

Securing federated learning in medical image analysis: a systematic review of privacy threats and defense mechanisms

Malika Abid, Mohammed Kamel Benkaddour, Mohamed Benouis, Amine Khaldi, Monalisa Sahu, Aditya Kumar Sahu

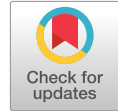
Angaben zur Veröffentlichung / Publication details:

Abid, Malika, Mohammed Kamel Benkaddour, Mohamed Benouis, Amine Khaldi, Monalisa Sahu, and Aditya Kumar Sahu. 2026. "Securing federated learning in medical image analysis: a systematic review of privacy threats and defense mechanisms." *Computer Modeling in Engineering & Sciences* 148 (1): 6. <https://doi.org/10.32604/cmes.2026.081055>.

Nutzungsbedingungen / Terms of use:

CC BY 4.0





REVIEW

Securing Federated Learning in Medical Image Analysis: A Systematic Review of Privacy Threats and Defense Mechanisms

Malika Abid¹, Mohammed Kamel Benkaddour¹, Mohamed Benouis², Amine Khaldi¹,
Monalisa Sahu³ and Aditya Kumar Sahu^{4,*}

¹Department of Computer Science and Information Technology, Artificial Intelligence and Information Technology Laboratory (LINATI), University of Kasdi Merbah Ouargla, Ouargla, Algeria

²Chair for Human-Centered AI, University of Augsburg, Universitätsstraße 6a, Augsburg, Germany

³Department of Software and System Engineering, School of Computer Science & Engineering, VIT-AP University, Beside AP Secretariat, Amaravati, Andhra Pradesh, India

⁴Department of Computer Science and Engineering, SRM University-AP, Amaravati, Andhra Pradesh, India

*Corresponding Author: Aditya Kumar Sahu. Email: aditya.s@srmmap.edu.in

Received: 22 February 2026; Accepted: 02 May 2026; Published: 27 July 2026

ABSTRACT: Federated Learning (FL) is a cutting-edge method in the medical imaging field that allows hospitals to collaboratively build models without revealing patient data. Nevertheless, FL is still vulnerable to numerous security and privacy issues, including, but not limited to, data poisoning, Byzantine attacks, and inference attacks. The existing literature has only partly dealt with this topic by focusing either on particular threats or on mitigation strategies, thus leaving the overall comprehension of the problems and their solutions in medical imaging as inadequate. The main threats to FL are systematically classified in this systematic review, with two major vulnerable assets, medical data and model parameters, being pointed out. We review existing countermeasures based on cryptographic techniques, secure aggregation, perturbation methods, and security protocols with an emphasis on their efficiency in ensuring patient privacy and model integrity. We also discuss the impact of FL in medical imaging, where it serves as a tool for privacy preservation and has the potential to improve diagnostic accuracy. Data heterogeneity, communication overhead, and lack of standardization are key challenges that are considered, as well as potential future research paths to explore for solving these problems. Overall, the systematic review reveals that, although federated learning provides enormous privacy-preserving benefits in medical imaging, its actual implementation needs to be very cautious regarding the merging of very strong security measures and the use of standard protocols so that the weaknesses are reduced, and the reliability of the diagnostics is increased.

KEYWORDS: Federated learning; medical image analysis; privacy preservation; security threats; defense mechanisms; healthcare data

1 Introduction

Rapid advancements in artificial intelligence (AI) and machine learning (ML) have significantly enhanced the accessibility and scalability of medical applications, reducing latency and improving operational efficiency [1]. Despite the sensitive nature of medical data, privacy preservation and security remain pressing concerns in healthcare settings. Traditional centralized ML approaches require aggregating raw patient data in a single location, exposing sensitive information to potential data breaches. Even though various regulations and technical provisions, such as the General Data Protection Regulation (GDPR),

the Gramm-Leach Bliley Act (GLBA), California Consumer Privacy Act (CCPA), the Health Insurance Portability and Accountability Act (HIPAA), the Children Online Privacy Protection Act (COPPA), and the Illinois Biometric Information Privacy Act (BIPA) seek to reduce these risks, the following problems still exist: lack of full coverage, difficulties in assessments, data gathering fairness, and decision-making issues [2,3].

Federated Learning is a new paradigm introduced to overcome these privacy threats. FL permits joint training of models across many clients without exchanging raw data, thereby minimizing the risk of data leakage [4]. The opportunities of FL in healthcare have been emphasized in many studies, but the challenges in implementing it in practice include client heterogeneity, fairness issues, and bias in resource distribution. Recent systematic review studies have reevaluated these challenges, especially in medical imaging, but they do not fully address key issues such as data heterogeneity, FL attacks, countermeasures, research opportunities, and the main uses of FL in medical imaging [5].

The temporal patterns of FL are provided in Table 1 in the form of the relative percent of general FL works compared to medical image FL, as well as the key methodological advances of each year. This timeline shows how initial approaches, including FedAvg, have evolved into sophisticated methods by incorporating concepts such as differential privacy, secure multiparty computation, split learning, and blockchain integration to support medical use cases.

Table 1: Temporal trends in federated learning methods: general FL vs. medical image analysis.

Year	Trend General FL (%)	Trend FL Medical Image (%)	Main Developments
2017	10%	5%	Foundations of FL, FedAvg introduced; early communication-efficient methods.
2018	20%	10%	Secure aggregation, early privacy-preserving mechanisms; first healthcare FL studies.
2019	35%	20%	Rise of Split Learning and hybrid architectures; growing interest in medical imaging.
2020	50%	35%	FedProx, heterogeneity handling, non-IID stability; early medical image FL benchmarks.
2021	65%	50%	Differential Privacy-based FL, HE/SMPC integration, defenses against poisoning and Byzantine attacks.
2022	75%	60%	Federated self-supervised learning, personalized FL, multi-site medical deployments.
2023	85%	75%	Large model FL, contrastive medical FL, multi-modal FL, standardized pipelines.

(Continued)

Table 1 (continued)

Year	Trend General FL (%)	Trend FL Medical Image (%)	Main Developments
2024–2025	92%	80%	Scalable medical FL systems, blockchain-FL integration, privacy auditing, regulatory-compliant deployments.
Early 2026	95%	85%	Recent advances emphasize asynchronous FL, diffusion models, and practical challenges such as efficiency, robustness, and privacy–utility trade-offs.

Overall, the temporal analysis shows rapid development in the general FL field. However, FL in medical imaging has become more stable, emphasizing privacy-preserving solutions, standardized pipelines, and secure multi-institutional deployments. This highlights the growing importance of protecting patient data and supporting teamwork learning in healthcare.

To systematically review the literature, [Table 2](#) summarizes surveys and studies on healthcare FL. It includes areas of focus, privacy and security protection mechanisms, attacks against FL, their findings, and gaps. The summary shows that although there is a growing focus on privacy and security protocols, major gaps remain in the analysis of FL methods, especially in medical imaging.

Main Contributions

The key findings of this systematic review are the following:

- We provide a curated and recent survey on methods of federated learning that have been used in medical image analysis, focusing on the privacy and security issues.
- We systematically examined the privacy threat and attack models in federated learning in medical imaging.
- We characterize and contrast the currently existing privacy-preserving defense mechanisms, their strengths and limitations, and their applicability.
- We list the current research gaps and directions of secure and privacy-conscious federated learning in healthcare.

Table 2: Overview of key literature on healthcare federated learning.

Reference	Domain	Privacy-Security Defense	FL Attacks	Key Findings	Gaps Identified
[6] 2022	IoMT	Yes	Yes	Comprehensive survey on the use of FL in IoMT.	Need for more comprehensive evaluations.
[7] 2023	IoHT	Yes	Yes	Introduces basic concepts and evaluates main solutions for IoHT data security and privacy.	Limited examples of privacy threats.

(Continued)

Table 2 (continued)

Reference	Domain	Privacy-Security Defense	FL Attacks	Key Findings	Gaps Identified
[8] 2023	IoHT	No	No	General overview of healthcare applications.	Lack of information on FL concepts.
[9] 2023	IoHT	No	No	General overview of healthcare applications.	Lack of security and privacy information.
[10] 2024	MIA	Yes	No	Focus on medical image analysis.	Need for additional security and privacy measures.
[11] 2025	IoMT	No	Yes	Focus on cloud and edge security.	Gaps in addressing privacy concerns.
[12] 2026	IoHT	Yes	Yes	Systematic review focusing on privacy-preserving and equitable AI in healthcare FL.	Limited technical evaluation of attack-defense trade-offs and system-level implementation.
[13] 2026	MIA	Yes	No	Reviews federated generative models for MIA and highlights recent advancements.	Lack of comprehensive analysis of privacy risks and defense integration.
[14] 2026	MIA	Yes	Yes	Provides a broad systematic review of FL in medical imaging, including challenges and applications.	Limited comparative evaluation and absence of unified analytical framework.

2 Systematic Review Methodology and Intended Audience

This section outlines the systematic methodology used to conduct a literature review on privacy-preserving FL for medical image analysis. It outlines the research objectives, research questions, literature search, study selection, quality assessment, and taxonomy structure of the review.

2.1 Intended Audience

This systematic review is intended for readers seeking a comprehensive and structured understanding of federated learning in the context of medical image analysis. It is particularly suited for the following:

- **Researchers and students** who are new to FL and want to build a clear conceptual foundation, including the fundamental workflow, challenges, and privacy threats.
- **Practitioners and healthcare data scientists** who aim to understand how FL is applied in medical imaging, the datasets commonly used, and the methodologies adopted in existing studies.
- **Researchers planning to work specifically on privacy-preserving FL** and who need an overview of current privacy techniques such as differential privacy, secure aggregation, homomorphic encryption, perturbation methods, and blockchain-based solutions.

- **Industry professionals and system developers** interested in implementing secure FL frameworks in real medical environments and evaluating their practical feasibility.
- **Policymakers and decision-makers** who require insights into privacy risks, regulatory considerations, and the potential of FL to enable secure and collaborative healthcare AI.

Overall, this systematic review provides a complete reference for those who want to understand how FL works in medical image analysis, what datasets and approaches are commonly used, and how privacy and security techniques are integrated into the current research.

2.2 Research Questions

The research questions (RQs) guiding this study are:

- **RQ1:** What are the critical privacy threats in federated learning in medical image analysis?
- **RQ2:** What types of defense mechanisms have been proposed against these privacy threats?
- **RQ3:** What is the effectiveness of current privacy approaches in real-world medical imaging applications?
- **RQ4:** What are the limitations of current approaches and what future directions can be explored?

[Section 2](#) provides the necessary background on federated learning, including its architecture, types, aggregation algorithms, data heterogeneity, and fairness considerations, thereby laying the foundation for answering **RQ1**. [Section 3](#) focuses on security and privacy challenges in federated learning, presenting various threat models and attack types, which directly contributes to answering **RQ1** and partially **RQ2**. [Section 4](#) explores the application of federated learning in medical image analysis, including datasets, practical implementations, and the integration of advanced techniques such as contrastive learning. This section supports the analysis of **RQ3** by highlighting real-world performance and trade-offs. [Section 5](#) provides a comprehensive discussion of privacy threats and corresponding defense strategies in medical imaging, along with a comparative analysis of existing solutions and available software platforms. This section primarily addresses **RQ2** and **RQ3**. Finally, the discussion on challenges and future directions in the same section addresses **RQ4** by identifying current limitations and outlining promising research opportunities.

2.3 Literature Search and Study Selection

This systematic review follows a structured methodology in accordance with the PRISMA guidelines. The processes of literature identification, screening, eligibility assessment, and final study inclusion are illustrated in the PRISMA flow diagram ([Fig. 1](#)).

The comprehensive search across major scientific databases resulted in a curated set of **150 studies**, distributed across primary publication sources as follows: IEEE Xplore/Conferences (49 studies, 32%), Elsevier/ScienceDirect (35 studies, 23%), MDPI Journals (20 studies, 13%), arXiv Preprints (16 studies, 11%), Springer (13 studies, 9%), ACM Digital Library (9 studies, 6%), Nature/Springer Nature (4 studies, 3%), and other sources including Wiley and Frontiers (4 studies, 2%). IEEE Xplore accounts for the largest share (34%), reflecting its strong emphasis on federated learning security, the Internet of Things, and medical imaging conferences. This is followed by Elsevier/ScienceDirect (23%), which provides high-quality surveys and applied research, while MDPI (13%) contributes practical healthcare-oriented studies. Additionally, arXiv (11%) highlights emerging and cutting-edge developments prior to formal peer review.

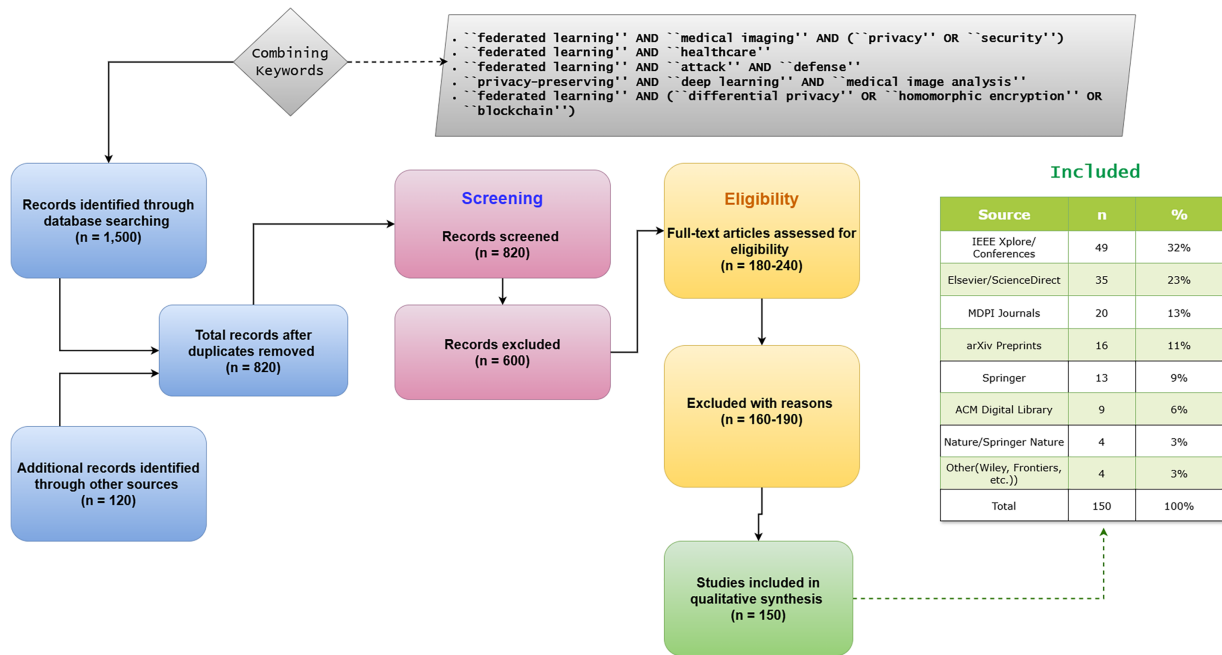


Figure 1: PRISMA flow diagram illustrating the study selection process for the systematic review on privacy-preserving federated learning in medical image analysis.

2.4 Quality Assessment

The researchers conducted a quality assessment of the included studies because they used specific criteria to evaluate study reliability.

- Clarity of research objectives and methodology.
- The study requires both experimental results and validation to reach its complete state.
- The study uses suitable privacy/security mechanisms which researchers implemented according to proper standards.
- The study investigates federated learning applications which exist in medical settings.

The researchers rated each study with the three quality levels of **high, medium, or low quality** to create trustworthy evidence which researchers could reproduce.

2.5 Taxonomy Structure

Fig. 2 presents the proposed taxonomy of Privacy-Preserving FL in medical image analysis. The literature was clustered into federated learning foundations, security and privacy mechanisms, medical imaging applications, healthcare-specific threats and mitigations, practical tools and challenges, and concluding remarks. The hierarchical structure allows readers to obtain a complete view of the subject matter while still allowing them to gather information in an organized manner.

This section details the systematic methodology followed to conduct the literature review on privacy-preserving FL in medical image analysis. It outlines the research objectives, research questions, data sources, search strategy, inclusion and exclusion criteria, study selection process, and taxonomy structure.

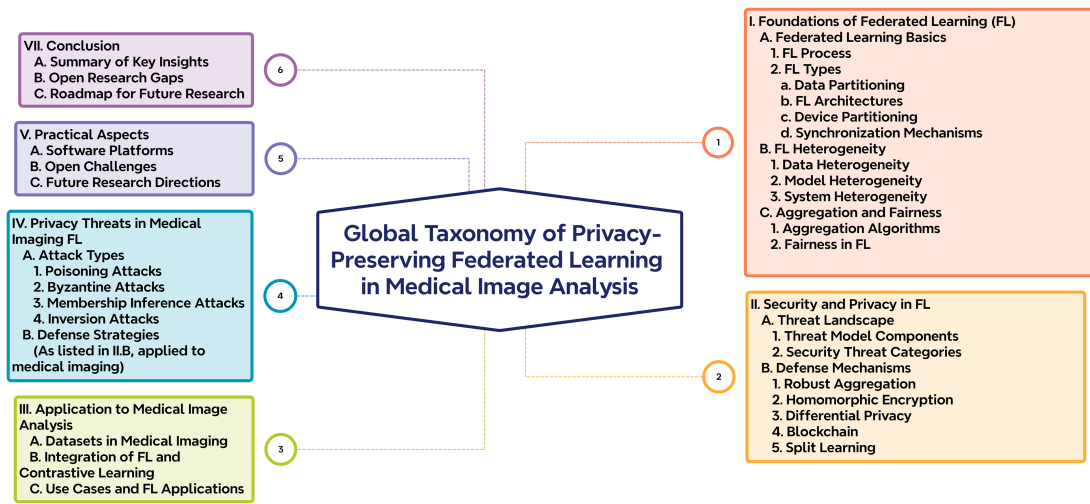


Figure 2: Global taxonomy of privacy-preserving federated learning in medical image analysis.

3 Background

This section offers an in-depth overview of federated learning, covering its various types, synchronization strategies, heterogeneity setting, aggregation methods, and fairness issues, as illustrated in Fig. 3.

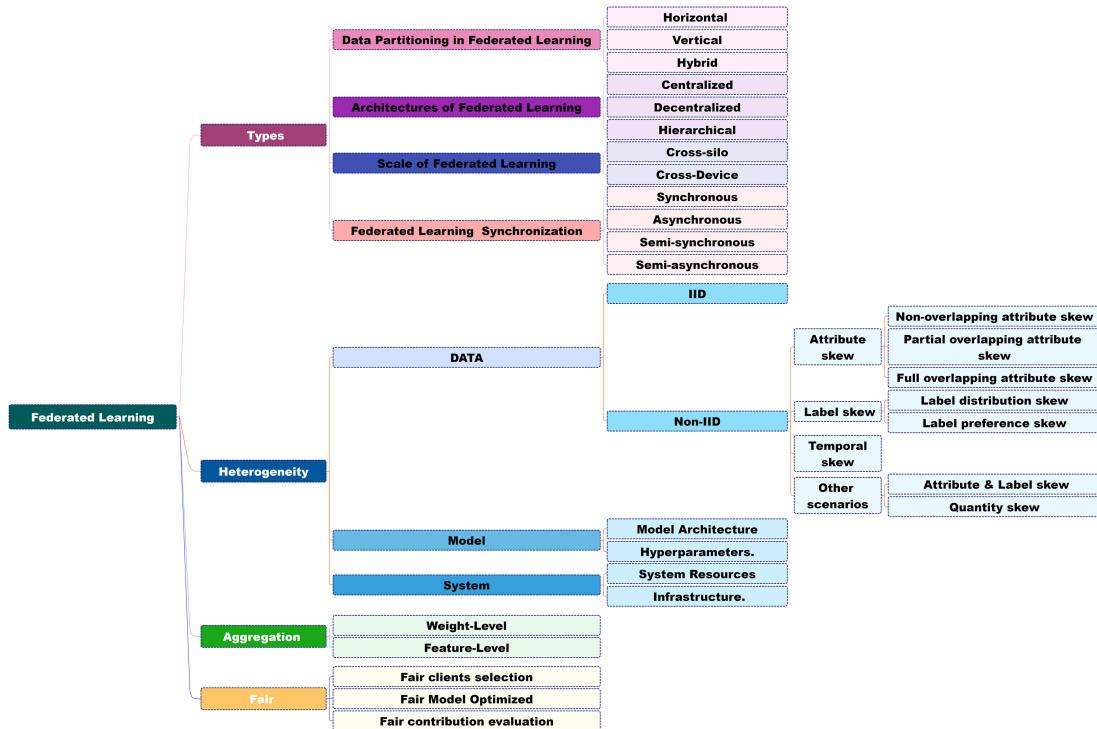


Figure 3: Overview of federated learning taxonomy covering learning types, heterogeneity challenges, aggregation levels, and fairness strategies.

3.1 FL

Google developed FL [3] as a system that enables machine learning model training across multiple devices and across distributed organizations while keeping individual data points confidential. The fundamental FL workflow involves two key steps: clients train on local datasets and send only model weights and parameters to a central server, as illustrated in Fig. 4. The server aggregates these updates through methods such as FedAvg to build an updated global model, which it sends back to clients for their next training session. The method protects data privacy while reducing communication requirements and addressing legal and ethical issues in data sharing, making it especially important for medical imaging research that requires strict privacy protections [15].

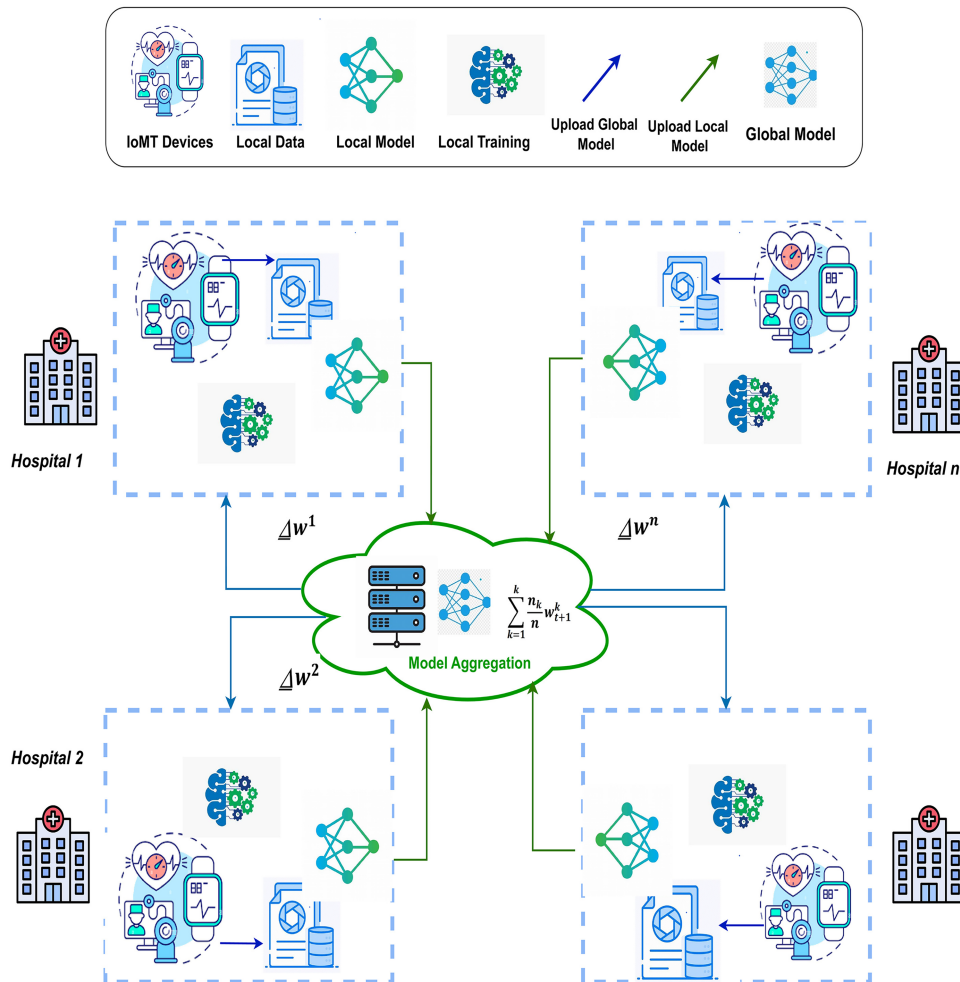


Figure 4: Federated learning architecture.

3.2 FL Types

The FL type can be analyzed based on the following set of characteristics:

3.2.1 Data Partitioning in FL

As shown in Fig. 5, data partitioning is essential to federated learning because it dictates how data is allocated across several clients, significantly influencing both model training and performance [4].

In cooperative healthcare research, each client gathers data on the same subject but attributes distinct characteristics to it. Horizontal partitioning allows clients to view specific feature subsets while sharing a common sample region; for instance, multiple hospitals may collaboratively train deep learning models on chest X-ray images, where each hospital holds images from different patients but with identical image features and labels [16]. Conversely, vertical partitioning allows clients to share a unified feature space while accessing specific sample subsets; for example, one institution may store MRI images, while another holds clinical attributes for the same patients [17]. The latter approach is useful in scenarios such as financial institutions, where client transaction data is used to train models. Numerous topics can be covered, but the records for various clients share the same transaction types. Hybrid partitioning is a data distribution method that simultaneously utilizes horizontal and vertical partitioning strategies. It is particularly effective in complex scenarios, such as multi-institutional research collaborations, where features and samples are distributed across participants to gain a comprehensive understanding of the subject.

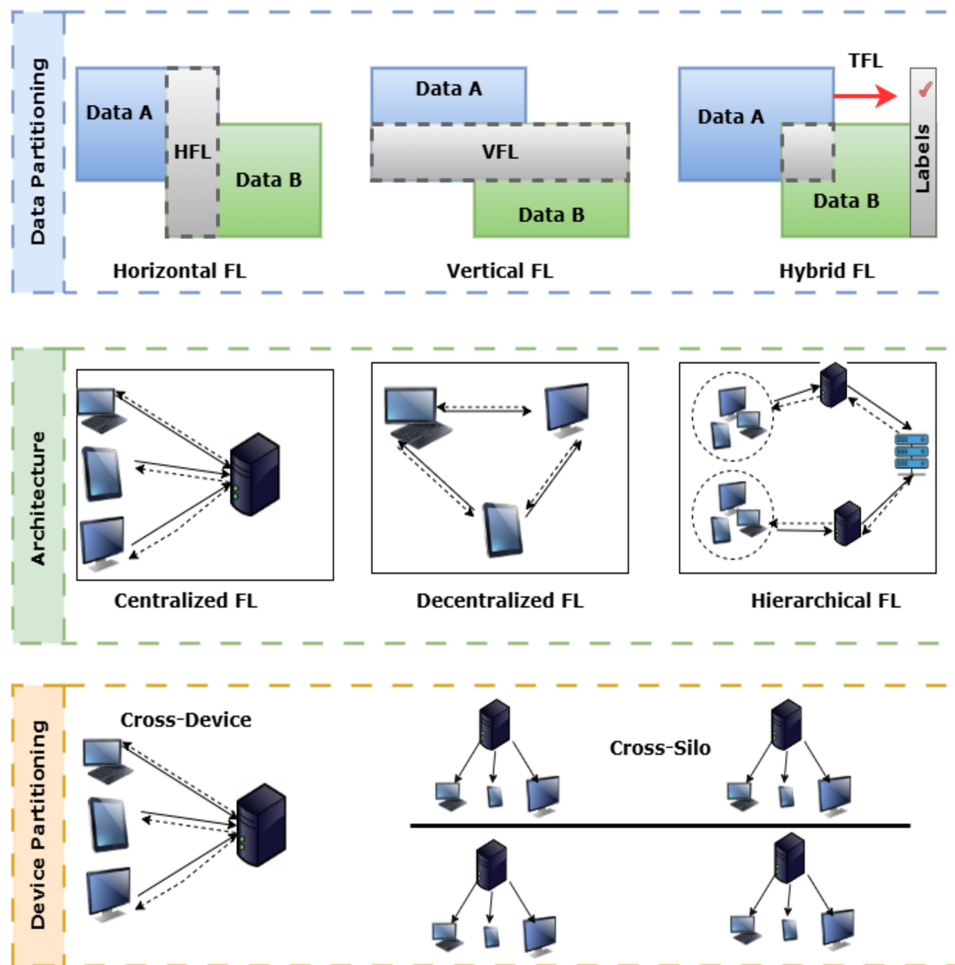


Figure 5: Overview of federated learning paradigms, illustrating data partitioning strategies (horizontal, vertical, and hybrid FL), architectural designs (centralized, decentralized, and hierarchical FL), and device partitioning scenarios (cross-device and cross-silo).

3.2.2 Architectures of FL

As illustrated in Fig. 5, there are primarily three federated learning architectures encouraging collaborative model training while preserving data privacy [18]. In a centralized framework, a server collects updates from several clients and combines them to oversee the training process. This allows for regular model updates and reduces management complexity. Conversely, the configuration presents a few shortcomings: it renders a single point of failure and is not highly scalable as the number of clients increases, such as hospitals locally training medical image segmentation models and sending updates to a central server for aggregation using FedAvg [19]. In a decentralized setup, clients can share information directly, improving fault tolerance and privacy. However, it creates hurdles to its coordination and can lead to somewhat inconsistent updates, given that clients may come and go at random, as peer-to-peer networks such as blockchain networks do. Radiology departments exchange model parameters directly, peer-to-peer, to eliminate reliance on a central server [20]. The hierarchical framework allows clients and servers to be organized into different tiers, with servers at lower tiers gathering updates for higher-tier clients. In this manner, it scales well and enables optimized communication.

3.2.3 Device Partitioning in FL

Based on the devices participating and the scale of the training process, federated learning may be divided into two primary types: Cross-Silo and Cross-Device, as shown in Fig. 5.

Cross-silo FL [21] is a collaborative approach among various organizations and institutions. This collaboration facilitates joint training of learning models while ensuring data privacy and compliance with legal standards. This approach is especially useful in sectors such as healthcare and finance, where stringent regulations prevent the sharing of sensitive information. Conversely, Cross-Device FL emphasizes collaboration among numerous devices or clients, such as smartphones and IoT devices [22]. This strategy allows applications to be customized to suit individual user preferences while maintaining the privacy and security of personal data.

3.2.4 Federation Synchronization Mechanism

Synchronization in federated learning is the process of combining local model updates from cooperating clients with the central aggregator node. Synchronous, asynchronous, semi-synchronous, and semi-asynchronous aggregations are the four fundamental synchronization mechanisms [23].

In synchronous aggregation, devices simultaneously forward their locally trained models. This method is helpful for continuous model updates and enhancing precision. However, it creates a heavy communication burden that can degrade convergence, particularly in large-scale or heterogeneous systems with numerous edge IoT devices. Conversely, asynchronous aggregation allows clients to update their local models at their convenience and communicate with the aggregator whenever they want, thereby addressing issues encountered when users switch devices. This approach reduces communication costs but may result in slower convergence and less accurate models by using stale or inconsistent information.

Semi-synchronous aggregation is an intermediate strategy in which the server receives updates after a group of clients has collected requests. This approach balances the speed of convergence and communication delay. Finally, semi-asynchronous aggregation combines elements of synchronous and asynchronous methods. In this case, the client performs a predefined number of local iterations before sending their updates to the server, which synchronously aggregates them at pre-programmed intervals. Proper tuning of the synchronization interval is critical for attaining optimal performance.

3.3 Heterogeneity in Federated Learning

To date, numerous novel federated learning algorithms have been introduced and assessed using standard benchmark datasets such as MNIST and CIFAR [24]. However, these algorithms often do not reliably enhance performance in heterogeneous settings, particularly in medical healthcare applications. Heterogeneity can be explored via the following dimensions: 1) data space heterogeneity, 2) model heterogeneity, and 3) system heterogeneity.

3.3.1 Data Heterogeneity

Data heterogeneity in federated learning refers to the distribution of data across participating clients, potentially affecting the training dynamics and the model's efficacy. In the case of Independent and Identically Distributed (IID) data, each client holds samples drawn from the same probability distribution, ensuring statistical similarity.

In contrast, non-IID data pose challenges because the data distributions across clients can differ considerably. Each client may exhibit distinct sample traits, as illustrated in Fig. 6. For example, variations may arise due to differences in scanner manufacturers, patient demographics, or imaging quality [25].

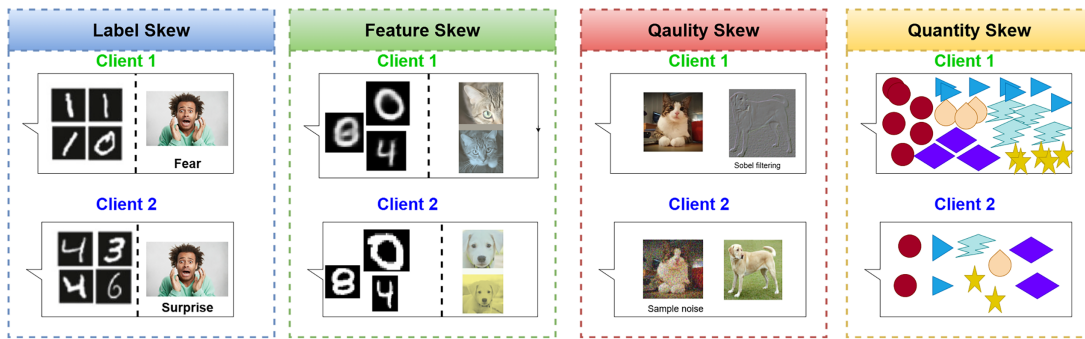


Figure 6: Examples of statistical heterogeneity in federated learning, illustrating label skew, feature skew, quality skew, and quantity skew across different clients.

Data heterogeneity can be classified into three categories: data drift, label skew, and data quality issues [26]. Data drift refers to changes in the proportions of a client's local samples for particular labels. Label skew encompasses disparities in label distributions, such as label distribution skew, which is often modeled by a Dirichlet distribution [27], and label preference skew, in which clients exhibit a partiality for certain labels. Data quality pertains to inconsistencies in sample quality among clients.

3.3.2 Model Heterogeneity

The different model architectures and hyperparameters that clients select for FL systems introduce model heterogeneity because they require different computational resources and have varying datasets and application requirements. For instance, devices with limited resources might use lightweight models, whereas systems with greater capacity might adopt more complex model architectures. Clients who use different hyperparameter settings for their learning rates and optimization methods will experience varying training outcomes because these settings affect their training process. The process of enabling different participants to work together effectively requires organizations to address model-level heterogeneity, as this affects their ability to maintain global model performance. The research demonstrates that model distillation together with federated personalization serves as an effective solution to this particular issue [24].

3.3.3 System Heterogeneity

The term system heterogeneity in FL refers to the fact that different clients have distinct infrastructure, communication skills, and computational capabilities. The devices used in this system range from high-performance servers to low-resource edge devices, including smartphones and Internet of Things sensors, because these devices have different processing power, memory capacity, storage, and network connectivity. The system faces challenges because existing differences create training duration issues, communication problems, and client disconnection during model updates. The system requires adaptive methods, including asynchronous updates and resource-aware training and client selection strategies, to achieve efficient system performance while maintaining fair participation among users, as in [28].

3.4 Aggregation Algorithms in Federated Learning

The aggregation of model updates from participating clients to generate a global model is very crucial [29]. At the weight level, the aggregation operation sums the weights (parameters) from local models trained independently on distinct clients to keep the global model up to date. It remains the most prominent form of aggregation in federated learning, with widely used technical examples being FedAvg [30] and FedProx [31]. Many recent studies in medical image analysis illustrate the use of weight-level aggregation in practice. For instance, FedSGDCOVID [32] employed a federated SGD approach for COVID-19 detection using chest X-ray images, whereas ResNetFed [33] utilized DP-SGD for privacy-preserving pneumonia detection.

Robust aggregation techniques, such as the trimmed mean or Krum, are used to withstand malicious client contributions by rejecting outliers or adversarial updates at the time of aggregation. For example, [34] proposed distance-based outlier suppression (DOS) to defend against poisoning attacks in federated learning for medical imaging.

In contrast, a feature-level aggregation focuses on merging extracted features or embeddings rather than raw model parameters. This approach is particularly relevant for high-quality feature representation learning. Recent examples include federated contrastive learning frameworks such as FedMoco [35], FedCL [36], SelfFed [37], and prototypical contrastive learning methods [38], which aggregate feature embeddings across clients to improve model generalization under non-IID data distributions. Techniques such as feature fusion, self-attention-based aggregation, hierarchical aggregation, and federated feature extraction enhance handling of data heterogeneity [28,39,40]. A detailed comparison between weight-level and feature-level aggregation is presented in Table 3.

Table 3: Comparison of weight-level and feature-level aggregation.

Aspect	Weight-Level Aggregation	Feature-Level Aggregation
Definition	Model weights	Feature representation
Advantages	Computational efficiency. Simplicity in implementation. Well-suited for large-scale federated systems.	Can handle highly heterogeneous data more effectively than weight-level aggregation. Preserves fine-grained feature information for downstream tasks.

(Continued)

Table 3 (continued)

Aspect	Weight-Level Aggregation	Feature-Level Aggregation
Challenges	Vulnerable to model poisoning attacks. Struggles with highly heterogeneous data distributions.	Higher computational and communication overhead due to larger feature vectors. Feature alignment across clients may be difficult, especially with non-IID data.
Use Cases	Mobile learning, similar data distributions.	Image classification, NLP tasks.
Robustness	May struggle with non-IID data.	More robust to non-IID data.

3.5 Fairness in FL

The execution of federated learning needs fairness measures that enable equal success and active participation from all client groups [41]. Fair client selection provides every client with an equal opportunity to participate in developing the global model for their organization [42]. The different availability patterns of clients, along with their differences in data quality and resource access, create conditions that result in some clients being less represented. The process of fair model optimization establishes equal performance standards for all clients [43] while handling non-IID data by balancing model accuracy with equitable treatment. The primary task is to eliminate performance discrepancies across clients while maintaining the overall functionality of the global model. The methodology of fair Contribution Evaluation [44] establishes methods to measure client work and deliver proper value for their effort, which relies on Shapley value-based techniques as the preferred approach. The challenge of measuring client contributions becomes more complicated because clients exhibit different data distributions and distinct computing capabilities. The success of federated learning systems depends on solving these problems, which must be resolved before their ethical implementation can occur.

4 Security in FL

Federated learning effectively safeguards privacy, yet it remains vulnerable to various threats that could compromise its security and operational functionality. Tackling these vulnerabilities and mitigating associated risks are essential for maximizing the effectiveness of FL in practical applications. This section offers an extensive scientific evaluation of the threats to FL along with the respective countermeasures.

4.1 Threats in FL

The threat modeling method involves systematically identifying, analyzing, and prioritizing risks relevant to a system, application, or dataset. To comprehend the risks of federated learning, given its inherently distributed nature, a threat model must be developed in the context of medical data privacy [45]. The framework enables different sets of customers, including mobile devices and institutions, to train a common model without exchanging raw data. The risk analysis identifies vulnerabilities, enabling enforcement of security requirements to protect confidential data [46].

4.1.1 Components of a Threat Model

An effective threat model for federated learning must consider the assets that need protection and the threat actors that aim to exploit the system's vulnerabilities. Ensuring the security of confidential data is essential in a federated medical data system. This includes patient data, medical records, and treatment histories to maintain privacy. Alternatively, other parameters, weights, and gradients serve as a layer of protection for the accuracy and integrity of the global model, which is essential to ensuring that the federated system effectively safeguards sensitive medical data against potential breaches. However, additional points of possible attack arise from clients themselves: client devices, whether smartphones or IoT devices, that might be used as gateways for data manipulation or interception. In addition, any communication channel that is not protected against communication interception or malicious interference is extremely unwise. In terms of threat actors, there are external attackers seeking unauthorized access to data, models, or relevant communications. Insider threats, including employees or personnel with some degree of legitimate access, might also revoke certain privileges in a manner that undermines the sensible handling of sensitive information or alters model updates. Beyond this, competitors may also be a threat by trying to pierce the federated model or shared data for insights or intellectual property [47].

4.1.2 Categories of Security Threats in FL

In federated learning, these security threats challenge the effectiveness of any system and the assurance of participant confidentiality. Malformed clients pose serious threats by carrying out data- or model-poisoning attacks and free-riding. Moreover, federated learning raises significant privacy concerns, as clients may inadvertently leak private data during model updates. There is a threat of inference attacks, such as model inversion, which extract sensitive information from the shared model [45]. The different categories of security threats in federated learning are illustrated in Fig. 7.

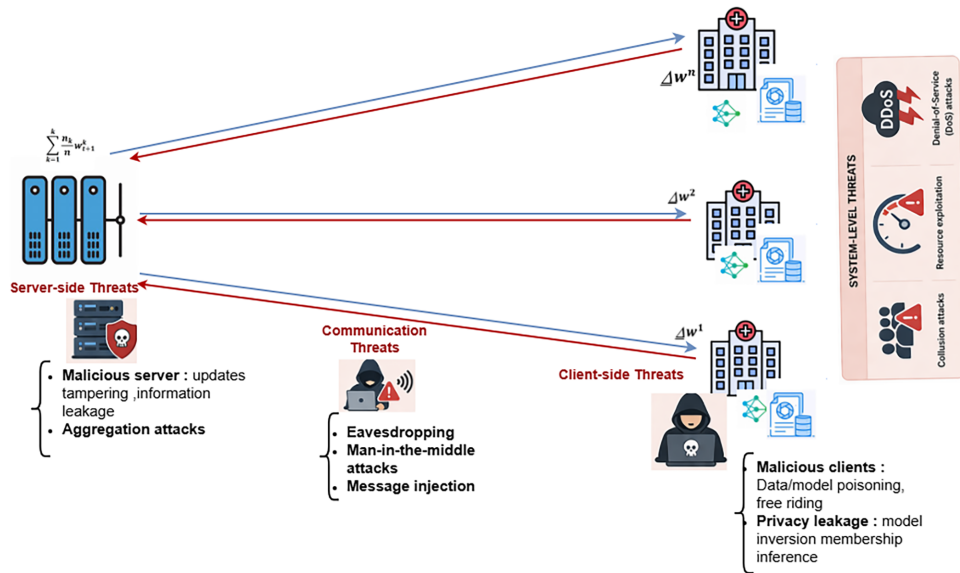


Figure 7: Security threats in FL, including client-side, server-side, and communication-based attacks.

If the server is malicious, it can always tamper with the aggregation process or extract private information from client updates, thereby undermining the solution's integrity on a global scale. Not only that, there are several loopholes in the server view aggregation process, as it is entirely unaware of adversary actions; hence, such malicious updates can adversely affect the model's operation or perform tasks they are not supposed to.

Threats to communication include eavesdropping by adversaries external to the FL system, during which the adversaries may be able to recover sensitive information from the model updates intercepted while being sent from a client to the server; and also man-in-the-middle attacks, leading to interference by way of altering the messages, injecting bogus updates, or outright disrupting the training.

Inside attacks include collusion, in which a group of clients or entities actively works to undermine the system's integrity through coordinated poisoning attacks or privacy breaches. At the system level, the concern centers on resource exploitation, in which attackers target less secure clients or exploit system heterogeneity and resource limitations. Additionally, denial-of-service (DoS) attacks threaten by flooding servers or blocking communication paths, hindering efficient training and model updates [46,48].

4.2 Security and Privacy Solutions in FL

Implementing multiple solutions to protect federated learning systems will safeguard their security and privacy by addressing distinct security weaknesses while enhancing data security Fig. 8. Hybrid security approaches combine multiple specialized methods, combining cryptographic techniques and perturbation methods to create comprehensive security solutions [45]. The protection of data and operational functions depends heavily on cryptographic security methods. Additive homomorphic encryption enables encrypted data processing, secret sharing distributes information across multiple users to prevent unauthorized access, and secure multiparty computation (SMPC) enables different parties to collaborate without disclosing their private data [49]. Data encryption using secure communication protocols provides essential protection by safeguarding information during client-server communication, preventing unauthorized access and interception. The emerging split learning method enables clients to work with only a small portion of the model, reducing the risk of disclosing sensitive information. The Krum, Trimmed Mean, and Baffle aggregation algorithms block adversarial breaches by creating model updates that lack irregularities. The application of global and local differential privacy perturbation methods to model updates introduces controlled noise while protecting the identity of individual data points. The process of model perturbation alters the model's gradients, thereby enhancing the protection of confidential data [50]. Anonymization techniques, such as de-identification, ensure that personal data cannot be linked back to individuals. Furthermore, blockchain technology enhances the reliability and transparency of federated learning frameworks by maintaining an unchangeable log of client actions and model updates. The integration of these approaches provides a robust safeguard for federated learning systems and ensures the confidentiality of sensitive data.

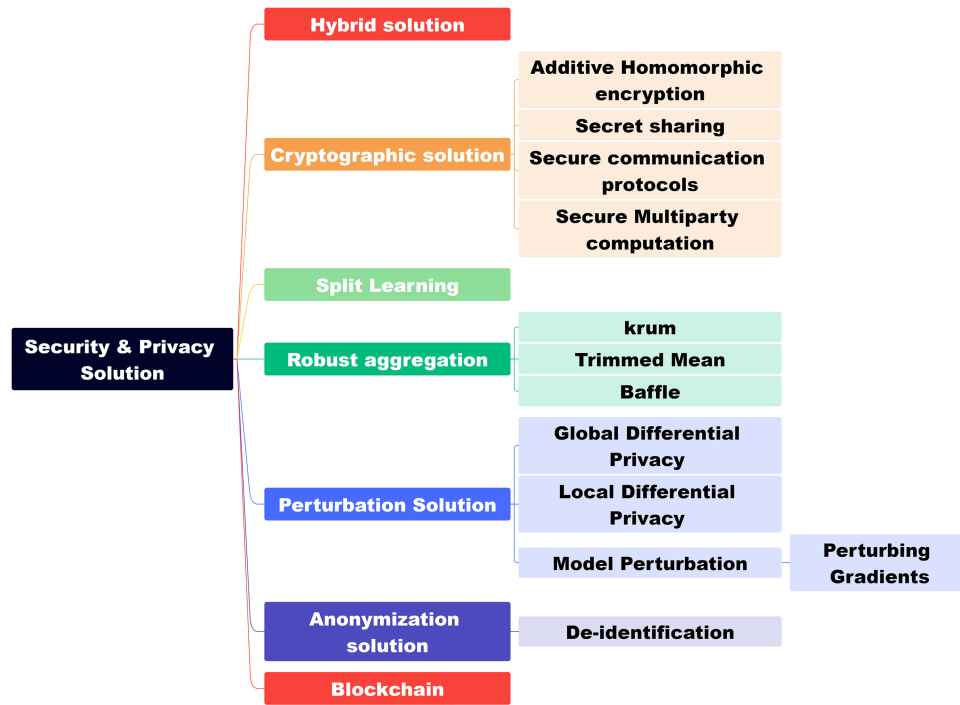


Figure 8: Comprehensive framework for security and privacy solutions in data management.

5 FL and Medical Image Analysis

The healthcare system requires advanced computational methods for medical image analysis to process scans, confirm medical diagnoses, create treatment plans, and monitor disease progression. The disease progression monitoring process employs multiple methods, including machine learning, deep learning, and image processing techniques, to identify abnormalities and separate body parts from their associated tissues. Medical professionals use Convolutional Neural Networks (CNNs) as their primary algorithm to classify and identify medical images containing tumors and lesions.

This method is often employed in X-ray, MRI, and CT imaging for tumor detection. Medical image analysis is a fundamental requirement for creating three-dimensional models, which medical professionals use for surgical planning and radiation therapy visualization. The current situation still faces multiple challenges: no annotated data is available, medical facilities use different imaging methods, and models struggle to interpret their results [51]. Medical imaging systems transform federated learning, which enables remote model development without exposing patient data to outsiders, and through other advanced technological methods. The development process ensures the delivery of precise medical treatment that meets specific patient needs and time requirements [10].

5.1 Medical Imaging Datasets

Federated learning in medical imaging is a promising method for improving diagnostic precision while maintaining patient confidentiality. This approach allows multiple healthcare entities to jointly train machine learning models without the exchange of sensitive information. FL assists in creating strong models applicable to diverse medical imaging tasks. Fig. 9 illustrates significant applications of FL in this field, emphasizing particular datasets and their applications.

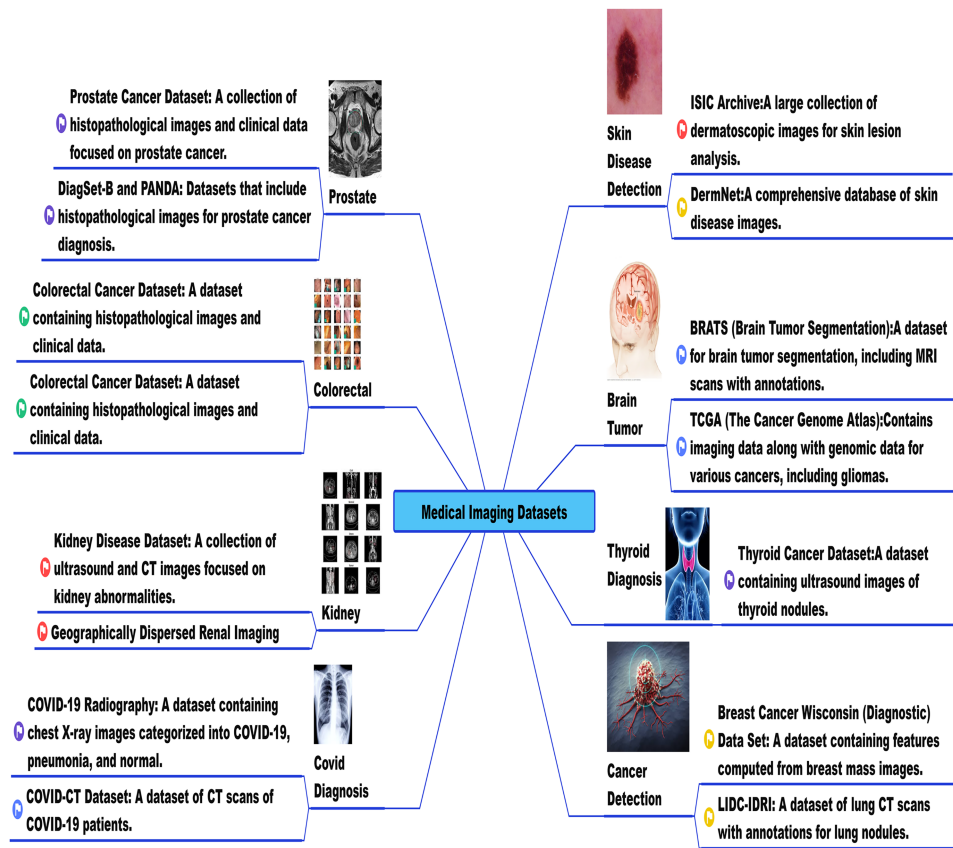


Figure 9: Comprehensive overview of collaborative medical imaging datasets in federated learning.

Medical imaging datasets are key elements that scholars must use to create models of detection and diagnosis of various medical conditions. ISIC Archive offers a wide range of dermatoscopic images, which researchers use to learn the skin lesions, such as melanoma and many other skin disorders [52]. The data set can be used to create diagnostic algorithms that can aid dermatologists in the diagnosis of skin diseases. DermNet is a useful learning tool, which facilitates research through the provision of a vast database of dermatological images and data on different skin diseases [22].

MRI scans that are annotated by experts are provided in the BRATS dataset [53], and the experts can be used to segment brain tumors and identify and locate them to facilitate their research. Imaging data is available in the Cancer Genome Atlas TCGA, which is utilized by researchers without genomic data to enhance covariate analysis in neuro-oncology studies in several different cancer types, including gliomas [54]. The project uses multi-mode research to increase the knowledge of scientists concerning tumor biology.

The Thyroid Cancer Dataset is comprised of ultrasound images of thyroid nodules, which are utilized by researchers to conduct research in thyroid diagnosis [55]. The images are used as training information to enable the researchers to develop models that are able to distinguish between benign and malignant nodules in order to aid in early diagnosis and the decision to treat.

The Breast Cancer Wisconsin Diagnostic Data Set [56] offers significant properties obtained by researchers on a breast mass image as a way to construct the breast cancer detection algorithms that can promote the early diagnosis and enhance patient outcome. Similarly, the LIDC-IDRI dataset was an

annotated dataset of lung CT scans, which has been useful in conducting research and creating algorithms to detect lung nodules and lung cancer diagnosis [57].

Kidney Disease Dataset is the data that includes records of ultrasound and CT scans to indicate abnormalities of the kidneys, and the data was used to develop models capable of distinguishing between kidney tumors and kidney stones [58]. The Geographically Dispersed Renal Imaging repository is a repository of Imaging data that is contributed by several institutions, to facilitate collaborative research activities without violating patient privacy [59].

Researchers will utilize the Colorectal Cancer Dataset since it has histopathological images and clinical data on which they will develop models to identify colorectal cancer, as well as analyze tumor properties as outlined in [60]. The classification of colorectal cancer is performed with the LC25000 dataset, which will assist in creating helpful diagnostic tools [61].

The Prostate Cancer Dataset is a dataset of prostate cancer with histopathological images and clinical data associated with prostate cancer diagnosis, according to which researchers can create models to identify cancerous tissue and enhance the accuracy of diagnostic methods, as stated in the article, published in [62]. The DiagSet-B and PANDA datasets combined with each other will be offered as the machine learning training data that will improve both detection techniques and treatment strategies [63].

This dataset, namely COVID-19 Radiography, is the set of chest X-ray images of COVID-19 patients, with three possible categories, i.e., COVID-19, pneumonia, and normal. Such data is helpful to create models to determine COVID-19 in X-rays [64]. As stated in the article in reference 41, the COVID-CT Dataset offers CT scans of patients with COVID-19 in order to aid in the creation of diagnostic algorithms that will enhance medical response activities during the pandemic. A combination of these datasets is important to continuing to develop machine learning applications in medical diagnostics in various fields.

5.2 FL and Contrastive Learning in Medical Imaging

Federated contrastive learning establishes a modern approach to medical imaging that effectively addresses privacy concerns, non-IID data distribution, and the lack of labeled datasets. The federated learning framework enables contrastive networks to tackle non-IID problems through their two-step learning method [65]. The system undergoes a joint pre-training phase during which both parties share their features to process unlabeled data. The client-based system enables users to learn through active comparison of features. The system employs federated supervised learning to enhance its capacity to operate with limited labeled data. Multiple systems have been created to support contrastive learning within federated learning environments, which are needed for medical image assessment. One notable work, FedMoCo, introduced in 2021, was among the pioneers in federated contrastive learning for medical imaging [35]. This method enables the transfer of specific metadata alongside self-adaptive aggregation processes to address privacy concerns and data insufficiencies, making it particularly valuable for COVID-19 detection applications. The combination of FL and contrastive learning with medical applications creates systems that protect user privacy and work in distributed environments. This method solves the problem posed by having both inadequate and diverse data types. The researchers use contrastive learning across their collection of unlabeled datasets to boost diagnostic model performance, thereby driving medical research and advancing healthcare technology.

5.3 FL Applications in Medical Imaging

The use of federated learning in medical imaging applications spans multiple domains [66], improving diagnostic processes and patient treatment methods. The algorithms used in this system play a vital

role in medical image categorization, helping doctors make more accurate diagnoses. The initial method enables medical professionals to assess different health conditions through comprehensive image analysis. Segmentation serves as an essential element of this procedure because it enables the division of images into parts that can be analyzed in depth. The analysis of tumors benefits from segmentation techniques, which provide scientists with tools to identify and study abnormal growths observed in medical imaging. Medical imaging detection functions as an essential system because it helps determine whether patients have medical conditions, allowing doctors to start treatment as soon as possible. The process of creating three-dimensional models from two-dimensional image slices involves using reconstruction techniques to combine the outputs from the slices. The process enables better visualization, which helps to understand complex systems. Surgical procedures and educational programs depend on these models to provide accurate information about body structures. The new medical imaging methods that emerge from federated learning technology create a new research area for scientific study [67]. Table 4 provides a summary of various applications of deep learning and federated learning in the realm of medical imaging.

Table 4: Summary of federated learning applications in medical imaging.

Application Area	Reference	Dataset	Imaging Modality	Methods	Target Condition
Skin Disease	Deng et al. [68] 2025	HAM10K, MSK	Dermatoscopic Images	FL, Classification, ResNet-101	Various Skin Diseases
	Liu et al. [36] 2023	HAM1000	Dermatoscopic Images	FL, DenseNet-121	Various Skin Diseases
Lung Cancer	Usharani and Selvapandian [69] 2025	Iraq Oncology Hospital	3D CT Scan	FL, ResNet50, Detection	Lung Cancer
	Meda et al. [70] 2025	LIDC-IDRI	CT Images	FL, DKCN, Fuzzy clustering	Lung Cancer
COVID-19	Alhafiz and Basuhail [71] 2025	COVID-19 CT	CT Scans	FL, CNN, Non-IID	COVID-19 Classification
	Khowaja et al. [37] 2025	COVID-19 Radiology	Chest X-ray	FL, ViT	COVID-19 Classification
	Noman et al. [72] 2023	COVID-19 Radiology	Chest X-ray	FL, CNNs	COVID-19 Classification
	Liu et al. [73] 2024	COVID-19 Radiology	Chest X-ray	FCL, Foundation Models	Tuberculosis Diagnosis
	Rana and Marwaha [74] 2025	COVID-19 Radiology	Chest X-ray	FL, Autoencoder	Pneumonia Detection
Brain Tumor	Onaizah et al. [75] 2025	Brain tumor dataset	MRI	FL, SiCNN	Brain tumor classification
	Monisha and Rahman [76] 2025	CE-MRI	MRI	FL, YOLOv11	Brain tumor detection
	Sivakumar et al. [77] 2025	Figshare, SARTAJ, Br35H	MRI	FL, FedAvg, FedProx, CNN	Brain tumor classification
	El Badaoui et al. [78] 2025	Multimodal MRI	MRI	FL, Quality-based aggregation	Tumor segmentation
	Roy et al. [79] 2025	Medical images	MRI	Semi-synchronous FL, Chaos encryption	Secure image sharing

(Continued)

Table 4 (continued)

Application Area	Reference	Dataset	Imaging Modality	Methods	Target Condition
Thyroid Nodule	Xiang et al. [80] 2025	Ultrasound	Ultrasound	FL, Attention UNet	Segmentation
	Lee et al. [81] 2021	Ultrasound	Ultrasound	FL, VGG19, ResNet50	Classification
	Chen et al. [82] 2025	Medical images	Ultrasound	Personalized FL (Prototype-based)	Classification
Breast Cancer	AlSalman et al. [83] 2024	VINDR-MAMMO	Mammography	FL, DNN	Detection
	Li et al. [84] 2022	BreakHis	Microscopic	FL, ResNet, DenseNet	Detection
	Amritanjali and Gupta [85] 2025	BRCA	Radiology	Centralized vs. FL	Detection
	Karthiga et al. [86] 2025	Medical datasets	Imaging	FL + Explainable AI	Cancer detection
	Liang et al. [87] 2026	Medical images	Imaging	DP-FL, Vision Transformer (LoRA)	Classification
Kidney Disease	Mohammed et al. [88] 2024	Kidney images	Ultrasound/X-ray	FL, Reinforcement learning	Kidney disease
	Vekaria et al. [89] 2024	Renal datasets	Imaging	Federated transfer learning	Kidney abnormalities
	Liu et al. [90] 2025	Medical images	Imaging	HE + DP (DPSHE)	Privacy-preserving analysis
Prostate Cancer	Kong et al. [63] 2024	PANDA	Histopathology	Federated attention learning	Diagnosis
	Ren et al. [91] 2026	Medical segmentation datasets	Imaging	Domain generalization FL	Segmentation
Colon Cancer	Hossain et al. [92] 2024	LC25000	Histopathology	FL, Inception-V3	Classification
	Kuang et al. [93] 2026	Medical images	Imaging	Semi-supervised FL	Segmentation
General / Multi-task	Zhao et al. [94] 2025	Medical datasets	Multi-modal	Federated prototypical learning	Classification
	Niu et al. [95] 2025	Medical images	Imaging	Semi-asynchronous FL + Diffusion	Segmentation

6 Privacy Threats and Mitigation Strategies in FL for Medical Imaging

This section is systematically structured to examine the security and privacy issues linked to federated learning within medical image analysis. In Fig. 10, we provide a detailed overview to aid in understanding the distinct components of security and privacy in this field.

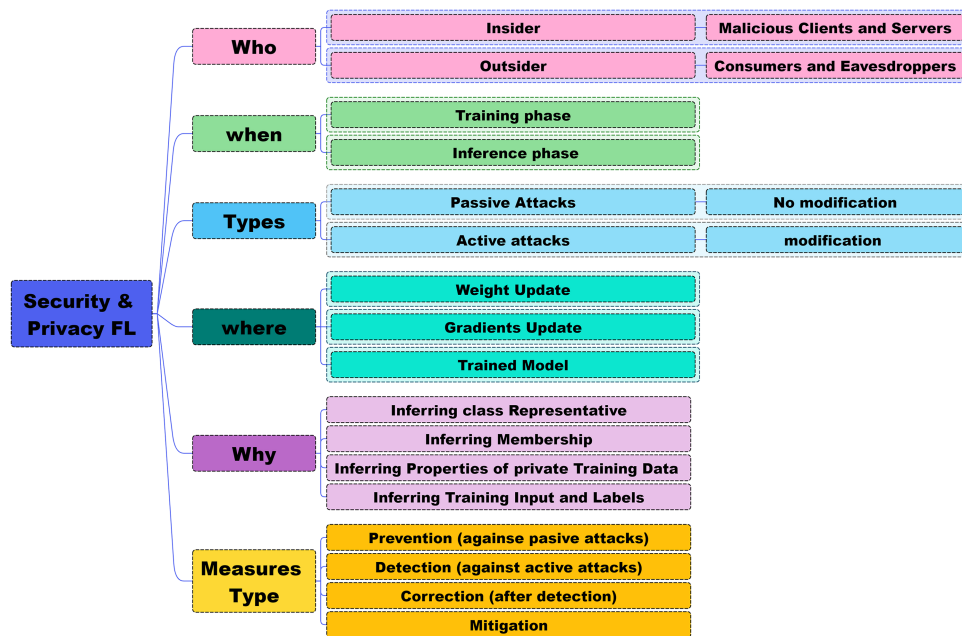


Figure 10: Overview of security and privacy mechanisms in federated learning for medical applications.

In this section, the scope of privacy threats and defensive mechanisms in FL will be systematically studied, and the applications in the medical sphere will be considered. Threats are categorized into client-side, server-side, and communication-level threats, including data poisoning, membership inference, model inversion, and man-in-the-middle attacks. The consequences of every threat, practical examples, and their possible consequences to the medical field have been explored in detail.

In addition, we evaluate advanced protection techniques, including differential privacy, secure aggregation, and homomorphic encryption, and evaluate their effectiveness and inability to mitigate these threats. To provide a broad picture, the systematic review includes real-life case studies, and the barriers to achieving a balance among privacy, utility, and computational efficiency are identified. Prospects for future research are offered. The proposed study aims to be an important resource for researchers, practitioners, and policymakers committed to developing secure, privacy-focused FL systems for medical applications.

6.1 Privacy Threats in FL for Medical Imaging

Different privacy attack objectives are connected with retrieving information about the training dataset in the model parameters in the course of the training or the post-training phase. The opponents can attack several stages to break the data secrecy and obtain sensitive data, such as model parameters, raw data, and the state of available information in federated learning training. In this discussion, we discuss various methods of data privacy attacks: poisoning attacks, Byzantine attacks, and membership-inference attacks, as shown in Fig. 11.

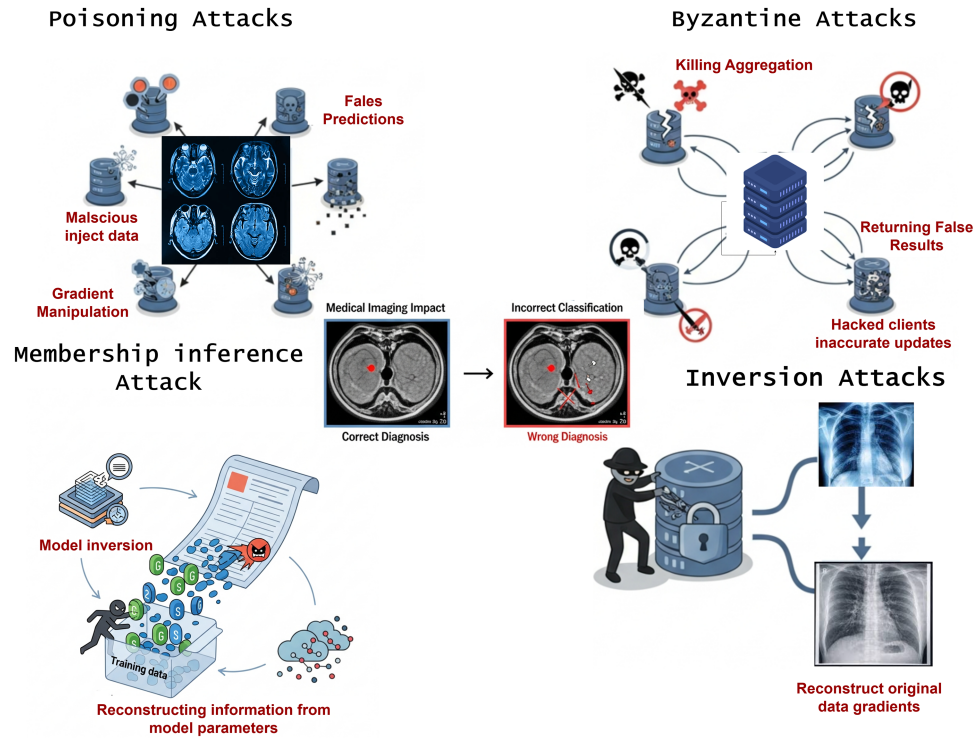


Figure 11: Privacy threats in FL for medical imaging.

6.1.1 Poisoning Attack

Poisoning attacks occur when malicious clients use false information to disrupt the training process, leading to a decline in model performance [96]. The system experiences operational malfunctions, resulting in incorrect classifications and predictions that yield particularly harmful outcomes in fields that depend on absolute accuracy. The medical imaging field faces serious consequences when false predictions lead to incorrect patient diagnoses and treatment decisions [97]. The two main types of poisoning attacks are data poisoning and model poisoning. Data poisoning involves manipulating the source training data, corrupting the training system. The label flipping technique misleads a model by altering the medical image labels it uses to identify objects. Backdoor attacks use hidden triggers embedded in their training data to carry out their operations. A backdoor attack uses specific visual patterns to show a malignant tumor as a benign tumor, which puts the patient at risk of receiving an incorrect diagnosis. Model poisoning occurs when compromised clients deliver model updates containing corrupted data to the system [98]. The attackers use gradient manipulation as their primary method to alter the gradients they send to the central server, thereby affecting how the system learns [99]. The medical imaging field uses this method to alter the model system, leading to the system missing essential elements and resulting in incorrect diagnoses and unsuitable medical treatments. The two types of poisoning attacks create major threats to federated learning system security, which medical imaging operations face because even one error can result in death for patients who need treatment.

6.1.2 Byzantine Attack

The attack scenario in Byzantine begins when certain participants, or even the server, target malicious operations that disrupt the entire task model training process. The attack also poses a significant threat

to medical imaging, as it undermines the fundamental diagnostic and treatment paradigms that medical practitioners use. Byzantine servers perform two harmful actions: either killing the aggregation process or returning false results to users, resulting in a significant drop in model performance [100,101].

Byzantine attacks are a term for malicious behavior that may take many forms. There is a particular case in which hacked clients provide the world model with inaccurate updates, which, in turn, deceives the learning process. The model will produce incorrect classifications of medical images, leading to a wrong diagnosis for the patient.

The type of attack consists of several different approaches, both simple in nature, such as random noise injection, and advanced approaches that try to mimic actual updates with the effect of minimizing model performance. An attack occurs when an attacker delivers updates that appear authentic but diminish the model's ability to recognize critical medical imaging warnings, tumors, and lesions. These attacks pose a serious threat to federated learning systems, especially in medical imaging, potentially leading to false model predictions that endanger patient lives [102]. The group learning process should be secured against the Byzantine attacks, and internal breaches and partiality should be prevented.

6.1.3 Membership Inference Attack

Membership inference attacks present considerable risks to the privacy of sensitive medical records [103]. Such attacks enable adversaries to extract private details about the training datasets. Various inference attacks exist, including model inversion and membership inference attacks [104,105].

The exploitation of model parameters in order to reconstruct information about a person can result in the disclosure of patient confidential information through model inversion. Membership inference attacks, on the other hand, aim to find out whether a given data point, for example, a particular medical image, was included in the training data. Although these attacks do not necessarily fully reconstruct the data, they can still reveal meaningful information, such as whether a particular patient has developed a specific medical condition.

Inference attacks can be categorized into various forms, such as membership inference, which determines whether a given data point is present in a training dataset, and property inference, which extracts specific characteristics of the training data [106]. In medical imaging, property inference is particularly concerning because it can disclose sensitive patient data, eroding confidence in federated learning systems. Consequently, it is imperative to develop robust defensive strategies to shield these systems, ensuring the preservation of patients' privacy and trust.

6.1.4 Inversion Attacks

The problem of inversion attack is a real privacy threat in federated learning, as it aims to reconstruct the original training data from gradients shared by participants. That is, this type of attack exploits information stored in model updates sent to a central server. The attack proceeds by aggregating the attacker's gradients and using optimization techniques to reload the original data. Thus, it can be rebuilt to recover confidential files, including medical images, or to gain access to other personal information [107].

Inversion attacks aim to reveal information about the training data. For example, attackers could determine whether a specific medical image was in the training set or infer certain characteristics of the data, including evidence of a specific medical condition. These attacks can be classified into different categories. For example, membership inference attacks aim to determine whether a specific data point (e.g., a patient image) was used during training. On the contrary, property inference attacks seek general properties or characteristics of the training data without reconstructing specific data instances [106,108].

Instead, property inference attacks aim to identify general properties or characteristics of the training data without reconstructing a particular data instance.

These attacks are very crucial in medical imaging. To determine whether a particular image of a patient was trained into the model, an adversary can examine the model's changes, even though it is not fully reconstructed. This move poses a grave threat to data security and underscores the need for robust security protocols to safeguard patients' confidential data in federated learning systems.

Table 5 displays a complete taxonomy of table types of attacks in federated learning based on the type of the attacker, the main purpose of the attack and its real-life implementation. This categorization points out to the risks of model integrity and the significance of active protection measures in such a sensitive area as medical imaging.

Table 5: Taxonomy of attacks in federated learning: threat actors, goals, and consequences.

Attack Category	Attacker	Goal	Real-World Scenario	Attacker Benefit
Model Inversion	Client	Reconstruct sensitive local data from model updates	Attacker extracts patient MRI images from gradients.	Data Theft
Member Inference	Client	Ascertain if a specific individual is in the training dataset	Insurance firm checks if a patient is in a dataset.	Privacy Violation
Data Poisoning	Client	Inject harmful or misleading data into the training set	Hospital mislabels pneumonia cases to manipulate AI.	Bias Introduction
Model Poisoning	Client Server Man-in-the-Middle	Inject manipulated updates that corrupt the learning process	Client: Malicious hospital poisons updates. Server: Aggregator introduces bias. Man-in-the-Middle: Alters updates in transit.	Model Degradation
Backdoor Attack	Client	Insert hidden triggers for later misuse	Watermark in MRI images causes targeted misclassification.	Covert Control
Byzantine Attack	Clients	Disrupt model convergence with conflicting updates	Multiple hospitals inject noisy gradients to disrupt training.	Denial-of-Service

Table 6 summarizes key examples of real-world attack instantiations in federated learning systems (especially in medical imaging) and are presented in Table 6. Each of the entries describes the attack plan, data sets utilized and defense mechanisms. The findings highlight the practicality of such threats and support the urgency of the development of privacy preserving methods.

Table 6: Attack strategies in federated learning: case studies, datasets, and mitigation techniques.

Attack Type	Author	Year	Technique	Dataset(s)	Defense / Mitigation Strategy
Poisoning Attacks	Jin and Li [34]	2022	Backdoor attack	CXR, ISIC	FedDetect: Uses Isolation Forest to identify anomalous client behavior. Adjusts client influence via adaptive weight decay.
	Alkhunaizi et al. [109]	2022	Label flipping, Gaussian noise	CXR, HAM10000	Distance-based Outlier Suppression (DOS) for robust aggregation.
	Kumar et al. [110]	2025	Data poisoning	ChestX-ray, HAM10000, Camelyon17	FL-AGMA: Introduces an attack budget metric, employs Krum and trimmed mean.
	Yu et al. [111]	2026	Data poisoning (gradient manipulation)	Medical imaging datasets	Dweighted: Dual-reweighting with PCA and K-means clustering to detect malicious clients and adjust aggregation weights.
Byzantine Attacks	Moulahi et al. [112]	2023	Malicious clients	CXR	Blockchain-based secure aggregation.
	Mu et al. [113]	2024	Malicious clients	CXR	Blockchain-based secure aggregation.
Adversarial Attacks	Darzi et al. [114]	2023	Adversarial sample generation	MRI (tumor)	No specific mitigation; adversarial inputs crafted to fool the global model.
	Dao and Nguyen [115]	2023	Gradient inversion attack	CXR, MRI (brain)	Differential Privacy: Protects against gradient-based image reconstruction.
	Das et al. [116]	2024	Gradient leakage	CXR, MRI (brain)	Gradient perturbation as a countermeasure.

These tables collectively illustrate the evolving threat landscape in federated learning for medical imaging, emphasizing both the technical sophistication of recent attacks and the growing arsenal of defense strategies aimed at preserving data integrity and patient privacy.

6.2 Defense Strategies in FL for Medical Imaging

6.2.1 Robust Aggregation

The importance of powerful aggregation strategies in Federated Learning systems is that they reduce the effects of malicious upgrades by compromised clients as much as possible [29]. Such methods, including Krum, trimmed mean, and baffle, aim to prevent the inclusion of outlier updates, thereby protecting the aggregated model against attacks such as poisoning and Byzantine threats [117]. Krum selects reliable updates based on their proximity to other updates, thereby minimizing the risk of being influenced by invalid or malicious information while maintaining accurate results. The trimmed mean approach measures the tendency of client updates by ordering them, discarding a specified percentage of the most extreme values, and then computing the mean of the remaining values. By removing harmful updates and greatly consolidating the client updates, Baffle makes federated learning models resistant to data poisoning and adversarial attacks. Both methodologies require specific parameters to be used optimally, such as a distance threshold and the number of clients in Krum, or the trimming percentage in the trimmed mean [118]. The techniques are necessary to ensure the integrity and reliability of federated learning systems.

6.2.2 Homomorphic Encryption Techniques

Homomorphic encryption means that one can perform calculations on encrypted data without decrypting it. This will ensure that private medical data remains private during training and is highly protected against various attack vectors, a characteristic attributed to the methodology [119]. This aspect is essential, especially in the gathering and handling of medical records. There are three homomorphic encryption types: partially homomorphic encryption (PHE), where either multiplication or addition is permitted; somewhat homomorphic encryption (SHE), where a limited number of operations on encrypted information is permitted; and fully homomorphic encryption (FHE), where both operations are permitted. Although PHE is viewed as a giant leap in some applications, FHE is on a different plane due to its generality and the ability to handle very complex tasks, such as the secure transmission of data for machine learning within a collective community. The potential benefits of homomorphic encryption are matched by significant implementation challenges, most of which stem from high computational complexity. Modern work aims to optimize these procedures to effectively profile systems, making this technology viable for daily applications and establishing standard integration techniques within existing system infrastructures [120,121]. Lastly, the current developments are expected to significantly enhance the safety of medical data and provide a true analysis.

6.2.3 Differential Privacy

Differential privacy is a secure, well-defined model of privacy protection that aims to ensure the confidentiality of individual data points in datasets. A counter view is that the use of controlled randomness or noise in both a model's updates and outputs is a technique in differential privacy [122]. This would ensure that, even when the data of a particular person is included or excluded, the overall result is not distorted too much, making it difficult for an attacker to deduce sensitive information about that person. This plan provides the patient with maximum privacy. As the machine learning and data analysis environment evolves, differential privacy will enable scientists and practitioners to build models from sensitive medical data and draw meaningful conclusions. Noise to the data can be easily tailored to the desired range of privacy to utility, and model features can fulfill these goals perfectly, ensuring they achieve the desired objectives [123,124]. Differential privacy offers a potential solution to improve regular health services, enabling them to handle and analyze patient data while complying with data confidentiality standards. The widespread adoption of various privacy methods has increased their use, making them an invaluable resource in the healthcare sector that enables secure decision-making based on research data.

6.2.4 Blockchain

The opportunities to improve the safety and integrity of the analysis of sensitive medical data have attracted significant interest in blockchain-based applications by FL, due to their capabilities to enhance the security of such analysis and improve its integrity [72,125,126]. Blockchain provides a decentralized, immutable ledger of transactions and thus fulfills the vital requirement of ensuring safe, reliable interactions in federated learning. The plan enables multiple clients to collectively train a shared model without storing their data in the cloud (Fig. 12). A transaction can be verified and transparent because all model updates are listed on the blockchain. This system not only confirms the usefulness of model updates but also controls access for legitimate clients, thereby reducing the risk posed by rogue elements seeking to undermine the model's integrity. Moreover, the impossibility of modifying blockchain records is a significant improvement in accountability, as any attempts to change the model can be identified. In this manner, the synergy between blockchain and federated learning improves the security infrastructure and trust among stakeholders, enabling the construction of a more secure and reliable machine learning application.

Federated learning using blockchain has security benefits, but it is impractical to implement in hospitals. Blockchain consensus mechanisms introduce additional computational and transaction latencies, which can make model aggregation more expensive and inappropriate in clinical settings where speed is of the essence. Also, the cost of running the network's blockchain nodes is not insignificant, particularly when the model must vary frequently. The immutable registry is also a challenge for storage, and introducing blockchain into current hospital IT systems (e.g., EHR) only complicates the task. These problems highlight the need for lightweight consensus algorithms and a scalable architecture for a healthcare setting [127,128]. The current expansion in the blockchain and federated learning spheres is investigating novel means to improve performance and scalability without compromising the high security standards.

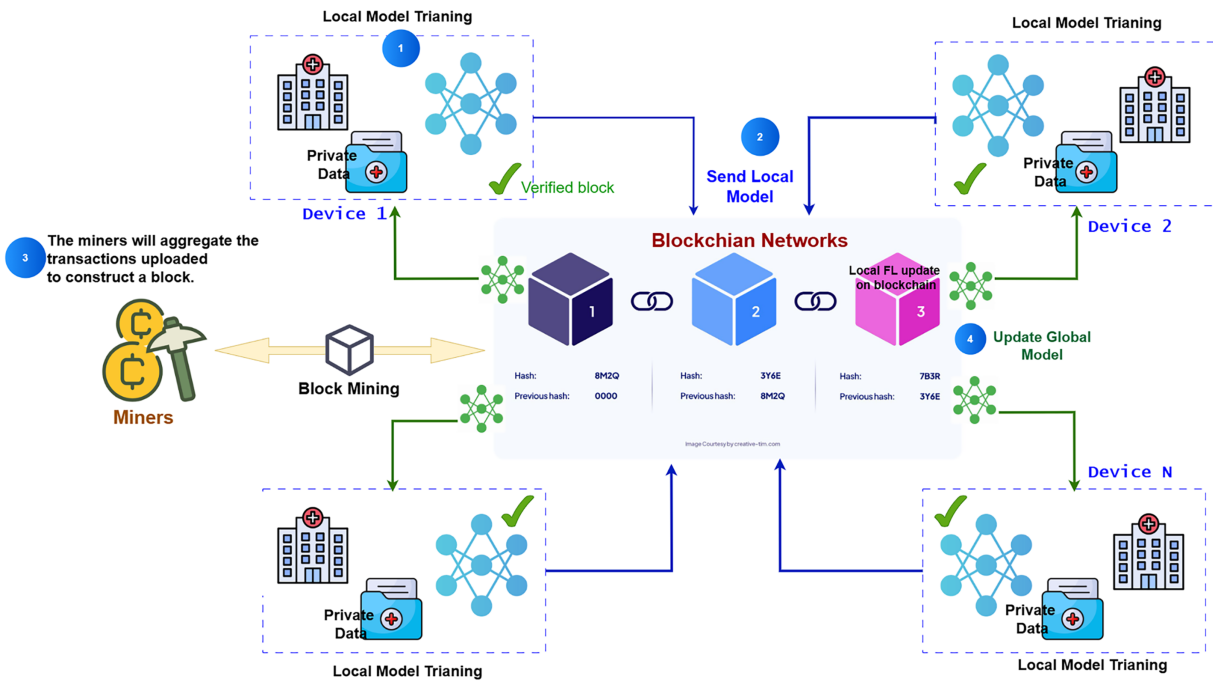


Figure 12: Overview of a blockchain-enabled federated learning framework for medical image analysis. Each participating device (e.g., hospitals or medical centers) trains a local model using private data that never leave the local site (Step 1). Instead of sharing raw data, local model updates are transmitted to the blockchain network (Step 2), where they are recorded as transactions. Miners validate these updates and aggregate them into blocks through a consensus mechanism (Step 3), ensuring integrity, traceability, and tamper resistance. The validated updates are then used to update the global model, which is redistributed to participating devices for the next training round (Step 4).

6.2.5 Split Federated Learning

Split federated learning (SFL) is an innovative cooperative learning approach that significantly enhances the management of medical data privacy while notably reducing instances of security violations [129]. SFL, as a hybrid of split learning and federated learning, ensures that raw medical data remains secure on client systems such as hospitals or clinics. It only transmits partial model updates to a central server. This partitioned learning approach can effectively prevent sensitive patient information from being compromised, making SFL particularly suitable for medical applications (Fig. 13). Furthermore, SFL establishes minute air gaps to protect itself through methods such as differential privacy to safeguard against data reconstruction, encryption to ensure secure communication, and message obfuscation to counter various gradient leakage attacks. These measures collectively provide the architecture with a robust stance against threats like data poisoning, model inversion, and man-in-the-middle attacks. In addition to these protective strategies, SFL

maximizes the efficiency of communication and computational resources, thus encouraging cooperation among healthcare organizations committed to developing precise and secure machine learning models [130]. Owing to these benefits, SFL presents a secure framework for advancing medical research and enhancing patient care while rigorously maintaining data privacy standards. The operational workflow of split federated learning is described below:

- The FL server initiates both the ‘client-side’ and ‘server-side models’.
- Each client retrieves a local version of the model and executes forward propagation using its own data, transmitting both the labels and the modified data to the Cloud server.
- The cloud server employs a server-side model to process the data and calculate gradients.
- These computed gradients are then transmitted to the clients by the cloud server.
- Clients and the cloud server modify their respective ‘client-side model’ and ‘server-side model’, subsequently uploading them to the FL-server server for aggregation purposes.

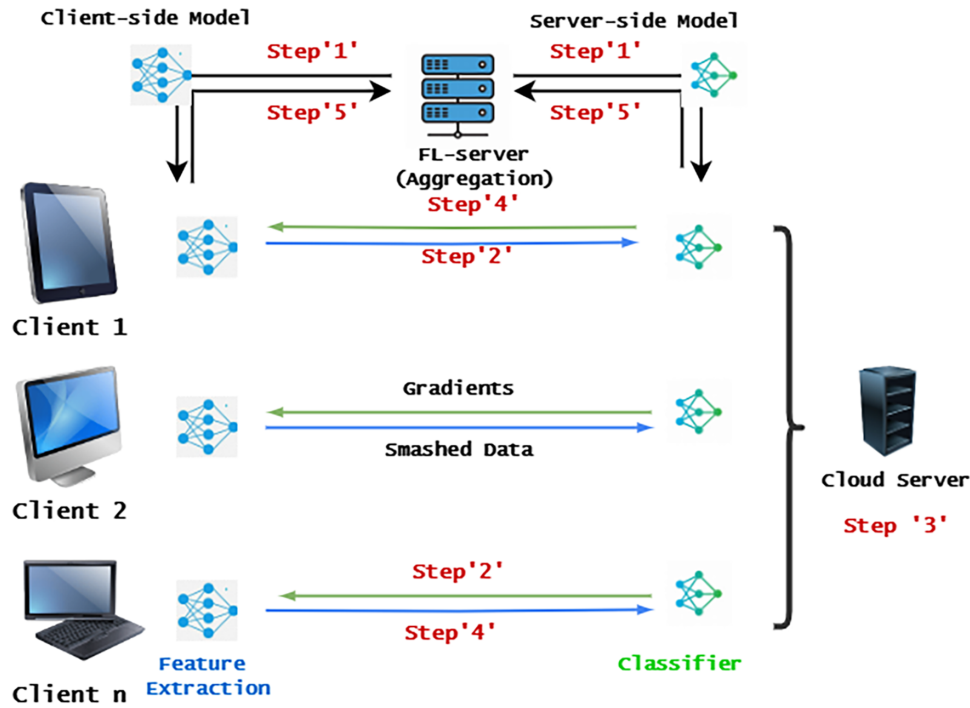


Figure 13: Split federated learning framework.

6.3 Comparative Analysis of Defense Strategies in FL for Medical Imaging

A detailed summary of the defense strategies applied in federated learning for medical imaging is presented in Table 7, highlighting the datasets, publication years, and key methodological approaches.

These methods, summarized in Table 7, demonstrate the applicability of secure federated learning approaches to diverse medical imaging challenges, ensuring both collaborative efficiency and the protection of sensitive patient data. To provide a structured analytical perspective, Fig. 14 illustrates the relationship between major privacy threats, corresponding defense mechanisms, and their associated trade-offs in federated learning systems for medical imaging.

Table 7: Summary of defense approaches and methods in federated learning for medical imaging.

Category	Author	Year	Dataset	Approach / Key Method
Split Federated Learning	Zheng et al. [131]	2024	CXR	CNN (Classification)
	Shiranthika et al. [132]	2024	Blastocyst, HAM10K	U-Net
	Zheng et al. [133]	2022	Retina, BoneAge, BraTS	ResNet34
	Yang et al. [134]	2022	U-shaped	RoS-FL: Robust Split Federated Learning
Homomorphic Encryption	Ku et al. [135]	2022	Diverse healthcare	Re-encryption server, IoMT data protection
	Zhang et al. [136]	2023	HAM10000	DNN, Dropout-tolerant scheme for robustness, Adversary prevention from inferring private medical data
	Wibawa et al. [137]	2022	COVID-19 X-ray	Privacy-preserving FL for X-ray images using CNN
	Dutil et al. [138]	2021	Medical imaging datasets	Application of homomorphic encryption for secure medical image processing
Differential Privacy	Lian et al. [139]	2022	—	Collaborative CNN training
	Ho et al. [32]	2022	Chest X-ray	CNN, privacy-aware collaborative training
	Riedel et al. [33]	2023	COVID-19 Chest Radiographs	ResNet-50, secure collaborative model training
	Ahmed et al. [140]	2024	Chest X-ray	DP-enabled FL model for COVID-19 detection

Fig. 14 provides an extensive summary of significant privacy issues in FL, along with associated security strategies and their effectiveness in reducing these threats. As shown, methods like DP, HE, secure aggregation, and blockchain-based approaches are very important for keeping sensitive medical data safe from attacks including poisoning, Byzantine, inference, and model inversion threats.

From a quantitative benchmarking point of view, these security systems are usually tested using criteria like model accuracy, communication overhead, computing cost, and privacy assurances. The image shows that while advanced protections make systems more secure and private, they also add extra work to the system, thus it's important to test performance before putting them into use.

Also, the fact that these defenses can be combined makes things even more difficult. Using more than one security measure, like DP with secure aggregation or HE, can make security assurances stronger, but it also makes it harder to balance privacy strength, communication cost, and computing efficiency. Joint optimization of these strategies continues to be an essential research avenue to properly reconcile these conflicting objectives.

Lastly, defense methods have a big effect on how useful a model is. As the chart shows, more privacy-preserving techniques may hurt prediction performance by adding noise, encrypting processing, or making data less accessible. So, it's important to find the right balance between protecting privacy and making the model useful, especially in sensitive areas like medical imaging, where accuracy has a direct impact on clinical decision-making.

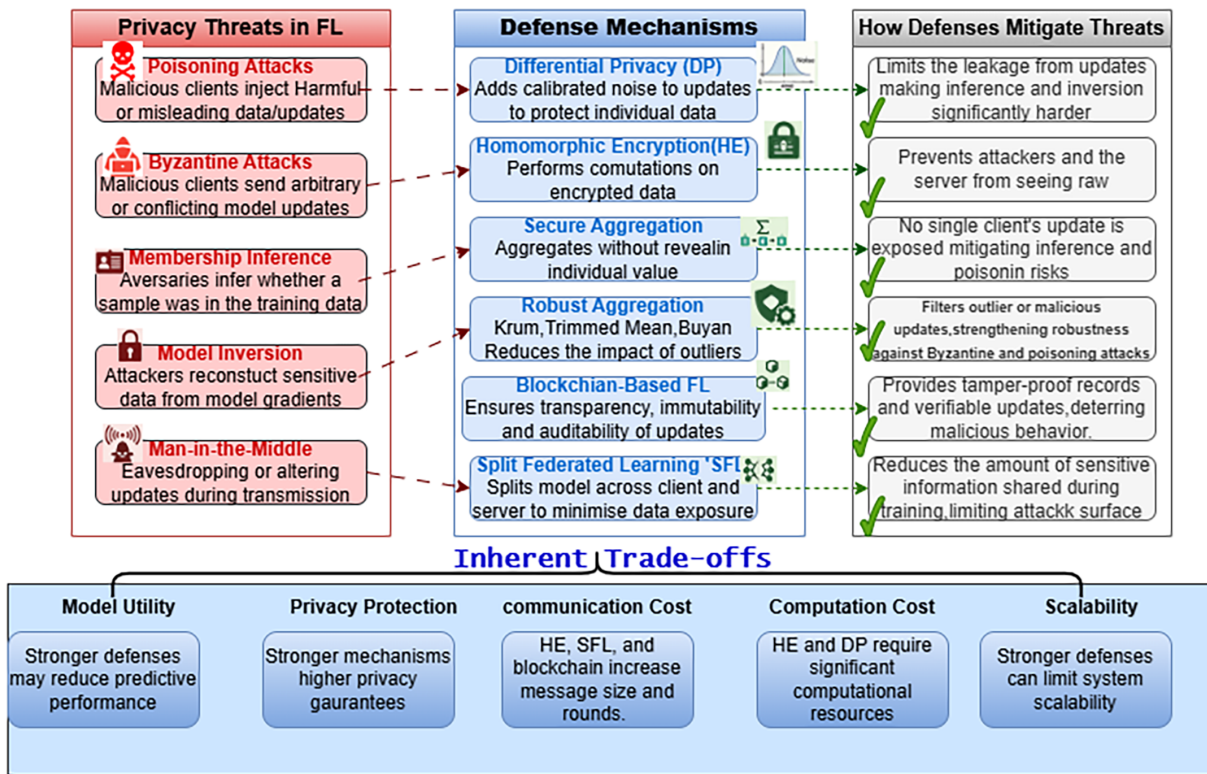


Figure 14: Effective FL system design requires balancing privacy, utility, efficiency, and scalability based on the medical application and threat model.

6.4 Software Platforms for Medical Data

Numerous FL platforms have been released to enable federated learning in the medical field, each with distinct features specifically designed to meet the requirements of healthcare applications.

- **PySyft**: The most popular such open-source library will perform machine learning in private and secure ways without losing data access. This will permit data scientists to conduct computations on distributed data within a privacy-preserved [141].
- **OpenFL (Open Federated Learning)**: In support of cross-collaborative machine learning between organizations but with privacy and security on the data in use [142].
- **PriMIA**: Intended for further advancing contributions in the context of privacy-preserving medical image analysis through federated learning techniques; applications focus on medical imaging, providing tools for privacy-preserving analysis of medical images [143].
- **Fed-BioMed**: An open-source federated learning software tailored for use in real-world medical applications that can allow researchers and practitioners to develop and deploy machine learning models while following all national regulations pertaining to data protection [144].
- **TensorFlow Federated (TFF)**: An open-source framework that allows developers to build machine learning models using federated learning principles. TFF is built on TensorFlow and provides tools for simulating federated learning environments [145].
- **Federated Learning Framework (FLF)**: basically, a federation learning stack designed for health-specific data to build a wholesome environment to develop and deploy federated learning applications [146].
- **Leaf**: Federated learning framework that provides a simple interface for researchers to play around with federated algorithms, focusing on health-related data [147].

- FATE (Federated AI Technology Enabler): Open source Project Provides a safe and efficient federated learning framework. Enable collaborative machine learning across organizations while keeping data privacy [148].
- Silo: An application for federated learning, which allows organizations to cooperate in their efforts on machine learning without divulging any of the sensitive data that they might use in making machine learning applications and applications focusing on privacy and security for healthcare use [149].

Consequently, these platforms represent a significant advancement in the incorporation of federated learning within the healthcare industry, as they facilitate a collaborative framework that ensures the protection of sensitive medical information.

6.5 Challenges and Future Directions for Federated Learning in Medical Image Analysis

Today, federated learning of medical images faces several inherent challenges that affect its effectiveness and trustworthiness [11]. Another major issue is that the image data is not standardized across different healthcare facilities. This problem is caused by significant variations across imaging modalities, acquisition procedures, and patient demographics, leading to biases in model performance and generalizability. Thus, there is a strong need to develop powerful medical-use algorithms capable of learning in non-IID data.

Another serious problem with small datasets is that they are also affected by differences in data quality. Labeling data incorrectly or inconsistently may significantly affect a model's learning, especially in highly specialized areas of medicine, where annotation methods are often low-precision, and the importance of properly labeled data for effective model training is often overlooked [11].

Another critical aspect is the effectiveness of communication, as the frequency of data transfers between clients and the central server can slow work and consume significant bandwidth, especially in settings with limited resources. These problems can result in a situation where federated learning cannot be deployed due to computational and communication constraints. Clients may lack the required resources or a stable communication infrastructure to perform computationally intensive tasks or ensure smooth communication [11]. In addition, compatibility between image formats and systems, including Digital Imaging and Communications in Medicine (DICOM) [10] which is utilized to handle, store and transfer medical imaging data; Fast Healthcare Interoperability Resources (FHIR), a standard published by the Health Level Seven International (HL7), which is used to determine the structure and semantics of clinical documents; and Clinical Document Architecture (CDA), another HL7 standard defining the structure and semantics of clinical documents are also an interesting challenge to make [150]. There are additional data standards for imaging in hospitals, which make it difficult to integrate data across institutions. Such a separation may complicate the exchange and interpretation of medical images, thereby affecting the success of the models employed in federated learning. The effectiveness of medical-image-based federated learning programs will be determined by the efficiency of the participating institutions in transmitting data in a standardized format.

Inconsistency in privacy and security is a major threat to the integrity of the FL system in the face of poisoning attacks. Malicious entities can exploit vulnerabilities in FL systems to intrude on them and retrieve confidential patient information, or inject malicious updates to manipulate the model's integrity. To enable the successful implementation of federated learning in medical imaging, there is a strong need to address these challenges to ensure models are secure and accurate. Table 8 below provides an in-depth overview of the different defense mechanisms and methods intended to mitigate the challenges of the medical imaging field.

Table 8: Challenges, threats, and mitigation strategies in federated learning for medical imaging.

Challenge	Where It Occurs	Threat Type	Problem Description	Proposed Solution
Data Heterogeneity	Domain adaptation via feature alignment	Model Bias	Medical imaging datasets from different institutions vary in quality, resolution, and demographic/geographical distributions, leading to biased global models.	Normalization techniques (e.g., federated batch normalization)
Privacy Concerns	Secure aggregation protocols	Model Inversion Attacks	Gradients or model updates may inadvertently reveal sensitive patient data, allowing adversaries to reconstruct training samples.	Differential privacy with noise injection
Communication Overhead	Model update compression techniques	Data Leakage	Frequent transmission of model parameters increases the risk of eavesdropping, man-in-the-middle (MitM) attacks, and metadata leakage.	Hybrid encryption (homomorphic encryption + TLS)
Limited Local Data	Federated anomaly detection frameworks	Data Poisoning	Clients with small local datasets are highly susceptible to poisoning attacks, where malicious samples disproportionately affect global model convergence.	Byzantine-robust aggregation (e.g., Krum, Trimmed Mean)
Non-IID Data	Personalized model heads with shared feature extractors	Adversarial Attacks	Skewed distributions of labels and features across clients increase vulnerability to adversarial perturbations, degrading model performance.	Federated adversarial training
Scalability Limitations	Proof-of-work and reputation-based scoring	Sybil Attacks	Decentralized client participation allows adversaries to create multiple fake identities, injecting malicious updates to degrade model performance.	Blockchain-based identity management
Resource Constraints	Adaptive client selection based on resource availability	Model Degradation	Edge devices with limited computational resources struggle to train high-quality local models, negatively impacting the global model.	Lightweight architectures(e.g., MobileNet for medical imaging)

Future research in federated learning tailored for medical image analysis should concentrate on developing advanced algorithms that effectively address data heterogeneity and improve generalization across diverse datasets. Enhancing privacy measures with differential privacy and secure multi-party computation is crucial to minimizing data leakage and countering adversarial attacks. Consistent data formats, standardized labeling policies, and uniform communication protocols would facilitate interoperability among healthcare institutions, promoting broader adoption of FL. The successful integration of FL models into clinical workflows is essential to ensure that they are not only accurate but also practical for real-world medical applications. Employing FL in continuous learning systems and long-duration studies could lead to more adaptable models, offering valuable insights into disease progression and treatment efficacy. Addressing these vital areas would significantly advance medical image analysis through FL, thereby enhancing patient outcomes and transforming healthcare technology.

7 Conclusion

This systematic review provides a comprehensive and structured analysis of privacy and security challenges in federated learning (FL) for medical image analysis, based on 152 PRISMA-curated studies. Beyond summarizing existing work, the review introduces a unified analytical perspective linking FL system components, threat models, and defense mechanisms, enabling a clearer understanding of their interdependencies and trade-offs. Our findings show that, although FL offers a promising paradigm for privacy-preserving collaborative learning, its effectiveness remains constrained by key challenges such as data heterogeneity, vulnerability to adversarial attacks (including poisoning, inference, and Byzantine threats), and the inherent trade-offs between model accuracy, privacy guarantees, and computational efficiency. In particular, no single defense mechanism provides a complete solution, and combining techniques such as differential privacy, secure aggregation, and encryption often introduces additional computational and communication overhead. From a comparative perspective, current research can be broadly categorized into mature solutions (e.g., secure aggregation and basic differential privacy), partially explored approaches (e.g., hybrid privacy-preserving frameworks and personalization strategies), and open challenges, especially in scalable deployment, standardized evaluation, and robustness under real-world clinical conditions. Therefore, future research should focus on developing unified and adaptive frameworks that jointly optimize privacy, utility, and efficiency, as well as on establishing standardized benchmarking protocols and improving resilience against adaptive adversaries. Moreover, addressing system-level constraints such as communication cost, energy efficiency, and integration with clinical infrastructures is essential for real-world adoption. Ultimately, bridging the gap between theoretical advances and practical healthcare applications will be critical to achieving trustworthy, scalable, and clinically viable federated learning systems capable of delivering meaningful improvements in medical image analysis.

Acknowledgement: The Article Processing Charge (APC) for this publication was funded by SRM University-AP, Andhra Pradesh.

Funding Statement: The Article Processing Charge (APC) for this publication was funded by SRM University-AP, Andhra Pradesh.

Author Contributions: The authors confirm contribution to the paper as follows: study conception and design: Malika Abid, Mohammed Kamel Benkaddour and Aditya Kumar Sahu; data collection: Malika Abid and Amine Khaldi; analysis and interpretation of results: Malika Abid, Mohammed Kamel Benkaddour, Mohamed Benouis, Monalisa Sahu and Aditya Kumar Sahu; draft manuscript preparation: Malika Abid, Monalisa Sahu and Mohamed Benouis. All authors reviewed and approved the final version of the manuscript.

Availability of Data and Materials: Not applicable.

Ethics Approval: Not applicable.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Faiyazuddin M, Rahman SJQ, Anand G, Siddiqui RK, Mehta R, Khatib MN, et al. The impact of artificial intelligence on healthcare: a comprehensive review of advancements in diagnostics, treatment, and operational efficiency. *Health Sci Rep.* 2025;8(1):e70312. doi:10.1002/hsr2.70312.
2. Phang K, Kaabi J. Privacy in flux: a 35-year systematic review of legal evolution, effectiveness, and global challenges (US/EU focus with international comparisons). *J Cybersecur Privacy.* 2025;5(4):103.
3. McMahan B, Moore E, Ramage D, Hampson S, y Arcas BA. Communication-efficient learning of deep networks from decentralized data. In: Singh A, Zhu J, editors. *Proceedings of the 20th International Conference on Artificial Intelligence and Statistics.* Vol. 54. London, UK: PMLR; 2017. p. 1273–82.

4. Yang Q, Liu Y, Cheng Y, Kang Y, Chen T, Yu H. Federated learning. Berlin, Germany: Springer; 2022.
5. Li M, Jiang Y, Zhang Y, Zhu H. Medical image analysis using deep learning algorithms. *Front Public Health*. 2023;11:1273253. doi:10.3389/fpubh.2023.1273253.
6. Ali M, Naeem F, Tariq M, Kaddoum G. Federated learning for privacy preservation in smart healthcare systems: a comprehensive survey. *IEEE J Biomed Health Inform*. 2022;27(2):778–89. doi:10.1109/jbhi.2022.3181823.
7. Coelho KK, Nogueira M, Vieira AB, Silva EF, Nacif JAM. A survey on federated learning for security and privacy in healthcare applications. *Comput Commun*. 2023;207(1):113–27. doi:10.1016/j.comcom.2023.05.012.
8. Bashir AK, Victor N, Bhattacharya S, Huynh-The T, Chengoden R, Yenduri G, et al. Federated learning for the healthcare metaverse: concepts, applications, challenges, and future directions. *IEEE Internet Things J*. 2023;10(24):21873–91.
9. Reddy KD, Reddy T, Reddy TG. A comprehensive survey on federated learning techniques for healthcare informatics. *Comput Intell Neurosci*. 2023;2023(1):8393990. doi:10.1155/2023/8393990.
10. Guan H, Yap PT, Bozoki A, Liu M. Federated learning for medical image analysis: a survey. *Pattern Recognit*. 2024;151(3):110424. doi:10.1016/j.patcog.2024.110424.
11. Albshaier L, Almarri S, Albuali A. Federated learning for cloud and edge security: a systematic review of challenges and AI opportunities. *Electronics*. 2025;14(5):1019.
12. Mir BA, Abbas SR, Lee SW. Federated learning in healthcare ethics: a systematic review of privacy-preserving and equitable medical AI. *Healthcare*. 2026;14(3):306.
13. Mahmood H, Alamgir Z, Javed ST, Karim S, Awais M. Federated generative models in medical imaging: current advances, challenges, and future directions. *IEEE Access*. 2026;14:5197–217.
14. Ghosh D, Mehjabin M, Rayed ME, Mridha M, Kabir MM. Advancements and challenges of federated learning in medical imaging: a systematic literature review. *Artif Intell Rev*. 2026;59(2):87. doi:10.1007/s10462-025-11489-z.
15. Moshawrab M, Adda M, Bouzouane A, Ibrahim H, Raad A. Securing federated learning: approaches, mechanisms and opportunities. *Electronics*. 2024;13(18):3675.
16. Malik H, Anees T. Federated learning with deep convolutional neural networks for the detection of multiple chest diseases using chest X-rays. *Multimed Tools Appl*. 2024;83(23):63017–45. doi:10.1007/s11042-023-18065-z.
17. Cao K, Zhang Y, Zhao Y, Zhang J, Chen H. A multicenter bladder cancer MRI dataset and baseline evaluation of federated learning in clinical application. *Sci Data*. 2024;11(1):1147. doi:10.1038/s41597-024-03971-0.
18. Rieke N, Hancox J, Li W, Milletari F, Roth HR, Albarqouni S, et al. The future of digital health with federated learning. *npj Digital Med*. 2020;3(1):119. doi:10.1038/s41746-020-00323-1.
19. Fareed S, Yi D, Hussain B, Uddin S, Arif A, Tajoor AN. FedSegNet: a federated learning framework for 3D medical image segmentation. *Int J Ethical AI Appl*. 2025;1(2):30–46.
20. Shahzad A, Chen W, Zhang Y, Kumar R. Zero-trust medical image sharing: a secure and decentralized approach using blockchain and the IPFS. *Symmetry*. 2025;17(4):551.
21. Huang C, Huang J, Liu X. Cross-silo federated learning: challenges and opportunities. *arXiv:2206.12949*. 2022.
22. Bajwa MN, Muta K, Malik MI, Siddiqui SA, Braun SA, Homey B, et al. Computer-aided diagnosis of skin diseases using deep neural networks. *Appl Sci*. 2020;10(7):2488. doi:10.3390/app10072488.
23. Arbaoui M, Brahmia M, Rahmoun A, Zghal M. Federated learning survey: a multi-level taxonomy of aggregation techniques, experimental insights, and future frontiers. *ACM Trans Intell Syst Technol*. 2024;15(6):113.
24. Ye M, Fang X, Du B, Yuen PC, Tao D. Heterogeneous federated learning: state-of-the-art and research challenges. *ACM Comput Surv*. 2023;56(3):79.
25. Al-Saleh A, Tejani GG, Mishra S, Sharma SK, Mousavirad SJ. A federated learning-based privacy-preserving framework for brain tumor detection from CT scans. *Sci Rep*. 2025;15(1):12345. doi:10.1038/s41598-025-07807-8.
26. Zhu H, Xu J, Liu S, Jin Y. Federated learning on non-IID data: a survey. *Neurocomputing*. 2021;465:371–90. doi:10.1016/j.neucom.2021.07.098.
27. Rauber TW, Braun T, Berns K. Probabilistic distance measures of the Dirichlet and Beta distributions. *Pattern Recognit*. 2008;41(2):637–45. doi:10.1016/j.patcog.2007.06.023.
28. Liu B, Lv N, Guo Y, Li Y. Recent advances on federated learning: a systematic survey. *Neurocomputing*. 2024;597(4):128019. doi:10.1016/j.neucom.2024.128019.

29. Pillutla K, Kakade SM, Harchaoui Z. Robust aggregation for federated learning. *IEEE Trans Signal Process.* 2022;70:1142–54. doi:10.1109/tsp.2022.3153135.
30. Li X, Huang K, Yang W, Wang S, Zhang Z. On the convergence of FedAvg on Non-IID data. *arXiv:1907.02189.* 2020.
31. Li H, Richtárik P. On the convergence of FedProx with extrapolation and inexact prox. *arXiv:2410.01410.* 2024.
32. Ho TT, Tran KD, Huang Y. FedSGDCOVID: federated SGD COVID-19 detection under local differential privacy using chest X-ray images and symptom information. *Sensors.* 2022;22(10):3728.
33. Riedel P, von Schwerin R, Schaudt D, Hafner A, Späte C. ResNetFed: federated deep learning architecture for privacy-preserving pneumonia detection from COVID-19 chest radiographs. *J Healthc Inform Res.* 2023;7(2):203–24. doi:10.1007/s41666-023-00132-7.
34. Jin R, Li X. Backdoor attack is a devil in federated GAN-based medical image synthesis. In: *International Workshop on Simulation and Synthesis in Medical Imaging.* Cham, Switzerland: Springer; 2022. p. 154–65.
35. Dong N, Voiculescu I. Federated contrastive learning for decentralized unlabeled medical images. *arXiv:2109.07504.* 2021.
36. Liu Z, Wu F, Wang Y, Yang M, Pan X. FedCL: Federated contrastive learning for multi-center medical image classification. *Pattern Recognit.* 2023;143(1):109739. doi:10.1016/j.patcog.2023.109739.
37. Khowaja A, Dev S, Anwar MA, Linguraru M. SelfFed: self-supervised federated learning for data heterogeneity and label scarcity in medical images. *Expert Syst Appl.* 2025;261(9):125493. doi:10.1016/j.eswa.2024.125493.
38. Wu H, Zhang B, Chen C, Qin J. Federated semi-supervised medical image segmentation via prototype-based pseudo-labeling and contrastive learning. *IEEE Trans Med Imag.* 2024;43(2):649–61. doi:10.1109/TMI.2023.3314430.
39. Qi P, Chiaro D, Guzzo A, Ianni M, Fortino G, Piccialli F. Model aggregation techniques in federated learning: a comprehensive survey. *Future Gener Comput Syst.* 2024;150(6245):272–93. doi:10.1016/j.future.2023.09.008.
40. Moshawrab M, Adda M, Bouzouane A, Ibrahim H, Raad A. Reviewing federated learning aggregation algorithms: strategies, contributions, limitations and future perspectives. *Electronics.* 2023;12(10):2287.
41. Vucinich S, Zhu Q. The current state and challenges of fairness in federated learning. *IEEE Access.* 2023;11:80903–14. doi:10.1109/access.2023.3295412.
42. Li J, Chen T, Teng S. A comprehensive survey on client selection strategies in federated learning. *Comput Netw.* 2024;251(6):110663. doi:10.1016/j.comnet.2024.110663.
43. Sabah F, Chen Y, Yang Z, Azam M, Ahmad N, Sarwar R. Model optimization techniques in personalized federated learning: a survey. *Expert Syst Appl.* 2024;243(10):122874. doi:10.1016/j.eswa.2023.122874.
44. Guo P, Yang Y, Guo W, Shen Y. A fair contribution measurement scheme for federated learning with non-IID data. *Sensors.* 2024;24(15):4967. doi:10.20944/preprints202406.0127.v1.
45. Khan M, Glavin FG, Nickles M. Federated learning as a privacy solution—an overview. *Procedia Comput Sci.* 2023;217:316–25. doi:10.1016/j.procs.2022.12.227.
46. Liu P, Xu X, Wang W. Threats, attacks and defenses to federated learning: issues, taxonomy and perspectives. *Cybersecurity.* 2022;5(1):4. doi:10.1186/s42400-021-00105-6.
47. Lyu L, Yu H, Yang Q. Threats to federated learning: a survey. *arXiv:2003.02133.* 2020.
48. Li Y, Guo Z, Yang N, Chen H, Yuan D, Ding W. Threats and defenses in federated learning life cycle: a comprehensive survey and challenges. *arXiv:2407.06754.* 2024.
49. Yaacoub JPA, Noura HN, Salman O. Security of federated learning with IoT systems: issues, limitations, challenges, and solutions. *Internet Things Cyber-Phys Syst.* 2023;3:155–79.
50. Li Z, Sharma V, Mohanty SP. Preserving data privacy via federated learning: challenges and solutions. *IEEE Consum Electron Magaz.* 2020;9(3):8–16. doi:10.1109/mce.2019.2959108.
51. Guan H, Liu M. Domain adaptation for medical image analysis: a survey. *IEEE Trans Biomed Eng.* 2022;69(3):1173–85. doi:10.1109/tbme.2021.3117407.
52. Cassidy B, Kendrick C, Brodzicki A, Jaworek-Korjakowska J, Yap MH. Analysis of the ISIC image datasets: usage, benchmarks and recommendations. *Med Image Anal.* 2022;75(4):102305. doi:10.1016/j.media.2021.102305.
53. Ghaffari M, Sowmya A, Oliver R. Automated brain tumor segmentation using multimodal brain scans: a survey based on models submitted to the BraTS 2012–2018 challenges. *IEEE Rev Biomed Eng.* 2020;13:156–68.

54. Tomczak K, Czerwińska P, Wiznerowicz M. Review the cancer genome atlas (TCGA): an immeasurable source of knowledge. *Contemporary Oncol/Współczesna Onkologia*. 2015;2015(1):68–77. doi:10.5114/wo.2014.47136.
55. Habchi Y, Himeur Y, Kheddar H, Boukabou A, Atalla S, Chouchane A, et al. AI in thyroid cancer diagnosis: techniques, trends, and future directions. *Systems*. 2023;11(10):519.
56. Agarap AFM. On breast cancer detection: an application of machine learning algorithms on the Wisconsin diagnostic dataset. In: *Proceedings of the 2nd International Conference on Machine Learning and Soft Computing*. New York, NY, USA: ACM; 2018. p. 5–9.
57. Jacobs C, van Rikxoort EM, Murphy K, Prokop M, Schaefer-Prokop CM, van Ginneken B. Computer-aided detection of pulmonary nodules: a comparative study using the public LIDC/IDRI database. *Eur Radiol*. 2016;26(7):2139–47. doi:10.1007/s00330-015-4030-7.
58. Pande SD, Agarwal R. Multi-class kidney abnormalities detecting novel system through computed tomography. *IEEE Access*. 2024;12(21):21147–55. doi:10.1109/access.2024.3351181.
59. Gharaibeh M, Alzu'bi D, Abdullah M, Hmeidi I, Nasar MRA, Abualigah L, et al. Radiology imaging scans for early diagnosis of kidney tumors: a review of data analytics-based machine learning and deep learning approaches. *Big Data Cogn Comput*. 2022;6(1):29.
60. Shaban M, Awan R, Fraz MM, Azam A, Tsang YW, Snead D, et al. Context-aware convolutional neural network for grading of colorectal cancer histology images. *IEEE Trans Med Imag*. 2020;39(7):2395–405. doi:10.1109/tmi.2020.2971006.
61. Borkowski AA, Bui MM, Thomas LB, Wilson CP, DeLand LA, Mastorides SM. Lung and colon cancer histopathological image dataset (LC25000). *arXiv:1912.12142*. 2019.
62. Ayyad SM, Shehata M, Shalaby A, El-Ghar MA, Ghazal M, El-Melegy M, et al. Role of AI and histopathological images in detecting prostate cancer: a survey. *Sensors*. 2021;21(8):2586. doi:10.3390/s21082586.
63. Kong F, Wang X, Xiang J, Yang S, Wang X, Yue M, et al. Federated attention consistent learning models for prostate cancer diagnosis and Gleason grading. *Comput Struct Biotechnol J*. 2024;23:1439–49. doi:10.1016/j.csbj.2024.03.028.
64. Afshar P, Heidarian S, Enshaei N, Naderkhani F, Rafiee MJ, Oikonomou A, et al. COVID-CT-MD, COVID-19 computed tomography scan dataset applicable in machine learning and deep learning. *Sci Data*. 2021;8(1):121. doi:10.1038/s41597-021-00900-3.
65. Mu X, Shen Y, Cheng K, Geng X, Fu J, Zhang T, et al. FedProc: prototypical contrastive federated learning on non-IID data. *Fut Gener Comput Syst*. 2023;143:93–104.
66. Upreti D, Yang E, Kim H, Seo C. A comprehensive survey on federated learning in the healthcare area: concept and applications. *Comput Model Eng Sci*. 2024;140(3):2239–74. doi:10.32604/cmesci.2024.048932.
67. Chen X, Wang X, Zhang K, Fung KM, Thai TC, Moore K, et al. Recent advances and clinical applications of deep learning in medical image analysis. *Med Image Anal*. 2022;79:102444. doi:10.1016/j.media.2022.102444.
68. Deng Z, Yang Y, Suzuki K. Federated active learning framework for efficient annotation strategy in skin-lesion classification. *J Investig Dermatol*. 2025;145(2):303–11. doi:10.1016/j.jid.2024.05.023.
69. Usharani C, Selvapandian A. FedLRes: enhancing lung cancer detection using federated learning with convolution neural network (ResNet50). *Neural Comput Appl*. 2025;37:8273–84.
70. Meda A, Nelson L, Jagdish M. DKCN-Net: deep kronecker convolutional neural network-based lung disease detection with federated learning. *Comput Biol Chem*. 2025;116:108376.
71. Alhafiz M, Basuhail A. The data heterogeneity issue regarding COVID-19 lung imaging in federated learning: an experimental study. *Big Data Cogn Comput*. 2025;9(1):11. doi:10.3390/bdcc9010011.
72. Noman AA, Rahaman M, Pranto TH, Rahman RM. Blockchain for medical collaboration: a federated learning-based approach for multi-class respiratory disease classification. *Healthc Anal*. 2023;3:100135.
73. Liu C, Luo Y, Xu Y, Du B. Foundation models matter: federated learning for multi-center tuberculosis diagnosis via adaptive regularization and model-contrastive learning. *World Wide Web*. 2024;27(3):30. doi:10.1007/s11280-024-01266-3.
74. Rana N, Marwaha H. Pneumonia detection from X-ray images using federated learning—an unsupervised learning approach. *Measur Sensors*. 2025;37(4):101410. doi:10.1016/j.measen.2024.101410.

75. Onaizah AN, Xia Y, Hussain K. FL-SiCNN: an improved brain tumor diagnosis using siamese convolutional neural network in a peer-to-peer federated learning approach. *Alexandria Eng J.* 2025;114:1–11.
76. Monisha SMA, Rahman R. Brain tumor detection in MRI based on federated learning with YOLOv11. *arXiv:2503.04087.* 2025.
77. Sivakumar N, Khan AR, Umar S, Ravikumar RN, Bremnavas I, Lunagaria M, et al. A hybrid brain tumor classification using FL with FedAvg and FedProx for privacy and robustness across heterogeneous data sources. *IEEE Access.* 2025;13(2):57705–19. doi:10.1109/access.2025.3549440.
78. El Badaoui R, Bonmati E, Argyriou V, Villarini B. Federated learning using quality-based aggregation method for brain tumour segmentation on multimodality medical images. *Intell Syst Appl.* 2025;28(5):200601. doi:10.1016/j.iswa.2025.200601.
79. Roy A, Mahanta DR, Mahanta LB. A semi-synchronous federated learning framework with chaos-based encryption for enhanced security in medical image sharing. *Results Eng.* 2025;25(2):103886. doi:10.1016/j.rineng.2024.103886.
80. Xiang Z, Tian X, Liu Y, Chen M, Zhao C, Tang LN, et al. Federated learning via multi-attention guided UNet for thyroid nodule segmentation of ultrasound images. *Neural Netw.* 2025;181(12):106754. doi:10.1016/j.neunet.2024.106754.
81. Lee H, Chai YJ, Joo H, Lee K, Hwang JY, Kim S, et al. Federated learning for thyroid ultrasound image analysis to protect personal information: validation study in a real health care environment. *JMIR Med Inform.* 2021;9(5):e25869.
82. Chen C, Pan H, Zhang K, Li Z, Yu F. Prototype-based personalized federated learning for medical image classification. *Knowl Based Syst.* 2025;326(12):114021. doi:10.1016/j.knosys.2025.114021.
83. AlSalman H, Al-Rakhami MS, Alfakih T, Hassan MM. Federated learning approach for breast cancer detection based on DCNN. *IEEE Access.* 2024;12:40114–38. doi:10.1109/access.2024.3490012.
84. Li L, Xie N, Yuan S. A federated learning framework for breast cancer histopathological image classification. *Electronics.* 2022;11(22):3767. doi:10.3390/electronics11223767.
85. Amritanjali A, Gupta R. Federated learning for privacy preserving intelligent healthcare application to breast cancer detection. In: *Proceedings of the 26th International Conference on Distributed Computing and Networking.* New York, NY, USA: ACM; 2025. p. 302–6.
86. Karthiga B, Praneeth K, Saravanan V, Rao TRK. Enhancing cancer detection in medical imaging through federated learning and explainable artificial intelligence: a hybrid approach for optimized diagnostics. *Egypt Inform J.* 2025;31(19):100751. doi:10.1016/j.eij.2025.100751.
87. Liang W, Zhang W, Yan H, Zong Y, Yan C. DP-FViT: differentially private federated vision transformer with LoRA for secure and accurate medical image classification. *Biomed Signal Process Control.* 2026;114:109388.
88. Mohammed MA, Lakhan A, Abdulkareem KH, Deveci M, Dutta AK, Memon S, et al. Federated-reinforcement learning-assisted IoT consumers system for kidney disease images. *IEEE Trans Consum Electron.* 2024;70(4):7163–73. doi:10.1109/tce.2024.3384455.
89. Vekaria V, Gandhi R, Chavarkar B, Shah H, Bhadane C. Identification of kidney disorders in decentralized healthcare systems through federated transfer learning. *Procedia Comput Sci.* 2024;233:998–1010.
90. Liu X, Sun H, Sun N, Jia B, Xiao D. DPSHE: a privacy-preserving federated learning scheme based on homomorphic encryption and differential privacy for medical image. *Neurocomputing.* 2025;661:131931.
91. Ren Y, Li Y, Sun J, Chen H, Ma X, Ren B. FedCA: federated domain generalization for medical image segmentation via cross-client feature style transfer and adaptive style alignment. *Expert Syst Appl.* 2026;311:131394.
92. Hossain MM, Islam MR, Ahamed MF, Ahsan M, Haider J. A collaborative federated learning framework for lung and colon cancer classifications. *Technologies.* 2024;12(9):151. doi:10.3390/technologies12090151.
93. Kuang J, Bian X, Feng S, Pei S, Liu Z, Lan R, et al. Federated semi-supervised medical image segmentation with temporal fluctuation aggregation and pseudo-label relation mining. *Pattern Recognit.* 2026;177(1):113338. doi:10.1016/j.patcog.2026.113338.

94. Zhao Z, Pang S, Wang L, Qiao S, Zhao Y, Wang S, et al. MedFedProto: a semi-supervised classification framework for medical images based on federated prototypical learning. *Exp Syst Appl*. 2025;300(1):130332. doi:10.1016/j.eswa.2025.130332.
95. Niu K, Cai J, Feng X. SAFedHDM: semi-asynchronous federated learning with highlight diffusion model for medical image segmentation. *Inf Fusion*. 2025;126(Pt B):103615.
96. Tolpegin V, Truex S, Gursoy ME, Liu L. Data poisoning attacks against federated learning systems. In: *Computer Security—ESORICS 2020*. Cham, Switzerland: Springer; 2020. p. 480–501.
97. Gu K, Zhao W, Tan J, Yang Z, Li X, Jia W. Two-dimensional privacy-preserving federated learning scheme against poisoning attacks. *IEEE Trans Depend Secure Comput*. 2026;23(3):5509–25. doi:10.1109/tdsc.2026.3656703.
98. Zhou X, Xu M, Wu Y, Zheng N. Deep model poisoning attack on federated learning. *Fut Internet*. 2021;13(3):73. doi:10.3390/fi13030073.
99. Guo H, Wang H, Song T, Zheng T, Hua Y, Guan H, et al. Poisoning with a pill: circumventing detection in federated learning. In: *Proceedings of the AAAI Conference on Artificial Intelligence*. Palo Alto, CA, USA: AAAI; 2026, 40, 21432–40.
100. Shi J, Wan W, Hu S, Lu J, Zhang LY. Challenges and approaches for mitigating byzantine attacks in federated learning. In: *2022 IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*. Piscataway, NJ, USA: IEEE; 2022. p. 139–46.
101. Dong Q, Dai Z, Gao Y, Zheng Y, Fu A, Susilo W. FORCE: byzantine-resilient decentralized federated learning via game-theoretic contribution aggregation. *IEEE Trans Inf Forensics Secur*. 2026;21:3182–96.
102. Mohil M, Mohil A, Mohil AS. Federated learning for enhancing reliability and security in medical image analysis against adversarial threats. *ITEGAM-JETIA*. 2026;12(57):1045–53. doi:10.5935/jetia.v12i57.3209.
103. Hu H, Salcic Z, Sun L, Dobbie G, Zhang X. Source inference attacks in federated learning. In: *2021 IEEE International Conference on Data Mining (ICDM)*. Piscataway, NJ, USA: IEEE; 2021. p. 1102–7.
104. Rao B, Zhang J, Wu D, Zhu C, Sun X, Chen B. Privacy inference attack and defense in centralized and federated learning: a comprehensive survey. *IEEE Trans Artif Intell*. 2025;6(2):333–53. doi:10.1109/tai.2024.3363670.
105. Shi Q, Ren L, He X. Enhancing black-box membership inference attacks in federated learning. *J Inf Secur Appl*. 2026;96:104302. doi:10.1016/j.jisa.2025.104302.
106. Bai L, Hu H, Ye Q, Li H, Wang L, Xu J. Membership inference attacks and defenses in federated learning: a survey. *ACM Comput Surv*. 2024;57(4):89. doi:10.1145/3704633.
107. Huang Y, Gupta S, Song Z, Li K, Arora S. Evaluating gradient inversion attacks and defenses in federated learning. In: *Advances in Neural Information Processing Systems*. Red Hook, NY, USA: Curran Associates, Inc.; 2021. p. 7232–41.
108. Sotthiwat E, Zhang C, Xiao X, Zhen L. Safeguarding federated learning from data reconstruction attacks via gradient dropout. *IEEE Trans Inf Forensics Secur*. 2026;21(4):1874–88. doi:10.1109/tifs.2026.3659401.
109. Alkhunaizi N, Kamzolov D, Takáč M, Nandakumar K. Suppressing poisoning attacks on federated learning for medical imaging. In: *International Conference on Medical Image Computing and Computer-Assisted Intervention*. Cham, Switzerland: Springer; 2022. p. 673–83.
110. Kumar KN, Mohan CK, Cenkeramaddi LR, Awasthi N. Minimal data poisoning attack in federated learning for medical image classification: an attacker perspective. *Artif Intell Med*. 2025;159(1):103024. doi:10.1016/j.artmed.2024.103024.
111. Yu X, Zhou Y, Zheng P, Wang W, Liao S. A dual-reweighting defense strategy against data poisoning attacks in medical image classification models. *J Imag Inform Med*. 2026;15(6):3429. doi:10.1007/s10278-026-01886-3.
112. Moulahi W, Jdey I, Moulahi T, Alawida M, Alabdulatif A. A blockchain-based federated learning mechanism for privacy preservation of healthcare IoT data. *Comput Biol Med*. 2023;167(3):107630. doi:10.1016/j.compbiomed.2023.107630.
113. Mu J, Kadoch M, Yuan T, Lv W, Liu Q, Li B. Explainable federated medical image analysis through causal learning and blockchain. *IEEE J Biomed Health Inform*. 2024;28(6):3206–18. doi:10.1109/jbhi.2024.3375894.
114. Darzi E, Dubost F, Sijtsema NM, van Ooijen PMA. Exploring adversarial attacks in federated learning for medical imaging. *arXiv:2310.06227*. 2023.

115. Dao TN, Nguyen TP. Performance analysis of gradient inversion attack in federated learning with healthcare systems. *Rev J Electron Commun.* 2023;13(3–4):65–72. doi:10.21553/rev-jec.338.
116. Das BC, Amini MH, Wu Y. Privacy risks analysis and mitigation in federated learning for medical images. *arXiv:2311.06643.* 2024.
117. Grama M, Musat M, Muñoz-González L, Passerat-Palmbach J, Rueckert D, Alansary A. Robust aggregation for adaptive privacy preserving federated learning in healthcare. *arXiv:2009.08294.* 2020.
118. Shao Y, Li J, Shi L, Wei K, Ding M, Li Q, et al. Robust model aggregation for heterogeneous federated learning: analysis and optimizations. *IEEE Trans Emerg Topics Comput.* 2026;14(1):160–71. doi:10.1109/tetc.2025.3647650.
119. Lessage X, Collier L, Ouytsel CHBV, Legay A, Mahmoudi S, Massonet P. Secure federated learning applied to medical imaging with fully homomorphic encryption. In: 2024 IEEE 3rd International Conference on AI in Cybersecurity (ICAIC). Piscataway, NJ, USA: IEEE; 2024. p. 1–12.
120. Xie Q, Jiang S, Jiang L, Huang Y, Zhao Z, Khan S, et al. Efficiency optimization techniques in privacy-preserving federated learning with homomorphic encryption: a brief survey. *IEEE Internet Things J.* 2024;11(14):24569–80. doi:10.1109/jiot.2024.3382875.
121. Yanez P, Yadav N. Homomorphic encryption for secure healthcare artificial intelligence. *Discov Artif Intell.* 2026;6(1):200. doi:10.1007/s44163-026-00920-1.
122. Mohammadi M, Vejdanihemmat M, Lotfinia M, Rusu M, Truhn D, Maier A, et al. Differential privacy for medical deep learning: methods, tradeoffs, and deployment implications. *npj Digital Med.* 2026;9(1):93. doi:10.1038/s41746-025-02280-z.
123. Fu J, Hong Y, Ling X, Wang L, Ran X, Sun Z, et al. Differentially private federated learning: a systematic review. *arXiv:2405.08299.* 2024.
124. Ouadrhiri AE, Abdelhadi A. Differential privacy for deep and federated learning: a survey. *IEEE Access.* 2022;10(2):22359–80. doi:10.1109/access.2022.3151670.
125. Gupta M, Kumar M, Gupta Y. A blockchain-empowered federated learning-based framework for data privacy in lung disease detection system. *Comput Human Behav.* 2024;158:108302. doi:10.1016/j.chb.2024.108302.
126. Nguyen DC, Ding M, Pathirana PN, Seneviratne A, Zomaya AY. Federated learning for COVID-19 detection with generative adversarial networks in edge cloud computing. *IEEE Internet Things J.* 2022;9(12):10257–71. doi:10.1109/jiot.2021.3120998.
127. Qu Y, Uddin MP, Gan C, Xiang Y, Gao L, Yearwood J. Blockchain-enabled federated learning: a survey. *ACM Comput Surv.* 2022;55(4):70. doi:10.1145/3524104.
128. Zhang H, Jiang S, Xuan S. Decentralized federated learning based on blockchain: concepts, framework, and challenges. *Comput Commun.* 2024;216(1):140–50. doi:10.1016/j.comcom.2023.12.042.
129. Thapa C, Chamikara MAP, Camtepe SA. Advancements of federated learning towards privacy preservation: from federated learning to split learning. In: ur Rehman MH, Gaber MM, editors. *Federated Learning Systems: Towards Next-Generation AI.* Berlin, Germany: Springer; 2021. p. 79–109.
130. Lokesh GH, Hukkeri GS, Jhanjhi NZ, Lin H. Split federated learning for secure IoT applications. *Inst Eng Technol.* 2024 [cited 2026 Apr 20]. Available from: <https://digital-library.theiet.org/doi/abs/10.1049/PBSE025E>.
131. Zheng J, Chen Y, Lai Q. PPSFL: privacy-preserving split federated learning for heterogeneous data in edge-based Internet of Things. *Fut Gener Comput Syst.* 2024;156:231–41.
132. Shiranthika C, Hadizadeh H, Saeedi P, Bajić V. Adaptive asynchronous split federated learning for medical image segmentation. *IEEE Access.* 2024;12(1):182496–515. doi:10.1109/access.2024.3511430.
133. Zhang M, Qu L, Singh P, Kalpathy-Cramer J, Rubin DL. SplitAVG: a heterogeneity-aware federated deep learning method for medical imaging. *arXiv:2107.02375.* 2022.
134. Yang Z, Chen Y, Huangfu H, Ran M, Wang H, Li X, et al. Robust split federated learning for U-shaped medical image networks. *arXiv:2212.06378.* 2022.
135. Ku H, Susilo W, Zhang Y, Liu W, Zhang M. Privacy-preserving federated learning in medical diagnosis with homomorphic re-Encryption. *Comput Stand Interfaces.* 2022;80(2):103583. doi:10.1016/j.csi.2021.103583.

136. Zhang L, Xu J, Kumar PV, Sharma PK, Ghosh U. Homomorphic encryption-based privacy-preserving federated learning in IoT-enabled healthcare system. *IEEE Trans Netw Sci Eng.* 2023;10(5):2864–80. doi:10.1109/tNSE.2022.3185327.
137. Wibawa F, Catak FO, Sarp S, Kuzlu M, Cali U. Homomorphic encryption and federated learning based privacy-preserving CNN training: cCOVID-19 detection use-case. *arXiv:2204.07752.* 2022.
138. Dutil F, See A, Di Jorio L, Chandelier F. Application of homomorphic encryption in medical imaging. *arXiv:211007768.* 2021.
139. Lian Z, Yang Q, Wang W, Zeng Q, Alazab M, Zhao H, et al. DEEP-FEL: decentralized, efficient and privacy-enhanced federated edge learning for healthcare cyber physical systems. *IEEE Trans Netw Sci Eng.* 2022;9(5):3558–69.
140. Ahmed R, Maddikunta PKR, Gadekallu TR, Alshammari NK, Hendaoui FA. Efficient differential privacy enabled federated learning model for detecting COVID-19 disease using chest X-ray images. *Front Med.* 2024;11:1409314. doi:10.3389/fmed.2024.1409314.
141. Ziller A, Trask A, Lopardo A, Szymkow B, Wagner B, Bluemke E, et al. PySyft: a library for easy federated learning. In: ur Rehman MH, Gaber MM, editors. *Federated Learning Systems: Towards Next-Generation AI.* Cham, Switzerland: Springer; 2021. p. 111–39.
142. Foley P, Sheller MJ, Edwards B, Pati S, Riviera W, Sharma M, et al. OpenFL: the open federated learning library. *Phys Med Biol.* 2022;67(21):214001. doi:10.1088/1361-6560/ac97d9.
143. Ziller A, Passerat-Palmbach J, Ryffel T, Usynin D, Trask A, Junior IDLC, et al. Privacy-preserving medical image analysis. *arXiv:2012.06354.* 2020.
144. Cremonesi F, Vesin M, Cansiz S, Bouillard Y, Balelli I, Innocenti L, et al. Fed-BioMed: open, transparent and trusted federated learning for real-world healthcare applications. *arXiv:2304.12012.* 2023.
145. Patil R, Gupta D, Gururaj HL. Federated learning using TensorFlow. In: *Federated Learning Techniques and Its Application in the Healthcare Industry.* Singapore: World Scientific; 2024. p. 171–89.
146. Witt L, Heyer M, Toyoda K, Samek W, Li D. Decentral and incentivized federated learning frameworks: a systematic literature review. *IEEE Internet Things J.* 2022;10(4):3642–63.
147. Caldas S, Duddu SD, Wu P, Li T, Konečný J, McMahan HB, et al. Leaf: a benchmark for federated settings. *arXiv:1812.01097.* 2018.
148. Aledhari M, Razzak R, Parizi RM, Saeed F. Federated learning: a survey on enabling technologies, protocols, and applications. *IEEE Access.* 2020;8:140699–725.
149. Laforcade J. Casser les silos via un réseau de connaissances: une approche collaborative de l'expertise, avec la plateforme i2Kn de Meetsys. *I2D-Inf Donnees Doc.* 2023;60(1):95–8. doi:10.3917/i2d.231.0095.
150. Cremonesi F, Planat V, Kalokyri V, Kondylakis H, Sanavia T, Resinas VMM, et al. The need for multimodal health data modeling: a practical approach for a federated-learning healthcare platform. *J Biomed Inform.* 2023;141:104338.