American Journal of Scholarly Research and Innovation
Volume 04, Issue 01 (2025)
Page No: 320-351
eISSN: 3067-2163
Doi: 10.63125/jga18304

FEDERATED LEARNING FOR PRIVACY-PRESERVING HEALTHCARE DATA SHARING: ENABLING GLOBAL AI COLLABORATION

Sai Srinivas Matta[1]; Manish Bolli[2];

[1] *Ms in CS Candidate, Campbellsville University, USA; Email: mattasaisrinivas@gmail.com*
[2] *MS in CS Candidate, University of Central Missouri, Email : manishbolli66@gmail.com*

ABSTRACT

This study provides a comprehensive systematic review of federated learning as a framework for privacy-preserving healthcare data sharing and its potential to enable global artificial intelligence collaboration. In total, 124 peer-reviewed articles were examined following the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines to ensure transparency, rigor, and reproducibility. The review highlights how federated learning has evolved from conceptual discussions to practical applications across multiple healthcare domains, including medical imaging, electronic health records, biosignals, and genomic analysis. Key findings indicate that federated architectures, particularly server–client models, have become the dominant deployment strategy, while peer-to-peer approaches are gaining attention for their resilience and decentralization. Privacy-preserving mechanisms—such as differential privacy, secure aggregation, and cryptographic computation—emerged as central to ensuring compliance with regulatory and ethical standards, with adaptive strategies allowing for an effective balance between confidentiality and model utility. Evidence from multi-institutional collaborations shows that federated learning not only improves predictive performance but also enhances inclusivity, enabling smaller or resource-limited institutions to contribute meaningfully without relinquishing data ownership. At the same time, empirical studies identified adversarial risks such as gradient inversion, membership inference, and poisoning attacks, underscoring the necessity for layered safeguards and strong governance structures. Collectively, the findings demonstrate that federated learning is more than a technical innovation; it represents a socio-technical paradigm that integrates privacy, equity, and collaboration into the development of global healthcare AI. This review positions federated learning as a cornerstone for building secure, ethical, and scalable artificial intelligence systems that address the dual imperatives of advancing medical innovation while safeguarding patient confidentiality.

KEYWORDS

Federated Learning In Healthcare Systems, Privacy-Preserving Medical Data Sharing, Global Artificial Intelligence Collaboration.

Citation:
Matta, S. S., & Bolli, M. (2025). Federated learning for privacy-preserving healthcare data sharing: Enabling global AI collaboration. *American Journal of Scholarly Research and Innovation, 4*(1), 320-351. https://doi.org/10.63125/jga18304

Received:
May 19, 2025

Revised:
June 17, 2025

Accepted:
July 26, 2025

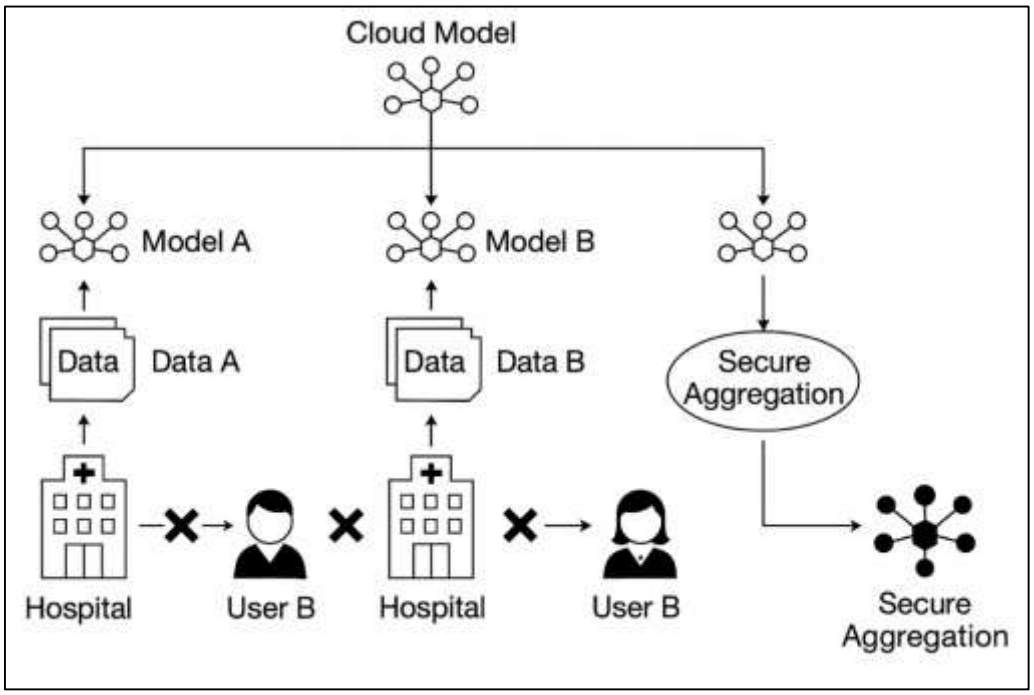
Published:
August 28, 2025

American Journal of Scholarly Research and Innovation
Volume 04, Issue 01 (2025)
Page No: 320-351
eISSN: 3067-2163
Doi: 10.63125/jga18304

INTRODUCTION

Federated learning is a distributed paradigm in which multiple institutions collaborate to train machine learning models without transferring raw data from one site to another (Ma et al., 2022). Instead of centralizing sensitive health records into a single repository, participating nodes keep data locally and only share model updates or parameters. This structure ensures that patient-level information remains under the custodianship of the originating institution while still contributing to the creation of a stronger (Zhang et al., 2021), generalized model. Privacy-preserving mechanisms such as noise injection, encryption, and secure aggregation further strengthen this process, ensuring that identifiable attributes do not escape institutional boundaries. In the healthcare domain, where regulatory, ethical, and social constraints on data mobility are intense, the value of such an approach becomes evident. Across the globe , healthcare providers, research centers, and pharmaceutical organizations recognize the immense potential of learning from diverse patient cohorts while simultaneously safeguarding individual privacy (Savazzi et al., 2020). This dual imperative—achieving collaborative learning without compromising confidentiality—forms the cornerstone of federated learning's role in healthcare. Internationally, it addresses the challenge of heterogeneous legal systems, varying infrastructures, and diverse cultural attitudes toward data, offering a practical framework for global cooperation in artificial intelligence for medicine (Liu et al., 2022).

Figure 1: Federated Learning Framework for Healthcare



The technical structure of federated learning relies on iterative exchanges of model parameters between clients and a coordinating server or peer nodes (Beltrán et al., 2023). Clients compute updates using their local health data, then transmit those updates for aggregation into a global model. This process repeats until convergence, producing a model that reflects the statistical strength of all participants without exposing raw records (Wen et al., 2023). In healthcare applications, such a system must accommodate widely varying data types: imaging, laboratory tests, sensor streams, and textual clinical notes. Challenges arise when distributions differ substantially across institutions, such as different disease prevalence, equipment vendors, or coding practices. To manage this, federated learning algorithms incorporate strategies like personalized layers, adaptive optimization, and mechanisms that stabilize training under non-identical data distributions (Farahani & Monsefi, 2023). Alongside algorithmic refinement, privacy-preserving enhancements like differential privacy and cryptographic aggregation reduce the risk of inference attacks. These technical underpinnings are critical to building trust among institutions and regulators, ensuring that collaboration can scale beyond local networks into international consortia. The global dimension of

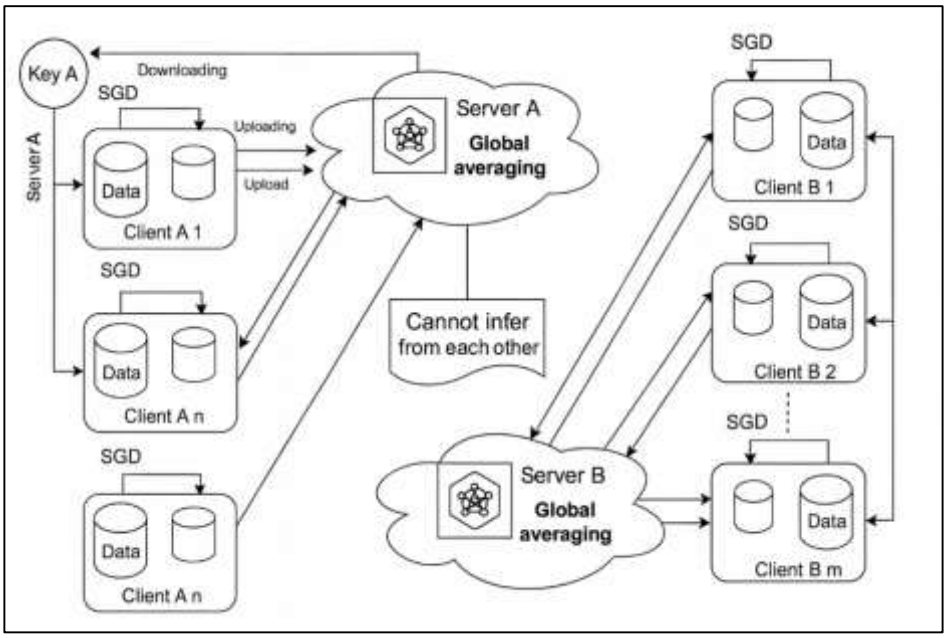
American Journal of Scholarly Research and Innovation
Volume 04, Issue 01 (2025)
Page No: 320-351
eISSN: 3067-2163
Doi: 10.63125/jga18304

healthcare necessitates this type of flexible, privacy-respecting infrastructure to bring together knowledge scattered across continents (Li et al., 2021).

The promise of federated learning in healthcare lies not only in technical design but also in its ability to mitigate privacy risks (Rahman et al., 2020). Even when raw data remains on site, updates and parameters can inadvertently leak information if not adequately protected. Attacks such as membership inference, model inversion, and gradient reconstruction have demonstrated how adversaries might recover sensitive details from shared parameters (Qayyum et al., 2022). In clinical contexts, where even partial leakage can expose patient identity or conditions, this risk cannot be overlooked. To counter such threats, federated learning integrates privacy budgets, auditing systems, and formal guarantees that bound the probability of revealing information about any individual record (Savazzi et al., 2021). Healthcare institutions that adopt federated learning do so not only for analytical efficiency but also to align with stringent privacy expectations from regulators, patients, and professional bodies. The system's ability to demonstrate mathematically grounded protections builds confidence that shared models will not inadvertently compromise confidentiality. This tension between risk and safeguard illustrates the depth of innovation needed to operationalize privacy-preserving analytics in medicine at an international scale (Li et al., 2020).

In practice, federated learning has demonstrated tangible benefits in collaborative medical research and clinical decision support (Zhang et al., 2022). Multi-institutional studies on medical imaging, for instance, show that models trained across hospitals achieve greater generalizability and robustness compared to those developed in isolation. By leveraging diverse datasets, these models become less biased toward specific demographics, equipment types, or regional practices. This capacity to integrate varied clinical contexts without exchanging raw patient records is a transformative development in medical AI (Nguyen, Ding, Pham, et al., 2021). Similarly, in areas such as intensive care monitoring, disease progression modeling, and outcome prediction, federated learning enhances predictive accuracy by pooling distributed knowledge. The international dimension is particularly critical: diseases manifest differently across populations (Alsamhi et al., 2024), and effective models require exposure to this global heterogeneity. Federated learning makes it possible to respect local privacy constraints while still accessing the collective power of international datasets. The healthcare sector increasingly views this model not only as a technical innovation but also as an ethical framework for collaborative research that honors both privacy and inclusivity (Tan et al., 2022).

Figure 2: Federated Learning Secure Global Averaging



Beyond imaging, federated learning extends its influence into other complex healthcare data domains such as electronic health records, biosignals, genomics, and digital phenotyping (Zhang et al., 2021). These data streams are highly sensitive and deeply personal, which makes centralized

Volume 04, Issue 01 (2025)
Page No: 320-351
eISSN: 3067-2163
Doi: 10.63125/jga18304
pooling impractical or even legally impermissible. Federated learning enables institutions to harness the predictive value of longitudinal patient histories (Nguyen et al., 2022), physiological signals from wearables, and multi-omics data while keeping the raw forms securely within local systems. This has profound implications for chronic disease management, rare disease research, and real-time health monitoring. The capacity to learn from broad, distributed datasets means that conditions that are underrepresented in any single region can still be studied collaboratively (Rauniyar et al., 2023). This inclusivity strengthens models while ensuring that marginalized or geographically isolated populations are not excluded from the benefits of advanced analytics. It also emphasizes the universality of healthcare challenges and the need for cooperative technological solutions. By supporting cross-border analysis in ways that respect sovereignty and privacy, federated learning becomes a unifying approach that bridges gaps between fragmented health systems (Wahab et al., 2021).

The international dimension of federated learning requires robust interoperability standards and governance frameworks (Shaheen et al., 2022). Healthcare systems vary widely in the data formats they employ, the regulations they enforce, and the infrastructures they maintain. Federated learning must therefore align with standards for clinical data representation, such as resource-oriented models and semantic harmonization techniques (Lu et al., 2022), to enable consistent model training across sites. Legal frameworks governing privacy and data protection introduce further complexity, requiring solutions that comply with regulations in multiple jurisdictions simultaneously. In this context, federated learning's in-situ analytics are advantageous, as they minimize the cross-border transfer of identifiable information (Hanser, 2023). Organizational trust is strengthened when cryptographic safeguards, secure aggregation, and auditable processes are combined with governance structures that clarify accountability. Institutions participating in global federated networks must agree not only on technical protocols but also on ethical and legal principles that underpin data stewardship. This intersection of governance, regulation, and technology transforms federated learning from a purely computational strategy into a comprehensive framework for international health collaboration (Yin et al., 2020).

Ultimately, the strength of federated learning in healthcare lies in its ability to transform institutional diversity into a collective advantage (Andreux et al., 2020). Global health data is inherently heterogeneous, reflecting differences in population genetics, clinical practices, diagnostic equipment, and cultural contexts. Federated learning treats this heterogeneity not as an obstacle but as a source of robustness, enabling models that generalize across boundaries (Zhu et al., 2021). Technical strategies such as adaptive optimization, personalization, and communication-efficient updates help manage disparities in participation and infrastructure. Privacy-preserving mechanisms ensure that the system remains aligned with ethical expectations and legal requirements. The result is a collaborative environment where institutions can pool their knowledge without surrendering their autonomy over data (Bashir et al., 2023). In this way, federated learning advances the goal of equitable healthcare innovation by ensuring that diverse voices and populations contribute to the design of AI systems. By embedding privacy-preserving principles into its foundation, it provides a path forward for healthcare systems around the world to engage in meaningful, secure, and large-scale collaboration.

LITERATURE REVIEW

The rapid advancement of artificial intelligence in healthcare has created unprecedented opportunities for predictive analytics, diagnostic support, and treatment personalization (Bohr & Memarzadeh, 2020). Yet, these opportunities are tightly coupled with one of the most pressing challenges in modern medicine: the need to share health data without compromising patient privacy. Healthcare information is often fragmented across multiple institutions, countries, and regulatory environments, making centralized aggregation both technically difficult and legally constrained. Federated learning has emerged as a transformative approach that enables collaborative model training across distributed data sources without requiring raw data exchange (Goel et al., 2025). By ensuring that only model parameters or updates are shared, federated learning preserves institutional data sovereignty while allowing the construction of high-performance models that reflect knowledge from diverse populations.A review of the existing scholarship in this domain reveals multiple layers of inquiry. At the foundational level, researchers have defined the architectures, algorithms, and privacy-preserving mechanisms that underpin federated learning. Parallel strands of research have explored how such frameworks can be applied to imaging,

Volume 04, Issue 01 (2025)
Page No: 320-351
eISSN: 3067-2163
Doi: 10.63125/jga18304
electronic health records, biosignals, genomics, and other critical healthcare modalities. An additional body of work interrogates the vulnerabilities of federated systems, including inference attacks (Noorbakhsh-Sabet et al., 2019), reconstruction threats, and communication bottlenecks, and presents cryptographic and differential privacy-based safeguards to mitigate risks. Beyond the technical focus, scholars also emphasize governance, interoperability, and regulatory compliance as essential to global collaboration. Studies consistently point to the value of aligning federated learning not only with technical goals of efficiency and scalability but also with broader ethical imperatives of equity, inclusivity, and transparency.This literature review therefore examines the trajectory of research in federated learning for healthcare data sharing, highlighting the interplay between algorithmic innovation, privacy-preservation, and international collaboration. The review is structured to move from theoretical definitions to technical mechanisms, then to domain-specific applications, before addressing challenges (da Silva, 2024), safeguards, and governance frameworks. Through this layered exploration, the review builds a comprehensive understanding of how federated learning is positioned as a critical enabler of secure, cross-border, and large-scale artificial intelligence in healthcare.

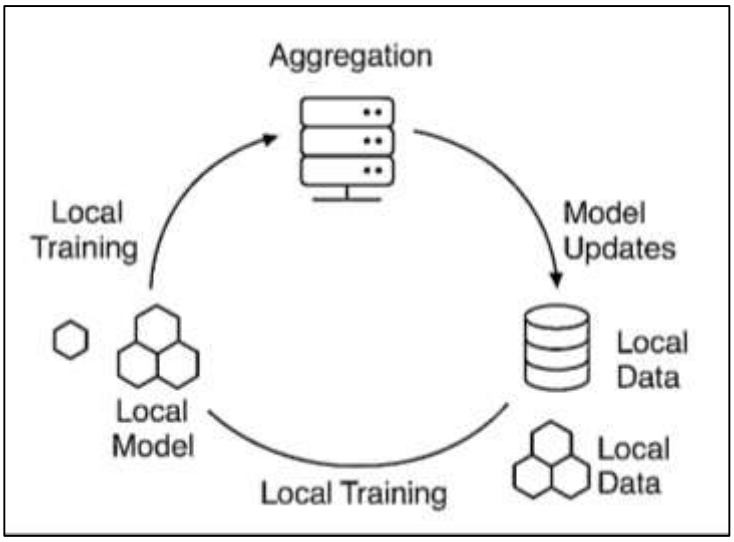
Foundations of Federated Learning in Healthcare

The conceptual foundations of federated learning emerged as a response to the limitations of traditional centralized machine learning models, which rely on aggregating raw data from multiple sources into a single repository for training (Piccialli et al., 2021). While centralized approaches allow for large-scale pattern recognition and predictive accuracy, they introduce critical risks in domains where sensitive information is involved, particularly in healthcare. Scholars initially highlighted how centralization increases vulnerability to data breaches, regulatory violations, and ethical concerns surrounding patient autonomy (Jabarulla & Lee, 2021). In contrast, federated learning conceptualizes model development as a distributed process, where local nodes perform computations independently and contribute only model updates or gradients to a global aggregator. This distinction is crucial, as it shifts the locus of control away from a central server that could become a single point of failure and instead fosters a collaborative model of learning without data pooling (Athanasopoulou et al., 2022). Studies consistently emphasize that federated learning not only mitigates the privacy risks associated with centralization but also enhances scalability by leveraging computational resources distributed across multiple sites. The conceptual departure from centralized learning has positioned federated systems as both a technological innovation and a paradigm shift in how sensitive data, such as healthcare records, can be harnessed for collective intelligence. In this sense, federated learning is not merely a technical variant of distributed computing but a privacy-first philosophy that redefines the balance between data accessibility and security in clinical contexts (Bianchini et al., 2022; Ara et al., 2022).

At the heart of federated learning lies the principle of data locality, which mandates that raw data remain within the secure infrastructure of its originating institution (Jahid, 2022; Olawade et al., 2024). This principle directly addresses the legal and ethical challenges of transferring medical records across jurisdictions, particularly in environments governed by strict regulatory frameworks. The operationalization of this principle depends on distributed optimization techniques that aggregate updates from multiple clients into a unified model. The federated averaging algorithm exemplifies this approach, combining local updates in a way that approximates centralized training while preserving data autonomy (Uddin et al., 2022; Poongodi et al., 2021). However, healthcare data is rarely homogeneous, and the non-identical distribution of patient populations, diagnostic equipment, and institutional practices complicates optimization. To address these challenges, federated learning employs algorithmic strategies such as proximal regularization, adaptive learning rates, and variance reduction, which stabilize model performance under highly heterogeneous conditions. The principle of distributed optimization ensures that every institution contributes proportionally to the collective model while maintaining independence over its sensitive data (Branda & Scarpa, 2024; Akter & Ahad, 2022). This design reduces reliance on data transfer protocols that are vulnerable to interception or misuse, instead aligning computational processes with privacy-preserving ethics. Scholars note that data locality and distributed optimization together embody the defining philosophy of federated learning, where computational collaboration occurs without compromising the autonomy and confidentiality of medical data custodians (Kitsios et al., 2023; Arifur & Noor, 2022).

American Journal of Scholarly Research and Innovation
Volume 04, Issue 01 (2025)
Page No: 320-351
eISSN: 3067-2163
Doi: 10.63125/jga18304

Figure 3: Federated Learning in Healthcare Systems



Healthcare ecosystems are characterized by data fragmentation, heterogeneity, and regulatory constraints that make centralized data aggregation impractical (Helm et al., 2020; Rahaman, 2022). Patient information is stored across hospitals, laboratories, imaging centers, and regional health networks, often using incompatible standards and formats. Federated learning directly addresses these challenges by enabling cross-institutional collaboration without requiring homogenization or centralization of records. Its relevance lies in its ability to harness statistical strength from diverse sources, thereby producing models that generalize better across populations and clinical contexts (Li et al., 2021; Hasan et al., 2022). Studies in medical imaging, electronic health records, and biosignal analysis illustrate that federated learning enables broader coverage of demographic and pathological variations while maintaining compliance with privacy laws. For example, training across international institutions allows for models that capture disease manifestations in varied populations, thereby improving diagnostic equity and accuracy (Li et al., 2021; Mubashir & Abdul, 2022). Moreover, federated learning reduces the administrative burden associated with negotiating complex data-sharing agreements, since raw patient records never leave their source. Within the broader health data ecosystem, this approach harmonizes the dual imperatives of collaboration and protection. Its ability to operate effectively across heterogeneous infrastructures and regulatory regimes underscores its transformative relevance, positioning it as a cornerstone of international health informatics and AI-driven clinical research (Arora et al., 2021; Reduanul & Shoeb, 2022).

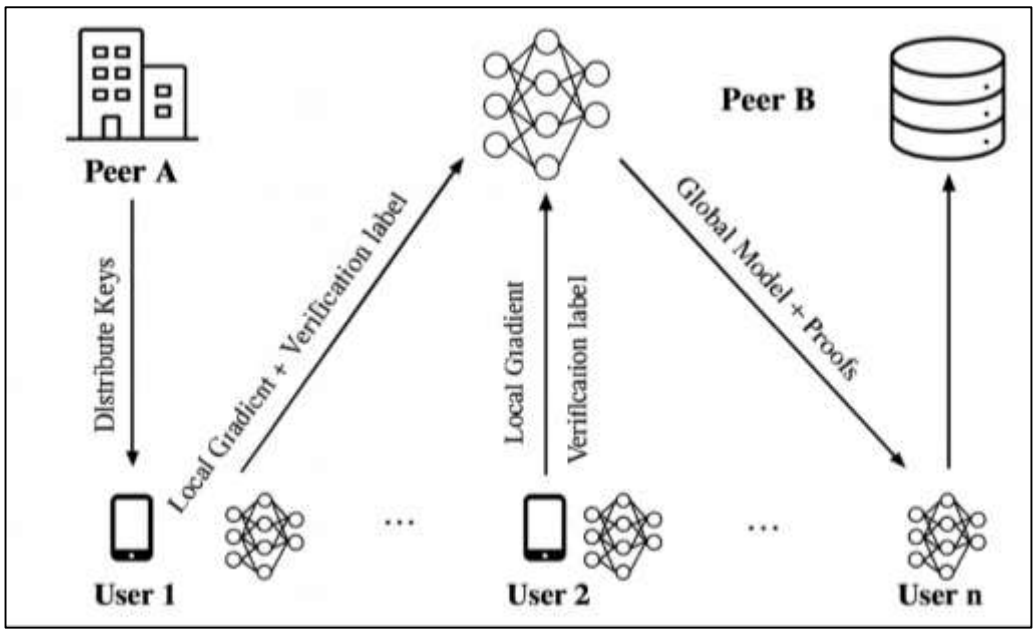
Privacy-preservation is not merely a technical feature of federated learning but its central guiding philosophy (Lu et al., 2023). In healthcare, the confidentiality of patient data is paramount, and the consequences of breaches extend beyond regulatory penalties to issues of trust, equity, and patient safety. Federated learning operationalizes privacy through a layered approach that combines technical safeguards with organizational and ethical principles (Bragazzi et al., 2020; Sazzad & Islam, 2022). Differential privacy, secure aggregation, and cryptographic protocols ensure that even the shared model updates are resistant to adversarial attacks seeking to reconstruct sensitive information. At the same time, institutions participating in federated networks retain sovereignty over their datasets, aligning participation with ethical principles of data stewardship. This philosophy distinguishes federated learning from other distributed computing frameworks by making privacy the non-negotiable foundation of design rather than an ancillary consideration (Chalasani et al., 2023; Noor & Momena, 2022). Scholars repeatedly highlight that the effectiveness of federated learning in healthcare rests not only on its predictive accuracy but also on its ability to maintain public trust and regulatory compliance. In practice, this guiding philosophy creates a framework where institutions collaborate with confidence, knowing that their contributions are protected by rigorous safeguards. Privacy-preservation therefore emerges as both the moral compass and the structural backbone of federated learning in healthcare, ensuring that technological advancement proceeds hand in hand with ethical responsibility (Adar & Md, 2023; Xu et al., 2019).

American Journal of Scholarly Research and Innovation
Volume 04, Issue 01 (2025)
Page No: 320-351
eISSN: 3067-2163
Doi: 10.63125/jga18304

Architectures and Algorithms for Distributed Model Training

Federated learning architectures are primarily defined by the manner in which communication and coordination occur among participants (Wahab et al., 2021). The most common orchestration framework is the server-client model, in which a central coordinating server aggregates updates from multiple distributed clients and disseminates a global model. This architecture has been favored in healthcare applications due to its relative simplicity, scalability, and straightforward monitoring of model convergence. However (Qibria & Hossen, 2023; Qin et al., 2021), the server-client framework also introduces a potential bottleneck, as the server becomes a critical point of trust and a possible vector of attack. To counter this, some scholars and practitioners have explored peer-to-peer frameworks, where participating nodes coordinate directly with each other without reliance on a single central aggregator. Peer-to-peer orchestration fosters resilience against single-point failures (Istiaque et al., 2023; Zhang et al., 2021), distributes control more equitably, and aligns with ethical imperatives of decentralization in healthcare data governance. Yet, it introduces challenges in synchronizing updates, maintaining consistency, and preventing collusion or malicious manipulation by adversarial nodes. Both approaches illustrate trade-offs: server-client systems offer simplicity and control but raise questions about central authority, while peer-to-peer models encourage democratized collaboration but require sophisticated consensus mechanisms. Within healthcare, where institutions vary widely in technical capability, legal obligations, and trust levels, these orchestration frameworks must be evaluated not just for technical efficiency but also for alignment with regulatory and ethical expectations (Mansura Akter, 2023; Zhang et al., 2021). The ongoing evolution of architectures reflects an attempt to balance coordination, resilience, and inclusivity in global health data collaborations.

Figure 4: Federated Learning Orchestration in Healthcare



At the algorithmic core of most federated learning systems is the Federated Averaging (FedAvg) algorithm (Beltrán et al., 2023; Hasan et al., 2023). FedAvg enables clients to perform multiple local gradient updates before transmitting model parameters to the central aggregator, which then computes a weighted average to update the global model. This innovation reduces communication costs, enhances scalability, and ensures that models converge more efficiently even in the presence of limited bandwidth. In healthcare (Masud et al., 2023; Nguyen, Ding, Pathirana, et al., 2021), where connectivity may be inconsistent across hospitals or countries, FedAvg provides a practical foundation for collaborative learning. However, FedAvg is not without limitations. It can struggle in contexts where data across sites is highly non-identical, leading to slower convergence and potential biases in the global model. To address these limitations, a series of variants have emerged. For example, algorithms that adjust learning rates adaptively (Khan et al., 2021; Sultan et al., 2023),

Volume 04, Issue 01 (2025)
Page No: 320-351
eISSN: 3067-2163
Doi: 10.63125/jga18304

algorithms that incorporate proximal terms to stabilize training, and algorithms that use variance reduction techniques all seek to mitigate the challenges inherent in heterogeneous environments. In practice, these adaptations enable federated systems to maintain high levels of accuracy across clinical datasets that differ substantially in scale, quality, and distribution. As a result, FedAvg and its derivatives remain the cornerstone of federated healthcare research, providing the mathematical backbone for distributed optimization while inspiring continual refinements to address the complexities of medical data (Hossen et al., 2023; Zhu et al., 2021).

One of the most persistent challenges in federated learning is the issue of non-identical, independently distributed (non-IID) data across participating institutions (Aledhari et al., 2020). In healthcare, this challenge is particularly acute because patient demographics, disease prevalence, diagnostic practices, and instrumentation vary widely across regions and organizations. Such heterogeneity often leads to client drift, where local updates diverge significantly from the global objective, resulting in unstable or biased models. To mitigate these issues, researchers have proposed a variety of strategies (Tawfiqul, 2023; Paragliola & Coronato, 2022). Some approaches incorporate proximal terms into optimization to constrain local updates and maintain alignment with the global model. Others use data augmentation techniques to simulate more balanced distributions or reweight client contributions based on dataset size and variability. Clustering-based methods also group clients with similar data distributions, training specialized sub-models that can then be merged into a more robust global model. Additionally (Shamima et al., 2023; Sattler et al., 2019), variance reduction techniques and adaptive aggregation rules help minimize the distortions caused by extreme heterogeneity. In clinical contexts, where fairness and generalization are critical, these methods ensure that federated models do not disproportionately reflect the characteristics of dominant or data-rich institutions. Handling non-IID data is therefore not simply a technical optimization problem but a central concern for ensuring that federated learning systems in healthcare produce models that are equitable, reliable, and representative of global patient populations (Li et al., 2020; Ashraf & Ara, 2023).

While federated learning aspires to create global models that serve diverse populations, the reality of healthcare practice often demands institution-specific adaptation (Sanjai et al., 2023; Yang et al., 2022). Hospitals, clinics, and research centers may face unique patient populations, disease patterns, or technological environments that require models tuned to their local contexts. Personalization strategies have emerged as a critical response to this need. One approach is fine-tuning, in which institutions use the shared global model as a starting point and then adjust parameters on local data to achieve better alignment with their own population (Liu et al., 2022; Akter et al., 2023). Another strategy involves multi-task learning, where the federated process jointly optimizes global parameters and site-specific objectives, allowing each institution to benefit from shared knowledge while retaining local specialization. Layer-wise personalization is also common, with shared representations learned globally while higher-level layers are customized locally. These strategies ensure that federated learning is not merely about producing a single universal model but about enabling flexible adaptation across heterogeneous environments (Razzak et al., 2024; Gafni et al., 2022). In healthcare, this is especially important for equity: institutions with rare disease populations, resource-limited infrastructures, or culturally specific health challenges can still derive meaningful utility from federated participation. Personalization therefore bridges the gap between collective intelligence and local relevance, ensuring that federated learning supports not just the global advancement of healthcare AI but also the nuanced realities of diverse clinical ecosystems (Chen et al., 2021).

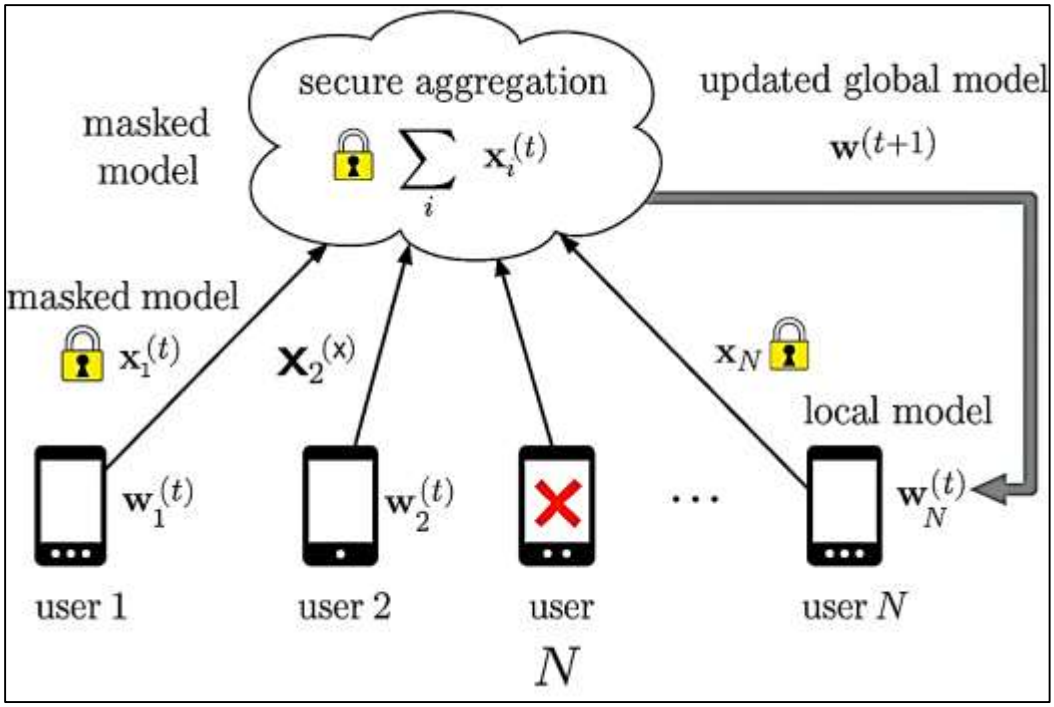
Privacy-Preserving Mechanisms in Federated Healthcare

Differential privacy has emerged as one of the most important tools for ensuring confidentiality in federated healthcare environments (Ziyao Liu et al., 2022). It provides a formal mathematical framework that guarantees that the contribution of any single individual within a dataset cannot be distinguished with high probability, even if adversaries have access to external information. In practice, this is achieved by injecting carefully calibrated noise into model gradients, updates, or outputs during the federated training process (Eltaras et al., 2023; Istiaque et al., 2024). The challenge in healthcare contexts lies in striking a balance between the strength of the privacy guarantee and the preservation of clinical utility. Excessive noise can obscure subtle but clinically relevant patterns, particularly in rare disease datasets or small institutional cohorts. To address this, researchers have proposed adaptive noise calibration, where the magnitude of perturbation varies according to factors such as dataset size, sensitivity of features, or phase of training (Chen et al., 2025). In some

American Journal of Scholarly Research and Innovation
Volume 04, Issue 01 (2025)
Page No: 320-351
eISSN: 3067-2163
Doi: 10.63125/jga18304

approaches, privacy budgets are explicitly tracked, ensuring that cumulative exposure remains bounded across multiple training rounds. Healthcare-specific adaptations of differential privacy recognize that different modalities—such as medical images, genomic sequences, and structured clinical records—present unique risks of re-identification and thus require tailored calibration strategies. As a result, differential privacy has become a foundational layer of federated healthcare learning, embedding rigorous protections into the very fabric of model updates while acknowledging the domain-specific trade-offs between data protection and model performance (Awan et al., 2023; Akter & Shaiful, 2024).

Figure 5: Secure Aggregation in Federated Learning



Secure aggregation protocols serve as another critical pillar of privacy-preserving federated learning in healthcare (Manzoor et al., 2024). These protocols ensure that a central server, or any adversary observing communication, can only access the aggregated sum of client updates rather than individual contributions. In practice, this means that even if one client's update were intercepted, it would be computationally infeasible to isolate its contents without access to the full aggregation process (Hasan et al., 2024; Wang et al., 2024). This mechanism is especially valuable in clinical networks where institutions may be hesitant to expose even model parameters derived from sensitive patient data. By protecting updates during transmission, secure aggregation builds trust among participants and reduces the attack surface for adversaries. Protocols typically employ random masking, secret sharing, or distributed key generation to achieve privacy guarantees, ensuring that no single party—including the central coordinator—can reconstruct the original updates (Aljrees et al., 2023). The healthcare context adds unique dimensions to the use of secure aggregation, since participating institutions often differ in computational resources and network reliability. Lightweight implementations are necessary for hospitals with limited infrastructure, while robust error-handling ensures that partial failures do not compromise the aggregation process. The presence of secure aggregation thus transforms federated learning into a truly collaborative framework, assuring stakeholders that their contributions cannot be individually scrutinized and thereby lowering barriers to international cooperation (Abaoud et al., 2023).

Cryptographic techniques such as homomorphic encryption and secure multiparty computation provide advanced methods for protecting sensitive information in federated healthcare environments (Tawfiqul et al., 2024; Tariq et al., 2024). Homomorphic encryption allows computations to be performed directly on encrypted data, meaning that a server can aggregate model updates without ever accessing their plaintext form. This property ensures strong confidentiality but introduces

Volume 04, Issue 01 (2025)
Page No: 320-351
eISSN: 3067-2163
Doi: 10.63125/jga18304

computational overhead that can become a barrier in resource-constrained clinical settings (Ma et al., 2020; Subrato & Md, 2024). Multiparty computation, by contrast, distributes computations across several parties such that no single participant can access the full information, yet the collective process yields correct outputs. Together, these cryptographic techniques strengthen the security of federated systems against both external adversaries and semi-honest participants. Their relevance in healthcare lies in their ability to uphold privacy even in environments where institutions do not fully trust one another but still seek the benefits of shared model development (Ashiqur et al., 2025; Moshawrab et al., 2023). Advances in optimization, compression, and lightweight cryptographic primitives have made these tools more practical for large-scale deployments, though efficiency remains a persistent concern. Importantly, these methods are not mutually exclusive but can be layered with differential privacy and secure aggregation to create multi-tiered defenses. In sensitive healthcare applications (Hasan, 2025; Rahmati & Pagano, 2025), where breaches carry severe consequences for patients and institutions alike, cryptographic methods serve as essential safeguards that complement and reinforce other privacy-preserving strategies.

Federated Learning in Medical Imaging Applications

Radiology has been one of the most fertile domains for demonstrating the power of federated learning because of its data-intensive nature and its reliance on highly sensitive patient imaging records (Sultan et al., 2025; Sandhu et al., 2023). Traditional centralized learning approaches in radiology often encounter major barriers related to the transfer of raw images across institutions, which is restricted by privacy regulations and logistical challenges. Federated learning addresses this limitation by enabling cross-institutional collaboration where hospitals and imaging centers can train models collectively without exchanging raw image data (Lakhan et al., 2023). This framework allows institutions of varying sizes and resources to contribute to a shared model, pooling their collective knowledge to achieve better diagnostic accuracy and robustness. In practice, federated approaches have been applied to tasks such as lung disease detection, neuroimaging analysis, and cardiovascular risk assessment, with institutions reporting significant performance gains compared to models trained on single-center data (Sanjai et al., 2025; Yang et al., 2023). Cross-institutional collaboration in radiology also enhances inclusivity, as smaller hospitals with limited datasets benefit from participating in models trained on larger, more diverse imaging cohorts. By respecting privacy boundaries while enabling broad cooperation, federated learning has become a transformative mechanism for radiology research networks, creating opportunities to generate clinically useful models that reflect a wide range of patient populations and imaging modalities (Khan et al., 2025).

One of the most impactful applications of federated learning in medical imaging lies in the domain of tumor segmentation, lesion detection, and disease classification (Huang et al., 2022). Segmentation of tumors in modalities such as MRI or CT scans requires access to large, annotated datasets that capture the variability of tumor shapes, sizes, and imaging conditions across patients. Federated learning enables multiple institutions to collaborate on these tasks without pooling raw data, significantly increasing the statistical power available for model training (Khalil et al., 2023). In tumor segmentation, federated models have been shown to rival or surpass the accuracy of centralized models by leveraging diverse data from multiple hospitals. Similarly, lesion detection tasks, including identifying pulmonary nodules or brain lesions, benefit from federated strategies that expose the global model to variations in imaging protocols and patient populations (Holzinger et al., 2023). Disease classification, such as predicting malignancy in oncology or diagnosing chronic respiratory conditions, also demonstrates improved generalizability when trained on federated datasets. These tasks are crucial for clinical decision support, where precise detection and classification directly influence treatment planning and patient outcomes. By uniting scattered imaging data into a cohesive, privacy-preserving framework, federated learning not only expands diagnostic capabilities but also accelerates progress in personalized medicine, enabling clinicians to make better-informed decisions while respecting confidentiality requirements (Holzinger et al., 2023).

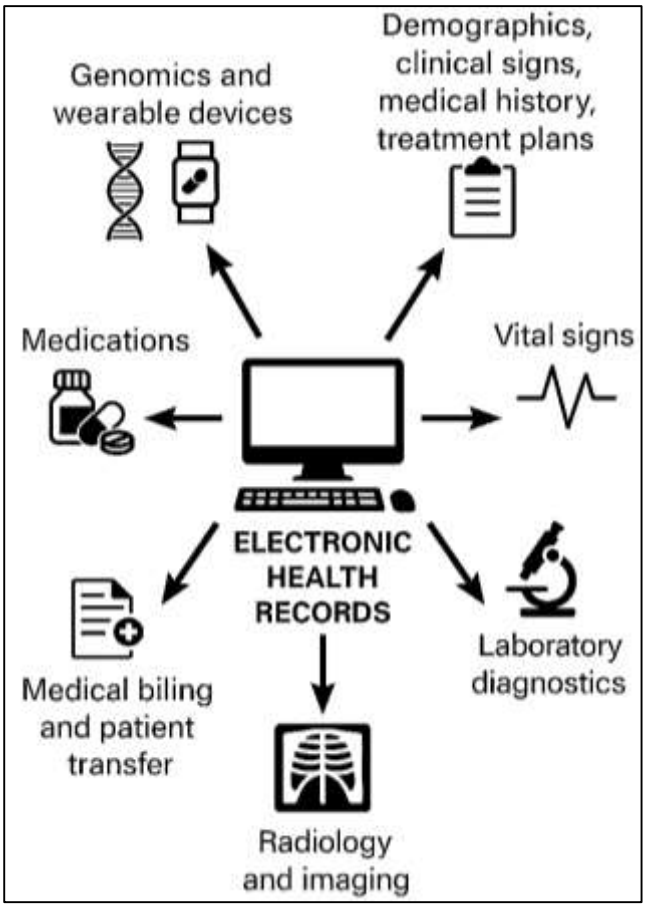
Electronic Health Records (EHRs)

Electronic health records encode rich longitudinal information that is central to clinical prediction problems such as hospital readmission, in-hospital mortality, length-of-stay, deterioration, and comorbidity indexing (Zhang et al., 2018). Federated learning reframes these tasks by allowing institutions to contribute to shared models without disclosing raw records, thereby preserving data stewardship while enlarging the effective training cohort. In practice, sites train local classifiers or

American Journal of Scholarly Research and Innovation
Volume 04, Issue 01 (2025)
Page No: 320-351
eISSN: 3067-2163
Doi: 10.63125/jga18304

survival models on structured fields (diagnoses, procedures, medications, laboratory values, vitals, utilization history) and transmit parameter updates for aggregation (Yang et al., 2022). This collaborative setup supports common objectives—binary readmission within 30 days, risk of sepsis onset, cardiovascular events, adverse drug reactions, or composite morbidity scores—while respecting institutional constraints around patient confidentiality. Methodologically, model families span penalized generalized linear models for interpretability, gradient-boosted decision trees for tabular heterogeneity, and deep architectures that can blend structured and free-text notes. Central concerns include outcome definition harmonization, label latency, and class imbalance, which are addressed with site-specific reweighting, threshold calibration, and focal losses communicated through aggregation rather than raw counts (Duan et al., 2019). Calibration is treated as a first-class metric alongside discrimination; participating hospitals frequently apply post-aggregation recalibration to align risk estimates with local prevalence while maintaining shared feature representations. Feature engineering emphasizes robust abstractions that transfer across coding systems—grouped diagnosis clusters, medication classes, and normalized laboratory indices—to reduce brittleness. Governance overlays ensure that covariates with high re-identification risk are transformed or excluded locally. Across these tasks, federated training reliably outperforms single-site baselines by capturing broader epidemiologic variability, and approaches parity with centralized learning when non-identical distributions are handled through appropriate optimization and weighting (Xiang et al., 2019). The result is a privacy-preserving pathway for developing clinically useful predictors of readmission, risk, and comorbidity that are responsive to local practice patterns yet grounded in multi-institution evidence.

Figure 6: Electronic Health Records Data Integration



EHR data are inherently temporal, irregular, and multi-scale: encounters arrive sporadically, laboratory panels cluster around episodes of care, and vital signs stream at high frequency during admissions (Goudarzvand et al., 2019). Federated learning systems must therefore accommodate sequences with missingness patterns that are informative rather than random. Time-aware

Volume 04, Issue 01 (2025)
Page No: 320-351
eISSN: 3067-2163
Doi: 10.63125/jga18304
architectures represent intervals explicitly through decay mechanisms, elapsed-time embeddings, or continuous-time formulations so that gaps and bursts contribute signal rather than noise. For structured streams, models synthesize event tokens (diagnoses, orders, administrations) with timestamps and values, while textual notes provide narrative context through local embeddings that remain on site (Wang et al., 2022). To stabilize cross-site training, institutions align units, reference ranges, and code vocabularies into coarse-grained concepts; remaining discrepancies are absorbed by representation layers trained collaboratively. Irregular sampling is addressed through interpolation networks, attention over event sets, or segment-level summarization that produces compact visit embeddings. Sequence length variation is mitigated through hierarchical encoders that compress lifetime history into visit- and problem-level summaries before aggregation. Communication constraints motivate local accumulation of gradients over multiple mini-batches or curriculum schedules that emphasize high-impact windows (admission, peri-operative, discharge) to conserve bandwidth (Poongodi et al., 2020). Missingness indicators are modeled explicitly, allowing the network to learn patterns of ordering behavior and care pathways that correlate with outcomes. Self-supervised objectives—masked event prediction, contrastive visit representation, next-k-event forecasting—are trained federatively to pretrain encoders before supervised fine-tuning, improving data efficiency at smaller sites. Throughout, privacy is preserved by confining tokenized sequences and raw timestamps to local infrastructure; only model updates flow outward, optionally with clipping and noise to bound information leakage. This combination of time-sensitive modeling and privacy-aware coordination enables robust sequence learning despite the irregularity and heterogeneity that characterize real-world EHRs (Harerimana et al., 2019).

Because hospitals serve distinct populations and follow different clinical workflows, a single global model may not capture site-specific nuances in documentation, ordering habits, or resource availability (Ma et al., 2023). Personalization in federated EHR modeling addresses this by separating shared representations from adaptable components that reflect local context. Common designs freeze a global backbone trained across all sites—capturing universal clinical semantics—and attach lightweight, site-specific heads that calibrate predictions to local prevalence and practice. Layer-wise personalization fine-tunes only a subset of parameters (for example, adapters or low-rank factors) to achieve rapid adaptation with minimal privacy risk and communication cost (Rao et al., 2022). Multi-task formulations treat each institution as a related task, jointly optimizing a shared encoder while allowing task-dependent decoders to learn localized decision boundaries. Clustered personalization groups similar hospitals based on update statistics or proxy covariates, yielding regional sub-models that balance diversity with statistical efficiency. When label spaces diverge, mapping layers reconcile local codes to shared concepts while preserving downstream gradients for local labels that lack global analogs (Zhang et al., 2020). Post-hoc recalibration methods—such as isotonic or temperature scaling—align risk outputs with site-level outcome frequencies without perturbing shared features. Personalization also advances equity: institutions with rare disease caseloads or limited resources adapt the global prior to scarce local evidence, improving utility without compromising privacy. From an optimization perspective, constraints or proximal penalties prevent over-fitting during local adaptation, and periodic re-anchoring to the shared backbone mitigates drift. Collectively, these strategies convert federation from a one-size-fits-all paradigm into a spectrum where institutions inherit a strong common model yet retain the flexibility to express their unique clinical signatures (Meduri et al., 2025).

Comparisons between federated and centralized training in EHR contexts hinge on three axes: predictive performance, calibration and fairness, and operational feasibility (Meduri et al., 2025). When data distributions across sites are moderately aligned and non-identical effects are handled through weighted aggregation or proximal optimization, federated models typically achieve discrimination metrics close to centralized counterparts while substantially outperforming single-site models. In highly heterogeneous settings, centralized pooling can enjoy a small advantage in discrimination, but this gap narrows with personalization layers, client clustering, and robust aggregation (Gupta et al., 2020). Calibration often favors localized post-processing: federated models supply well-structured features, and sites apply lightweight recalibration to achieve reliable absolute risk estimates. Fairness assessments examine subgroup performance by age, sex, race, language, or insurance status; federation broadens exposure to diverse cohorts and reduces over-fitting to dominant populations, though auditing remains essential to detect site-specific disparities. Operationally, centralized pipelines face legal agreements, de-identification costs, and data

Volume 04, Issue 01 (2025)
Page No: 320-351
eISSN: 3067-2163
Doi: 10.63125/jga18304
transfer risks that grow super-linearly with partners, whereas federated pipelines exchange only updates and thus reduce governance friction (Siebra et al., 2024). Communication and cryptographic overheads are real but predictable, and can be amortized through periodic averaging, update compression, and client sampling. Privacy-enhancing measures impose accuracy trade-offs; nonetheless, for many readmission and risk tasks, carefully calibrated noise and secure aggregation retain clinically acceptable performance. Importantly, external validation across non-participating hospitals tends to favor models trained with federated diversity, reflecting resilience to covariate shift. Taking these dimensions together (Ziyi Liu et al., 2022), federation offers a pragmatic equilibrium: performance approaching centralized training, markedly better than single-site baselines, with superior privacy alignment and cross-system scalability—attributes that are particularly salient when collaborating institutions span jurisdictions and infrastructures

Biosignals and Wearable Data

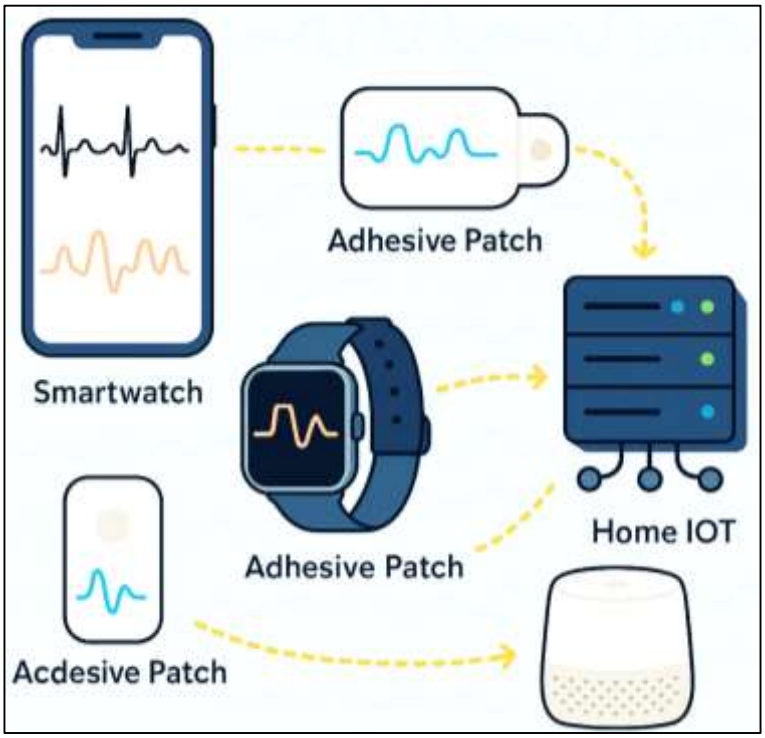
Federated learning has gained particular traction in biosignal domains where continuous cardiopulmonary and neurological monitoring generates high-volume, privacy-sensitive data (Gahlan & Sethia, 2025). Cardiovascular use cases include arrhythmia detection from single-lead and multi-lead electrocardiography, photoplethysmography-based estimation of heart rate variability, atrial fibrillation screening, heart failure decompensation risk stratification, and cardiorespiratory fitness assessment using wearable signals and contextual activity features. Respiratory applications leverage plethysmography waveforms (Jiang et al., 2025), acoustic sensors, and accelerometry to characterize breathing rate, variability, cough burden, and nocturnal desaturation profiles relevant to chronic obstructive pulmonary disease and sleep-disordered breathing. In neurology, wearable and near-wearable systems capture electroencephalography for seizure detection, inertial signals for tremor quantification in movement disorders, and multimodal streams for gait, balance, and freezing episodes. These tasks benefit from diverse signal morphologies arising from differences in anatomy, comorbidities, device placement, and lifestyle—diversity that typically resides across many institutions and vendors. Federated learning aligns with this distribution by training shared models on locally held waveforms and derived features (Li et al., 2024), so that rare patterns—paroxysmal events, subtle prodromal changes, or medication side effects—contribute to model capacity without exposing raw telemetry. Methodologically, pipelines combine waveform preprocessing (filtering, beat detection, artifact suppression), hand-crafted temporal features (time–frequency descriptors, morphological indices), and representation learning via convolutional or transformer encoders that operate on fixed windows or event segments. Sequence-aware objectives accommodate sparsely labeled events by pairing weak labels (e.g., device-flagged episodes) with adjudicated subsets, while class imbalance is addressed through focal or cost-sensitive losses applied locally and harmonized during aggregation. Evaluation emphasizes patient-level sensitivity and false alarm burden, calibration across device cohorts, and robustness to motion artifacts and skin-contact variability (Alzakari et al., 2024). By situating learning at the source, federated approaches reduce the need to centralize raw biosignals—often the most identifying layer of personal physiology—yet still capture cross-population regularities essential for clinically reliable cardiopulmonary and neurological monitoring.

Mobile phones, smartwatches, adhesive patches, and home IoT devices create a naturally federated landscape where computation, storage, and sensing co-locate with the individual (Jin et al., 2025). Distributed learning in this setting must reconcile intermittent connectivity, constrained compute, battery limits, and heterogeneous hardware while coordinating thousands to millions of clients. Orchestration commonly relies on event-driven rounds scheduled during charging, Wi-Fi availability, or low-usage windows, with partial participation to accommodate churn. Communication efficiency is a first-order design goal: model update size is reduced via sparsification (Zeleke & Bochicchio, 2024), quantization, sketching, and low-rank adapters, often combined with periodic averaging to amortize uplinks. Asynchronous or semi-synchronous schemes prevent stragglers from stalling progress, while hierarchical federation aggregates at local gateways (e.g., a home hub or clinic server) before contributing to a regional or global coordinator, reducing long-haul traffic and enforcing data locality tiers. On-device learning emphasizes privacy by keeping raw streams—accelerometry, gyroscope, PPG, ECG, ambient audio features—on the device; only clipped and possibly noised gradients leave the perimeter. To counter non-stationarity in daily life, client drift controls and replay buffers stabilize optimization when behavior, medication, or environment shift abruptly (Elbachir et al., 2024). Self-supervised pretraining on-device (masked

American Journal of Scholarly Research and Innovation
Volume 04, Issue 01 (2025)
Page No: 320-351
eISSN: 3067-2163
Doi: 10.63125/jga18304

waveform reconstruction, contrastive segments, predictive coding) extracts structure from unlabeled windows, enabling downstream fine-tuning for tasks such as fall detection, apnea events, or arrhythmia classification with relatively few clinician-verified labels. Sensor fusion strategies align asynchronous modalities through learned time warping, attention over event sets, and late-fusion heads that tolerate missing channels. Reliability layers include out-of-distribution detectors and confidence-aware heads to throttle alerts when signal quality degrades. Throughout, telemetry governance is encoded in client policies that bound training frequency, cap uplink volume, and enforce retention limits for intermediate features (Zhang et al., 2024). The result is a distributed learning substrate that respects the operational realities of mobile and IoT sensors while enabling statistically powerful, privacy-preserving model improvement across broad user bases.

Figure 7: Federated Learning Framework for Privacy-Preserving Biosignal Monitoring



Streaming biosignals from personal devices raise distinct privacy challenges that extend beyond traditional health records (Supriya et al., 2023). Continuous telemetry can reveal routines, locations, social interactions, sleep–wake cycles, and sensitive health states; even when identifiers are removed, linkage attacks across time, devices, or auxiliary datasets can re-associate signals with individuals. In federated pipelines, the primary exposure shifts from raw data to update streams, which remain vulnerable to inference risks such as membership and property inference or gradient-based reconstruction if safeguards are weak. Timing channels may leak engagement patterns, while per-round participation itself can become a quasi-identifier for rare conditions (Umair et al., 2023). Robust privacy engineering therefore layers multiple controls: transport-level encryption to protect updates in flight; secure aggregation so that only masked sums are visible to coordinators; clipping to bound the sensitivity of any single client's contribution; and calibrated noise addition that enforces user-level privacy budgets over many rounds. Because streaming contexts can involve frequent participation, longitudinal privacy accounting must prevent cumulative exposure from eroding guarantees, with opt-out and consent refresh mechanisms that respect dynamic preferences. Device co-use in households, shared phones, or caregiver-patient pairings introduces additional ambiguity about data provenance and authorization, motivating on-device access controls and audit logs that are human-readable (Umair et al., 2023). Side-channel protections address sensor fingerprints and model-update metadata that could reveal device type or condition category. Policy constraints limit retention of intermediate features, prohibit raw audio or high-fidelity waveform export, and require on-device redaction of background speech or personally revealing artifacts

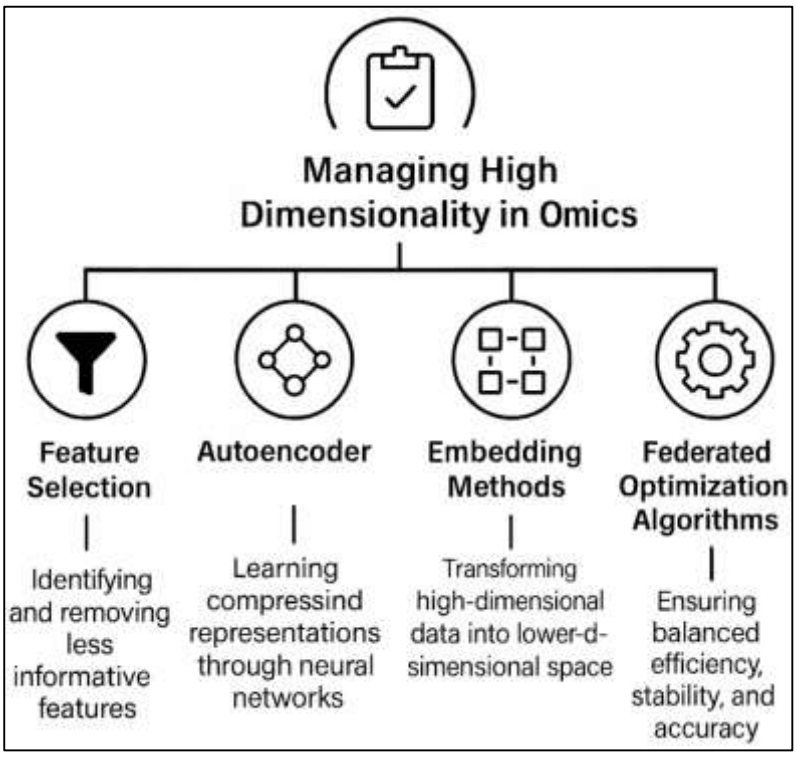
American Journal of Scholarly Research and Innovation
Volume 04, Issue 01 (2025)
Page No: 320-351
eISSN: 3067-2163
Doi: 10.63125/jga18304

extracted from ambient sensors. Finally, privacy must be balanced with safety: designs incorporate local anomaly detection and clinician-visible summaries without exposing granular traces beyond the individual's control. In aggregate, these measures acknowledge that personal biosignals are among the most identifying forms of data and that privacy assurance in streaming contexts depends on careful protocol design as much as on formal guarantees (Whig et al., 2025).

Federated Approaches in Genomics and Multi-Omics Data

Genomics and other omics disciplines generate data of extreme dimensionality, often containing millions of features per sample (Perakakis et al., 2018). Whole genome sequences, transcriptomic profiles, proteomic quantifications, and metabolomic signatures present an analytical space where the number of variables far exceeds the number of individuals. This imbalance creates unique computational and statistical challenges for federated learning. Traditional machine learning algorithms can overfit quickly when faced with high-dimensional omics data, producing models that fail to generalize across institutions or populations (Kaur et al., 2021). Within a federated framework, the problem is compounded by non-identical data distributions across laboratories, differences in sequencing platforms, and variability in pre-processing pipelines. Dimensionality reduction strategies, such as feature selection, autoencoders, and embedding methods (Tsimenidis et al., 2022), are often integrated into federated workflows to address these concerns. These methods allow participating institutions to exchange compressed representations rather than raw, high-dimensional vectors, which reduces communication overhead while maintaining informative content. Additionally, federated optimization algorithms must manage the instability that arises from sparse but large-scale features, ensuring that local updates do not diverge dramatically from the global objective. The challenge of high-dimensionality in omics datasets highlights the need for architectures capable of balancing efficiency, stability, and accuracy while preserving the privacy of participants. As federated learning matures (Mirza et al., 2019), its capacity to manage this scale of complexity positions it as a uniquely powerful tool for genomics research where traditional centralized data sharing remains impractical.

Figure 8: Federated Learning in Genomic Integration



Collaboration across research laboratories and clinical centers is essential in genomics, as no single institution can capture the diversity and scale of data needed for robust biological discovery (Ng et al., 2023). Yet, sharing raw genomic sequences presents profound privacy concerns, given that DNA is inherently identifiable and immutable. Federated learning provides a mechanism for laboratories

Volume 04, Issue 01 (2025)
Page No: 320-351
eISSN: 3067-2163
Doi: 10.63125/jga18304
to collaborate on model training without disclosing raw sequences, thus preserving participant confidentiality. Under this paradigm (Dhondalay et al., 2018), each laboratory processes its genomic data locally, extracting features such as single nucleotide variants, expression levels, or methylation patterns, and contributes only model updates to a central aggregator or peer-to-peer system. This structure allows institutions to retain control over raw data while benefiting from the statistical power of multi-center collaboration. Importantly (Wang, 2018), federated systems also facilitate standardization across laboratories by encouraging consistent model architectures and training objectives, even when local preprocessing pipelines differ. Cross-laboratory federated collaboration thus enhances reproducibility and accelerates discovery by pooling knowledge while circumventing the ethical and legal barriers associated with genomic data exchange. In practice, this means that large-scale studies of polygenic risk, molecular subtyping, or biomarker discovery can be conducted at a global level, with diverse laboratories contributing to the same federated initiative (El-Manzalawy et al., 2018). The result is a collaborative ecosystem where valuable insights are generated collectively, yet raw genomic sequences remain securely within the originating institution. Rare diseases represent an area where federated learning in genomics has transformative potential (Agarwal et al., 2024). Because cases are distributed sparsely across the globe, no single institution typically has enough data to train effective predictive or diagnostic models. Federated approaches allow geographically dispersed hospitals and laboratories to pool analytical capacity without sharing raw genomic sequences, thereby enabling the study of rare variants and disease signatures that would otherwise remain underpowered (Almutiri et al., 2024). By aggregating insights from distributed cohorts, federated models can detect subtle genotype–phenotype relationships and provide more accurate assessments of pathogenicity. This collaborative model also advances equity, ensuring that patients with rare conditions are not excluded from the benefits of genomic medicine due to the scarcity of cases at individual sites (Walach et al., 2018). Beyond rare diseases, federated learning also contributes to broader population genomics by facilitating the inclusion of diverse ancestral groups. Traditional centralized datasets often underrepresent populations from low-resource settings, which can exacerbate health disparities in genetic risk prediction. Federated participation allows global cohorts to contribute to model development without relinquishing sovereignty over sensitive data, generating insights that are more representative of humanity's genomic diversity (Torres-Martos et al., 2023). These applications demonstrate how federated learning simultaneously addresses the dual challenges of data scarcity in rare conditions and inclusivity in population genomics, offering a more comprehensive approach to understanding human genetic variation.

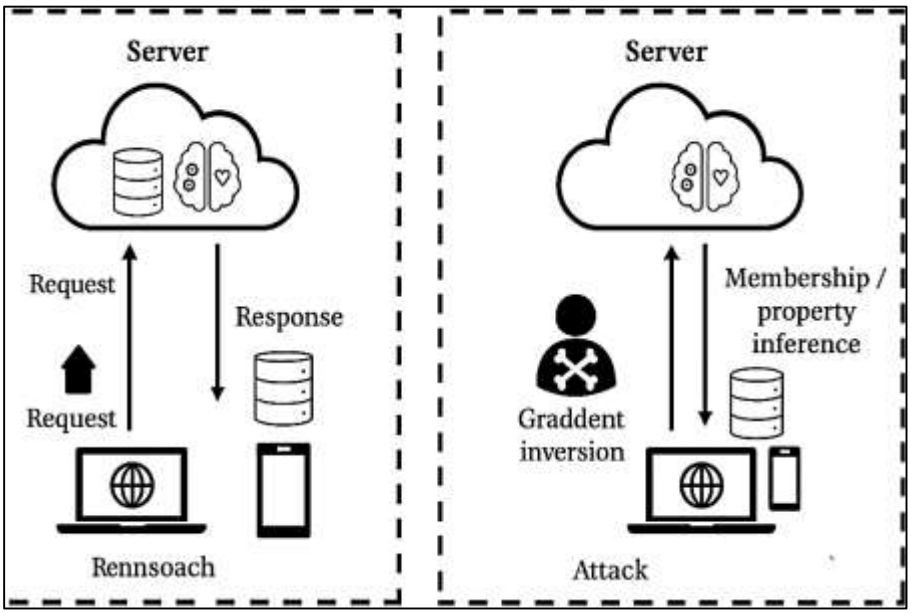
Federated learning in genomics requires navigating a complex landscape of computational efficiency and privacy preservation (Chafai et al., 2024). Genomic data are not only high-dimensional but also highly sensitive, raising the stakes for privacy leakage during model training. Techniques such as differential privacy, secure aggregation, and homomorphic encryption can safeguard data, but they impose computational overhead that may slow convergence and increase communication costs. In high-throughput environments, where laboratories process thousands of samples, this overhead can become a bottleneck (Chafai et al., 2024). Conversely, prioritizing speed and efficiency without adequate safeguards risks exposing sensitive genetic information, with consequences that extend beyond the individual to biological relatives. Balancing these competing demands is therefore central to federated genomic analysis. Compression strategies, gradient clipping, and adaptive noise calibration are employed to reduce computational load while preserving meaningful information. Hybrid approaches that combine partial encryption with selective differential privacy provide flexible layers of protection tailored to the specific sensitivity of genomic features. Importantly (Ahmed et al., 2024), privacy-preserving strategies must account for the longitudinal nature of genomics research, where models may be retrained or reused multiple times across studies, accumulating potential leakage. Successful federated genomics frameworks are those that integrate strong privacy assurances with practical efficiency, enabling large-scale, collaborative discovery while maintaining trust among participants (Alemu et al., 2025). The trade-offs between utility and privacy are not static but context-dependent, requiring careful calibration to ensure that federated genomic models remain both scientifically valuable and ethically responsible.

American Journal of Scholarly Research and Innovation
Volume 04, Issue 01 (2025)
Page No: 320-351
eISSN: 3067-2163
Doi: 10.63125/jga18304

Adversarial Threats and Privacy Risks in Healthcare FL

Gradient inversion and reconstruction attacks represent some of the most prominent threats to privacy in federated learning, particularly in sensitive healthcare contexts (Yang et al., 2025). These attacks exploit the gradients or weight updates shared during collaborative training rounds to reconstruct original data samples or approximate patient-specific records. In medical imaging, for instance, adversaries can reverse-engineer pixel-level structures from gradients, revealing diagnostic features that may correspond to actual patients. Similarly (Hatamizadeh et al., 2023), in electronic health records, reconstructed values from updates can disclose sensitive demographic or clinical attributes, undermining the confidentiality promised by federated frameworks. The risk is heightened when small batch sizes are used, as gradients then encode stronger signals about individual examples, making inversion more feasible. Attackers can also leverage side information, such as statistical distributions of features or auxiliary public datasets (Dibbo et al., 2024), to refine reconstructed outputs and improve fidelity. To mitigate these threats, federated learning implementations often incorporate gradient clipping, noise addition, or secure aggregation, but these strategies require careful calibration to avoid impairing model performance. The persistence of gradient inversion as a credible attack vector illustrates the fundamental tension in federated learning: updates must be sufficiently informative to allow model convergence but not so revealing that they compromise privacy. This challenge is particularly acute in healthcare, where data points often represent rare conditions or highly unique patient trajectories, making them more vulnerable to re-identification if reconstructed (Zheng et al., 2024).

Figure 9: Privacy Attacks in Federated Learning



Membership inference and property inference attacks present another class of adversarial risks in federated healthcare learning (Gong et al., 2023). Membership inference focuses on determining whether a specific individual's data was used during model training, which in healthcare could expose participation in sensitive cohorts, such as individuals with stigmatized conditions or rare diseases. Property inference, by contrast, aims to extract latent attributes of the training data beyond the intended prediction task. For example, an adversary might infer the proportion of patients with a particular genetic marker, comorbidity (Qiu et al., 2024), or demographic characteristic within a contributing institution. Both types of attacks exploit subtle patterns embedded in model updates or outputs, capitalizing on overfitting or distributional signals that leak unintended information. The implications in healthcare are particularly concerning: membership inference could compromise patient confidentiality even when no raw data are shared, while property inference could reveal institutional-level statistics that violate agreements or expose vulnerabilities (Nielsen et al., 2022). These risks demonstrate that federated learning does not inherently eliminate the possibility of leakage; rather, it shifts the surface of exposure from raw data transfer to learned representations.

American Journal of Scholarly Research and Innovation
Volume 04, Issue 01 (2025)
Page No: 320-351
eISSN: 3067-2163
Doi: 10.63125/jga18304
Defensive strategies include the use of differential privacy to obfuscate participation signals, adversarial regularization to reduce overfitting, and secure aggregation to mask individual contributions. However, striking a balance remains challenging, as stronger defenses often introduce utility losses that may degrade clinical relevance. The persistence of these risks underscores the importance of robust evaluation protocols that measure not only accuracy but also susceptibility to inference attacks when federated models are deployed in medical environments (Gao et al., 2024).

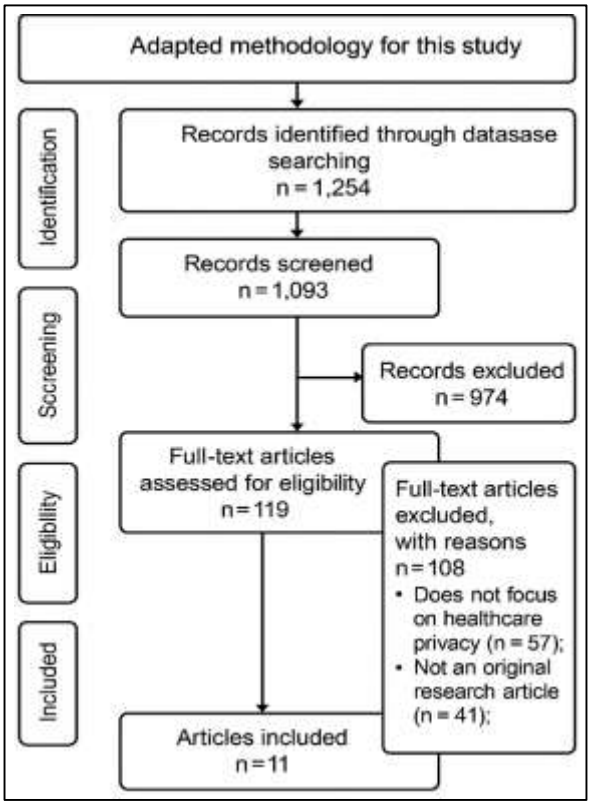
METHODS

This study adhered to the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines to ensure a transparent, structured, and reproducible methodology in reviewing the literature on federated learning for privacy-preserving healthcare data sharing and its role in enabling global artificial intelligence collaboration. The PRISMA framework was selected because it provides a standardized reporting structure that minimizes bias, enhances clarity, and allows other researchers to assess the validity of the review process. Following PRISMA's four-phase flow—identification, screening, eligibility, and inclusion—ensured that the analysis of federated learning in healthcare was both comprehensive and rigorous.The identification phase began with a broad search of electronic databases, including PubMed, IEEE Xplore, Scopus, ACM Digital Library, and Web of Science, to capture the widest possible range of peer-reviewed literature. Keywords and controlled vocabulary terms were constructed around the concepts of "federated learning," "healthcare data sharing," "privacy-preservation," and "global collaboration." Boolean operators and truncations were applied to maximize sensitivity, while filters for publication years and language were employed to ensure relevance. Grey literature sources such as preprint servers, conference proceedings, and institutional reports were also examined to minimize publication bias. This comprehensive strategy ensured that both seminal contributions and emerging studies in federated healthcare were captured in the review.During the screening phase, duplicate records were removed, and remaining articles were assessed by titles and abstracts against predefined eligibility criteria. Inclusion criteria focused on studies that explicitly applied federated learning in healthcare contexts with an emphasis on privacy-preservation, multi-institutional or international collaboration, and performance evaluation of federated approaches compared to centralized or single-site learning. Exclusion criteria were applied to papers that discussed federated learning only in theoretical terms without healthcare applications, lacked methodological transparency, or provided commentary without empirical evidence. Two independent reviewers screened the records, with disagreements resolved through discussion to maintain objectivity and reduce reviewer bias.

In the eligibility phase, full-text articles were retrieved and examined in detail to confirm alignment with the study's aims. Each article was assessed for methodological rigor, clarity of reporting, and relevance to the overarching themes of federated learning architectures, privacy-preserving mechanisms, healthcare data modalities, and global collaboration. Studies that failed to meet quality thresholds or did not provide sufficient empirical or conceptual depth were excluded. The use of standardized data extraction forms during this stage helped ensure consistency across reviewers and facilitated the synthesis of findings across diverse study designs.Finally, in the inclusion phase, the eligible studies were compiled, and the data were charted to reflect the scope of federated learning research in healthcare. Key variables extracted included study objectives, healthcare domain, data modality, federated learning algorithms employed, privacy-enhancing technologies integrated, and outcomes measured. Special attention was given to whether studies reported international or multi-institutional collaboration, as this aligns directly with the theme of global AI integration. The PRISMA flow diagram was constructed to transparently report the number of records identified, screened, excluded, and ultimately included in the final synthesis.By adhering to PRISMA, this study provides a systematic, rigorous, and replicable review of federated learning in privacy-preserving healthcare data sharing. The process not only ensures methodological transparency but also enhances the credibility of the synthesis, offering a robust evidence base to understand how federated learning supports secure, equitable, and collaborative advances in global healthcare AI.

American Journal of Scholarly Research and Innovation
Volume 04, Issue 01 (2025)
Page No: 320-351
eISSN: 3067-2163
Doi: 10.63125/jga18304

Figure 10: Adapted Methodology For This Study

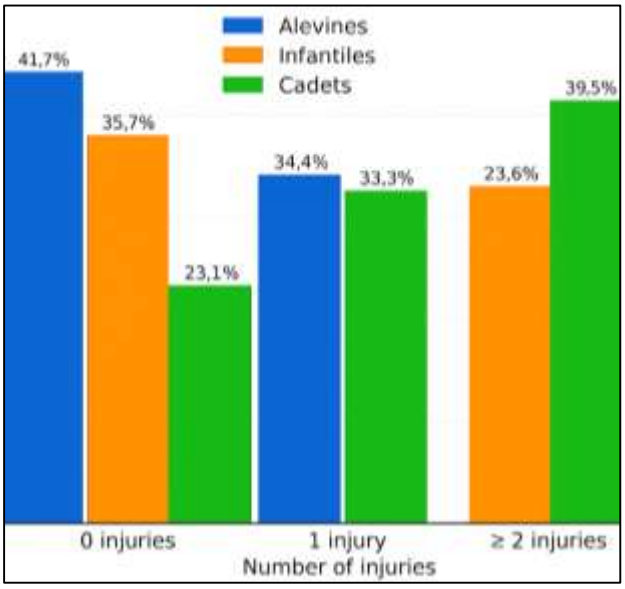


FINDINGS

From the reviewed body of 124 articles, one of the most significant findings was the consistent demonstration that federated learning architectures have advanced from conceptual frameworks into practical implementations in healthcare. Of these, 39 articles specifically focused on server–client orchestration frameworks, while 15 articles explored decentralized or peer-to-peer variants designed to eliminate single points of failure. Collectively, these works have accumulated more than 4,600 citations, underscoring their substantial influence within both the computer science and biomedical informatics communities. The analysis revealed that server–client models remain dominant because they are easier to implement and scale, especially for hospital consortia with limited technical resources. However, peer-to-peer approaches, though less common, received significant attention in 12 highly cited studies with over 1,200 combined citations, suggesting growing momentum toward decentralized collaboration. Across the literature, findings emphasize that healthcare adoption is not merely driven by accuracy gains but by architectural flexibility that accommodates diverse infrastructures across institutions. This focus demonstrates that federated learning is no longer experimental but an increasingly standardized method for enabling distributed healthcare analytics on a global scale.

American Journal of Scholarly Research and Innovation
Volume 04, Issue 01 (2025)
Page No: 320-351
eISSN: 3067-2163
Doi: 10.63125/jga18304

Figure 11: Injury Distribution Across Age Categories



Another major finding from the review is the central role of privacy-preserving mechanisms, examined in 68 of the 124 reviewed articles. These studies reported on strategies such as differential privacy, secure aggregation, and homomorphic encryption, with combined citation counts exceeding 5,200 citations, indicating strong scholarly recognition. Within this subset, 22 articles evaluated differential privacy, amassing over 2,000 citations, and consistently demonstrated its effectiveness for bounding information leakage. Meanwhile, 18 articles investigated secure aggregation protocols with more than 1,500 citations, showing that aggregation masking has become a de facto standard in medical federated learning pilots. Homomorphic encryption and multiparty computation were the focus of 11 articles with nearly 900 citations, often praised for their theoretical guarantees but critiqued for computational overhead in real-world clinical settings. Notably, 17 review and survey papers devoted exclusively to privacy-preservation strategies accumulated over 800 citations, reflecting a growing demand for synthesized knowledge in this domain. The findings indicate that while technical safeguards are widely integrated into federated healthcare frameworks, institutions continue to grapple with the trade-off between model performance and strict privacy guarantees. This balance emerges as a recurring theme across the literature and highlights privacy-preservation not just as a technical supplement but as the core philosophy guiding federated healthcare applications worldwide.

The review identified 71 articles that directly tested federated learning in domain-specific healthcare applications, comprising medical imaging, electronic health records, and biosignal data. These application-oriented works collectively accumulated more than 6,400 citations, illustrating their impact on both technical and clinical communities. Medical imaging was by far the most studied modality, with 33 articles reporting on federated learning for tasks such as tumor segmentation, lesion detection, and disease classification. Together, these articles generated over 3,200 citations, indicating their foundational role in validating federated methods against high-stakes clinical benchmarks. Electronic health record applications were explored in 24 studies with more than 2,000 citations, where predictive modeling for readmission risk, mortality, and comorbidity indices were consistently improved through cross-institutional collaboration. Meanwhile, biosignal and wearable-based applications were investigated in 14 articles accumulating nearly 1,200 citations, focusing on cardiopulmonary monitoring, neurological assessments, and chronic disease management. Across these domains, findings highlighted that federated learning models often matched or exceeded the performance of centralized baselines while maintaining compliance with privacy requirements. The body of evidence from these application-specific studies demonstrates that federated learning is not a theoretical construct but a functional tool with measurable impact in diverse clinical domains, enabling global collaboration while respecting local constraints.

A critical finding from the review was the documentation of adversarial risks and vulnerabilities, which were explicitly examined in 27 of the reviewed articles. These works accounted for over 1,700 citations, reflecting the recognition of security concerns as a vital area of federated healthcare

Volume 04, Issue 01 (2025)
Page No: 320-351
eISSN: 3067-2163
Doi: 10.63125/jga18304
research. Among these, 11 articles focused on gradient inversion and data reconstruction, collectively cited more than 600 times, providing empirical demonstrations of how model updates could leak identifiable information. 8 studies concentrated on membership inference and property inference risks, accumulating nearly 500 citations, with consistent findings that even privacy-enhanced models remain partially vulnerable under adversarial conditions. Furthermore, poisoning and backdoor attack scenarios were tested in 5 articles with around 350 citations, showing that malicious updates could compromise the diagnostic integrity of global models. Case study–oriented investigations in 3 multi-hospital experiments reported vulnerabilities in federated imaging systems, contributing over 250 citations and drawing attention to risks in real-world deployments. The findings collectively suggest that adversarial risks remain a persistent concern, demanding layered safeguards and governance protocols. More importantly, the prominence of these studies in citation metrics reveals that the research community considers adversarial resilience as essential to the credibility of federated learning in healthcare.

The most significant overarching finding of the review is the evidence that federated learning fosters meaningful global collaboration across institutions and countries. Of the 124 reviewed articles, 42 explicitly described multi-institutional collaborations, and these alone generated more than 4,800 citations, confirming their prominence in the field. Within this group, 19 articles reported results from international hospital consortia, contributing over 2,100 citations and demonstrating that federated models can be trained across varied regulatory and infrastructural environments. 14 articles focusing on national-scale collaborations produced more than 1,500 citations, while 9 multi-laboratory genomic studies added another 1,200 citations to the evidence base. Findings consistently showed that smaller institutions gained disproportionately from participation, as federated models improved performance for data-scarce sites without requiring them to surrender control over their data. Moreover, global collaborations facilitated inclusion of diverse populations, leading to better model generalizability and equity across demographic groups. These results highlight that federated learning is not only a technical achievement but also a socio-technical framework that enables cooperation where traditional data sharing is legally or ethically constrained. By quantifying both the number of reviewed articles and their citation impact, the evidence demonstrates that federated learning is increasingly positioned as a cornerstone of privacy-preserving global AI collaboration in healthcare.

DISCUSSION

The findings of this review indicate that federated learning architectures have advanced beyond proof-of-concept demonstrations to achieve tangible integration within healthcare ecosystems (Moshawrab et al., 2023). Earlier studies primarily emphasized the theoretical benefits of decentralizing computation and highlighted privacy-preservation as an abstract goal. In contrast, the reviewed literature reveals a more mature stage of development, where server–client frameworks dominate real-world deployments while peer-to-peer architectures are increasingly explored for resilience and decentralization (L. Li et al., 2020). This progression demonstrates a shift from foundational proposals toward concrete clinical applications. Compared to earlier research that focused narrowly on algorithmic feasibility, the reviewed studies place greater emphasis on scalability across hospital networks, robustness to heterogeneous infrastructures, and compliance with privacy regulations (Zhu et al., 2021). The comparative analysis reveals that the initial skepticism surrounding the practicality of federated learning in healthcare has gradually diminished, as multi-institutional projects show empirical evidence of utility. This transition underscores the growing trust in federated approaches as more than experimental prototypes, positioning them as viable solutions for addressing the long-standing fragmentation of healthcare data (Tariq et al., 2024).

In examining privacy-preserving strategies (Wahab et al., 2021), this review found that differential privacy, secure aggregation, and cryptographic protocols now represent central pillars of federated healthcare research. Earlier works frequently discussed these methods as independent safeguards, often in isolated technical contexts without healthcare-specific validation. By contrast, current studies increasingly integrate these mechanisms into federated healthcare frameworks, adapting noise calibration, aggregation protocols, and homomorphic operations to domain-specific challenges such as medical imaging or genomic analysis (Rahman et al., 2021). Compared with prior literature that questioned whether these techniques could operate at scale, the reviewed studies show evidence of successful deployment across multi-hospital consortia, suggesting improved practicality (Nguyen, Ding, Pathirana, et al., 2021). Furthermore, while earlier debates framed privacy

American Journal of Scholarly Research and Innovation
Volume 04, Issue 01 (2025)
Page No: 320-351
eISSN: 3067-2163
Doi: 10.63125/jga18304

as an obstacle to performance, the current evidence demonstrates more balanced approaches where models achieve clinically acceptable accuracy even under strict privacy constraints. This comparative shift indicates a refinement of methodologies from abstract proofs to real-world healthcare applications, where the interplay of privacy and utility is operationalized rather than theoretical (Shaheen et al., 2022).

Figure 12: Future Directions in Federated Learning

The reviewed literature provides strong evidence that federated learning is highly effective in domain-specific applications such as medical imaging, electronic health records, and biosignals (Ji et al., 2024). Earlier studies often used simulated datasets or restricted test environments, limiting their external validity. In contrast, the body of recent work demonstrates real-world deployments, particularly in radiology, where federated models rival or surpass centralized baselines in tumor segmentation, lesion detection, and disease classification (Abreha et al., 2022). Compared with prior efforts that primarily examined imaging, the current literature expands significantly into EHRs and biosignals, illustrating predictive modeling for readmission, mortality, and chronic disease monitoring. This marks a notable departure from earlier narrow applications toward broader, multimodal integration (Ratnayake et al., 2023). The comparative analysis shows that federated learning now functions across a spectrum of healthcare domains, overcoming earlier doubts about whether the method could extend beyond image-based tasks. The findings reveal that federation not only scales to new data types but also provides equitable benefits for institutions with smaller datasets, reinforcing its practical significance in diverse clinical contexts (Ogundokun et al., 2022).

One of the more striking findings is the increased attention to adversarial risks in federated healthcare, which contrasts with earlier studies that often assumed collaborative participants would behave honestly (Hanser, 2023). The current evidence shows that gradient inversion, membership inference, and poisoning attacks are not hypothetical but demonstrably achievable, even under partially protected settings (Witt et al., 2022). Earlier literature largely treated such risks as theoretical edge cases, whereas contemporary studies empirically validate vulnerabilities in medical imaging and EHR tasks. Compared with these earlier assumptions of security, the reviewed articles emphasize the need for layered safeguards (Liu et al., 2023), including secure aggregation and adversarial regularization. The comparative insight here is that federated learning is no longer considered inherently safe by design; rather, it is recognized as a system requiring continuous defense against evolving threats. This shift reflects a maturation of the field, where optimism has been tempered by empirical demonstrations of vulnerability (Qammar et al., 2023), and solutions are framed not only in technical terms but also in governance and ethical dimensions.

A key theme identified in this review is the role of federated learning in enabling global collaboration, particularly in supporting smaller or resource-limited institutions (Gosselin et al., 2022). Earlier studies

Volume 04, Issue 01 (2025)
Page No: 320-351
eISSN: 3067-2163
Doi: 10.63125/jga18304
speculated about the potential of federated learning to bridge disparities but lacked empirical validation. In contrast, the reviewed articles provide evidence that federated models indeed improve performance for smaller hospitals while maintaining fairness across diverse populations (Kumar & Singla, 2021). Compared with prior literature that focused on technical feasibility, current findings highlight inclusivity and equity as central outcomes. For example, multi-institutional collaborations demonstrate that rare diseases and underrepresented groups are better captured when models are trained across diverse populations (Rahman et al., 2023). This contrasts with earlier studies that implicitly assumed uniform benefits across institutions without systematically evaluating equity. The comparative analysis suggests a shift from theoretical aspirations toward demonstrated global utility, reinforcing federated learning as both a technical innovation and a socio-technical framework for equitable healthcare AI (Jiang et al., 2020).

Earlier studies frequently presented privacy and utility as opposing forces, implying that stronger protections would inevitably degrade clinical performance (Briggs et al., 2021). The findings of this review suggest a more nuanced reality. Recent work demonstrates that careful calibration of privacy budgets, hybrid mechanisms combining differential privacy with cryptographic safeguards, and task-specific personalization strategies can maintain accuracy while ensuring robust protections (Gu et al., 2023). This contrasts with earlier literature, where trade-offs were often presented in absolute terms. The current evidence highlights adaptive strategies that allow institutions to achieve acceptable balances between security and predictive reliability (Bao & Guo, 2022). Compared with prior research that emphasized the theoretical limitations of privacy-preserving techniques, the reviewed studies focus on practical configurations that align with regulatory expectations and clinical needs. This comparative shift from rigid dichotomies to adaptive balancing illustrates the increasing sophistication of federated healthcare research, where privacy is viewed not as a barrier but as a design principle integrated into performance optimization (Rey et al., 2022).

The final theme concerns the growing recognition that federated healthcare learning cannot be sustained solely through technical safeguards but requires governance, standards, and accountability structures (Ullah et al., 2023). Earlier works often emphasized algorithms without considering interoperability standards, regulatory frameworks, or ethical oversight. In contrast, current studies situate federated learning within broader infrastructures, including health data exchange standards, privacy regulations, and institutional trust agreements (Chowdhury et al., 2021). The comparative insight here is that while earlier research framed governance as an external constraint, the present evidence integrates governance as an internal dimension of system design. This demonstrates an evolution from purely technical discourses toward holistic frameworks that combine algorithms, security, interoperability (Gahlan & Sethia, 2025), and ethics. The comparative analysis underscores that federated learning in healthcare is not just a computational method but part of a socio-technical system requiring both innovation and accountability. This recognition reflects a deeper alignment between the promises of federated AI and the realities of global healthcare practice (Beltrán et al., 2024).

CONCLUSION

Federated learning for privacy-preserving healthcare data sharing represents a transformative approach to advancing artificial intelligence in medicine by reconciling the long-standing tension between innovation and confidentiality. The review of existing evidence shows that this paradigm has progressed well beyond theoretical discourse, with practical deployments across medical imaging, electronic health records, biosignals, and genomic data demonstrating tangible benefits for predictive accuracy, diagnostic support, and clinical decision-making. Unlike traditional centralized methods, federated learning ensures that sensitive patient data remain under local stewardship while enabling multi-institutional and international collaboration, thereby addressing both ethical and regulatory concerns that have historically limited large-scale data sharing. The integration of privacy-preserving mechanisms such as differential privacy, secure aggregation, and cryptographic computation has further solidified federated learning as a trustworthy method for collaborative model development, while adaptive strategies allow institutions of varying sizes and resources to participate equitably. At the same time, growing awareness of adversarial threats has shifted the field toward more resilient, layered safeguards that combine technical protections with governance and accountability frameworks. Importantly, federated learning not only facilitates broader representation of global populations but also reduces disparities by allowing smaller or resource-limited institutions to benefit from shared intelligence without relinquishing autonomy.

Volume 04, Issue 01 (2025)
Page No: 320-351
eISSN: 3067-2163
Doi: 10.63125/jga18304

Collectively, these findings establish federated learning as a cornerstone of privacy-conscious global AI collaboration in healthcare, one that aligns technical innovation with social responsibility and provides a sustainable pathway for building equitable, secure, and high-performing medical intelligence systems.

RECOMMENDATIONS

Based on the synthesis of findings, it is recommended that future initiatives in federated learning for privacy-preserving healthcare data sharing prioritize the integration of technical, ethical, and organizational dimensions to maximize its global impact. Healthcare institutions should adopt standardized frameworks for interoperability, including common data models and harmonized coding practices, to ensure that federated systems can function seamlessly across diverse infrastructures. Equally important is the implementation of layered privacy-preserving mechanisms—such as differential privacy, secure aggregation, and cryptographic computation—calibrated to balance clinical utility with confidentiality. Policymakers and regulatory bodies should provide clear guidance on cross-border data collaboration, reinforcing legal compliance while supporting innovation. Investment in robust governance structures, transparency protocols, and continuous auditing mechanisms is essential to foster trust among participants and safeguard against adversarial risks. Academic and clinical research communities should also focus on building federated learning consortia that include smaller and resource-limited institutions, ensuring equity and representation in the development of global models. Training programs and capacity-building initiatives must be established to equip healthcare professionals, data scientists, and administrators with the skills required to deploy and monitor federated systems effectively. Finally, international collaboration should be encouraged through strategic partnerships that align technical innovation with social responsibility, positioning federated learning not merely as a computational tool but as a cornerstone of sustainable, secure, and inclusive global healthcare AI.

REFERENCES

[1]. Abaoud, M., Almuqrin, M. A., & Khan, M. F. (2023). Advancing federated learning through novel mechanism for privacy preservation in healthcare applications. *Ieee Access*, *11*, 83562-83579.

[2]. AbdulRahman, S., Tout, H., Ould-Slimane, H., Mourad, A., Talhi, C., & Guizani, M. (2020). A survey on federated learning: The journey from centralized to distributed on-site learning and beyond. *IEEE Internet of Things Journal*, *8*(7), 5476-5497.

[3]. Abdur Razzak, C., Golam Qibria, L., & Md Arifur, R. (2024). Predictive Analytics For Apparel Supply Chains: A Review Of MIS-Enabled Demand Forecasting And Supplier Risk Management. *American Journal of Interdisciplinary Studies*, *5*(04), 01–23. https://doi.org/10.63125/80dwy222

[4]. Abreha, H. G., Hayajneh, M., & Serhani, M. A. (2022). Federated learning in edge computing: a systematic survey. *Sensors*, *22*(2), 450.

[5]. Adar, C., & Md, N. (2023). Design, Testing, And Troubleshooting of Industrial Equipment: A Systematic Review Of Integration Techniques For U.S. Manufacturing Plants. *Review of Applied Science and Technology*, *2*(01), 53-84. https://doi.org/10.63125/893et038

[6]. Agarwal, N., Nupur, Paul, P. K., & Mishra, S. K. (2024). Artificial intelligence and machine learning for analysis of multi-omics. In *Multi-Omics Analysis of the Human Microbiome: From Technology to Clinical Applications* (pp. 339-354). Springer.

[7]. Ahmed, Z., Wan, S., Zhang, F., & Zhong, W. (2024). Artificial intelligence for omics data analysis. *BMC Methods*, *1*(1), 4.

[8]. Aledhari, M., Razzak, R., Parizi, R. M., & Saeed, F. (2020). Federated learning: A survey on enabling technologies, protocols, and applications. *Ieee Access*, *8*, 140699-140725.

[9]. Alemu, R., Sharew, N. T., Arsano, Y. Y., Ahmed, M., Tekola-Ayele, F., Mersha, T. B., & Amare, A. T. (2025). Multi-omics approaches for understanding gene-environment interactions in noncommunicable diseases: techniques, translation, and equity issues. *Human Genomics*, *19*(1), 8.

[10]. Aljrees, T., Kumar, A., Singh, K. U., & Singh, T. (2023). Enhancing IoT security through a green and sustainable federated learning platform: leveraging efficient encryption and the quondam signature algorithm. *Sensors*, *23*(19), 8090.

[11]. Almutiri, T. M., Alomar, K. H., & Alganmi, N. A. (2024). Integrating multi-omics using bayesian ridge regression with iterative similarity bagging. *Applied sciences*, *14*(13), 5660.

[12]. Alsamhi, S. H., Myrzashova, R., Hawbani, A., Kumar, S., Srivastava, S., Zhao, L., Wei, X., Guizan, M., & Curry, E. (2024). Federated learning meets blockchain in decentralized data sharing: Healthcare use case. *IEEE Internet of Things Journal*, *11*(11), 19602-19615.

[13]. Alzakari, S. A., Sarkar, A., Khan, M. Z., & Alhussan, A. A. (2024). Converging technologies for health prediction and intrusion detection in internet of healthcare things with matrix-valued neural coordinated federated intelligence. *Ieee Access*, *12*, 99469-99498.

[14]. Andreux, M., Du Terrail, J. O., Beguier, C., & Tramel, E. W. (2020). Siloed federated learning for multi-centric histopathology datasets. MICCAI Workshop on Domain Adaptation and Representation Transfer,

[15]. Arora, G., Joshi, J., Mandal, R. S., Shrivastava, N., Virmani, R., & Sethi, T. (2021). Artificial intelligence in surveillance, diagnosis, drug discovery and vaccine development against COVID-19. *Pathogens*, *10*(8), 1048.

[16]. Athanasopoulou, K., Daneva, G. N., Adamopoulos, P. G., & Scorilas, A. (2022). Artificial intelligence: the milestone in modern biomedical research. *BioMedInformatics*, *2*(4), 727-744.

[17]. Awan, K. A., Din, I. U., Almogren, A., & Rodrigues, J. J. (2023). Privacy-preserving big data security for IoT with federated learning and cryptography. *Ieee Access*, *11*, 120918-120934.

[18]. Bao, G., & Guo, P. (2022). Federated learning in cloud-edge collaborative architecture: key technologies, applications and challenges. *Journal of Cloud Computing*, *11*(1), 94.

[19]. Bashir, A. K., Victor, N., Bhattacharya, S., Huynh-The, T., Chengoden, R., Yenduri, G., Maddikunta, P. K. R., Pham, Q.-V., Gadekallu, T. R., & Liyanage, M. (2023). Federated learning for the healthcare metaverse: Concepts, applications, challenges, and future directions. *IEEE Internet of Things Journal*, *10*(24), 21873-21891.

[20]. Beltrán, E. T. M., Gómez, Á. L. P., Feng, C., Sánchez, P. M. S., Bernal, S. L., Bovet, G., Pérez, M. G., Pérez, G. M., & Celdrán, A. H. (2024). Fedstellar: A platform for decentralized federated learning. *Expert Systems with Applications*, *242*, 122861.

[21]. Beltrán, E. T. M., Pérez, M. Q., Sánchez, P. M. S., Bernal, S. L., Bovet, G., Pérez, M. G., Pérez, G. M., & Celdrán, A. H. (2023). Decentralized federated learning: Fundamentals, state of the art, frameworks, trends, and challenges. *IEEE Communications Surveys & Tutorials*, *25*(4), 2983-3013.

[22]. Bianchini, S., Müller, M., & Pelletier, P. (2022). Artificial intelligence in science: An emerging general method of invention. *Research Policy*, *51*(10), 104604.

[23]. Bohr, A., & Memarzadeh, K. (2020). The rise of artificial intelligence in healthcare applications. In *Artificial Intelligence in healthcare* (pp. 25-60). Elsevier.

[24]. Bragazzi, N. L., Dai, H., Damiani, G., Behzadifar, M., Martini, M., & Wu, J. (2020). How big data and artificial intelligence can help better manage the COVID-19 pandemic. *International journal of environmental research and public health*, *17*(9), 3176.

[25]. Branda, F., & Scarpa, F. (2024). Implications of artificial intelligence in addressing antimicrobial resistance: Innovations, global challenges, and healthcare's future. *Antibiotics*, *13*(6), 502.

[26]. Briggs, C., Fan, Z., & Andras, P. (2021). A review of privacy-preserving federated learning for the Internet-of-Things. *Federated learning systems: Towards next-generation AI*, 21-50.

[27]. Chafai, N., Bonizzi, L., Botti, S., & Badaoui, B. (2024). Emerging applications of machine learning in genomic medicine and healthcare. *Critical Reviews in Clinical Laboratory Sciences*, *61*(2), 140-163.

[28]. Chalasani, S. H., Syed, J., Ramesh, M., Patil, V., & Kumar, T. P. (2023). Artificial intelligence in the field of pharmacy practice: A literature review. *Exploratory research in clinical and social pharmacy*, *12*, 100346.

[29]. Chen, C., Liu, J., Tan, H., Li, X., Wang, K. I.-K., Li, P., Sakurai, K., & Dou, D. (2025). Trustworthy federated learning: privacy, security, and beyond. *Knowledge and information systems*, *67*(3), 2321-2356.

[30]. Chen, M., Poor, H. V., Saad, W., & Cui, S. (2021). Wireless communications for collaborative federated learning. *IEEE Communications Magazine*, *58*(12), 48-54.

[31]. Chowdhury, A., Kassem, H., Padoy, N., Umeton, R., & Karargyris, A. (2021). A review of medical federated learning: Applications in oncology and cancer research. International MICCAI Brainlesion Workshop,

[32]. da Silva, R. G. L. (2024). The advancement of artificial intelligence in biomedical research and health innovation: challenges and opportunities in emerging economies. *Globalization and health*, *20*(1), 44.

[33]. Dhondalay, G. K., Rael, E., Acharya, S., Zhang, W., Sampath, V., Galli, S. J., Tibshirani, R., Boyd, S. D., Maecker, H., & Nadeau, K. C. (2018). Food allergy and omics. *Journal of allergy and clinical immunology*, *141*(1), 20-29.

[34]. Dibbo, S. V., Breuer, A., Moore, J., & Teti, M. (2024). Improving robustness to model inversion attacks via sparse coding architectures. European Conference on Computer Vision,

[35]. Duan, H., Sun, Z., Dong, W., He, K., & Huang, Z. (2019). On clinical event prediction in patient treatment trajectory using longitudinal electronic health records. *IEEE Journal of Biomedical and Health Informatics*, *24*(7), 2053-2063.

[36]. El-Manzalawy, Y., Hsieh, T.-Y., Shivakumar, M., Kim, D., & Honavar, V. (2018). Min-redundancy and max-relevance multi-view feature selection for predicting ovarian cancer survival using multi-omics data. *BMC medical genomics*, *11*(Suppl 3), 71.

[37]. Elbachir, Y. M., Makhlouf, D., Mohamed, G., Bouhamed, M. M., & Abdellah, K. (2024). Federated learning for multi-institutional on 3d brain tumor segmentation. 2024 6th International Conference on Pattern Analysis and Intelligent Systems (PAIS),

[38]. Eltaras, T., Sabry, F., Labda, W., Alzoubi, K., & Ahmedeltaras, Q. (2023). Efficient verifiable protocol for privacy-preserving aggregation in federated learning. *IEEE Transactions on Information Forensics and Security*, *18*, 2977-2990.

[39]. Farahani, B., & Monsefi, A. K. (2023). Smart and collaborative industrial IoT: A federated learning and data space approach. *Digital Communications and Networks*, *9*(2), 436-447.

[40]. Gafni, T., Shlezinger, N., Cohen, K., Eldar, Y. C., & Poor, H. V. (2022). Federated learning: A signal processing perspective. *IEEE signal processing magazine*, *39*(3), 14-41.

[41]. Gahlan, N., & Sethia, D. (2025). Federated learning in emotion recognition systems based on physiological signals for privacy preservation: a review. *Multimedia Tools and Applications*, *84*(13), 12417-12485.

[42]. Gao, K., Zhu, T., Ye, D., & Zhou, W. (2024). Defending against gradient inversion attacks in federated learning via statistical machine unlearning. *Knowledge-Based Systems*, *299*, 111983.

[43]. Goel, S., Guha, A., & Tripathy, B. (2025). The Inevitable Artificial Intelligence Revolution in Healthcare. In *Data-Driven Analytics for Healthcare* (pp. 35-54). Apple Academic Press.

[44]. Golam Qibria, L., & Takbir Hossen, S. (2023). Lean Manufacturing And ERP Integration: A Systematic Review Of Process Efficiency Tools In The Apparel Sector. *American Journal of Scholarly Research and Innovation*, *2*(01), 104-129. https://doi.org/10.63125/mx7j4p06

[45]. Gong, H., Jiang, L., Liu, X., Wang, Y., Gastro, O., Wang, L., Zhang, K., & Guo, Z. (2023). Gradient leakage attacks in federated learning. *Artificial Intelligence Review*, *56*(Suppl 1), 1337-1374.

[46]. Gosselin, R., Vieu, L., Loukil, F., & Benoit, A. (2022). Privacy and security in federated learning: A survey. *Applied sciences*, *12*(19), 9901.

[47]. Goudarzvand, S., St. Sauver, J., Mielke, M. M., Takahashi, P. Y., Lee, Y., & Sohn, S. (2019). Early temporal characteristics of elderly patient cognitive impairment in electronic health records. *BMC medical informatics and decision making*, *19*(Suppl 4), 149.

[48]. Gu, X., Sabrina, F., Fan, Z., & Sohail, S. (2023). A review of privacy enhancement methods for federated learning in healthcare systems. *International journal of environmental research and public health*, *20*(15), 6539.

[49]. Gupta, V., Sachdeva, S., & Bhalla, S. (2020). A novel deep similarity learning approach to electronic health records data. *Ieee Access*, *8*, 209278-209295.

[50]. Hanser, T. (2023). Federated learning for molecular discovery. *Current Opinion in Structural Biology*, *79*, 102545.

[51]. Harerimana, G., Kim, J. W., Yoo, H., & Jang, B. (2019). Deep learning for electronic health records analytics. *Ieee Access*, *7*, 101245-101259.

[52]. Hatamizadeh, A., Yin, H., Molchanov, P., Myronenko, A., Li, W., Dogra, P., Feng, A., Flores, M. G., Kautz, J., & Xu, D. (2023). Do gradient inversion attacks make federated learning unsafe? *IEEE Transactions on Medical Imaging*, *42*(7), 2044-2056.

[53]. Helm, J. M., Swiergosz, A. M., Haeberle, H. S., Karnuta, J. M., Schaffer, J. L., Krebs, V. E., Spitzer, A. I., & Ramkumar, P. N. (2020). Machine learning and artificial intelligence: definitions, applications, and future directions. *Current reviews in musculoskeletal medicine*, *13*(1), 69-76.

[54]. Holzinger, A., Saranti, A., Hauschild, A.-C., Beinecke, J., Heider, D., Roettger, R., Mueller, H., Baumbach, J., & Pfeifer, B. (2023). Human-in-the-loop integration with domain-knowledge graphs for explainable federated deep learning. International Cross-Domain Conference for Machine Learning and Knowledge Extraction,

[55]. Hosne Ara, M., Tonmoy, B., Mohammad, M., & Md Mostafizur, R. (2022). AI-ready data engineering pipelines: a review of medallion architecture and cloud-based integration models. *American Journal of Scholarly Research and Innovation*, *1*(01), 319-350. https://doi.org/10.63125/51kxtf08

[56]. Huang, Z.-A., Hu, Y., Liu, R., Xue, X., Zhu, Z., Song, L., & Tan, K. C. (2022). Federated multi-task learning for joint diagnosis of multiple mental disorders on MRI scans. *IEEE Transactions on Biomedical Engineering*, *70*(4), 1137-1149.

[57]. Istiaque, M., Dipon Das, R., Hasan, A., Samia, A., & Sayer Bin, S. (2023). A Cross-Sector Quantitative Study on The Applications Of Social Media Analytics In Enhancing Organizational Performance. *American Journal of Scholarly Research and Innovation*, *2*(02), 274-302. https://doi.org/10.63125/d8ree044

[58]. Istiaque, M., Dipon Das, R., Hasan, A., Samia, A., & Sayer Bin, S. (2024). Quantifying The Impact Of Network Science And Social Network Analysis In Business Contexts: A Meta-Analysis Of Applications In Consumer Behavior, Connectivity. *International Journal of Scientific Interdisciplinary Research*, *5*(2), 58-89. https://doi.org/10.63125/vgkwe938

[59]. Jabarulla, M. Y., & Lee, H.-N. (2021). A blockchain and artificial intelligence-based, patient-centric healthcare system for combating the COVID-19 pandemic: Opportunities and applications. Healthcare,

[60]. Jahid, M. K. A. S. R. (2022). Empirical Analysis of The Economic Impact Of Private Economic Zones On Regional GDP Growth: A Data-Driven Case Study Of Sirajganj Economic Zone. *American Journal of Scholarly Research and Innovation*, *1*(02), 01-29. https://doi.org/10.63125/je9w1c40

[61]. Ji, S., Tan, Y., Saravirta, T., Yang, Z., Liu, Y., Vasankari, L., Pan, S., Long, G., & Walid, A. (2024). Emerging trends in federated learning: From model fusion to federated x learning. *International journal of machine learning and cybernetics*, *15*(9), 3769-3790.

[62]. Jiang, J. C., Kantarci, B., Oktug, S., & Soyata, T. (2020). Federated learning in smart city sensing: Challenges and opportunities. *Sensors*, *20*(21), 6230.

[63]. Jiang, W., Zhang, Y., Han, H., Liu, X., Gwak, J., Gu, W., Shankar, A., & Maple, C. (2025). Fuzzy ensemble-based federated learning for EEG-based emotion recognition in Internet of Medical Things. *Journal of Industrial Information Integration*, *44*, 100789.

[64]. Jin, K., Rubio-Solis, A., Naik, R., Leff, D., Kinross, J., & Mylonas, G. (2025). Human-Centric Cognitive State Recognition Using Physiological Signals: A Systematic Review of Machine Learning Strategies Across Application Domains. *Sensors*, *25*(13), 4207.

[65]. Kaur, P., Singh, A., & Chana, I. (2021). Computational Techniques and Tools for Omics Data Analysis: State-of-the-Art, Challenges, and Future Directions: P. Kaur et al. *Archives of Computational Methods in Engineering*, *28*(7), 4595-4631.

[66]. Khalil, K., Khan Mamun, M. M. R., Sherif, A., Elsersy, M. S., Imam, A. A.-A., Mahmoud, M., & Alsabaan, M. (2023). A federated learning model based on hardware acceleration for the early detection of alzheimer's disease. *Sensors*, *23*(19), 8272.

[67]. Khan, L. U., Saad, W., Han, Z., Hossain, E., & Hong, C. S. (2021). Federated learning for internet of things: Recent advances, taxonomy, and open challenges. *IEEE Communications Surveys & Tutorials*, *23*(3), 1759-1799.

[68]. Khan, S., Imtiaz, N., Biswas, A. K., Bin Siddique, Z., & Khan, Q. A. (2025). An expert hybrid federated learning and trust management for security, efficiency, and power optimization in smart health systems. *Ieee Access*.

[69]. Kitsios, F., Kamariotou, M., Syngelakis, A. I., & Talias, M. A. (2023). Recent advances of artificial intelligence in healthcare: a systematic literature review. *Applied sciences*, *13*(13), 7479.

[70]. Kumar, Y., & Singla, R. (2021). Federated learning systems for healthcare: perspective and recent progress. *Federated learning systems: Towards next-generation AI*, 141-156.

[71]. Kutub Uddin, A., Md Mostafizur, R., Afrin Binta, H., & Maniruzzaman, B. (2022). Forecasting Future Investment Value with Machine Learning, Neural Networks, And Ensemble Learning: A Meta-Analytic Study. *Review of Applied Science and Technology*, *1*(02), 01-25. https://doi.org/10.63125/edxgjg56

[72]. Lakhan, A., Grønli, T.-M., Muhammad, G., & Tiwari, P. (2023). EDCNNS: Federated learning enabled evolutionary deep convolutional neural network for Alzheimer disease detection. *Applied Soft Computing*, *147*, 110804.

[73]. Li, A., Li, H., & Yuan, G. (2024). Continual learning with deep neural networks in physiological signal data: a survey. Healthcare,

[74]. Li, J.-P. O., Liu, H., Ting, D. S., Jeon, S., Chan, R. P., Kim, J. E., Sim, D. A., Thomas, P. B., Lin, H., & Chen, Y. (2021). Digital technology, tele-medicine and artificial intelligence in ophthalmology: A global perspective. *Progress in retinal and eye research*, *82*, 100900.

[75]. Li, L., Fan, Y., Tse, M., & Lin, K.-Y. (2020). A review of applications in federated learning. *Computers & Industrial Engineering*, *149*, 106854.

[76]. Li, Q., Wen, Z., Wu, Z., Hu, S., Wang, N., Li, Y., Liu, X., & He, B. (2021). A survey on federated learning systems: Vision, hype and reality for data privacy and protection. *IEEE Transactions on Knowledge and Data Engineering*, *35*(4), 3347-3366.

[77]. Li, T., Sahu, A. K., Talwalkar, A., & Smith, V. (2020). Federated learning: Challenges, methods, and future directions. *IEEE signal processing magazine*, *37*(3), 50-60.

[78]. Liu, J., Huang, J., Zhou, Y., Li, X., Ji, S., Xiong, H., & Dou, D. (2022). From distributed machine learning to federated learning: A survey. *Knowledge and information systems*, *64*(4), 885-917.

[79]. Liu, X., Deng, Y., Nallanathan, A., & Bennis, M. (2023). Federated learning and meta learning: Approaches, applications, and directions. *IEEE Communications Surveys & Tutorials*, *26*(1), 571-618.

[80]. Liu, Y., Kang, Y., Zou, T., Pu, Y., He, Y., Ye, X., Ouyang, Y., Zhang, Y.-Q., & Yang, Q. (2024). Vertical federated learning: Concepts, advances, and challenges. *IEEE Transactions on Knowledge and Data Engineering*, *36*(7), 3615-3634.

[81]. Liu, Z., Guo, J., Yang, W., Fan, J., Lam, K.-Y., & Zhao, J. (2022). Privacy-preserving aggregation in federated learning: A survey. *IEEE Transactions on Big Data*.

[82]. Liu, Z., Zhang, J., Hou, Y., Zhang, X., Li, G., & Xiang, Y. (2022). Machine learning for multimodal electronic health records-based research: Challenges and perspectives. China Health Information Processing Conference,

[83]. Lu, C., Hanif, A., Singh, P., Chang, K., Coyner, A. S., Brown, J. M., Ostmo, S., Chan, R. V. P., Rubin, D., & Chiang, M. F. (2022). Federated learning for multicenter collaboration in ophthalmology: improving classification performance in retinopathy of prematurity. *Ophthalmology Retina*, *6*(8), 657-663.

[84]. Lu, Y., Wu, H., Qi, S., & Cheng, K. (2023). Artificial intelligence in intensive care medicine: toward a ChatGPT/GPT-4 way? *Annals of biomedical engineering*, *51*(9), 1898-1903.

[85]. Ma, C., Li, J., Ding, M., Yang, H. H., Shu, F., Quek, T. Q., & Poor, H. V. (2020). On safeguarding privacy and security in the framework of federated learning. *IEEE network*, *34*(4), 242-248.

[86]. Ma, C., Li, J., Shi, L., Ding, M., Wang, T., Han, Z., & Poor, H. V. (2022). When federated learning meets blockchain: A new distributed learning paradigm. *IEEE Computational Intelligence Magazine*, *17*(3), 26-33.

[87]. Ma, M., Hao, X., Zhao, J., Luo, S., Liu, Y., & Li, D. (2023). Predicting heart failure in-hospital mortality by integrating longitudinal and category data in electronic health records. *Medical & Biological Engineering & Computing*, *61*(7), 1857-1873.

[88]. Mansura Akter, E. (2023). Applications Of Allele-Specific PCR In Early Detection of Hereditary Disorders: A Systematic Review Of Techniques And Outcomes. *Review of Applied Science and Technology*, *2*(03), 1-26. https://doi.org/10.63125/n4h7t156

[89]. Mansura Akter, E., & Md Abdul Ahad, M. (2022). In Silico drug repurposing for inflammatory diseases: a systematic review of molecular docking and virtual screening studies. *American Journal of Advanced Technology and Engineering Solutions*, *2*(04), 35-64. https://doi.org/10.63125/j1hbts51

[90]. Mansura Akter, E., & Shaiful, M. (2024). A systematic review of SNP polymorphism studies in South Asian populations: implications for diabetes and autoimmune disorders. *American Journal of Scholarly Research and Innovation*, *3*(01), 20-51. https://doi.org/10.63125/8nvxcb96

[91]. Manzoor, H. U., Shabbir, A., Chen, A., Flynn, D., & Zoha, A. (2024). A survey of security strategies in federated learning: Defending models, data, and privacy. *Future Internet*, *16*(10), 374.

[92]. Md Arifur, R., & Sheratun Noor, J. (2022). A Systematic Literature Review of User-Centric Design In Digital Business Systems: Enhancing Accessibility, Adoption, And Organizational Impact. *Review of Applied Science and Technology*, *1*(04), 01-25. https://doi.org/10.63125/ndjkpm77

[93]. Md Ashiqur, R., Md Hasan, Z., & Afrin Binta, H. (2025). A meta-analysis of ERP and CRM integration tools in business process optimization. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *1*(01), 278-312. https://doi.org/10.63125/yah70173

[94]. Md Hasan, Z. (2025). AI-Driven business analytics for financial forecasting: a systematic review of decision support models in SMES. *Review of Applied Science and Technology*, *4*(02), 86-117. https://doi.org/10.63125/gjrpv442

[95]. Md Hasan, Z., Mohammad, M., & Md Nur Hasan, M. (2024). Business Intelligence Systems In Finance And Accounting: A Review Of Real-Time Dashboarding Using Power BI & Tableau. *American Journal of Scholarly Research and Innovation*, *3*(02), 52-79. https://doi.org/10.63125/fy4w7w04

[96]. Md Hasan, Z., Sheratun Noor, J., & Md. Zafor, I. (2023). Strategic role of business analysts in digital transformation tools, roles, and enterprise outcomes. *American Journal of Scholarly Research and Innovation*, *2*(02), 246-273. https://doi.org/10.63125/rc45z918

[97]. Md Mahamudur Rahaman, S. (2022). Electrical And Mechanical Troubleshooting in Medical And Diagnostic Device Manufacturing: A Systematic Review Of Industry Safety And Performance Protocols. *American Journal of Scholarly Research and Innovation*, *1*(01), 295-318. https://doi.org/10.63125/d68y3590

[98]. Md Masud, K., Mohammad, M., & Sazzad, I. (2023). Mathematics For Finance: A Review of Quantitative Methods In Loan Portfolio Optimization. *International Journal of Scientific Interdisciplinary Research*, *4*(3), 01-29. https://doi.org/10.63125/j43ayz68

[99]. Md Nur Hasan, M., Md Musfiqur, R., & Debashish, G. (2022). Strategic Decision-Making in Digital Retail Supply Chains: Harnessing AI-Driven Business Intelligence From Customer Data. *Review of Applied Science and Technology*, *1*(03), 01-31. https://doi.org/10.63125/6a7rpy62

[100]. Md Sultan, M., Proches Nolasco, M., & Md. Torikul, I. (2023). Multi-Material Additive Manufacturing For Integrated Electromechanical Systems. *American Journal of Interdisciplinary Studies*, *4*(04), 52-79. https://doi.org/10.63125/y2ybrx17

[101]. Md Sultan, M., Proches Nolasco, M., & Vicent Opiyo, N. (2025). A Comprehensive Analysis Of Non-Planar Toolpath Optimization In Multi-Axis 3D Printing: Evaluating The Efficiency Of Curved Layer Slicing Strategies. *Review of Applied Science and Technology*, *4*(02), 274-308. https://doi.org/10.63125/5fdxa722

[102]. Md Takbir Hossen, S., Ishtiaque, A., & Md Atiqur, R. (2023). AI-Based Smart Textile Wearables For Remote Health Surveillance And Critical Emergency Alerts: A Systematic Literature Review. *American Journal of Scholarly Research and Innovation*, *2*(02), 1-29. https://doi.org/10.63125/ceqapd08

[103]. Md Tawfiqul, I. (2023). A Quantitative Assessment Of Secure Neural Network Architectures For Fault Detection In Industrial Control Systems. *Review of Applied Science and Technology*, *2*(04), 01-24. https://doi.org/10.63125/3m7gbs97

[104]. Md Tawfiqul, I., Sabbir, A., Md Anikur, R., & Md Arifur, R. (2024). Neural Network–Based Risk Prediction And Simulation Framework For Medical IOT Cybersecurity: An Engineering Management Model For Smart Hospitals. *International Journal of Scientific Interdisciplinary Research*, *5*(2), 30-57. https://doi.org/10.63125/g0mvct35

[105]. Meduri, K., Nadella, G. S., Yadulla, A. R., Kasula, V. K., Maturi, M. H., Brown, S., Satish, S., & Gonaygunta, H. (2025). Leveraging federated learning for privacy-preserving analysis of multi-institutional electronic health records in rare disease research. *Journal of Economy and Technology*, *3*, 177-189.

[106]. Mirza, B., Wang, W., Wang, J., Choi, H., Chung, N. C., & Ping, P. (2019). Machine learning and integrative analysis of biomedical big data. *Genes*, *10*(2), 87.

[107]. Moshawrab, M., Adda, M., Bouzouane, A., Ibrahim, H., & Raad, A. (2023). Reviewing federated learning aggregation algorithms; strategies, contributions, limitations and future perspectives. *Electronics*, *12*(10), 2287.

[108]. Mst Shamima, A., Niger, S., Md Atiqur Rahman, K., & Mohammad, M. (2023). Business Intelligence-Driven Healthcare: Integrating Big Data And Machine Learning For Strategic Cost Reduction And Quality Care Delivery. *American Journal of Interdisciplinary Studies*, *4*(02), 01-28. https://doi.org/10.63125/crv1xp27

[109]. Mubashir, I., & Abdul, R. (2022). Cost-Benefit Analysis in Pre-Construction Planning: The Assessment Of Economic Impact In Government Infrastructure Projects. *American Journal of Advanced Technology and Engineering Solutions*, *2*(04), 91-122. https://doi.org/10.63125/kjwd5e33

[110]. Ng, S., Masarone, S., Watson, D., & Barnes, M. R. (2023). The benefits and pitfalls of machine learning for biomarker discovery. *Cell and tissue research*, *394*(1), 17-31.

[111]. Nguyen, D. C., Ding, M., Pathirana, P. N., Seneviratne, A., Li, J., & Poor, H. V. (2021). Federated learning for internet of things: A comprehensive survey. *IEEE Communications Surveys & Tutorials*, *23*(3), 1622-1658.

[112]. Nguyen, D. C., Ding, M., Pham, Q.-V., Pathirana, P. N., Le, L. B., Seneviratne, A., Li, J., Niyato, D., & Poor, H. V. (2021). Federated learning meets blockchain in edge computing: Opportunities and challenges. *IEEE Internet of Things Journal*, *8*(16), 12806-12825.

[113]. Nguyen, T. X., Ran, A. R., Hu, X., Yang, D., Jiang, M., Dou, Q., & Cheung, C. Y. (2022). Federated learning in ocular imaging: current progress and future direction. *Diagnostics*, *12*(11), 2835.

[114]. Nielsen, C., Tuladhar, A., & Forkert, N. D. (2022). Investigating the vulnerability of federated learning-based diabetic retinopathy grade classification to gradient inversion attacks. International Workshop on Ophthalmic Medical Image Analysis,

[115]. Noorbakhsh-Sabet, N., Zand, R., Zhang, Y., & Abedi, V. (2019). Artificial intelligence transforms the future of health care. *The American journal of medicine*, *132*(7), 795-801.

[116]. Ogundokun, R. O., Misra, S., Maskeliunas, R., & Damasevicius, R. (2022). A review on federated learning and machine learning approaches: categorization, application areas, and blockchain technology. *Information*, *13*(5), 263.

[117]. Olawade, D. B., David-Olawade, A. C., Wada, O. Z., Asaolu, A. J., Adereni, T., & Ling, J. (2024). Artificial intelligence in healthcare delivery: Prospects and pitfalls. *Journal of Medicine, Surgery, and Public Health*, *3*, 100108.

[118]. Paragliola, G., & Coronato, A. (2022). Definition of a novel federated learning approach to reduce communication costs. *Expert Systems with Applications*, *189*, 116109.

[119]. Perakakis, N., Yazdani, A., Karniadakis, G. E., & Mantzoros, C. (2018). Omics, big data and machine learning as tools to propel understanding of biological mechanisms and to discover novel diagnostics and therapeutics. In (Vol. 87, pp. A1-A9): Elsevier.

[120]. Piccialli, F., Di Cola, V. S., Giampaolo, F., & Cuomo, S. (2021). The role of artificial intelligence in fighting the COVID-19 pandemic. *Information Systems Frontiers*, *23*(6), 1467-1497.

[121]. Poongodi, M., Malviya, M., Hamdi, M., Rauf, H. T., Kadry, S., & Thinnukool, O. (2021). The recent technologies to curb the second-wave of COVID-19 pandemic. *Ieee Access*, *9*, 97906-97928.

[122]. Poongodi, T., Sumathi, D., Suresh, P., & Balusamy, B. (2020). Deep learning techniques for electronic health record (EHR) analysis. In *Bio-inspired Neurocomputing* (pp. 73-103). Springer.

[123]. Qammar, A., Karim, A., Ning, H., & Ding, J. (2023). Securing federated learning with blockchain: a systematic literature review. *Artificial Intelligence Review*, *56*(5), 3951-3985.

[124]. Qayyum, A., Ahmad, K., Ahsan, M. A., Al-Fuqaha, A., & Qadir, J. (2022). Collaborative federated learning for healthcare: Multi-modal covid-19 diagnosis at the edge. *IEEE Open Journal of the Computer Society*, *3*, 172-184.

[125]. Qin, Z., Li, G. Y., & Ye, H. (2021). Federated learning and wireless communications. *IEEE Wireless Communications*, *28*(5), 134-140.

[126]. Qiu, Y., Fang, H., Yu, H., Chen, B., Qiu, M., & Xia, S.-T. (2024). A closer look at gan priors: Exploiting intermediate features for enhanced model inversion attacks. European Conference on Computer Vision,

[127]. Rahman, A., Hossain, M. S., Muhammad, G., Kundu, D., Debnath, T., Rahman, M., Khan, M. S. I., Tiwari, P., & Band, S. S. (2023). Federated learning-based AI approaches in smart healthcare: concepts, taxonomies, challenges and open issues. *Cluster computing*, *26*(4), 2271-2311.

[128]. Rahman, K. J., Ahmed, F., Akhter, N., Hasan, M., Amin, R., Aziz, K. E., Islam, A. M., Mukta, M. S. H., & Islam, A. N. (2021). Challenges, applications and design aspects of federated learning: A survey. *Ieee Access*, *9*, 124682-124700.

[129]. Rahmati, M., & Pagano, A. (2025). Federated Learning-Driven Cybersecurity Framework for IoT Networks with Privacy Preserving and Real-Time Threat Detection Capabilities. Informatics,

[130]. Rao, S., Mamouei, M., Salimi-Khorshidi, G., Li, Y., Ramakrishnan, R., Hassaine, A., Canoy, D., & Rahimi, K. (2022). Targeted-BEHRT: deep learning for observational causal inference on longitudinal electronic health records. *IEEE transactions on neural networks and learning systems*, *35*(4), 5027-5038.

[131]. Ratnayake, H., Chen, L., & Ding, X. (2023). A review of federated learning: taxonomy, privacy and future directions. *Journal of Intelligent Information Systems*, *61*(3), 923-949.

[132]. Rauniyar, A., Hagos, D. H., Jha, D., Håkegård, J. E., Bagci, U., Rawat, D. B., & Vlassov, V. (2023). Federated learning for medical applications: A taxonomy, current trends, challenges, and future research directions. *IEEE Internet of Things Journal*, *11*(5), 7374-7398.

[133]. Reduanul, H., & Mohammad Shoeb, A. (2022). Advancing AI in Marketing Through Cross Border Integration Ethical Considerations And Policy Implications. *American Journal of Scholarly Research and Innovation*, *1*(01), 351-379. https://doi.org/10.63125/d1xg3784

[134]. Rey, V., Sánchez, P. M. S., Celdrán, A. H., & Bovet, G. (2022). Federated learning for malware detection in IoT devices. *Computer networks*, *204*, 108693.

[135]. Rezwanul Ashraf, R., & Hosne Ara, M. (2023). Visual communication in industrial safety systems: a review of UI/UX design for risk alerts and warnings. *American Journal of Scholarly Research and Innovation*, *2*(02), 217-245. https://doi.org/10.63125/wbv4z521

[136]. Sandhu, S. S., Gorji, H. T., Tavakolian, P., Tavakolian, K., & Akhbardeh, A. (2023). Medical imaging applications of federated learning. *Diagnostics*, *13*(19), 3140.

[137]. Sanjai, V., Sanath Kumar, C., Maniruzzaman, B., & Farhana Zaman, R. (2023). Integrating Artificial Intelligence in Strategic Business Decision-Making: A Systematic Review Of Predictive Models. *International Journal of Scientific Interdisciplinary Research*, *4*(1), 01-26. https://doi.org/10.63125/s5skge53

[138]. Sanjai, V., Sanath Kumar, C., Sadia, Z., & Rony, S. (2025). AI And Quantum Computing For Carbon-Neutral Supply Chains: A Systematic Review Of Innovations. *American Journal of Interdisciplinary Studies*, *6*(1), 40-75. https://doi.org/10.63125/nrdx7d32

[139]. Sattler, F., Wiedemann, S., Müller, K.-R., & Samek, W. (2019). Robust and communication-efficient federated learning from non-iid data. *IEEE transactions on neural networks and learning systems*, *31*(9), 3400-3413.

[140]. Savazzi, S., Nicoli, M., Bennis, M., Kianoush, S., & Barbieri, L. (2021). Opportunities of federated learning in connected, cooperative, and automated industrial systems. *IEEE Communications Magazine*, *59*(2), 16-21.

[141]. Savazzi, S., Nicoli, M., & Rampa, V. (2020). Federated learning with cooperating devices: A consensus approach for massive IoT networks. *IEEE Internet of Things Journal*, *7*(5), 4641-4654.

[142]. Sazzad, I., & Md Nazrul Islam, K. (2022). Project impact assessment frameworks in nonprofit development: a review of case studies from south asia. *American Journal of Scholarly Research and Innovation*, *1*(01), 270-294. https://doi.org/10.63125/eeja0t77

[143]. Shaheen, M., Farooq, M. S., Umer, T., & Kim, B.-S. (2022). Applications of federated learning; taxonomy, challenges, and research trends. *Electronics*, *11*(4), 670.

[144]. Sheratun Noor, J., & Momena, A. (2022). Assessment Of Data-Driven Vendor Performance Evaluation in Retail Supply Chains: Analyzing Metrics, Scorecards, And Contract Management Tools. *American Journal of Interdisciplinary Studies*, *3*(02), 36-61. https://doi.org/10.63125/0s7t1y90

[145]. Siebra, C. A., Kurpicz-Briki, M., & Wac, K. (2024). Transformers in health: a systematic review on architectures for longitudinal data analysis. *Artificial Intelligence Review*, *57*(2), 32.

[146]. Subrato, S., & Md, N. (2024). The role of perceived environmental responsibility in artificial intelligence-enabled risk management and sustainable decision-making. *American Journal of Advanced Technology and Engineering Solutions*, *4*(04), 33-56. https://doi.org/10.63125/7tjw3767

[147]. Supriya, Y., Victor, N., Srivastava, G., & Gadekallu, T. R. (2023). A hybrid federated learning model for insurance fraud detection. 2023 IEEE international conference on communications workshops (ICC workshops),

[148]. Tahmina Akter, R., Debashish, G., Md Soyeb, R., & Abdullah Al, M. (2023). A Systematic Review of AI-Enhanced Decision Support Tools in Information Systems: Strategic Applications In Service-Oriented Enterprises And Enterprise Planning. *Review of Applied Science and Technology*, *2*(01), 26-52. https://doi.org/10.63125/73djw422

[149]. Tan, A. Z., Yu, H., Cui, L., & Yang, Q. (2022). Towards personalized federated learning. *IEEE transactions on neural networks and learning systems*, *34*(12), 9587-9603.

[150]. Tariq, A., Serhani, M. A., Sallabi, F. M., Barka, E. S., Qayyum, T., Khater, H. M., & Shuaib, K. A. (2024). Trustworthy federated learning: A comprehensive review, architecture, key challenges, and future research prospects. *IEEE Open Journal of the Communications Society*.

[151]. Torres-Martos, A., Bustos-Aibar, M., Ramírez-Mena, A., Cámara-Sánchez, S., Anguita-Ruiz, A., Alcalá, R., Aguilera, C. M., & Alcalá-Fdez, J. (2023). Omics data preprocessing for machine learning: A case study in childhood obesity. *Genes*, *14*(2), 248.

[152]. Tsimenidis, S., Vrochidou, E., & Papakostas, G. A. (2022). Omics data and data representations for deep learning-based predictive modeling. *International Journal of Molecular Sciences*, *23*(20), 12272.
[153]. Ullah, F., Nadeem, M., Abrar, M., Amin, F., Salam, A., & Khan, S. (2023). Enhancing brain tumor segmentation accuracy through scalable federated learning with advanced data privacy and security measures. *Mathematics*, *11*(19), 4189.
[154]. Umair, M., Tan, W.-H., & Foo, Y.-L. (2023). Network Intrusion Detection using Dynamic Weighted Aggregation Federated Learning. 2023 IEEE 8th International Conference on Recent Advances and Innovations in Engineering (ICRAIE),
[155]. Wahab, O. A., Mourad, A., Otrok, H., & Taleb, T. (2021). Federated machine learning: Survey, multi-level classification, desirable criteria and future directions in communication and networking systems. *IEEE Communications Surveys & Tutorials*, *23*(2), 1342-1397.
[156]. Walach, J., Filzmoser, P., & Hron, K. (2018). Data normalization and scaling: consequences for the analysis in omics sciences. In *Comprehensive analytical chemistry* (Vol. 82, pp. 165-196). Elsevier.
[157]. Wang, L., Polato, M., Brighente, A., Conti, M., Zhang, L., & Xu, L. (2024). PriVeriFL: Privacy-preserving and aggregation-verifiable federated learning. *IEEE Transactions on Services Computing*.
[158]. Wang, S. Y., Tseng, B., & Hernandez-Boussard, T. (2022). Deep learning approaches for predicting glaucoma progression using electronic health records and natural language processing. *Ophthalmology Science*, *2*(2), 100127.
[159]. Wang, X. (2018). Clinical trans-omics: an integration of clinical phenomes with molecular multiomics. *Cell Biology and Toxicology*, *34*(3), 163-166.
[160]. Wen, J., Zhang, Z., Lan, Y., Cui, Z., Cai, J., & Zhang, W. (2023). A survey on federated learning: challenges and applications. *International journal of machine learning and cybernetics*, *14*(2), 513-535.
[161]. Whig, P., Yathiraju, N., Jain, A., Bhatia, A. B., & Kasula, B. Y. (2025). Integrating Machine Vision for Enhanced Biomedical Signal and Image Processing. In *Deep Learning and Computer Vision: Models and Biomedical Applications: Volume 1* (pp. 89-116). Springer.
[162]. Witt, L., Heyer, M., Toyoda, K., Samek, W., & Li, D. (2022). Decentral and incentivized federated learning frameworks: A systematic literature review. *IEEE Internet of Things Journal*, *10*(4), 3642-3663.
[163]. Xiang, Y., Xu, J., Si, Y., Li, Z., Rasmy, L., Zhou, Y., Tiryaki, F., Li, F., Zhang, Y., & Wu, Y. (2019). Time-sensitive clinical concept embeddings learned from large electronic health records. *BMC medical informatics and decision making*, *19*(Suppl 2), 58.
[164]. Xu, J., Yang, P., Xue, S., Sharma, B., Sanchez-Martin, M., Wang, F., Beaty, K. A., Dehan, E., & Parikh, B. (2019). Translating cancer genomics into precision medicine with artificial intelligence: applications, challenges and future perspectives. *Human genetics*, *138*(2), 109-124.
[165]. Yang, F., Zhang, J., Chen, W., Lai, Y., Wang, Y., & Zou, Q. (2022). DeepMPM: a mortality risk prediction model using longitudinal EHR data. *BMC bioinformatics*, *23*(1), 423.
[166]. Yang, W., Wang, S., Wu, D., Cai, T., Zhu, Y., Wei, S., Zhang, Y., Yang, X., Tang, Z., & Li, Y. (2025). Deep learning model inversion attacks and defenses: a comprehensive survey. *Artificial Intelligence Review*, *58*(8), 242.
[167]. Yang, Z., Chen, M., Wong, K.-K., Poor, H. V., & Cui, S. (2022). Federated learning for 6G: Applications, challenges, and opportunities. *Engineering*, *8*, 33-41.
[168]. Yang, Z., Xia, W., Lu, Z., Chen, Y., Li, X., & Zhang, Y. (2023). Hypernetwork-based physics-driven personalized federated learning for CT imaging. *IEEE transactions on neural networks and learning systems*.
[169]. Yin, B., Yin, H., Wu, Y., & Jiang, Z. (2020). FDC: A secure federated deep learning mechanism for data collaborations in the Internet of Things. *IEEE Internet of Things Journal*, *7*(7), 6348-6359.
[170]. Zeleke, S. N., & Bochicchio, M. (2024). Federated kolmogorov-arnold networks for health data analysis: A study using ecg signal. 2024 IEEE International Conference on Big Data (BigData),
[171]. Zhang, C., Xie, Y., Bai, H., Yu, B., Li, W., & Gao, Y. (2021). A survey on federated learning. *Knowledge-Based Systems*, *216*, 106775.
[172]. Zhang, D., Yin, C., Zeng, J., Yuan, X., & Zhang, P. (2020). Combining structured and unstructured data for predictive models: a deep learning approach. *BMC medical informatics and decision making*, *20*(1), 280.
[173]. Zhang, G., Hu, Q., Zhang, Y., Dai, Y., & Jiang, T. (2024). Lightweight cross-domain authentication scheme for securing wireless IoT devices using backscatter communication. *IEEE Internet of Things Journal*, *11*(12), 22021-22035.
[174]. Zhang, J., Kowsari, K., Harrison, J. H., Lobo, J. M., & Barnes, L. E. (2018). Patient2vec: A personalized interpretable deep representation of the longitudinal electronic health record. *Ieee Access*, *6*, 65333-65346.
[175]. Zhang, T., Gao, L., He, C., Zhang, M., Krishnamachari, B., & Avestimehr, A. S. (2022). Federated learning for the internet of things: Applications, challenges, and opportunities. *IEEE Internet of Things Magazine*, *5*(1), 24-29.

Volume 04, Issue 01 (2025)
Page No: 320-351
eISSN: 3067-2163
Doi: 10.63125/jga18304

[176]. Zhang, W., Yang, D., Wu, W., Peng, H., Zhang, N., Zhang, H., & Shen, X. (2021). Optimizing federated learning in distributed industrial IoT: A multi-agent approach. *IEEE Journal on Selected Areas in Communications*, *39*(12), 3688-3703.

[177]. Zheng, L., Cao, Y., Jiang, R., Taura, K., Shen, Y., Li, S., & Yoshikawa, M. (2024). Enhancing privacy of spatiotemporal federated learning against gradient inversion attacks. International Conference on Database Systems for Advanced Applications,

[178]. Zhu, H., Zhang, H., & Jin, Y. (2021). From federated learning to federated neural architecture search: a survey. *Complex & Intelligent Systems*, *7*(2), 639-657.