentation), COVID-Xray, SEER |
| **Evaluation Metrics** | - Model Accuracy (%)- Privacy Leakage (ε-value)- Communication Cost (KB/round)- Convergence Rate (rounds to threshold accuracy)- Energy Consumption (if edge devices used) |
| **Experimental Design** | Simulated or real-world federated settings with non-IID data using frameworks like PySyft, Flower, or FATE |
| **Performance Benchmarks** | Targeting ≥ 90% of centralized accuracy, ε ≤ 1 for strong DP, minimized communication load, fast convergence |
| **Use Case Domains** | ICU monitoring, medical image classification, chronic disease prediction, wearable-based diagnostics |

## 6. Challenges and Open Research Problems

In light of the significant advancements witnessed in FL/DP within the healthcare domain, numerous pivotal challenges remain. A primary issue pertains to the data heterogeneity and non-IID (non-independent and identically distributed) attributes prevalent among hospitals or devices. Addressing non-IID (non-independent and identically distributed) data poses a significant challenge in FL, particularly in healthcare, where data can differ greatly among institutions. Techniques like FedProx alleviate this challenge by incorporating a proximal term into the objective function, enhancing the global model's resilience to local data heterogeneity. By normalizing client updates and taking into account the volatility in local data distributions, FedNova efficiently addresses statistical heterogeneity and increases FL efficiency [80,81]. By tailoring global models to each client's distinct data characteristics, personalized FL approaches—like Meta-Fed and PerFed—further enhance model performance and increase accuracy and relevance in decentralized healthcare settings. The optimum approach to strike a compromise between model generalization and customization in FL for healthcare use cases may be found by evaluating these approaches [82]. Significant variation exists in the quality, modality, and sampling frequency of medical data, which causes client drift and impedes model convergence.

By employing techniques such as quantization and sparsification for model compression, we can effectively minimize the volume of model updates sent between devices and the central server, which helps tackle communication overhead. Additionally, asynchronous communication methods can reduce waiting times and increase efficiency. Maintaining cumulative privacy budgets may be effectively achieved by using dynamic privacy budgets, in which we track and modify each client's privacy loss based on the sensitivity of the data. To ensure that privacy promises are maintained without compromising model performance, this may be further strengthened by applying sophisticated privacy accounting tools, like Moments Accountant, to accurately measure and control cumulative privacy loss across several training rounds [83,84]. In FL-DP systems, ethical factors—such as algorithmic bias and fairness—represent crucial but usually disregarded components. Existing healthcare imbalances may be exacerbated by models that are created using skewed or unrepresentative datasets because they may show varying degrees of efficacy across different demographic or socioeconomic groups.



(a)

```
Results: Device authenticate, data access, identify the normal and malicious node
Parameters: mg/dL,°C, mm/hg, $D_{id}$, $P_b$, contract address, ABI
first step verification
if contract address && ABI= = true then                  ▷ Checking deployed contract address and ABI Condition
    ack “true”;
else
    request not send;
    checking IoT sensor node authentication and identify malicious node
    if $D_{id}$ && $P_b$ == true then                         ▷ Checking Device ID and Public key for Sensor Node
        ack “true”;
    else
        Not Reg or malicious node;                                       ▷ Identification of Malicious Node
    end if
end if
checking sensors conditions and alert systems
if mg/dL < 70 || mg/dL > 140 then                          ▷ Checking Conditions for Patient Blood Glucose
    Alert generated;
else
    normal condition;
end if
checking sensors conditions and alert systems
if °C > 28 && °C < 45 then                              ▷ Checking Conditions for Patient Body Temperature
    $v_{con} = (v_{temp}*500)/1024$;
else if °C < 36.1 && °C > 37.2 then
    alert generated;
else
    normal condition;
end if
if mm/hg(s) > 30 && mm/hg(d) < 250 then                    ▷ Checking Conditions for Patient Blood Pressure
    $v_{out} = (v_{blood} * 500)/1024$;
else if mm/hg(s) < 60 || mm/hg(d) > 140 then
    alert generated;
else
    normal condition;
end if
Identify the NaN, unfilled and zero values
if data == NaN || unfilled || zero then                        ▷ Identification of Incorrect Device Data
    $D_{prob}$ generated;
else
    normal condition;
end if
```

(c)

```
Results: Create $P_{id}$, $D_{id}$, $P_{updation}$, $D_{updation}$
Parameters: registered new $D_{id}$, $P_{id}$ and retrieve patient data
device authentication
if $D_{id}$, $P_b$, contract address && ABI == true then    ▷ Verification contract address, ABI, Device ID and Public Key
    device authenticate;
else
    Rejected the hospital node or malicious node;
end if
create patient ID ($P_{id}$)
if Patient information($P_{inf}$) == unique then                           ▷ Verification of Patient Information
    $P_{id}$ created;                                      ▷ If Patient information are Unique, Patient ID created
else
    Error;
end if
create device ID ($D_{id}$)
if device information($D_{inf}$) == unique then                             ▷ Verification of Device Information
    $D_{id}$ created;                                       ▷ If Device information are Unique, Device ID created
else
    Error;
end if
Patient information updation and device information updation
if $P_{id}$ or $D_{id}$, $P_b$, contract address and ABI == true then
    information ready to update;    ▷ Verification contract address, ABI, Device ID or Patient ID and Public Key
else
    Error;
end if
Update the Patient data
if $P_{id}$, $P_b$, contract address and ABI == true then   ▷ Verification contract address, ABI, Patient ID and Public Key
    update the patient data;
else
    Error;
end if
```

(b)

```
Results: Retrieve remote patient data, normal data, and update of the patient data
Parameters: $D_{id}$, $P_b$, $P_{updation}$
check the clinic node authentication
if $D_{id}$, $P_b$, contract address && ABI == true then    ▷ Verification contract address, ABI, Device ID and Public Key
    device authenticate;
else
    Rejected the clinic node or malicious node;
end if
Retrieve patient medical record
if $P_{id}$, $P_b$ == true then                                       ▷ Verification of Patient ID and Public key
    ready to fetch data;
else
    Error;
end if
Update the Patient data
if $P_{id}$, $P_b$, contract address && ABI == true then    ▷ Verification contract address, ABI, Patient ID and Public Key
    update the patient data;
else
    Error;
end if
```

Figure 5. Rule-based AI smart contracts for remote healthcare system nodes. (a) Smart contract logic for the Remote Sensor Node, detailing device authentication, sensor data validation (blood glucose, body temperature, and blood pressure), and identification of incorrect or malicious data inputs. (b) Smart contract logic for the clinic node, including node authentication, retrieval of patient medical records, and update of patient health data. (c) Smart contract logic for the hospital node, covering patient and device ID creation, patient and device data updates, and hospital node authentication. Reprinted from V. Puri et al. [74]

Furthermore, the possibility of accountability is severely hampered by the absence of widely recognized fairness indicators and open auditing procedures. To ensure fair and responsible application in clinical settings, fairness assessments must be incorporated into future research [85,86]. This variability is difficult for traditional optimization strategies to manage, leading to skewed or less generalizable global models. This situation emphasizes the necessity for adaptive aggregation and customized FL methods that are adapted to the distinct data distributions of each client [87].

Furthermore, the application of FL in large hospital networks is severely limited by the scalability and communication inefficiencies. Bandwidth is strained by the frequent transmission of model parameters, especially when dealing with high-dimensional medical data like genetic information or CT scans. Despite the fact that techniques like quantization and sparsification have been put forth, their performance often suffers as a result. Furthermore, achieving stable and rapid convergence becomes increasingly challenging with a multitude of clients and inconsistent participation. Personalization strategies, including fine-tuning or meta-learning, facilitate the adaptation of global models to local contexts; however, they frequently exhibit a lack of consistency and standardization within clinical environments [88].

The integration of DP into practical FL frameworks presents its own set of obstacles. The meticulous calibration of noise to ensure privacy preservation while simultaneously maintaining utility is a complex endeavor, particularly when addressing multiple data modalities and markedly imbalanced datasets. While local DP provides enhanced protection, it adversely affects model performance [89]. Additionally, numerous extant studies neglect to account for the cumulative privacy budget across successive training rounds, thereby engendering risks of privacy leakage [90]. Another significant limitation is the absence of real-time, large-scale FL benchmarks in the healthcare sector. The majority of research relies on small-scale public datasets that fail to accurately represent real-world scenarios, including missing values, streaming data, or constraints related to clinical decision-making. There exists an urgent requirement for open-source frameworks, longitudinal testbeds, and privacy-aware simulators to validate FL-DP frameworks on a larger scale [91]. Addressing these challenges will be critical for the development of secure, scalable, and clinically applicable FL systems in the realm of precision medicine.

Despite the widespread emergence of FL-DP frameworks, the majority remain predominantly restricted to controlled environments, exhibiting limited applicability in real-world settings. Numerous frameworks exhibit a deficiency in their integration with established clinical systems, encounter difficulties with heterogeneous and incomplete datasets, and confront scalability challenges stemming from resource limitations and network instability. Although blockchain-enabled architectures enhance security measures, they frequently introduce latency and impose significant computational overhead. Moreover, scant research investigates the adoption of these systems by clinicians or their long-term reliability. These constraints underscore a persistent disparity between theoretical frameworks and the development of practical, scalable solutions within the healthcare sector [92].

Data imbalance and missing data are ubiquitous in actual healthcare datasets; however, they continue to be inadequately addressed within contemporary FL-DP frameworks. Asymmetrical class distributions, exemplified by infrequent disease instances or marginalized demographics, have the potential to skew models towards prevalent classes, thereby diminishing diagnostic accuracy. In a similar vein, the presence of absent data attributable to inconsistent record-keeping or sensor malfunctions can impair model efficacy and hinder convergence. Therefore, it is imperative that resilient imputation methodologies, weighted loss functions, and adaptive sampling strategies are integrated and rigorously assessed in forthcoming research endeavours [93,94].

## 7. Conclusion

This review offers an extensive synthesis of FL/DP specifically within the framework of real-time, secure, and scalable artificial intelligence systems in healthcare. In contrast to prior reviews that predominantly concentrate on either FL/DP in a segregated manner, our study distinctively amalgamates both frameworks while underscoring practical implementation through edge computing, blockchain technology, and infrastructures associated with the Internet of Medical Things (IoMT). The manuscript makes a significant contribution by delineating regulatory compliance with HIPAA, GDPR, and HL7, advocating for benchmarking methodologies, and accentuating domain-specific latency constraints necessary for achieving real-time efficacy. Through comparative evaluations, meticulously curated tables, and architectural analyses, this study provides a definitive roadmap for researchers and practitioners aspiring to deploy privacy-preserving AI solutions within decentralized healthcare ecosystems.

Notwithstanding its comprehensiveness, the review is not without certain limitations. It does not encompass a thorough meta-analysis of model efficacy across various studies utilizing standardized metrics or cohesive datasets. Furthermore, although the paper elaborates on implementation frameworks and proposes benchmarks, it does not empirically validate the FL-DP systems examined, which may constrain the empirical rigor anticipated by some technical audiences. Additionally, while the dynamic challenges associated with deploying these systems in low-resource or heterogeneous healthcare environments are acknowledged, they are not extensively quantified. Addressing these deficiencies through longitudinal deployments, real-world simulations, and collaborative efforts across institutions remains a pivotal direction for forthcoming research.

Future investigations ought to delve into adaptive privacy mechanisms, including privacy amplification through subsampling and dynamic noise scaling, in order to enhance the equilibrium between privacy and utility across a variety of healthcare contexts. The improvement of scalability via effective federated averaging methodologies, such as FedProx, FedNova, and asynchronous aggregation, has the potential to considerably diminish communication overhead while enhancing convergence. Furthermore, empirical case studies of cross-institutional deployment—especially within resource-limited or multi-hospital settings—are crucial for substantiating the robustness and interoperability of Federated Learning with Differential Privacy (FL-DP) systems. Such initiatives will not only facilitate the reconciliation of theoretical frameworks with practical applications but also expedite the secure and ethical integration of artificial intelligence into clinical practices.

**Author Contributions:** All authors have read and agreed to the published version of the manuscript.

**Acknowledgment:** The authors would like to acknowledge the Department of Computer and Information Science, Southern Arkansas University, Arkansas, USA, and the Department of computer science and engineering, Chittagong Independent University, 12 Jamal Khan Rd, Chattogram, Bangladesh, for their support.

**Conflicts of Interest:** The authors declare no conflict of interest.

## 8. References

[1] E. A. Abed and T. Aguili, “Automated Medical Image Captioning Using the BLIP Model: Enhancing Diagnostic Support with AI-Driven Language Generation,” Diyala J. Eng. Sci. , vol. 18, no. 2, pp. 228–248, Jun. 2025, doi: 10.24237/DJES.2025.18215.

[2] S. D. A. Ahmed, T. Abbas, and A. R. Abbas, “Review of Detecting Text generated by ChatGPT Using Machine and Deep-Learning Models: A Tools and Methods Analysis,” Diyala J. Eng. Sci. , vol. 18, no. 1, pp. 34–54, Mar. 2025, doi:

10.24237/DJES.2025.18102.

[3] P. Rajpurkar et al., “CheXNet: Radiologist-Level Pneumonia Detection on Chest X-Rays with Deep Learning,” Int. J. Sci. Res. Sci. Technol., vol. 12, no. 1, pp. 34–36, Nov. 2017, Accessed: Jun. 01, 2025. [Online]. Available: http://arxiv.org/abs/1711.05225

[4] B. Singh, A. Chandra, D. Joshi, N. Semwal, G. Kukreti, and U. Saxena, “Application of Artificial Intelligence Techniques in Healthcare,” AI Soc. Bus. World A Compr. Approach, pp. 67–101, Oct. 2024, doi: 10.2174/9789815256864124010005.

[5] A. K. Momani, “Implications of Artificial Intelligence on Health Data Privacy and Confidentiality,” Jan. 2025, Accessed: Jun. 01, 2025. [Online]. Available: https://arxiv.org/pdf/2501.01639

[6] Y. Madinabonu, “Challenges and Opportunities for AI in Healthcare,” Int. J. Law Policy, vol. 2, no. 7, pp. 11–15, Jul. 2024, doi: 10.59022/IJLP.203.

[7] A. E. Abdelkareem, “Performance Analysis of Deep Learning based Signal Constellation Identification Algorithms for Underwater Acoustic Communications,” Diyala J. Eng. Sci. , vol. 17, no. 3, pp. 1–14, Sep. 2024, doi: 10.24237/DJES.2024.17301.

[8] N. Abbasi and D. A. Smith, “CYBERSECURITY IN HEALTHCARE: SECURING PATIENT HEALTH INFORMATION (PHI), HIPPA COMPLIANCE FRAMEWORK AND THE RESPONSIBILITIES OF HEALTHCARE PROVIDERS,” J. Knowl. Learn. Sci. Technol. ISSN 2959-6386, vol. 3, no. 3, pp. 278–287, Sep. 2024, doi: 10.60087/JKLST.VOL3.N3.P.278-287.

[9] K. Switala, “Medical Data in the Digital Era - Legal Challenges Related to Providing Information Security, Applying GDPR and Respecting the Professional Secrecy,” 2023 46th ICT Electron. Conv. MIPRO 2023 - Proc., pp. 1457–1466, 2023, doi: 10.23919/MIPRO57284.2023.10159891.

[10] A. Aloqaily, E. E. Abdallah, R. Al-Zyoud, E. Abu Elsoud, M. Al-Hassan, and A. E. Abdallah, “Deep Learning Framework for Advanced De-Identification of Protected Health Information,” Futur. Internet 2025, Vol. 17, Page 47, vol. 17, no. 1, p. 47, Jan. 2025, doi: 10.3390/FI17010047.

[11] A. V. Pargaien, S. Pargaien, A. Nawaz, and T. Kumar, “A Review on the Integration of Artificial Intelligence in Healthcare,” 5th Int. Conf. Electron. Sustain. Commun. Syst. ICESC 2024 - Proc., pp. 880–884, 2024, doi: 10.1109/ICESC60852.2024.10689737.

[12] D. Srikannan, “Integrated Diagnosis, Treatment and Prognosis in Healthcare using Artificial Intelligence,” Indian J. Artif. Intell. Neural Netw., vol. 4, no. 3, pp. 1–5, May 2024, doi: 10.54105/IJAINN.C1086.04030424.

[13] T. Siradanai, C. L. Kok, C. K. Ho, Y. Y. Koh, and T. H. Teo, “Artificial Intelligence in Healthcare Systems,” Proc. - 2024 IEEE 17th Int. Symp. Embed. Multicore/Many-core Syst. MCSoC 2024, pp. 54–57, 2024, doi: 10.1109/MCSOC64144.2024.00019.

[14] M. Aggarwal, V. Khullar, and N. Goyal, “A comprehensive review of federated learning: Methods, applications, and challenges in privacy-preserving collaborative model training,” Appl. Data Sci. Smart Syst., pp. 570–575, Jan. 2024, doi: 10.1201/9781003471059-73.

[15] S. H. Moon and W. Hee Lee, “Privacy-Preserving Federated Learning in Healthcare,” 2023 Int. Conf. Electron. Information, Commun. ICEIC 2023, 2023, doi: 10.1109/ICEIC57457.2023.10049966.

[16] M. Butt et al., “A Fog-Based Privacy-Preserving Federated Learning System for Smart Healthcare Applications,” Electron. 2023, Vol. 12, Page 4074, vol. 12, no. 19, p. 4074, Sep. 2023, doi: 10.3390/ELECTRONICS12194074.

[17] J. Sen, H. Waghela, S. Rakshit, J. Sen, H. Waghela, and S. Rakshit, “Privacy in Federated Learning,” Data Priv. - Tech. Appl. Stand., Jan. 2025, doi: 10.5772/INTECHOPEN.1006677.

[18] “Federated Learning in Healthcare: A Path Towards Decentralized and Secure Medical Insights– IJSREM.” https://ijsrem.com/download/federated-learning-in-healthcare-a-path-towards-decentralized-and-secure-medical-insights/ (accessed Jun. 01, 2025).

[19] X. Xu, Q. Wu, and J. Wen, “Real-World Application of Federated Learning for Collaborative Medical Image Classification: A Case Study in Shenzhen’s Hospitals and Research Institutions,” Dec. 2024, doi: 10.31219/OSF.IO/S2RN9.

[20] C. Bandla, “Distributed Database Architectures for Federated Medical Training”, doi: 10.48175/IJARSCT-22774.

[21] A. Soliman, A. Mohamed, E. Yaacoub, N. V. Navkar, and A. Erbad, “Intelligent DRL-Based Adaptive Region of Interest for Delay-sensitive Telemedicine Applications,” Oct. 2023, Accessed: Aug. 01, 2025. [Online]. Available: https://arxiv.org/pdf/2310.05099

[22] 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,” Healthc. 2024, Vol. 12, Page 2587, vol. 12, no. 24, p. 2587, Dec. 2024, doi: 10.3390/HEALTHCARE12242587.

[23] D. Ganesh and O. B. V. Ramanaiah, “Edge Federated Learning for Smart HealthCare Systems: Applications and Challenges,” 4th Int. Conf. Sustain. Expert Syst. ICSES 2024 - Proc., pp. 1727–1735, 2024, doi: 10.1109/ICSES63445.2024.10763213.

[24] D. C. Nguyen et al., “Federated Learning for Smart Healthcare: A Survey,” ACM Comput. Surv., vol. 55, no. 3, Jan. 2022, doi: 10.1145/3501296;WGROUP:STRING:ACM.

[25] F. Li et al., “Harnessing artificial intelligence in sepsis care: advances in early detection,

personalized treatment, and real-time monitoring," Front. Med., vol. 11, p. 1510792, Jan. 2024, doi: 10.3389/FMED.2024.1510792/XML/NLM.

[26] A. Boussina, S. Shashikumar, F. Amrollahi, H. Pour, M. Hogarth, and S. Nemati, "Development & Deployment of a Real-time Healthcare Predictive Analytics Platform," Proc. Annu. Int. Conf. IEEE Eng. Med. Biol. Soc. EMBS, 2023, doi: 10.1109/EMBC40787.2023.10340351.

[27] B. Charan, D. Jaswanth, E. Hemanth, and M. S. Naidu, "Machine Learning and Deep Learning Approaches for Healthcare Predictive Analytics," 5th Int. Conf. Electron. Sustain. Commun. Syst. ICESC 2024 - Proc., pp. 1698–1707, 2024, doi: 10.1109/ICESC60852.2024.10689833.

[28] G. A. Tsihrintzis et al., "Federated Learning: Navigating the Landscape of Collaborative Intelligence," Electron. 2024, Vol. 13, Page 4744, vol. 13, no. 23, p. 4744, Nov. 2024, doi: 10.3390/ELECTRONICS13234744.

[29] B. Yurdem, M. Kuzlu, M. K. Gullu, F. O. Catak, and M. Tabassum, "Federated learning: Overview, strategies, applications, tools and future directions," Heliyon, vol. 10, no. 19, p. e38137, Oct. 2024, doi: 10.1016/J.HELIYON.2024.E38137.

[30] S. Annamalai, N. Sangeetha, M. Kumaresan, D. Tejavarma, G. H. Vardhan, and A. S. Kumar, "Application Domains of Federated Learning," Model Optim. Methods Effic. Edge AI Fed. Learn. Archit. Fram. Appl., pp. 127–144, Jan. 2024,doi: 10.1002/9781394219230.CH7;SUBPAGE:STRING:ABSTRACT;WEBSITE:WEBSITE:PERICLES;CTYPE:STRING:BOOK.

[31] K. Daly, H. Eichner, P. Kairouz, H. B. McMahan, D. Ramage, and Z. Xu, "Federated Learning in Practice: Reflections and Projections," Oct. 2024, doi: 10.1109/TPS-ISA62245.2024.00026.

[32] R. Danger, "Differential Privacy : What is all the noise about ?," pp. 1–27.

[33] H. K. Gedawy, C. Mellon, U. Khaled, A. Harras, T. Bui, and T. Tanveer, "RealFL: A Realistic Platform for Federated Learning," pp. 313–317, Oct. 2023, doi: 10.1145/3616388.3623799.

[34] S. Ben Othman and M. Getahun, "Leveraging blockchain and IoMT for secure and interoperable electronic health records," Sci. Rep., vol. 15, no. 1, pp. 1–25, Dec. 2025, doi: 10.1038/S41598-025-95531-8;SUBJMETA=166,4077,639;KWRD=ENERGY+SCIENCE+AND+TECHNOLOGY,ENGINEERING.

[35] C. Li, N. Kumar, Z. Song, Z. Liang, and Y. Chen, "Optimizing differential privacy in a federated learning framework: strategies for dynamic clipping and privacy allocation," Eng. Res. Express, vol. 7, no. 1, p. 015231, Jan. 2025, doi: 10.1088/2631-8695/ADA2DB.

[36] M. A. Mohammed et al., "Federated-Reinforcement Learning-Assisted IoT Consumers System for Kidney Disease Images," IEEE Trans. Consum. Electron., vol. 70, no. 4, pp. 7163–7173, 2024, doi: 10.1109/TCE.2024.3384455.

[37] M. A. Mohammed, M. K. A. Ghani, A. Lakhan, B. AL-Attar, and W. Khaled, "Federated Learning-Driven IoT and Edge Cloud Networks for Smart Wheelchair Systems in Assistive Robotics," Iraqi J. Comput. Sci. Math., vol. 6, no. 1, p. 9, Mar. 2025, doi: 10.52866/2788-7421.1241.

[38] M. A. Mohammed et al., "Energy-efficient distributed federated learning offloading and scheduling healthcare system in blockchain based networks," Internet of Things, vol. 22, p. 100815, Jul. 2023, doi: 10.1016/J.IOT.2023.100815.

[39] "International Research Journal on Advanced Science Hub." https://rspsciencehub.com/index.php/journal (accessed Jun. 05, 2025).

[40] Y. Li, C. Wang, and L. Xu, "Enhancing Collaborative Medical Image Diagnosis Using Federated Learning: A Case Study from Shenzhen's Top Hospitals," Dec. 2024, doi: 10.31219/OSF.IO/BCEPF.

[41] G. M. Raj, M. G. Morley, and M. Eslami, "Federated Learning for Diabetic Retinopathy Diagnosis: Enhancing Accuracy and Generalizability in Under-Resourced Regions," Oct. 2024, doi: 10.1109/URTC65039.2024.10937616.

[42] N. Jagan Mohan, R. Murugan, and T. Goel, "DR-FL: A Novel Diabetic Retinopathy Grading with Federated Learning Using Fundus Images," Healthc. Res. Relat. Technol., pp. 355–366, 2023, doi: 10.1007/978-981-99-4056-1_24.

[43] K. B. Nampalle, P. Singh, U. V. Narayan, and B. Raman, "Vision Through the Veil: Differential Privacy in Federated Learning for Medical Image Classification," Jun. 2023, Accessed: Jun. 05, 2025. [Online]. Available: https://arxiv.org/pdf/2306.17794

[44] A. Sharma, T. Tripathi, and A. Majumdar, "Enhancing Edge-based Cardiovascular Diagnosis through Federated Learning and IoT," 2024 15th Int. Conf. Comput. Commun. Netw. Technol. ICCCNT 2024, 2024, doi: 10.1109/ICCCNT61001.2024.10724661.

[45] F. S. Shahazad Niwazi Qurashi, "Federated Machine Learning Using The Internet Of Medical Things For Cardiac Disease Detection," Tuijin Jishu/Journal Propuls. Technol., vol. 44, no. 4, pp. 2719–2733, Oct. 2023, doi: 10.52783/TJJPT.V44.I4.1338.

[46] J. Jonnagaddala and Z. S. Y. Wong, "Privacy preserving strategies for electronic health records in the era of large language models," npj Digit. Med., vol. 8, no. 1, pp. 1–3, Dec. 2025, doi: 10.1038/S41746-025-01429-0;SUBJMETA=228,692,700;KWRD=HEALTH+CARE,HEALTH+SERVICES.

[47] A. Ganji, D. Usha, and P. S. Rajakumar, "Hybrid Machine Learning Framework with Data Analytics Model for Privacy-Preserved Intelligent Predictive Maintenance in Healthcare IoT," J. Comput. Sci.,

vol. 21, no. 1, pp. 1–12, Nov. 2024, doi: 10.3844/JCSSP.2025.1.12.

[48] S. M. Attya et al., “Harnessing Federated Learning for Secure Data Sharing in Healthcare Systems,” Conf. Open Innov. Assoc. Fruct, pp. 390–399, 2024, doi: 10.23919/FRUCT64283.2024.10749928.

[49] M. E. Yahiaoui et al., “Federated Learning with Privacy Preserving for Multi- Institutional Three-Dimensional Brain Tumor Segmentation,” Diagnostics, vol. 14, no. 24, p. 2891, Dec. 2024, doi: 10.3390/DIAGNOSTICS14242891.

[50] F. Isensee, P. Kickingereder, W. Wick, M. Bendszus, and K. H. Maier-Hein, “Brain Tumor Segmentation and Radiomics Survival Prediction: Contribution to the BRATS 2017 Challenge,” Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 10670 LNCS, pp. 287–297, 2018, doi: 10.1007/978-3-319-75238-9_25.

[51] C. Ji, C. Baoluo, G. Zhiyong, Q. Jing, and W. Zumin, “COVID-19 Classification Algorithm Based on Privacy Preserving Federated Learning,” Lect. Notes Inst. Comput. Sci. Soc. Telecommun. Eng. LNICST, vol. 488 LNICST, pp. 161–173, 2023, doi: 10.1007/978-3-031-34586-9_13.

[52] S. S. Chowa et al., “An automated privacy-preserving self-supervised classification of COVID-19 from lung CT scan images minimizing the requirements of large data annotation,” Sci. Rep., vol. 15, no. 1, pp. 1–20, Dec. 2025, doi: 10.1038/S41598-024-83972-6;SUBJMETA=114,1305,1564,631;KWRD=IMAGE+PROCESSING,MACHINE+LEARNING.

[53] H. Mehta, W. Krichene, A. Thakurta, A. Kurakin, and A. Cutkosky, “Differentially Private Image Classification from Features,” Nov. 2022, Accessed: Jun. 05, 2025. [Online]. Available: https://arxiv.org/pdf/2211.13403

[54] B. Sazdov et al., “Prediction of Hospital Readmission using Federated Learning,” Int. Conf. Syst. Signals, Image Process., vol. 2023-June, 2023, doi: 10.1109/IWSSIP58668.2023.10180282.

[55] K. ; Al-Jumaili, H. Kadhim Tayyeh, A. Sabah, and A. Al-Jumaili, “Balancing Privacy and Performance: A Differential Privacy Approach in Federated Learning,” Comput. 2024, Vol. 13, Page 277, vol. 13, no. 11, p. 277, Oct. 2024, doi: 10.3390/COMPUTERS13110277.

[56] M. H. Fares, A. M. Saad, and E. Saad, “Towards Privacy-Preserving Medical Imaging: Federated Learning with Differential Privacy and Secure Aggregation Using a Modified ResNet Architecture,” Dec. 2024, Accessed: Aug. 01, 2025. [Online]. Available: https://arxiv.org/pdf/2412.00687

[57] Y. Cheng, W. Li, S. Qin, and T. Tu, “Differential Privacy Federated Learning Based on Adaptive Adjustment,” Comput. Mater. Contin., vol. 82, no. 3, pp. 4777–4795, Mar. 2025, doi: 10.32604/CMC.2025.060380.

[58] M. van Dijk and P. H. Nguyen, “Considerations on the theory of training models with differential privacy,” Fed. Learn. Theory Pract., pp. 29–55, Jan. 2024, doi: 10.1016/B978-0-44-319037-7.00009-0.

[59] A. Pustozerova, J. Baumbach, and R. Mayer, “Analysing Utility Loss in Federated Learning with Differential Privacy,” Proc. - 2023 IEEE 22nd Int. Conf. Trust. Secur. Priv. Comput. Commun. Trust. 2023, pp. 1230–1235, 2023, doi: 10.1109/TRUSTCOM60117.2023.00167.

[60] A. Elgabli and W. Mesbah, “A Novel Approach for Differential Privacy-Preserving Federated Learning,” IEEE Open J. Commun. Soc., 2024, doi: 10.1109/OJCOMS.2024.3521651.

[61] Z. Yu, Z. Lu, S. Lu, Y. Cui, X. Tang, and J. Wu, “Adaptive Differential Privacy via Gradient Components in Medical Federated Learning,” Proc. - 2024 IEEE Int. Conf. Bioinforma. Biomed. BIBM 2024, pp. 3929–3934, 2024, doi: 10.1109/BIBM62325.2024.10822141.

[62] K. M. Babu, E. Bhavitha, M. Mythri, A. Anusha, B. S. Chandana, and C. Gazala Akhtar, “Privacy-Preserving Federated Learning for Healthcare: A Synergistic Approach using Differential Privacy and Homomorphic Encryption,” SSRN Electron. J., Nov. 2024, doi: 10.2139/SSRN.5088943.

[63] D. Bhulakshmi and D. S. Rajput, “FedDL: personalized federated deep learning for enhanced detection and classification of diabetic retinopathy,” PeerJ Comput. Sci., vol. 10, p. e2508, Dec. 2024, doi: 10.7717/PEERJ-CS.2508/FIG-10.

[64] R. Vavekanand, “Data Security and Privacy in Genomics Research: A Comparative Analysis to Protect Confidentiality,” Stud. Med. Heal. Sci., vol. 1, no. 1, pp. 23–31, May 2024, doi: 10.48185/SMHS.V1I1.1158.

[65] H. Li, R. Monger, E. Pishgar, and M. Pishgar, “ICU Readmission Prediction for Intracerebral Hemorrhage Patients using MIMIC III and MIMIC IV Databases,” medRxiv, p. 2025.01.01.25319859, Jan. 2025, doi: 10.1101/2025.01.01.25319859.

[66] D. Beals, L. Simon, F. Rogers, and S. Pogroszewski, “Revolutionizing Diabetic Retinopathy Screening: Integrating AI-Based Retinal Imaging in Primary Care,” J. C., vol. 14, no. 1, Dec. 2025, doi: 10.1080/28338073.2024.2437294.

[67] J. Chung and J. Teo, “Single classifier vs. ensemble machine learning approaches for mental health prediction,” Brain Informatics, vol. 10, no. 1, pp. 1–10, Dec. 2023, doi: 10.1186/S40708-022-00180-6/FIGURES/2.

[68] J. Hong, D. Lee, A. Hwang, T. Kim, H. Y. Ryu, and J. Choi, “Rare disease genomics and precision medicine,” Genomics Informatics 2024 221, vol. 22, no. 1, pp. 1–11, Dec. 2024, doi: 10.1186/S44342-024-00032-1.

[69] R. Ahmed, P. K. R. Maddikunta, T. R. Gadekallu, N. K. Alshammari, and F. A. Hendaoui, “Efficient differential privacy enabled federated learning model for detecting COVID-19 disease using chest

X-ray images," Front. Med., vol. 11, p. 1409314, Jun. 2024, doi: 10.3389/FMED.2024.1409314/BIBTEX.

[70] A. G. C. de Sá et al., "Explainable Machine Learning for ICU Readmission Prediction," Sep. 2023, Accessed: Jun. 06, 2025. [Online]. Available: https://arxiv.org/pdf/2309.13781

[71] A. Laouamri, S. Cherbal, Y. Mosbah, C. Benrebbouh, and K. Kharoubi, "Blockchain Approach for Healthcare Using Fog Topology and Lightweight Consensus," https://aip.vse.cz/doi/10.18267/j.aip.256.html, vol. 14, no. 1, pp. 128–154, 2025, doi: 10.18267/J.AIP.256.

[72] S. B. Prasad, A. R. Ashok Kumar, and R. V. Honnungar, "Blockchain-Based Scalability Solutions for IoT: A Decentralized Design to Enhance Performance and Security," Proc. CONECCT 2024 - 10th IEEE Int. Conf. Electron. Comput. Commun. Technol., 2024, doi: 10.1109/CONECCT62155.2024.10677307.

[73] A. M. Al-Madni, X. Ying, M. Tawfik, and Z. A. T. Ahmed, "An Optimized Blockchain Model for Secure and Efficient Data Management in Internet of Things," 2024 IEEE Int. Conf. Inf. Technol. Electron. Intell. Commun. Syst. ICITEICS 2024, 2024, doi: 10.1109/ICITEICS61368.2024.10624817.

[74] V. Puri, A. Kataria, and V. Sharma, "Artificial intelligence-powered decentralized framework for Internet of Things in Healthcare 4.0," Trans. Emerg. Telecommun. Technol., vol. 35, no. 4, p. e4245, Apr. 2024, doi: 10.1002/ETT.4245;WGROUP:STRING:PUBLICATION.

[75] M. Sajjad et al., "Raspberry Pi assisted face recognition framework for enhanced law-enforcement services in smart cities," Futur. Gener. Comput. Syst., vol. 108, pp. 995–1007, Jul. 2020, doi: 10.1016/J.FUTURE.2017.11.013.

[76] "Body temperature norms: MedlinePlus Medical Encyclopedia." https://medlineplus.gov/ency/article/001982.htm (accessed Jun. 11, 2025).

[77] Islam, M.A., Mostofa, K.Z., Mohafez, H., Hossen, M.J., Low, F.W., Vasiliev, M., Islam, S.M.S. and Nur-E-Alam, M., 2024. Combination of Sensors-Based Monitoring System and Internet of Things (IoT): A Survey and Framework for Remote and Intensive Care Unit Patients. In Non-Invasive Health Systems based on Advanced Biomedical Signal and Image Processing (pp. 413-439). CRC Press.

[78] A. Shahnaz, U. Qamar, and A. Khalid, "Using Blockchain for Electronic Health Records," IEEE Access, vol. 7, pp. 147782–147795, 2019, doi: 10.1109/ACCESS.2019.2946373.

[79] P. T. S. Liu, "Medical Record System Using Blockchain, Big Data and Tokenization," Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 9977 LNCS, pp. 254–261, 2016, doi: 10.1007/978-3-319-50011-9_20.

[80] M. Subramanian, V. Rajasekar, V. E. Sathishkumar, K. Shanmugavadivel, and P. S. Nandhini, "Effectiveness of Decentralized Federated Learning Algorithms in Healthcare: A Case Study on Cancer Classification," Electron. 2022, Vol. 11, Page 4117, vol. 11, no. 24, p. 4117, Dec. 2022, doi: 10.3390/ELECTRONICS11244117.

[81] H. Pathipati, L. N. B. Ramisetti, D. N. Reddy, S. Pesaru, M. Balakrishna, and T. Anitha, "Optimizing Cancer Detection: Swarm Algorithms Combined with Deep Learning in Colon and Lung Cancer using Biomedical Images," Diyala J. Eng. Sci. , vol. 18, no. 1, pp. 91–102, Mar. 2025, doi: 10.24237/DJES.2025.18105.

[82] K. Yin and J. Mao, "Personalized Federated Learning with Adaptive Feature Aggregation and Knowledge Transfer," Oct. 2024, Accessed: Jul. 31, 2025. [Online]. Available: https://arxiv.org/pdf/2410.15073

[83] W. Xie et al., "JointSQ: Joint Sparsification-Quantization for Distributed Learning," Proc. IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit., pp. 5778–5787, 2024, doi: 10.1109/CVPR52733.2024.00552.

[84] S. Song, S. Du, Y. Song, and Y. Zhu, "Communication-Efficient and Private Federated Learning with Adaptive Sparsity-Based Pruning on Edge Computing," Electron. 2024, Vol. 13, Page 3435, vol. 13, no. 17, p. 3435, Aug. 2024, doi: 10.3390/ELECTRONICS13173435.

[85] M. A. Sufian, L. Alsadder, W. Hamzi, S. Zaman, A. S. M. S. Sagar, and B. Hamzi, "Mitigating Algorithmic Bias in AI-Driven Cardiovascular Imaging for Fairer Diagnostics," Diagnostics 2024, Vol. 14, Page 2675, vol. 14, no. 23, p. 2675, Nov. 2024, doi: 10.3390/DIAGNOSTICS14232675.

[86] Y. Huang et al., "A scoping review of fair machine learning techniques when using real-world data," J. Biomed. Inform., vol. 151, p. 104622, Mar. 2024, doi: 10.1016/J.JBI.2024.104622.

[87] S. Chen, W. Liu, X. Zhang, H. Xu, W. Lin, and X. Chen, "Adaptive Personalized Federated Learning for Non-IID Data with Continual Distribution Shift," 2024 IEEE/ACM 32nd Int. Symp. Qual. Serv., pp. 1–6, Jun. 2024, doi: 10.1109/IWQOS61813.2024.10682851.

[88] A. K. Nair, J. Sahoo, and E. D. Raj, "Exploring Communication Efficient Strategies in Federated Learning Systems," Fed. Learn. Princ. Paradig. Appl., pp. 153–182, Jan. 2024, doi: 10.1201/9781003497196-7/EXPLORING-COMMUNICATION-EFFICIENT-STRATEGIES-FEDERATED-LEARNING-SYSTEMS-AKARSH-NAIR-JAYAKRUSHNA-SAHOO-EBIN-DENI-RAJ.

[89] S. Guo, Z. Su, Z. Tian, and S. Yu, "Utility-Aware Privacy-Preserving Federated Learning through Information Bottleneck," Proc. - 2022 IEEE 21st Int.

Conf. Trust. Secur. Priv. Comput. Commun. Trust. 2022, pp. 680–686, 2022, doi: 10.1109/TRUSTCOM56396.2022.00097.

[90] J. Yuan et al., "Privacy as a Resource in Differentially Private Federated Learning," Proc. - IEEE INFOCOM, vol. 2023-May, 2023, doi: 10.1109/INFOCOM53939.2023.10228953.

[91] Y. Li, G. Xu, X. Meng, W. Du, and X. Ren, "LF3PFL: A Practical Privacy-Preserving Federated Learning Algorithm Based on Local Federalization Scheme," Entropy 2024, Vol. 26, Page 353, vol. 26, no. 5, p. 353, Apr. 2024, doi: 10.3390/E26050353.

[92] K. Sehimi, F. Bendaoud, and H. H. Benderbal, "A review of Scalability Solutions in Blockchain-based Electronic Health Record Systems," ICNSC 2023 - 20th IEEE Int. Conf. Networking, Sens. Control, 2023, doi: 10.1109/ICNSC58704.2023.10319026.

[93] M. M. K. Dandu, J. Jain, S. Vijayabaskar, P. Goel, A. Shivarudra, and S. Bhatt, "Assessing the Impact of Data Imbalance on the Predictive Performance of Machine Learning Models," Proc. Int. Conf. Contemp. Comput. Informatics, IC3I 2024, pp. 1062–1068, 2024, doi: 10.1109/IC3I61595.2024.10829313.

[94] D. Roy, A. Roy, and U. Roy, "Learning from Imbalanced Data in Healthcare: State-of-the-Art and Research Challenges," Stud. Comput. Intell., vol. 1132, pp. 19–32, 2024, doi: 10.1007/978-981-99-8853-2_2.