Aridax International Journal of Research in Science & Technology
HJPARAM Publication | Open Access | Peer Reviewed

ISSN: XXXX-XXXX (Online)
Vol. 1, Issue 1 (Sep–Oct 2026), pp. 25–33
DOI: 10.XXXXX/hjparam.XXXX

REVIEW ARTICLE Received: 26 October 2026 | Revised: 08 November 2026 | Accepted: 12 November 2026 | Published: 18 November 2026

A Comprehensive Review on Privacy-Preserving Federated Learning Frameworks for Healthcare IoT Using Blockchain and Edge Intelligence

Mokshita Sharma[1,*], Nitesh Gupta[2] and Anurag Shrivastava[3]

[1] *Department of Computer Science, NRI Institute of Information Science & Technology ,Bhopal, M.P., India, mokshita1008@gmail.com*
[2] *Department of Computer Science, NRI Institute of Information Science & Technology ,Bhopal, M.P., India, 9.nitesh@gmail.com*
[3] *Research Scholar, Department of Computer Science, SAGE University, Bhopal, Madhya Pradesh, India, anurag.shri08@gmail.com, ORCID: 0000-0002-6252-6724*
*** Corresponding author:** *mokshita1008@gmail.com*

Abstract

The fast growth of the healthcare Internet of Things (IoT) solutions resulted in the generation of vast amounts of confidential medical data, with an equally growing concern regarding data protection and data use, amongst other factors. This review article will cover the most cutting-edge developments in federated learning (FL) frameworks for privacy-preserving blockchain integration and edge computing in healthcare. At a theoretical level, it became clear that the current centralized machine-learning methods are associated with the risks of data-privacy loss, regulatory impediments, and resource-constraint costs. In this situation, federated learning emerges as a very promising new paradigm capable of accommodating decentralized model training without raw data sharing, thereby further ensuring data privacy and security. In recent years, several contributions have been made combining secure characteristics for data privacy during training and aggregation and well-known techniques such as Fully Homomorphic Encryption (FHE), Secure Multi-Party Computation SMPC, and Differential Privacy (DP). Moreover, the paper also touches upon the possibilities of blockchain to create secure, transparent, and immutable updates to the models using methodologies like a Proof of Authority (PoA) and Delegated Proof of Stake (DPoS). Moreover, directing edge computing into the design could further enhance systems scalability and minimize latency within the healthcare domain. The text addresses the issues like non-IID data distribution, class imbalance, communication overhead, and convergence problems in the federated setting. Emerging methodologies such as cross-domain federated learning, multitask learning, and adaptive aggregation strategies were discussed to enhance the model's generalization and efficiency levels. The overall goal of the paper is to propose and develop a combination of federated learning together with blockchain and privacy-preserving technologies to enhance secure, scalable, and efficient health IoT systems.

Keywords: *Federated Learning, Healthcare IoT, Blockchain, Differential Privacy, Edge Computing, Secure Machine Learning*

1. Introduction

The rapid expansion of technology has immensely changed healthcare, with smart systems that greatly improve patient care, diagnosis, and care taking. IoT related to healthcare has lately received a lot of attention as it enables data collection from wearable products, sensors, and other smart medical devices. These systems produce incredible amounts of heterogeneous data streams, allowing healthcare practitioners to make data-informed decisions at the right time. Healthcare IoT has advanced patient access to effective and primary healthcare services in terms of efficiency and efficacy while considering additional difficulties of resource-limited circumstances-from remote patient monitoring services to medical accessibility for chronic patients. However, from the exponential growth of such personal sensitive data, it also gave rise to concerns of ethics and security with respect to the privacy of data [1]. Given that predictions and clinical decision support rely increasingly on artificial intelligence (AI) and machine learning (ML) models, patient information confidentiality has become a must. To safeguard the sensitive healthcare data from unauthorized access, breaches, and abuses while allowing for insights that can benefit a patient, privacy-preserving AI techniques are required. Techniques, such as encryption, anonymization, and differential privacy, are crucial to the data protection while they are stored, transmitted, or processed. In addition to that, the regulatory framework and ethical stand emphasize patient privacy as a necessary line in the design of intelligent systems that would, from the beginning, encompass security and trust [2].

Traditional centralized learning methods, in which data from various sources is pooled into a single data repository to train models, are not efficient in healthcare. Not only do these methods expose data to potential attacks when shared, data leakage, and ownership but also they get into regulatory and communication challenges. These centralized computing systems cannot handle easily,

© 2026 The Author(s). Published by HJPARAM Publication under CC BY 4.0

distributed, and heterogeneously the array of data inputs from multiple healthcare institutions and devices [3]. Therefore, the deployment of decentralized and privacy-aware learning is a pressing issue to such conditions. In this respect, we believe that emerging paradigms such as federated learning in combination with privacy-preserving mechanisms and distributed technologies offer a titillating way forward in terms of secure and efficient healthcare data analytics. The Figure 1 illustrates a privacy-preserving healthcare system where IoT devices collect data, federated learning enables decentralized model training, and blockchain ensures secure data sharing, authentication, and analytics.

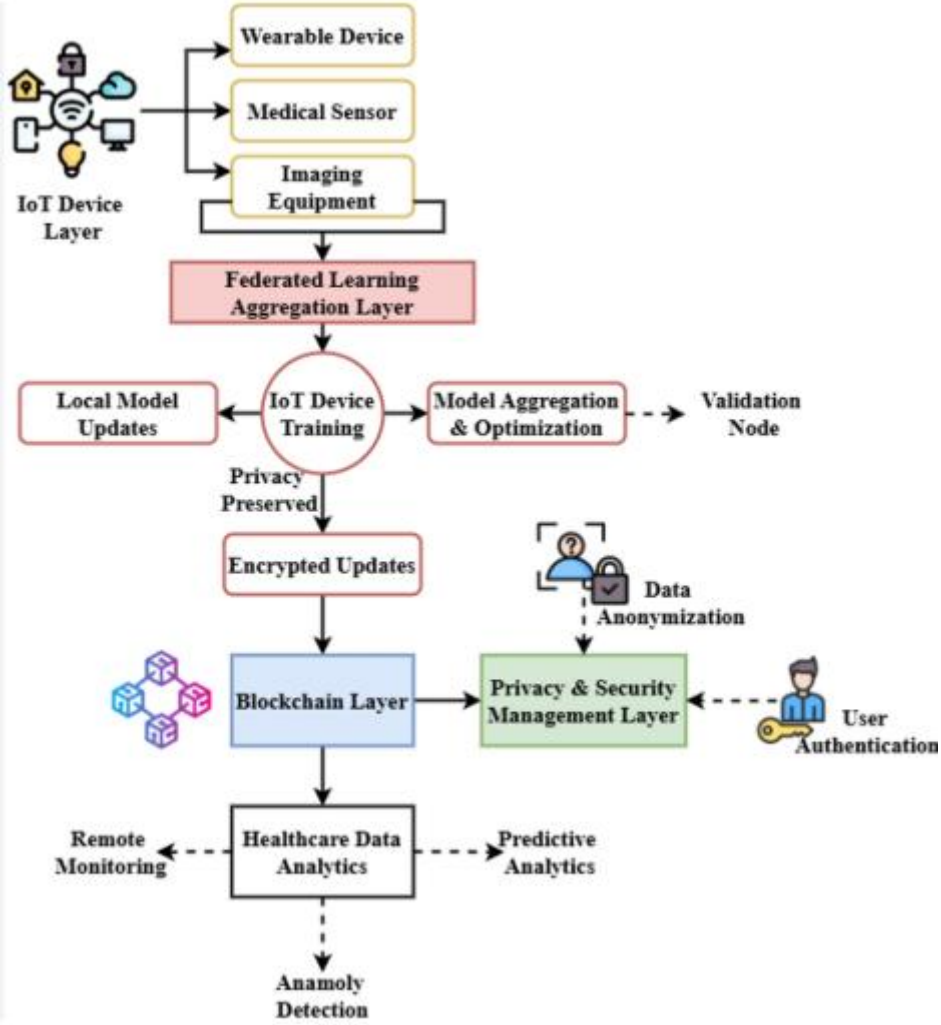

Figure 1. Federated Learning-Based Secure Healthcare Architecture Integrating IoT and Blockchain

2. Fundamentals of Federated Learning

Federated learning (FL) has been proposed as a distributed paradigm in machine learning that enables a multi-client network to train collaboratively on a shared global model, without sharing raw data such as from hospitals, IoT devices, or mobile devices. FL keeps the data on the client device but only transfers updates such as weight or gradient in regard to the model to the central aggregator server. By performing so, it secures privacy under the pretext of keeping financial intelligence centralized. In healthcare settings, FL needs to be strongly recommended wherever the requirements of confidentiality require regulatory support and safe collaboration of research across institutions [4].

Concept and Architecture: - Federated Learning is decentralized in its essence where a number of clients may stack up cooperation toward a global model while keeping their local client data safe. This architecture would consist mainly of three components, viz., client devices, a central server (or aggregator) and communication protocols. Many client devices would be in existence; they could include, for instance, hospitals or other medical systems, with and fitted with IoT capabilities. In this setup, they would store local datasets and develop models independently from each other; meanwhile, the central server would initialize a commonly known global model, then distribute it to the clients and aggregate the updates trained locally and provided by them [5]. The global model is initially sent from the server to all clients participating in a typification of the FL architecture. These clients train this global model on local data and alike, and in turn, obtain parameter updates. The updates acquire the status of transmission to the server without moving raw data. The server uses algorithms such as Federated Averaging (FedAvg) to accumulate these updates and derive a new

© 2026 The Author(s). Published by HJPARAM Publication under CC BY 4.0

global model [6]. This latter is propagated down to the clients for additional rounds of training, resulting in convergence theoretically.

Both synchronous and asynchronous communication are supported in the architecture, thereby facilitating the seamless handling of client groups with heterogeneous computational capabilities. Moreover, an advanced architecture can easily incorporate edge computing, blockchain, privacy-preserving, and data security for utilization in distribute healthcare systems.

Federated Learning Workflow: - Federated learning comes down then to an iterative, multi-round, and collaborative model, sharing training between the central server and certain clients with deep learning abilities. At initialization, the server serves each model, which was already greatly decentralized, to all clients together. These clients learn the parameters of their models by minimizing loss using local data. A model found on each client is trained by the corresponding client over its local dataset.

Once each client model has been fully trained, updates based on the global models are returned to the server, basically gradients or even model weights. None of these contain raw data, thus preserving client-privacy. Then the server aggregates into one those respective modifications via weighted averaging, where the weights may reflect the size or nature of the data each client brings in [7]. The aggregated modifications adjust the global model to all clients accordingly.

The new global model is sent back to the user, and the cycle is repeated several times until the model offers the best result before convergence. Future workflows could introduce tactics for selecting the best clients, secure aggregation, and approaches including differential privacy to enhance efficacy and security outcomes. The iterative nature of this process ensures that the model is continuously improving while also ensuring decentralized data handling suitable for domains like healthcare that are highly sensitive to data leakage. Table 1 presents the key advantages of Federated Learning in healthcare systems [8]. It highlights how Federated Learning ensures data privacy by keeping patient information localized, thereby minimizing the risk of data breaches. The approach supports regulatory compliance by avoiding direct data sharing across institutions. It enhances security by eliminating centralized data storage, which is often vulnerable to cyberattacks. The framework is highly scalable, enabling collaboration among multiple hospitals and IoT devices. It also supports real-time learning through continuous updates from distributed medical data sources. Additionally, communication overhead is reduced as only model parameters are exchanged instead of complete datasets [9]. Federated Learning enables personalization by adapting models to local patient data and improves robustness in handling heterogeneous and non-IID data. Furthermore, it reduces infrastructure costs and enhances overall prediction accuracy by leveraging knowledge from diverse data sources.

Table 1. Advantages in Healthcare Systems

Aspect	Advantages of Federated Learning in Healthcare
Data Privacy	Patient data remains local, reducing risk of breaches
Regulatory Compliance	Supports GDPR, HIPAA by avoiding data sharing
Security	Minimizes exposure of sensitive medical data
Scalability	Enables collaboration across multiple hospitals/devices
Real-Time Learning	Supports continuous model updates from IoT devices
Reduced Communication	Only model updates are shared, not full datasets
Personalization	Models adapt to local patient data patterns
Robustness	Handles heterogeneous and distributed data effectively
Cost Efficiency	Reduces need for centralized storage infrastructure
Improved Accuracy	Learns from diverse datasets without compromising privacy

3. Privacy-Preserving Techniques in FL

In Federated Learning, one of the foremost principles is safeguarding privacy; it ensures that sensitive data remains private even as distributed model training is being conducted. By using these techniques, we can be assured that private user information is never going to be leaked; plus, the cooperation of the federated learning processes is thereby enabled [10]. Key techniques that are also considered part of this are Fully Homomorphic Encryption, Secure Multiparty Computation, and Differential Privacy; these enhance the security, confidentiality, and general trust for how healthcare data analytics applications work.

Fully Homomorphic Encryption (FHE):- Fully Homomorphic Encryption (FHE) is an advanced cryptographic technique that allows computations to be directly performed on ciphertext without the need for decryption. This is important for federated learning, where FHE can guarantee that model updates created at the clients are still encrypted during transmission and aggregation, thereby not leaking sensitive information. This becomes idealized in scenarios such as healthcare systems being that data privacy remains core [11]. Operations such as addition and multiplication carried out on ciphertexts- this ensures data privacy while the very environment stays untrusted. Intense in terms of computational workload, FHE provides strong security guarantees and is now being increasingly optimized for

© 2026 The Author(s). Published by HJPARAM Publication under CC BY 4.0

practical deployment in some privacy-sensitive applications.

Secure Multiparty Computation (SMC):- Secure Multiparty Computation (SMC) is a cryptographic protocol that allows multiple parties or users to collaboratively perform a mathematical function on their independent inputs that they do not want revealed to one another. In federated learning, various clients send updates to be securely aggregated by the use of SMC so that no one client will have a full view of the data used. The method involves encoding data so that it can be divided to random encrypted shares and then scattered among the participants in such a way that the information from any one share alone will be unhelpful in accurately reconstructing the real data [12]. SMC increases trust in a very decentralized system, particularly in the area of healthcare, whereby these institutions could collaboratively train a model while painstakingly protecting the confidentiality and security of data of the patients.

Differential Privacy (DP):- Differential Privacy is a statistical technique that aims to protect individual data records when a controlled amount of noise is injected at data or model outputs. In the case of federated learning, the model update received by the central server is made private through differential privacy. With such a system in place, the probability of sensitive information about any individual being extrapolated is low. Privacy guarantee may be varied on the basis of a parameter called the privacy budget (ε), with a lower value denoting enhanced privacy. Differential Privacy also prevents inferences relative to attacks such as membership or attribute inference, making it the most suitable for any scenario in health research [13]. The utility derived from this mixture ensures personal data protection remain paramount even while working towards accurate training of a model.

4. Blockchain Integration in Federated Learning

The integration of blokchain technology and Federated Learning (FL) is proving to be excellent for adding security, transparency, and trust within decentralized healthcare settings. FL is capable of collaboratively learning from multiple datasets without transference, but it still retains a central pushing entity threatening until its security collapses. In fact, its contradictions, along with other reasons such as transparency and possible manipulation of model updates, made blockchain a more secure choice [14]. Blockchain provides a decentralized, tamper-proof ledger of all transactions and updates for the model. Its features combine to ensure that the integrated solution brings additional value to these systems with respect to highly trustworthy and accountable environments, particularly within healthcare-centered IoT settings with patient data being exposed to those peculiar values contextually for making critical decisions.

Enhancing security and data integrity are the fundamental roles of the technology in federated learning. Therefore, in the context of traditional FL systems, model updates are sent between clients and the central server; however, this may pose potential risks in terms of data poisoning, model tampering, or malicious access. In a layer of security, the use of blockchain allows secure recording of model updates as transactions on a distributed ledger to render it a guarantee that once information has been held by the ledger, it should not be conceivable to be altered or removed. In the case of any suspicious modification or meddling with model updates, it will be in the scope of immutability, thus mitigating an extent the importance of model updates [15]. The use of verification on the blockchain means different critical nodes verify transactions as they come before transactions are accepted, thus eliminating the possibility of data being changed or manipulated in any way. This is in addition to durability and trustworthiness on critical domains such as healthcare and toward the greater reliability and security-related advancements of federated learning.

Consensus protocols are crucial to sustaining integrity and managing efficiency in blockchain-enabled federated learning systems. These protocols ensure that all participating nodes agree on a transaction's validity and the state of the ledger. Among different consensus algorithms, PoA and DPoS proved highly efficient and beneficial for healthcare applications due to low computational overhead. PoA operates on a chain of trusted validators authorized to create and validate blocks, making it very efficient for private networks, like the ones of hospital consortia. Because validators are identifiable and accountable, PoA provides faster transaction processing, thereby reducing lag compared to traditional protocols. On the contrary, DPoS gives more democratic control, where stakeholders vote on the selection of delegates, which are capable of validating transactions and maintaining the blockchain [16]. This is the method that improved scalability and performance while maintaining the balance between efficacy and decentralization. DPoS reduces power consumption and speeds up consensus, which makes it excellent for real-time federated learning scenarios using large-scale healthcare IoT systems. The choice between PoA and DPoS depends on the application requirements, with PoA being more suitable for controlled environments and DPoS for semi-decentralized networks requiring more scalability.

Another vital aspect of blockchain integration in federated learning is the deployment of smart contracts for model aggregation and coordination. Smart contracts are self-enforcing programs that lay down the rules and requirements to follow and execute them on the blockchain with no need for intermediaries. In the federated learning context, these smart contracts may be used to oversee the entire training process-from client participation, through to validation of model updates, aggregation of parameter data, and release of rewards or incentives [17]. For example, during model-training stages, validation of the authenticity from locally trained models that clients uploaded is performed, and they are utilized with predefined algorithms for aggregation, such as weighted averaging. Such an automatic process assuring fairness and transparency will thus minimize human involvement and

© 2026 The Author(s). Published by HJPARAM Publication under CC BY 4.0

errors. In addition to that, smart contracts could work in an incentive mechanism to promote honest client interaction. The reward system could site them. Smart contracts make that trustworthy. They allow all parties to assess the process of learning to approve their model, ensuring integrity. Some challenges need to be addressed. The computational limits, the high gas cost, and the important security vulnerabilities when designing a smart contract can be well-bounded.

The integration of blockchain and true learning gives a safe, clear, and decentralized frame for the mutual training of models in the health sector [18]. By making the data integrity robust, enabling efficient consensus mechanisms, and automation through smart contracts, this model comprehensively deals with central challenges concerning, for instance, privacy, trust, and scalability in order to pave the way for truly intelligent new-generation health solutions. Table 2 presents a concise comparison of recent studies highlighting how AI, IoT, and Blockchain technologies are integrated to enhance healthcare system efficiency, data security, patient monitoring, and privacy protection.

Table 2. Summary of Review on AI, IoT, Blockchain, and Security Applications in Healthcare Systems

Ref	Focus	Method	Results	Limitations
[1]	Blockchain-based federated learning for healthcare IoT	Blockchain + Federated Learning	94%	High computational overhead; scalability issues
[2]	AI integration in healthcare	ML and DL for diagnostics & decision support	94%	Data privacy; limited standardization
[3]	Transformative AI in healthcare	AI tools for diagnosis & patient management	95%	Ethical concerns; integration challenges
[4]	Medical open databases influence	Analysis of open datasets for AI	92%	Privacy risks; data heterogeneity
[5]	Sociotechnical challenges of ML in healthcare	ML deployment in social welfare	90%	Lack of explainability; user resistance
[6]	Federated learning from research to real-world	Federated Learning in healthcare	94%	Communication overhead; data imbalance
[7]	Predictive analytics for patient outcomes	ML for disease prediction	94%	Data quality bias; low interpretability
[8]	ML algorithms in healthcare	Review of ML methods	92%	Scalability; legacy system integration
[9]	AI, DL, QML in healthcare	Hybrid AI and quantum ML	96%	High computational requirements; limited implementation
[10]	Early detection of chronic kidney disease	ML with lifestyle & demographic data	93%	Small dataset; generalization challenges
[11]	Parallel split learning in healthcare	Data distribution-aware clustering	94%	Parameter tuning; synchronization overhead
[12]	Interpretable ML for hospital efficiency	Explainable AI models	93%	Trade-off between complexity & interpretability
[13]	ML in cardiac arrest	Predictive ML models for early warning	92%	Reliance on high-quality real-time data
[14]	Optimization algorithms for ML	Genetic and swarm optimization	95%	Computational complexity; parameter tuning
[15]	Clinician perceptions of ML-CDSS	Survey + ML for oesophageal cancer	91%	Resistance from clinicians; workflow integration

5. Role of Edge Computing in Healthcare IoT

Edge computing enables Healthcare IoT systems to be more efficient and responsive by bringing computation to the data source. In traditional cloud architectures, data from medical sensors and wearable devices need to be transmitted to centralized servers for processing, causing delays, bandwidth consumption, and potential privacy issues. Edge computing simply bypasses these problems through on-site data processing at the IoT device-locally, such as a smart monitor, gateway, or hospital-edge server.

Edge computing is a hallmark validating local processing permissions that notably gravitates towards real-time decision facilitation in critical healthcare situations such as emergency monitoring, disease detection, real-time tracking of patient data. Simultaneously, this approach does pull up healthcare systems' dependency on internet connectivity, rendering the entire sector more reliable in remote or resource-bound environments [19]. Furthermore, edge computing ensures data privacy by not nudging highly sensitive patient information across networks. Although edge computing integrates well with highly modern technologies such as federated learning, the fusion of these advanced technologies facilitates local trainers to one of the most efficient and secure models, thereby promising accuracy and asset. To summarize, edge computing is the backbone for modern healthcare IoT, promising quicker processing, stronger security, and the scalability of deploying intelligent medical applications [20].

Edge-Based Model Training: - Edge model training involves machine learning training techniques directly

© 2026 The Author(s). Published by HJPARAM Publication under CC BY 4.0

performed on edge devices rather than using centralized cloud infrastructure. The definition in the health IoT system involves the functioning of edge devices which may include wearable sensory systems, mobile health applications, smart diagnostic equipment, or distant hospital servers. An advantageous way for securing sensitive medical data, it guarantees that patients' information remains local, while still helping to improve models. In this, each edge device independently trains a model from its own dataset, capturing the local pattern or characteristics of the local environment or patient population [21]. Trained locally, these models can be translated into a global model with federated learning, wherein only the model parameters have been shared, instead of the raw data. Thereby reducing the privacy risk, it also complies with stringent healthcare regulations.

An edge-forgetted model strategy also allows personalization, as now the model data starts to fit in as per the various patient conditions to yield highly accurate, context-aware estimates. For example, smart wearables monitoring heart rate can learn very specific personal patterns for a patient to enhance early detection of irregularities. When the computation is amplified subject to several edge nodes, the overall system allows better efficiency, reducing farther reliance on the central resources. The trials are also there on the path where tiny computational power and energy limitations and inconstant devices need to be wiped out. Various techniques associated with model compression, lightweight architectures, and efficient optimization algorithms are often exercised to handle these restrictions. However, with all of these melons hanging out on the plate, edge-based model training is a strong requirement for a secure, efficient, and personalized view of healthcare analytics in distributed environments.

Latency and Scalability Improvements: - Edge computing in health IoT embeds simplicity in the applications too. By taking advantages of edge resources and reacting immediately thus bringing the analytics closer to the data source, failure or queuing issues are not hindrances. This taps into low-latency broadband internet or some kind of local access. Compounded with an extra layer of consideration, with hardware-supporting security, it is helpful for not just monitoring but also enabling decisions quickly [22]. Quite frankly, edge computing is the optimal compromise for scalability and speed on the uninterrupted delivery of health services. In light of certain applications, such as remote patient surveys, it is critical that response times be fast enough to prevent terminal outcomes. For instance, at the moment an edge device senses any abnormal vital signs, it can issue an alert without consultation with some cloud service as originally intended. By maintaining such a responsive pace, the patients' safety and quality-coverage issues are addressed.

Edge computing scales up a healthcare system to a level far beyond the latency reduction it offers. Brought on by an apparatus of various devices and sensors, it would be quite challenging for their centralized systems to provide for such data volumes. Edge computing thus hosts computations on individual devices and nodes, thus preventing insufficiency and optimizing system functioning. The reduction in network bandwidth usage further helps in enhancing scalability as only essential data or processed results need to be transmitted to the cloud. This makes the system highly efficient and cost effective, particularly in large-scale deployments like smart hospitals or national healthcare networks. Overall, edge computing supports healthcare IoT systems to provide continual operation under these growing data demands that maintain high performance while being responsive and reliable.

6. Data Challenges in Federated Learning

Federated Learning (FL) has to address quite a few challenging, data-centric problems in order to enhance model performance and efficiency, mainly in the healthcare roster. Among these, non-IID (non-iidly distributed) data is a substantial point of controversy, where data across different clients, such as, hos-itals or devices, varies greatly in terms of distribution, features, and class representation. Such variety makes it difficult for the global model to ever converge effectively and often output biased and less generalized predictions. Another significant stumbling block includes the class distribution, which is prevalent among many medical datasets due to the rarer occurrence of certain conditions or diseases than in normal cases. This imbalance may lead to models biased towards the majority class; thus, dramatically reducing the accuracy and sensitivity in detecting rare but severely important conditions and acting on clinical decision-making [23].

In linked mentioning of how high populations in many urban cities interact with large amounts of diversely distributed data, a clear relationship arises between spatial and locational traverses associated with this communicable engagement; essentially, once these operations are completed, the continuous processing of such data is required. Addressing these issues lies at the heart of research in decentralized, high-dimensional chaos for the use of internet-scale distributed systems. Classification based on community connection is a broader issue pursued in this architect-landmark context. For answering the types of questions that will eventually enable systems to adjust to fluctuations, this present nexus was established, consisting of techniques for scalability and reliability-many-sided attacks. Given a definite motivation, we thus believe that migratory computation, discussions meant to transform differential concepts, embody layers and layers of meaning [24]. Table 2 highlights the key data challenges in Federated Learning, showing that non-IID data leads to poor model generalization, class imbalance causes biased predictions toward majority classes, and communication overhead increases latency and resource consumption, collectively affecting the efficiency and accuracy of distributed learning systems.

© 2026 The Author(s). Published by HJPARAM Publication under CC BY 4.0

Table 3. Data Challenges in Federated Learning

Challenge	Description	Impact in Federated Learning	Techniques / Solutions
Non-IID Data Distribution	In federated learning, data across different clients (e.g., hospitals or IoT devices) is not identically distributed. Each client may have data with different feature distributions, sample sizes, or class labels due to demographic, regional, or device-level variations.	Leads to poor model convergence, biased global models, and reduced generalization performance because the global model struggles to learn from heterogeneous data.	Data sharing strategies (limited), federated averaging improvements (FedAvg+, FedProx), domain adaptation, transfer learning, personalized FL models, and adaptive client selection.
Class Imbalance Handling	Occurs when certain classes (e.g., disease cases) are underrepresented compared to others in local datasets. In healthcare, rare diseases often have fewer samples compared to normal cases.	Causes biased predictions toward majority classes, reducing model sensitivity and recall for minority (critical) classes, which can lead to incorrect medical decisions.	Oversampling (SMOTE), undersampling, class weighting, cost-sensitive learning, focal loss, and balanced aggregation techniques across clients.
Communication Overhead	Refers to the large amount of data exchanged between clients and the central server during multiple training rounds, especially in large-scale federated systems.	Increases latency, bandwidth consumption, and energy usage, making the system inefficient and slower, particularly in IoT and edge environments.	Model compression, gradient quantization, sparse updates, fewer communication rounds, asynchronous training, and client selection strategies.

7. Advanced Learning Approaches

The swiftly growing domain of Distributed Artificial Intelligence is seeing the emergence of many subtle learning techniques aimed at making Federated Learning (FL) both effective and flexible. Federated Learning, the traditional one focuses on making a collaborative model without raw data sharing, is completely unsuited to the real-world healthcare situations, where manifold issues like varying tasks, problems of the poor quality in labeled data, and heterogeneity of data, all are included in offering a complex scenario to tackle. In response to the problem, methods such as Cross-Domain Federated Learning, Multi-Task Learning, and Federated Transfer Learning have been put forward. These techniques build on the conventional FL framework, extending its application to include improved sharing of knowledge, better generalization in the model, and capturing the efficient learning from dissimilar environments.

Cross-Domain Federated Learning (CDFL) is conceived for addressing the situation where the participating clients bring data from different domains having diverse feature distributions/data structures. For instance, in healthcare settings, hospitals collect different types of patient data including medical imaging, electronic health records, laboratory results, and wearable sensor data. These datasets may not have the same feature space, making incorporation by standard federated learning quite challenging. Under a cross-domain federated learning framework, a heterogeneous domain will have the chance to leverage agglomerate learning while respecting data privacy. It eludes satisfactory techniques that seek to narrow the gap of different data sets, though cannot transform this gap at the modeling stage. Domain adaptation, for example, forms the highly effective approach for removing such source domain disparities by learning domain- invariant features. Cross-domain federated learning (CDFL) exploits the principle of such domain-invariant feature learning, enabling models to learn generalized knowledge that can be transferred between healthcare settings [25]. This approach enhances the robustness of the models in day-to-day predictive scenarios and operating ability in an assortment of clinical environments.

Multi-Task Learning (MTL) is yet another innovation that has been built upon this framework. MTL is the training of a single model to perform several tasks simultaneously by sharing representations across tasks. In many healthcare applications, the prediction problems are interdependent. For example, predicting the risks of disease, hospital readmission, and patient mortality often share the same clinical factors. Therefore, rather than many individual models for each task, MTL helps one model to learn shared representations which benefit all tasks. When combined with federated learning, MTL allows multiple institutions to collaboratively train models with variably related but disparate goals while preserving data privacy. This not only supports learning efficiency but also assists in ensuring the prevention of overfitting when limited individual datasets are involved [26]. Furthermore, MTL in federated learning, by holding separate shared global parameters and task-specific local parameters at the same time, is an adaptation to task-specific variations. This hybrid structure guarantees the generalised patterns are captured across clients while preserving specialized knowledge for individualised tasks.

There is another established method Federated Transfer Learning (FTL) which acts as a scaffolding to expand the capability of federated learning in the presence of little overlap in the feature space or sample space of the datasets. When we gain the mitigating ability for federated learning in the context of healthcare, other complications arise with the fact that participating institutions might cater to different patient populations or have dissimilar sorts of medical data, thus making direct collaborative training a challenging task. The biggest mitigation of federated transfer learning is in the realm of transferring all the knowledge it has to work for from one domain or task to another, while retaining privacy.

© 2026 The Author(s). Published by HJPARAM Publication under CC BY 4.0

A good instance would be in one hospital that has a large database for cardiovascular disease prediction creating a model that can share learned model knowledge with another hospital having limited data but facing the same clinical challenges. Using all available transfer learning techniques, the model trained in the domain from the source is tailored to the target domain, improving model performance considerably in the scarcity of local data [27].

In the scope of medical research where labeled data is scarce and expensive to acquire, federated transfer learning is of crucial use. This method makes possible knowledge sharing and collaboration among models without divulging confidential information. FTL further brings together diverse datasets that do not match in feature space for cross-institutional data sharing in healthcare. Overall, such advanced learning paradigms expand pivotal capabilities while working with federated learning systems. Cross-domain federated learning promotes cooperation over different datasets; multi-task learning boosts efficiency through jointly learning related tasks, while federated transfer learning leads knowledge sharing back and forth crossing domains with limited data overlapped [28]. All of these strategies work wonders addressing the key drawbacks of traditional federated learning and supporting advancements in intelligent, scalable, and privacy-preserving systems in healthcare.

8. Conclusion and Future Work

This article outlines a detailed examination of Federated Learning (FL) in integration with privacy-preserving techniques, blockchain, and edge computing for healthcare IoT systems. Traditional Machine Learning (ML) in centralized purposes faces serious challenges to patient dataset privacy, security, and scalability. Federated learning offers a potential remedy to these challenges, allowing distributed model training to be implemented without sharing raw data, thus ensuring confidentiality as well as compliance with respected regulations. The article deliberated further on fundamental privacy enhancing mechanisms such as Fully Homomorphic Encryption, Secure Multiparty Computation, and Differential Privacy-the very or some of the mechanisms that beef up data protection during model training as well as communication; thus, the rest of it barely touches on other applicable privacy enhancing mechanisms amidst precipitation from the uproar. Information is intertwined to border likelihood in a course certain basic description and may be conducive to joint discussion on whether it is allied to an ability to certify agreement. With the important integration of technology, smart blockchain, into a healthcare system, more transparency and trust were offered about decentralized ledgers, consensus mechanisms, and smart contracts. Moreover, a discussion underscored the importance of edge computing in order to improve real-time processing, reduce latency, and support scalable health care system appeal.

They also explored advanced learning approaches like multitask learning, federated transfer learning, and cross-domain federated learning for tackling the challenges related to data heterogeneity and lack of labeled data. Combining these technologies forms a robust backbone for resting on the development of secure, efficient, and sophisticated healthcare systems for managing large-scale distributed data that will also maintain privacy and performance. Despite significant advancements, several research opportunities remain in the domain of federated learning for healthcare IoT. Future work can focus on developing more efficient algorithms to handle highly non-IID data and improve model convergence in heterogeneous environments.

References

[1] W. Moulahi, I. Jdey, T. Moulahi, M. Alawida, and A. Alabdulatif, “A blockchain-based federated learning mechanism for privacy preservation of healthcare IoT data,” Computers in Biology and Medicine, vol. 167, 2023, Art. no. 107630.

[2] Bonthu, Mohan Gandhi, et al. "The evolution of healthcare and artificial intelligence integration." *Artificial Intelligence in Patient Counselling*. Academic Press, 2026. 51-76.

[3] Kulkova, Julia, et al. "From theory to therapy: integrating artificial intelligence for transformative healthcare innovation." *Health Systems* (2026): 1-18.

[4] Yang, Albert, et al. "Assessing the Evolution and Influence of Medical Open Databases on Biomedical Research and Health Care Innovation: A 25-Year Perspective With a Focus on Privacy and Privacy-Enhancing Technologies." *Journal of Medical Internet Research* 28 (2026): e58954.

[5] Reinmund, Tyler, Lars Kunze, and Marina Jirotka. "Sociotechnical Challenges of Machine Learning in Healthcare and Social Welfare." *arXiv preprint arXiv:2601.11417* (2026).

[6] Bakas, Spyridon, et al. "Federated Learning in Healthcare: From Research to Real-World Deployment." *Annual Review of Biomedical Engineering* 28 (2026).

[7] Ghosh, Manthan, and Deepa Das. "Enhancing Patient Outcomes With Machine Learning in Healthcare Predictive Analytics." *Responsible Analytics for Superior Health Quality Outcomes*. IGI Global Scientific Publishing, 2026. 145-176.

[8] Núñez-Valdez, Edward Rolando. "Special Issue on Algorithms and Applications of Machine Learning Techniques for Healthcare." *Algorithms* 19.1 (2026): 53.

[9] Fatunmbi, Temitope Oluwatosin. "Harnessing AI, Deep Learning and Quantum Machine Learning for Healthcare driven applications: A Systemic overview." *Frontier Robotics and Artificial Intelligence Journal* 5.1 (2026): 1-29.

[10] Valencia, Mc Neil, et al. "Early Detection of Chronic Kidney Disease in Men Using Lifestyle and Demographic Indicators: A Machine Learning Approach for Primary Healthcare Settings." *Healthcare*. Vol. 14. No. 3. MDPI, 2026.

[11] Arafat, Md Tanvir, et al. "Data distribution aware clustering for parallel split learning in healthcare applications." *Future Generation Computer Systems* 174 (2026): 107911.

[12] Marengo, Agostino, et al. "Beyond the Black Box: Interpretable Machine Learning for Hospital Efficiency Assessment." *IEEE Access* (2026).

[13] Descatha, Alexis, and Dominique Savary. "Machine Learning in cardiac arrest: from Artificial Intelligence, Value-Based Healthcare, to prevention." *Resuscitation* (2026).

[14] Indu, V. Thanammal, M. Elumalai, and LA Anto Gracious. "Optimization Algorithms for Machine Learning Model Enhancement in Healthcare." *AI Model Design and Data Management for Disease Prediction*. IGI Global Scientific Publishing, 2026. 159-192.

© 2026 The Author(s). Published by HJPARAM Publication under CC BY 4.0

[15] Webb, Catherine, et al. "Health care professionals' perceptions of machine learning based clinical decision support systems for oesophageal cancer management." *Computers in Biology and Medicine* 200 (2026): 111373.

[16] Aparna, Mudiyala, Battula Srinivasa Rao, and Mallela Siva Naga Raju. "AI Revolution in Healthcare: Digital Health Services Empowered by Machine Learning and Deep Learning." *Digital Cities* (2026): 1-12.

[17] Zhang, Yunsheng, et al. "AI-driven blockchain technology in smart healthcare system: Opportunities, challenges and future implications." *Computer Science Review* 60 (2026): 100909.

[18] Achouri, Youssouf, et al. "Towards quantum-enabled security for IoT-driven smart healthcare systems." *Cluster Computing* 29.2 (2026): 123.

[19] Vasamsetty, Chaitanya, et al. "Enhancing Interactive Wireless Communication in Healthcare With Wearable Devices and Smart Healthcare Systems." *International Journal of Communication Systems* 39.1 (2026): e70311.

[20] Muniappan, Swarna, Naveen Jeyaraman, and Madhan Jeyaraman. "Sensor network and blockchain platform for the future smart healthcare system." *Advances in Fog Computing and the Internet of Things for Smart Healthcare*. Elsevier, 2026. 175-184.

[21] Shafik, Wasswa. "Overview of fog computing and iot-based technology in smart healthcare systems." *Fundamentals of Fog Computing and the Internet of Things for Smart Healthcare*. Elsevier, 2026. 17-34.

[22] Adeniyi, Abidemi Emmanuel, et al. "Fog computing and IoT-Based technology security and privacy in smart healthcare systems." *Fundamentals of Fog Computing and the Internet of Things for Smart Healthcare*. Elsevier, 2026. 189-214.

[23] Balaji, Sangeetha, et al. "Cryptography-based fog computing and IOT-based technology in smart healthcare systems." *Fundamentals of Fog Computing and the Internet of Things for Smart Healthcare*. Elsevier, 2026. 253-272.

[24] Shanmugam, P., M. Mohamed Iqbal, and M. Amanullah. "Cognitive Cyber-Physical Security With IoT: A Solution to Smart Healthcare System." *Securing Cyber-Physical Systems: Fundamentals, Applications and Challenges* (2026): 109-131.

[25] Buhas, Bogdan Adrian, et al. "Transition to a digital perioperative pathway for robot-assisted radical prostatectomy: impact on patient outcomes and adherence." *BJU international* 137.3 (2026): 473-479.

[26] Ahmadbekov, Behzodbek, and Shukurbek Tuychibekov. "Perioperative Outcomes and Prognostic Impact of Postoperative Complications in a 68 Patient Cohort Undergoing Colorectal Cancer Resection." *Journal of Clinical and Biomedical Research* 1.2 (2026): 42-50.

[27] Pasquini, Pietro, et al. "Effect of diaphragmatic resection versus stripping in advanced ovarian cancer: impact on patient complications in a large retrospective cohort study at a tertiary referral center." *Annals of Surgical Oncology* 33.2 (2026): 1099-1108.

[28] Gupta, Sunil, Monit Kapoor, and Sanjoy Kumar Debnath. "Cybersecurity risks and threats in healthcare." *Artificial Intelligence-Enabled Security for Healthcare Systems: Safeguarding Patient Data and Improving Services*. Cham: Springer Nature Switzerland, 2025. 39-64.

 © 2026 The Author(s). Published by HJPARAM Publication under CC BY 4.0