Received: 29 July 2024 | Revised: 28 November 2024 | Accepted: 18 March 2025 | Published online: 4 April 2025

REVIEW

Artificial Intelligence and Applications
2025, Vol. 00(00) 1–12
DOI: 10.47852/bonviewAIA52023976

Addressing Privacy-Preservation in Healthcare Using Federated Learning: A Survey

Faria Karamat[1], Atta Ur Rahman[1], Bibi Saqia[2,*], Adeel Zafar[1] and Waqas Ali Khan[1]

[1]*Riphah Institute of Systems Engineering, Riphah International University Islamabad, Pakistan*

[2]*Department of Computer Science, University of Science and Technology Bannu, Pakistan*

Abstract: The healthcare data are rapidly increasing, and protecting patient-sensitive information becomes challenging. This paper surveys the use of federated learning (FL) to address privacy in the healthcare industry. FL is a decentralized machine learning (ML) approach, where the ML process is distributed across multiple devices, without relying on a central server or coordinator. In recent years, FL has obtained significant attention, especially in scenarios where data privacy is top concern. This work attempts to discover the progress made so far regarding protecting healthcare information. This work explores the privacy risks related to a centralized healthcare system and also discusses the FL conceptual framework, which addresses many concerns. An extensive survey of various FL architectures and protocols designed for healthcare environments is conducted. It also investigates novel ways to deploy FL approaches using advanced encryption methods, like homomorphic and secure multi-party encryption, to improve privacy concerns. Moreover, this work covers the practical limitations and challenges of FL in the realm of healthcare, which include communication costs, model aggregation techniques, and scaling concerns. It also highlights new trends and directions in this field. Finally, the study discusses clinical applications of FL, namely personalized medicine, predictive analytics, or scaling issues.

Keywords: federated learning, centralized approaches, healthcare data, privacy preservation, decentralized data analysis

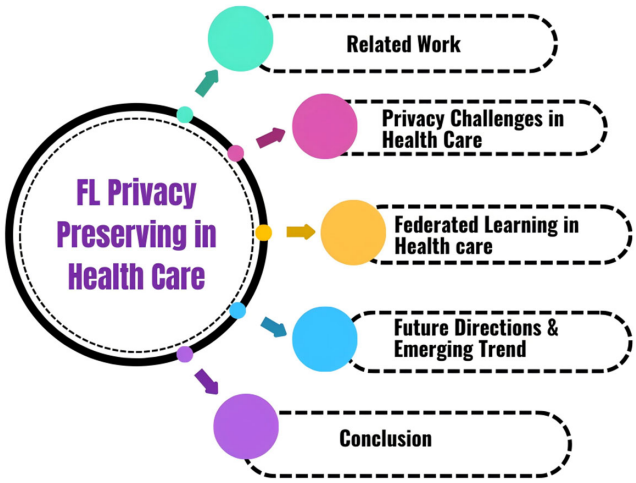
1. Introduction

The amount of healthcare data is growing, which poses serious privacy issues. Several techniques including federated Learning (FL) have evolved to overcome these challenges while allowing significant insights to be extracted from the data [1]. These data provide huge insights, which may be used to advance clinical research and improve patient care. However, it needs to preserve and mitigate concerns about third-party access to sensitive medical records [2]. In the past, huge datasets of patient details were shared and processed by experts using a centralized healthcare system [3]. The centralized approach has made a stunning improvement, while it has created various issues related to confidentiality and security concerns [4]. Due to central processing, healthcare systems were at risk of information breaches, unintentional disclosures, and undesirable access to information [5]. With the passage of time and rapid increase in healthcare data, techniques to combine model updates from multiple devices without exposing individual data points were desired, which allows collaborative model training while keeping the privacy of patient data. To address these problems, a paradigm called FL has been deployed [6]. FL computes model updates locally on the specific devices, utilizing solely the data accessible to only those devices. This implies that sensitive patient data remain within the devices, which increases the privacy protection of the data [7]. This new idea could completely change how healthcare data are analyzed. It would let different organizations work together to make strong models, while still keeping control of their private information.

Figure 1 defines healthcare privacy preservation by FL. Concentrating healthcare elements utilizing technology-enabled clarifications to provide illness forecast and increase patient gratification. This facilitated medical growth, but it has some demerits as well such as privacy at risk [8]. FL addresses many privacy issues that arise in centralized healthcare systems, including breaches, unapproved access to data, and a lack of control over patient information. Centralized systems increase risk by concentrating critical data in one place. The implementation of regulations like as GDPR and HIPAA has made decentralized systems like FL essential for safe data handling. Through the upgradation of electronic medical databases and extensive usage of wearable expertise [9], there's now more healthcare evidence than earlier. This upsurge in data obtainability has elevated worries near openings, illegal access, and latent misappropriation of complex data [10]. To identify these apprehensions, FL occurs as a means to protect confidentiality, changing old-fashioned techniques of examining data [11]. Related to integrating everything in a centralized location, FL extends the training of simulations through diverse strategies permitting healthcare administrations to retain the mechanism of their records [12]. This dispersed method meaningfully expands data defense by reducing the hazard of a single disaster element [13]. With the FL approach, medicinal specialists could cooperate to shape models deprived of the allocation of rough records of patients. This

*Corresponding author: Bibi Saqia, Department of Computer Science, University of Science and Technology Bannu, Pakistan. Email: saqiaktk@ustb.edu.pk

Figure 1
Healthcare privacy preservation by FL



creates a supportive atmosphere in which organizations cooperatively improve medicinal awareness [14]. The key goal of this study is to systematically review studies on the usage of FL for keeping confidentiality in healthcare analysis. It pursues to deliver an inclusive thought of how FL could progress healthcare analytics into an era of improved privacy and collaboration by examining the existing state of the field, emphasizing key schemes, and discovering trials and chances [15]. This paper uses the FL technique to predict heart issues in IoT-based electronic health records. This combination of FL offers a valuable predictive analytics procedure that maintains data confidentiality [16]. The work published by [17] reviews the existing studies and highlights challenges and latent upcoming uses that can influence the healthcare system. The FL occurs as a creator in the multifaceted demesne of data secrecy and cooperative study in healthcare posing a technique to equilibrium patient confidentiality protection with information detection [18]. This study discovers the important policies, applications, and confines to offer a complete appreciation of how FL can determine healthcare systems into a new modified and combined policy.

2. Literature Review

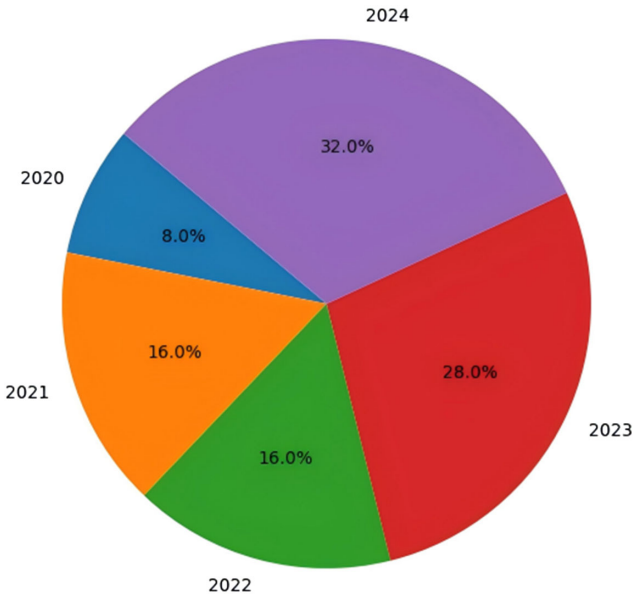
Data security strategies in the healthcare domain have received a lot of attention in the current era, due to the rising amount of delicate patient archives and the condition to observe confidentiality rules similar to HIPAA (Health Insurance Portability and Accountability Act) in the US and GDPR (General Data Protection Regulation) in the EU.

In this section, we inspect the study on privacy-preserving methods in healthcare, concentrating on FL employed for time-series information. The development of larger models and datasets has led to a rise in the use of distributed DL, which uses many

Table 1
The study using FL approaches in healthcare

Study	Key contribution	Model
[19]	Review of applications in FL	FL
[20]	Combined method for classification and identification of brain tumor	FL with transfer learning
[21]	Privacy-preserving speech-based cerebral anxiety identification	FL
[22]	Systematic literature review of FL in medical context	FL vs. ML
[23]	FL-based privacy-preserving smart healthcare system	FL-based Differential Privacy
[24]	Comprehensive survey on FL for privacy preservation in healthcare	FL+ IOMT
[25]	FL and differential privacy for medical image analysis	FL-based Differential Privacy
[26]	Cancer patients based on FL	diagnosis model using FL
[27]	Fog-based privacy-preserving FL for health [28] care	FL+ CNN +Fog computing
[29]	Insights through blockchain-enabled FL for precision medicine	Blockchain + FL
[30]	Taxonomy and trends in FL for medical applications	FL vs. AI vs. ML
[31]	Novel mechanism for privacy preservation in healthcare applications	FL as a privacy-preserving approach
[32]	Framework for privacy-preserving FL in IoMT	FL + IOMT
[33]	FL for prediction of long-lasting kidney infections	FL
[34]	Advancing healthcare informatics for privacy and security through FL paradigms	FL
[35]	Recent methodological advances in FL for healthcare	FL
[36]	Digital healthcare framework for patients with disabilities based on deep FL schemes	Deep FL
[37]	Client selection and resource allocation via graph neural networks for efficient FL in healthcare environments	Graph Neural Networks
[38]	FL-enabled approach towards healthcare analytics over fog computing	FL + Fog Computing
[39]	Heterogeneity-aware personalized FL framework for intelligent healthcare applications in IoMT environments	Personalized FL + IOMT
[40]	Unified fair FL for digital healthcare	FL with h Unified Fairness Objective (FedUFO)
[41]	FL system with data fusion for healthcare using multi-party computation and additive secret sharing	FL + Multi-Party Computation
[42]	FL meets blockchain in decentralized data sharing: Healthcare use case	Blockchain + FL

Figure 2
The number of studies published using FL approaches for healthcare



processing units (such as GPUs and TPUs) to shorten training times [43]. They examine several decentralized approaches and assess how they work with healthcare analytics. Jones and Patel's case studies and application analysis provided valuable insight into the advantages and challenges of decentralized frameworks before our research [44]. In their work, Rehm et al. [45] deal with regulatory issues related to sharing healthcare record. The study includes an in-depth analysis of privacy legal guidelines, which include HIPAA and GDPR, and the implications for information sharing within healthcare. Understanding the criminal panorama is pivotal and informs our discussion of the demanding situations and considerations related to regulatory compliance within the context of FL. Different studies synthesized the most recent innovations in FL by exploring and synthesizing emerging traits [46]. This observation sheds light on the latest tendencies in federated architectures, privacy-maintaining algorithms, and packages. The ahead-searching perspective contributes to our discussion of the future instructions of FL in healthcare, enriching our understanding of the evolving landscape [47]. Figure 2 represents the number of studies published using FL approaches for healthcare.

There have been several recent surveys on the use of FL in healthcare. For instance, Silva and Soto [48] conducted an extensive survey focusing on privacy-preserving mechanisms within FL frameworks. Another study by Chernyshev et al. [49] explored FL applications specifically in personalized medicine. Moreover, Iroju et al. [50] reviewed the use of FL in medical imaging, providing insights into its strengths and limitations in this area. Unlike these studies, our review focuses on the broader application of FL in various healthcare domains, highlighting both established methods and emerging trends. We also address the technical challenges, such as data heterogeneity and communication efficiency, which are critical in healthcare settings. Finally, we suggest potential directions for future research, including the integration of FL with other privacy-enhancing technologies like homomorphic encryption.

3. Research Methodology

This comprehensive survey employs a multifaceted approach encompassing literature review and survey methodologies to provide a refined understanding of the current landscape and future directions in privacy-preserving healthcare analytics.

3.1. Literature review

The literature review methodology adopts a systematic approach to collect and analyze relevant studies related to FL in healthcare. Key search terms such as "Federated Learning", "healthcare analytics", and "privacy preservation" were defined to query databases, including PubMed, IEEE Xplore, and Google Scholar. Studies were screened based on predefined inclusion criteria to ensure comprehensive coverage of privacy-preserving healthcare analytics.

3.2. Survey design and data collection

To supplement the literature review findings, a structured survey was released to get evaluations from researchers, practitioners, and specialists actively working in privacy-keeping analytics in healthcare using FL. The questionnaire covered problems consisting of privacy-retaining strategies and federated systems. It additionally highlighted applications, emerging trends, and problems.

The ballot becomes primarily based on topics identified inside the literature. Academic networks, enterprise-precise websites, and research groups have been the various distribution channels used. The survey includes an eclectic blend of respondents based totally on their qualifications and contributions to Healthcare FL. The survey findings were tested both subjectively and numerically to have a better knowledge of present practices, potential challenges, and guidelines. Table 1 presents related work regarding privacy preserving in FL. This literature review was focused on extracting important information including methods, challenges, applications, privacy-preserving technologies, etc. The structured framework is a basis for synthesizing knowledge.

3.3. Data synthesis and analysis

Data from the survey and literature changed into blended and subjected to thematic analysis to become aware of crucial tendencies, styles, and insights. This synthesis aimed to bring together data from literature and expert first-hand experiences to create a cohesive story that illustrated the current realm of privacy-retaining analytics in healthcare with FL. A detailed review of the form of research techniques used inside the concern was supplied via the methodological classification that became used to arrange research in keeping with their processes and techniques. A comprehensive investigation is ensured via the triangulation of procedures, which permits a detailed portrayal of the nation of privacy-keeping healthcare analytics nowadays. In this sizeable survey, the foundation for a full understanding and discussion is shaped by the mixed insights from the literature and survey comments.

4. Privacy Challenges in Healthcare Data Analytics

Privacy issues in healthcare data analytics contain hazards of illegal access, data breaches, and re-identification of anonymized accounts. Distribution data across organizations raise these hazards, while lawful and moral submission remains multifaceted. Balancing data usefulness with confidentiality safety is an

Table 2
Issues of centralized/traditional approach in healthcare

Issues	Description
Privacy and data limitation	FL method for breast cancer revealing based on DCNN [51].
Limited Interoperability	Challenges in integrating data from disparate systems hinder seamless collaboration and information exchange [50].
Slow Data Access and Retrieval	Retrieving patient data can be time-consuming, impacting timely decision-making, especially in emergencies [52].
Challenges in Collaboration	Data sharing between institutions requires complex agreements and may involve legal and privacy concerns [53].
Scalability Concerns	Analysis of the outcomes and scalability of FL for medicinal imaging [54].
Patient Empowerment and Control	Patients have limited influence over how their data is utilized, and the data-sharing process may lack transparency [55].
Data quality, bias, and strategic	problems in reinforcement learning of healthcare applications [56]
The Ambiguity of Data Ownership & Control	Uncertainty concerning facts possession and controls, which may make a contribution to disputes and worries [57].
Design, application, and issues	Challenges, applications, and design features of FL [58]

important apprehension. Table 2 describes the related issues of centralized/traditional approach in healthcare.

4.1. Centralized approaches and vulnerabilities

The traditional approach of centralized healthcare information analytics has been a cornerstone of clinical studies and affected personal care. Significant privacy issues have been related to this approach, even though. Centralized records repositories attract unauthorized access due to the abundance of patient information they contain [59]. Sensitive information being focused in a single region raises the opportunity of sizable data breaches, which may compromise patient privacy, confidentiality, and self-belief. Data breaches in healthcare no longer only expose sufferers to the threat of identity robbery and economic fraud but also have broader implications for public health [60]. The compromise of sensitive clinical information can lead to the erosion of the affected person's acceptance as true within healthcare structures, delaying individuals from sharing important data with their healthcare vendors. As healthcare institutions turn out to be trustees of full-size electronic fitness records [61], wearable tool facts, and diagnostic imaging, the want to toughen defenses in opposition to cyber threats becomes paramount. Figure 3 represents the privacy challenges in healthcare.

4.2. Evolving regulatory landscape

The ever-changing criminal frameworks meant to defend patient statistics in addition complicate the privacy state of affairs

Figure 3
Privacy challenges in healthcare

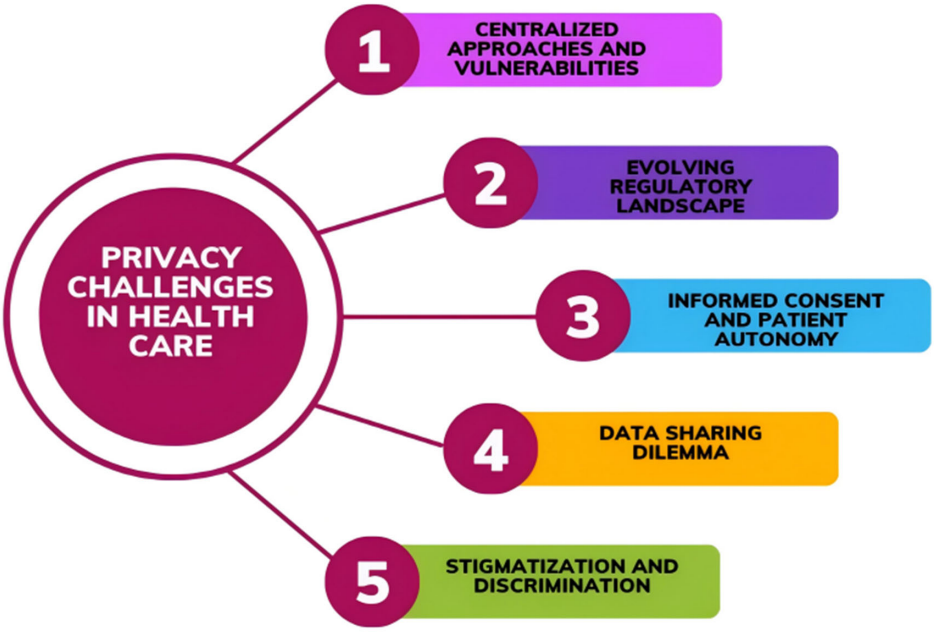
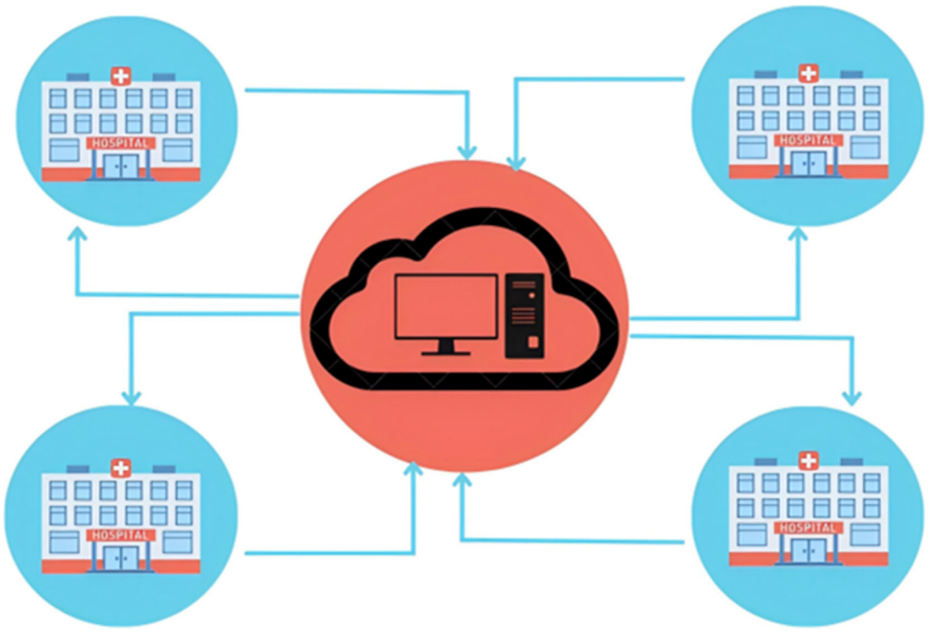


Figure 4
Federated learning approach



within the healthcare industry [62]. Laws just like the HIPAA in the United States and the GDPR in the European Union impose strict policies on healthcare companies and carriers [63]. In addition to being required through regulation, following these tips is morally necessary for healthcare-associated records [64]. Robust security features, open information policies, and a proactive approach to privacy hazard mitigation are essential to fulfill those legislative responsibilities.

4.3. Informed consent and patient autonomy

The concept of Autonomy of the Patient and Informed Consent introduces another layer of complexity to privacy-demanding situations in healthcare. As scientific centers collect and take a look at patient data for clinical investigations, getting informed permission is important [65]. Patients must obtain sufficient records on the supposed usage, accessibility, and reason of their data. However, making sure significant knowledgeable consent is difficult, specifically inside the context of huge-scale facts analytics where the particular uses of statistics may also change over time. The dynamic nature of healthcare research and the potential for unforeseen applications of statistics introduce challenges in keeping transparency and upholding patient autonomy [66]. Striking a stability between advancing scientific information and respecting affected person autonomy calls for modern solutions that cross past conventional consent models [67]. Figure 4 indicates the FL approach.

4.4. Data-sharing dilemma

Collaborative research and information sharing are cornerstones of scientific progress; however, in healthcare, locating the appropriate equilibrium among sharing information for collective advantage and protective personal privacy is problematic. While centralized methods facilitate data sharing for studies, they inherently reveal datasets to broader audiences, raising concerns about unintended disclosures. This tension is the supply of the dilemma among the need to pursue clinical advances and shield privacy. To remedy this war, privacy-maintaining techniques are important. They permit healthcare

Table 3
Privacy-preserving algorithms in federated learning

Algorithm	Key features	Applications in healthcare
Homomorphic Encryption [68]	Permits calculations on encoded information deprived of decryption.	Secure computation of aggregate statistics on sensitive patient data
Secure Multi-Party Computation [69]	Permits bashes together to calculate a function over their efforts although observance of those efforts is secretive.	Collaborative model training without exposing raw patient data
Differential Privacy [70]	Adds noise to the data to protect individual privacy during statistical analysis.	Aggregated data analysis with a provable level of privacy protection

Table 4
Summary of federated learning architectures in healthcare

Architecture type	Key characteristics	Applications in healthcare
Horizontal FL [71]	Multiple institutions have data on the same features but different samples.	Collaborative disease prediction, shared diagnostic models
Vertical FL [72]	Institutions have data on different features of the same samples.	Integrated patient data for comprehensive diagnostics
Federated Transfer Learning [73]	Utilizes pre-trained models and fine-tunes them on local data.	Improved model performance for specific healthcare tasks

businesses to take part in broader research while not having to compromise the confidentiality of sufferers' facts [74].

4.5. Stigmatization and discrimination

The privacy challenges extend beyond technical and regulatory issues to encompass societal influences. The disclosure of genetic or clinical predispositions can cause discrimination and stigma in the healthcare context [75]. Patients may not seek clinical attention or screen important data if they worry about social outcomes or discrimination. For instance, the revelation of a genetic predisposition to a certain disease can affect employment, coverage, and private relationships [76]. The moral quandary is balancing the clinical advantages of analytics with the damage that might be as a result of misinterpretation or misuse of the facts.

5. Federated Learning: A Privacy-Preserving Paradigm in Healthcare

The Healthcare system through its different groups of patient investigation history has extended efforts with the duty of opposite the possible for data-driven visions with the requirement to defend patient confidentiality. In this modern field, where the capacity of healthcare archives is growing, a distinctive model referred to as FL is developing as a transformative force [77]. This devolved device grasping method holds the capacity to transform the healthcare field highlighting the specific confidentiality problematic conditions connected to the central archives style.

5.1. Decentralized machine learning

FL emerges as a strong solution to the privacy challenges posed by centralized healthcare data analytics. At its core, a decentralized machine learning paradigm called FL allows model training to take place over a network of servers or devices that are hosting local data. Unlike traditional machine learning models that require centralized data aggregation, FL allows the training of models directly on the local data sources [78]. Table 3 privacy-preserving algorithms in FL. The key distinction lies in the collaborative nature of model training. Instead of pooling raw data into a central repository, FL enables the training of models locally on each device [79]. Instead of sending raw data to a central server for aggregation, just the model changes are sent.

FL decentralizes the model training process to solve the issues of patient confidentiality and data sharing. Only model updates are shared, and data stay on local devices, lowering the possibility of breaches and guaranteeing adherence to privacy laws like GDPR and HIPAA.

5.2. Understanding federated learning

FL, at its core, is a machine learning paradigm that decentralizes data collection and aggregation [80]. The FL allows collaborative learning between multiple devices and servers that each hold their data. The model can be trained on these devices; the only thing that is sent to the central server, instead of the raw data, is the updates. This fundamental shift in strategy has several advantages, particularly in the healthcare sector where sensitive patient data is critical. The FL ensures that data are kept confidential by eliminating the need for raw data to be transmitted. This guarantees that the information about the patient stays within the confines of the company that created it [81]. This gives the patients an added sense of trust and security, in addition to conforming to legal standards.

5.3. Maintaining confidentiality of data in healthcare

The confidentiality of patient data is dominant in healthcare domains. The FL is intended to attain this. The traditional techniques can be skilled by devolved information without a vital to unify accumulation [82]. The sensitivity of data crack throughout programmed is compact, and healthcare organizations can preserve control over intimate datasets. Consider a condition wherever some clinics cooperate to make a perfect that expects a medicinal situation. The FL permits the individual hospital to train its model with native data, deprived of the requirement to share the raw data with additional clinics. These different datasets are employed to connect the cooperative intellect that offers esteemed visions and does not negotiate discrete patient confidentiality.

5.4. Applications of federated learning in healthcare

The FL through its prominence on decentralized method exercise and information confidentiality has arisen as a radical model in healthcare domains [83]. This transformative method unlocks a countless of uses that influence cooperative intellect deprived of cooperating the privacy of complex persistent information. The following sections explore various domains in which FL has driven significant progress in the design of healthcare procedures.

5.5. Predictive analytics

The FL performed an essential part in evolving prognostic analysis inside the healthcare area [84]. Organizations collaboratively progress to defined prognostic simulations for illness evolution, patient consequences, and possible health difficulties deprived of the essential central accumulation of patient information. Figure 3 represents different FL approaches. This concerted strategy involves exercising traditional techniques on different enduring datasets agreeing for the abstraction of visions from many organizations. The conclusion is further appropriately precise in the prediction of disease perfection, reckoning human lives at high danger, and improving treatment strategies, resulting in proactive and tailor-made healthcare

interventions [85]. Table 4 presents the summary of FL architectures in healthcare. FL has demonstrated enormous promise in medicinal properties particularly in predictive analytics and tailored treatment. FL promotes the creation of highly accurate illness prediction models and individualized treatment plans by enabling models to be trained across several institutions without exchanging raw data, protecting patient privacy while enhancing healthcare results.

5.6. Disease diagnosis

FL may additionally increase the accuracy and performance of contamination diagnosis. Diagnostic models can be trained on local datasets without revealing raw patient data by utilizing collaborative insights from diverse datasets sourced from various healthcare organizations. The collaborative introduction of those models involves integrating know-how from numerous establishments to provide more complete and correct diagnostic equipment. This technique helps to enhance diagnostic talents, decrease misdiagnosis rates, and create fashions that are adaptable to exclusive patient companies and healthcare settings. Figure 5 shows FL for privacy-preserving in healthcare.

5.7. Treatment optimization

FL gives a framework for geared treatment plans and boosted healing interventions primarily based on collaborative insights gleaned from a whole lot of affected person businesses. Healthcare professionals can use this method to create models that predict remedy effects primarily based on affected person traits, genetic variables, and treatment records. These fashions had been skilled. Collaboration without the need to reveal relevant patient details can result in extra personalized remedy tips, fewer unwanted facet outcomes, and higher remedy consequences interventions.

5.8. Clinical research and trials

FL promotes inter-institutional collaboration in clinical trials and studies while respecting patient privacy and confidentiality. Institutional facts are probably aggregated for studies without liberating the raw facts. Models can also be created together to examine remedy effectiveness adverse reactions, and patient responses across many patient corporations. The collaborative studies method shortens the look at periods and optimizes statistical strength by employing using large datasets. It additionally complements generalizability interventions.

5.9. Personalized medicine

Personalized medicine greatly benefits from FL. It accomplishes this by using tailoring medical care to the precise wishes of every affected person through integrating insights from decentralized records. This method makes it feasible to create customized models that account for factors specific to every affected person. These include lifestyle, clinical records, and genetics. Without unveiling particular patient facts, the ways may be educated throughout several establishments. This results in healthcare strategies which are correct, changed, and the top quality. Table 5 shows the comparison of privacy terms in centralized and decentralized healthcare approaches.

5.10. Public health surveillance

FL makes it possible to actively examine data acquired from many geographic places, which enhances public fitness surveillance talents. Without requiring crucial data sharing, this technique enables the creation of models to track disease outbreaks, identify health trends, and forecast population health

Figure 5
Federated learning for privacy preserving in healthcare

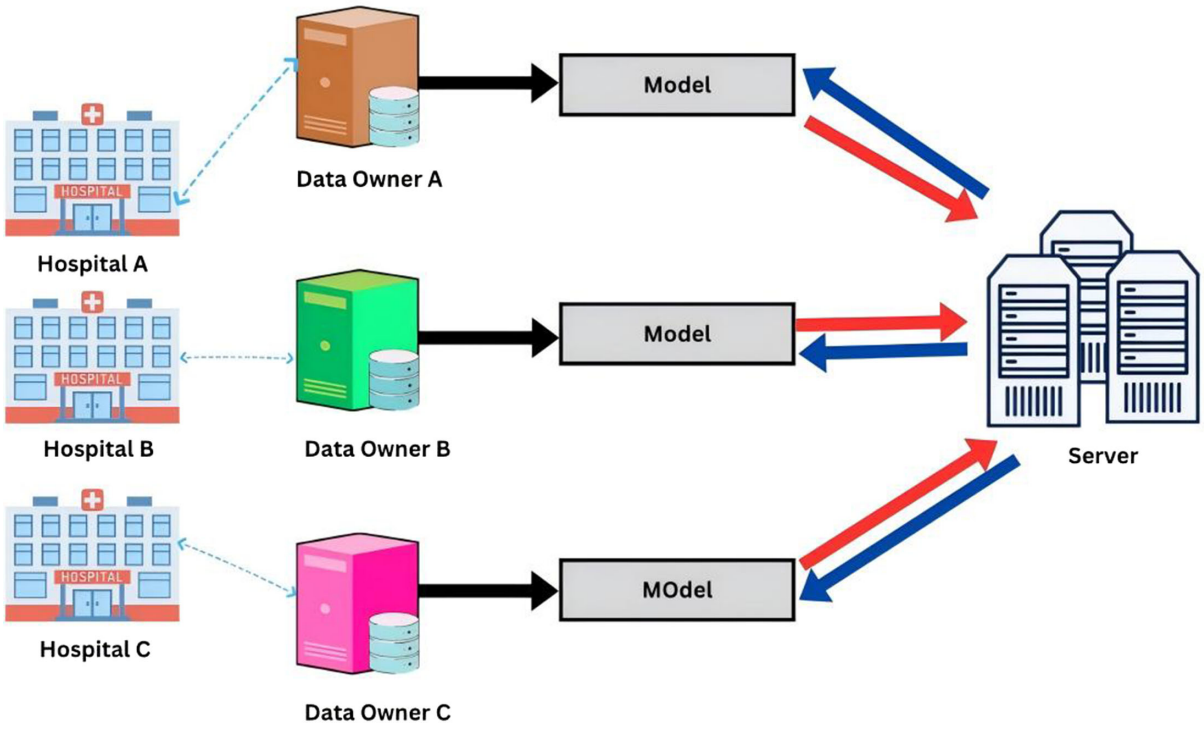


Table 5
Comparison of privacy terms in centralized and decentralized healthcare approaches

Privacy terms	Centralized approach	Decentralized approach
Data Encryption	40%	90%
Anonymization Techniques	30%	80%
Consent Management	30%	70%
Fine-Grained Access Control	20%	80%
Transparency & Auditability	30%	90%
Minimization of Data Collection	20%	80%
User Authentication & Authorization	40%	90%
Regulatory Compliance	40%	90%

impacts. This technique makes it feasible to become aware of infectious illnesses earlier, enforce public health treatments more effectively, and assess health developments in a diverse population.

6. Advantages of FL in Healthcare

6.1. Patient privacy protection in federated learning

This ensures that no health institution will be denied full authority to the healthcare data developed within its zones [86]. This decentralized approach protects privacy by reducing the risk of unintentional disclosures or unwanted access.

6.2. Compliance with regulatory standards

FL serves as a solution that adheres to the rigorous standards of healthcare data and has the potential to improve decision-making in the medical field [87]. They would be essential to assist in navigating within a regulatory environment so complex by controlling the extent of data sharing and providing precise control of updates to a model.

6.3. Dynamic consent

Healthcare research is often dynamic, and this challenges the traditional static nature of informed consent [88]. The FL reduces the requirement for consent to extensive data sharing by only transmitting model updates [89]. The updated model pursues the goals to respect autonomy that healthcare research in the evolution of patient rights has pushed toward.

6.4. Collaborative insights without data exchange

FL, with the ability to let multiple health organizations collaborate in developing a model without actually sharing raw data from patients, is eased by technologies [90]. This joint effort paves the way for a blend of multifarious datasets that, in turn, lead to the development of generalizable models and more reliably robust.

6.5. Future directions and emerging trends

The healthcare system endures to contend with confidentiality anxieties though determined to influence progressive skills for upgraded enduring care, numerous imminent instructions, and developing inclinations are composed to form the setting of privacy-preserving healthcare by FL. The most prominent direction is the modification of FL techniques and policies to improve confidentiality and security while preserving the usefulness of common models through different healthcare datasets. Moreover, merging FL with extra privacy-enhancing technologies like different data encrypted techniques to reinforce privacy health systems. One other important feature is the importance of moral thoughts and lawful outlines for FL rehearsal with strategies for enduring accord, data organization, and clearness in ideal training besides calculation rules. The union of blockchain, edge calculating FL, and developing tools such as these embraces the potential of dispersed and safe data sharing through the healthcare ecology. By embracing these future directions and emerging trends, stakeholders in the healthcare industry can foster innovation, protect patient privacy, and provide healthcare solutions that are based on personal data to enhance.

Future studies should concentrate on improving FL privacy-preserving capabilities through its integration with cutting-edge encryption techniques like safe multi-party computing and homomorphic encryption. Additionally, resolving model accuracy concerns in diverse settings and enhancing communication effectiveness would increase FL's efficacy in protecting patient privacy.

7. Practical Limitations and Challenges

Despite its advantages, FL presents real-world difficulties in the healthcare industry, especially when it comes to controlling communication expenses and model aggregation. While non-IID data between devices make model convergence more difficult, constant synchronization across devices raises overhead. Furthermore, device heterogeneity makes model aggregation procedures much more difficult, which lowers FL's effectiveness in actual healthcare environments.

While this survey highlights the current state of FL in healthcare, significant gaps remain, particularly in the areas of model aggregation, communication efficiency, and regulatory compliance. Future research should focus on developing robust FL architectures that can handle heterogeneous healthcare environments, integrate cutting-edge encryption technologies, and improve scalability without compromising privacy.

8. Conclusion

In conclusion, this study provides a thorough examination of potential privacy-preserving strategies in the healthcare industry, emphasizing the transformative significance of FL. A review of the literature and relevant research was conducted with a focus on the experience and summarization of the existing knowledge on the advantages, disadvantages, and potential opportunities of decentralized ways of learning. However, the value of the research is assumed by the sources Smith and Davis [57], and Wang et al. [91] gave the researchers additional perspectives on the peculiarities of the healthcare-FL connection. Looking back at our results, we find that FL is a valuable way to protect privacy while promoting the collective intelligence of decentralized healthcare data. To combat the continued challenges of centralization, including data security, interoperability, and patient sovereignty, inventive answers are required. The FL is a remedy for even the largest and most serious impediments of centralized strategies. The collaborative training approach overcomes the difficulties of exchange while simultaneously preserving patients' confidentiality. Thus, privacy-preserving analytics in healthcare is a future where FL retains significant potential. Advancements in federated architectural systems and blockchain technology are shaping the future of healthcare analytics. As researchers and clinicians continue to

grapple with healthcare data complexity, FL stands out as a prime tool for preserving and advancing healthcare analytics. The survey is beneficial to understanding this dynamic area and acts as a guide for future efforts in chasing privacy-conscious healthcare innovations.

Ethical Statement

This study does not contain any studies with human or animal subjects performed by any of the authors.

Conflicts of Interest

The authors declare that they have no conflicts of interest to this work.

Data Availability Statement

Data sharing is not applicable to this article as no new data were created or analyzed in this study.

Author Contribution Statement

Faria Karamat: Conceptualization, Data curation, Writing – original draft, Conceptualization. **Atta Ur Rahman:** Investigation, Resources, Supervision. **Bibi Saqia:** Methodology, Writing – review & editing, Visualization. **Adeel Zafar:** Validation, Project administration**. Waqas Ali Khan:** Formal analysis.

References

[1] Dash, S., Shakyawar, S. K., Sharma, M., & Kaushik, S. (2019). Big data in healthcare: Management, analysis and future prospects. *Journal of Big Data*, *6*(1), 54. https://doi.org/10.1186/s40537-019-0217-0

[2] Jaime, F. J., Muñoz, A., Rodríguez-Gómez, F., & Jerez-Calero, A. (2023). Strengthening privacy and data security in biomedical microelectromechanical systems by IoT communication security and protection in smart healthcare. *Sensors*, *23*(21), 8944. https://doi.org/10.3390/s23218944

[3] Feldman, K., Johnson, R. A., & Chawla, N. V. (2018). The state of data in healthcare: Path towards standardization. *Journal of Healthcare Informatics Research*, *2*(3), 248–271. https://doi.org/10.1007/s41666-018-0019-8

[4] Abouelmehdi, K., Beni-Hessane, A., & Khaloufi, H. (2018). Big healthcare data: Preserving security and privacy. *Journal of Big Data*, *5*(1), 1. https://doi.org/10.1186/s40537-017-0110-7

[5] Chandra, S., Ray, S., & Goswami, R. T. (2017). Big data security in healthcare: Survey on frameworks and algorithms. In *2017 IEEE 7th International Advance Computing Conference*, 89–94. https://doi.org/10.1109/IACC.2017.0033

[6] Majeed, A., Zhang, X., & Hwang, S. O. (2022). Applications and challenges of federated learning paradigm in the big data era with special emphasis on COVID-19. *Big Data and Cognitive Computing*, *6*(4), 127. https://doi.org/10.3390/bdcc6040127

[7] Martínez Beltrán, E. T., Pérez, M. Q., Sánchez, P. M. S., Bernal, S. L., Bovet, G., Pérez, M. G., . . . , & Celdrán, A. H. (2023). Decentralized federated learning: Fundamentals, state of the art, frameworks, trends, and challenges. *IEEE Communications Surveys & Tutorials*, *25*(4), 2983–3013. https://doi.org/10.1109/COMST.2023.3315746

[8] Oh, S. R., Seo, Y. D., Lee, E., & Kim, Y. G. (2021). A comprehensive survey on security and privacy for electronic health data. *International Journal of Environmental Research and Public Health*, *18*(18), 9668. https://doi.org/10.3390/ijerph18189668

[9] Tresp, V., Overhage, J. M., Bundschus, M., Rabizadeh, S., Fasching, P. A., & Yu, S. (2016). Going digital: A survey on digitalization and large-scale data analytics in healthcare. In *Proceedings of the IEEE*, *104*(11), 2180–2206. https://doi.org/10.1109/JPROC.2016.2615052

[10] Khan, M. F., & AbaOud, M. (2023). Blockchain-integrated security for real-time patient monitoring in the Internet of Medical Things using federated learning. *IEEE Access*, *11*, 117826–117850. https://doi.org/10.1109/ACCESS.2023.3326155

[11] Alam, T., & Gupta, R. (2022). Federated learning and its role in the privacy preservation of IoT devices. *Future Internet*, *14*(9), 246. https://doi.org/10.3390/fi14090246

[12] Nguyen, D. C., Pham, Q. V., Pathirana, P. N., Ding, M., Seneviratne, A., Lin, Z., . . . , & Hwang, W. J. (2022). Federated learning for smart healthcare: A survey. *ACM Computing Surveys*, *55*(3), 60. https://doi.org/10.1145/3501296

[13] Rathore, S., Kwon, B. W., & Park, J. H. (2019). BlockSecIoTNet: Blockchain-based decentralized security architecture for IoT network. *Journal of Network and Computer Applications*, *143*, 167–177. https://doi.org/10.1016/j.jnca.2019.06.019

[14] Ali, A., Al-rimy, B. A. S., Tin, T. T., Altamimi, S. N., Qasem, S. N., & Saeed, F. (2023). Empowering precision medicine: Unlocking revolutionary insights through blockchain-enabled federated learning and electronic medical records. *Sensors*, *23*(17), 7476. https://doi.org/10.3390/s23177476

[15] Hiwale, M., Walambe, R., Potdar, V., & Kotecha, K. (2023). A systematic review of privacy-preserving methods deployed with blockchain and federated learning for the telemedicine. *Healthcare Analytics*, *3*, 100192. https://doi.org/10.1016/j.health.2023.100192

[16] Bebortta, S., Tripathy, S. S., Basheer, S., & Chowdhary, C. L. (2023). Fedehr: A federated learning approach towards the prediction of heart diseases in IoT-based electronic health records. *Diagnostics*, *13*(20), 3166. https://doi.org/10.3390/diagnostics13203166

[17] Singh, B. (2023). Federated learning for envision future trajectory smart transport system for climate preservation and smart green planet: Insights into global governance and SDG-9 (industry, innovation and infrastructure). *National Journal of Environmental Law*, *6*(2), 6–17.

[18] Markkandan, S., Bhavani, N. P. G., & Nath, S. S. (2024). A privacy-preserving expert system for collaborative medical diagnosis across multiple institutions using federated learning. *Scientific Reports*, *14*(1), 22354. https://doi.org/10.1038/s41598-024-73334-7

[19] Li, L., Fan, Y., Tse, M., & Lin, K. Y. (2020). A review of applications in federated learning. *Computers & Industrial Engineering*, *149*, 106854. https://doi.org/10.1016/j.cie.2020.106854

[20] Albalawi, E., TR, M., Thakur, A., Kumar, V. V., Gupta, M., Khan, S. B., & Almusharraf, A. (2024). Integrated approach of federated learning with transfer learning for classification and diagnosis of brain tumor. *BMC Medical Imaging*, *24*(1), 110. https://doi.org/10.1186/s12880-024-01261-0

[21] Cui, Y., Li, Z., Liu, L., Zhang, J., & Liu, J. (2022). Privacy-preserving speech-based depression diagnosis via federated learning. In *2022 44th Annual International Conference of the IEEE Engineering in Medicine & Biology Society*, 1371–1374. https://doi.org/10.1109/EMBC48229.2022.9871861

[22] Pfitzner, B., Steckhan, N., & Arnrich, B. (2021). Federated learning in a medical context: A systematic literature review.

ACM Transactions on Internet Technology, *21*(2), 50. https://doi.org/10.1145/3412357

[23] Li, J., Meng, Y., Ma, L., Du, S., Zhu, H., Pei, Q., & Shen, X. (2022). A federated learning based privacy-preserving smart healthcare system. *IEEE Transactions on Industrial Informatics*, *18*(3), 2021–2031. https://doi.org/10.1109/TII.2021.3098010

[24] Ali, M., Naeem, F., Tariq, M., & Kaddoum, G. (2023). Federated learning for privacy preservation in smart healthcare systems: A comprehensive survey. *IEEE Journal of Biomedical and Health Informatics*, *27*(2), 778–789. https://doi.org/10.1109/JBHI.2022.3181823

[25] Adnan, M., Kalra, S., Cresswell, J. C., Taylor, G. W., & Tizhoosh, H. R. (2022). Federated learning and differential privacy for medical image analysis. *Scientific Reports*, *12*(1), 1953. https://doi.org/10.1038/s41598-022-05539-7

[26] Ma, Z., Zhang, M., Liu, J., Yang, A., Li, H., Wang, J., . . . , & Li, M. (2022). An assisted diagnosis model for cancer patients based on federated learning. *Frontiers in Oncology*, *12*, 860532. https://doi.org/10.3389/fonc.2022.860532

[27] Butt, M., Tariq, N., Ashraf, M., Alsagri, H. S., Moqurrab, S. A., Alhakbani, H. A. A., & Alduraywish, Y. A. (2023). A fog-based privacy-preserving federated learning system for smart healthcare applications. *Electronics*, *12*(19), 4074. https://doi.org/10.3390/electronics12194074

[28] Huma, Z. E., Tariq, N., & Zaidi, S. (2024). Predictive machine learning models for early diabetes diagnosis: Enhancing accuracy and privacy with federated learning. *Journal of Computing & Biomedical Informatics*, *8*(01), 1–17.

[29] Ali, A., Ali, H., Saeed, A., Ahmed Khan, A., Tin, T. T., Assam, M., . . . , & Mohamed, H. G. (2023). Blockchain-powered healthcare systems: Enhancing scalability and security with hybrid deep learning. *Sensors*, *23*(18), 7740. https://doi.org/10.3390/s23187740

[30] Rauniyar, A., Hagos, D. H., Jha, D., Håkegård, J. E., Bagci, U., Rawat, D. B., & Vlassov, V. (2024). Federated learning for medical applications: A taxonomy, current trends, challenges, and future research directions. *IEEE Internet of Things Journal*, *11*(5), 7374–7398. https://doi.org/10.1109/JIOT.2023.3329061

[31] 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. https://doi.org/10.1109/ACCESS.2023.3301162

[32] Nair, A. K., Sahoo, J., & Raj, E. D. (2023). Privacy preserving federated learning framework for IoMT based big data analysis using edge computing. *Computer Standards & Interfaces*, *86*, 103720. https://doi.org/10.1016/j.csi.2023.103720

[33] Nandhini, J. M., Joshi, S., & Anuratha, K. (2022). Federated learning based prediction of chronic kidney diseases. In *2022 1st International Conference on Computational Science and Technology*, 1–6. https://doi.org/10.1109/ICCST55948.2022.10040317

[34] Thummisetti, B. S. P., &Atluri, H. (2024). Advancing healthcare informatics for empowering privacy and security through federated learning paradigms. *International Journal of Su Development in Computing Science*, *6*(1), 1–16.

[35] Zhang, F., Kreuter, D., Chen, Y., Dittmer, S., Tull, S., Shadbahr, T., . . . , & Roberts, M. (2024). Recent methodological advances in federated learning for healthcare. *Patterns*, *5*(6), 101006. https://doi.org/10.1016/j.patter.2024.101006

[36] Lakhan, A., Hamouda, H., Abdulkareem, K. H., Alyahya, S., & Mohammed, M. A. (2024). Digital healthcare framework for patients with disabilities based on deep federated learning schemes. *Computers in Biology and Medicine*, *169*, 107845. https://doi.org/10.1016/j.compbiomed.2023.107845

[37] Messinis, S. C., Protonotarios, N. E., Arapidis, E., & Doulamis, N. (2024). Client selection and resource allocation via graph neural networks for efficient federated learning in healthcare environments. In *Proceedings of the 17th International Conference on PErvasive Technologies Related to Assistive Environments*, 606–612. https://doi.org/10.1145/3652037.3663906

[38] Tripathy, S. S., Bebortta, S., Chowdhary, C. L., Mukherjee, T., Kim, S., Shafi, J., & Ijaz, M. F. (2024). FedHealthFog: A federated learning-enabled approach towards healthcare analytics over fog computing platform. *Heliyon*, *10*(5), e26416. https://doi.org/10.1016/j.heliyon.2024.e26416

[39] Sachin, D. N., Annappa, B., Hegde, S., Abhijit, C. S., & Ambesange, S. (2024). Fedcure: A heterogeneity-aware personalized federated learning framework for intelligent healthcare applications in IoMT environments. *IEEE Access*, *12*, 15867–15883. https://doi.org/10.1109/ACCESS.2024.3357514

[40] Zhang, F., Shuai, Z., Kuang, K., Wu, F., Zhuang, Y., & Xiao, J. (2024). Unified fair federated learning for digital healthcare. *Patterns*, *5*(1), 100907. https://doi.org/10.1016/j.patter.2023.100907

[41] Muazu, T., Mao, Y., Muhammad, A. U., Ibrahim, M., Kumshe, U. M. M., & Samuel, O. (2024). A federated learning system with data fusion for healthcare using multi-party computation and additive secret sharing. *Computer Communications*, *216*, 168–182. https://doi.org/10.1016/j.comcom.2024.01.006

[42] Alsamhi, S. H., Myrzashova, R., Hawbani, A., Kumar, S., Srivastava, S., Zhao, L., . . . , & Curry, E. (2024). Federated learning meets blockchain in decentralized data sharing: Healthcare use case. *IEEE Internet of Things Journal*, *11*(11), 19602–19615. https://doi.org/10.1109/JIOT.2024.3367249

[43] Tang, Z., Shi, S., Wang, W., & Li, B. (2020). Communication-efficient distributed deep learning: A comprehensive survey. *arXiv Preprint:2003.06307*.

[44] Schneider, P. (2018). Managerial challenges of Industry 4.0: An empirically backed research agenda for a nascent field. *Review of Managerial Science*, *12*(3), 803–848. https://doi.org/10.1007/s11846-018-0283-2

[45] Rehm, H. L., Page, A. J. H., Smith, L., Adams, J. B., Alterovitz, G., Babb, L. J., . . . , & Birney, E. (2021). GA4GH: International policies and standards for data sharing across genomic research and healthcare. *Cell Genomics*, *1*(2), 100029. https://doi.org/10.1016/j.xgen.2021.100029

[46] Ji, S., Tan, Y., Saravirta, T., Yang, Z., Liu, Y., Vasankari, L., . . . , & 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. https://doi.org/10.1007/s13042-024-02119-1

[47] Madduri, R., Li, Z., Nandi, T., Kim, K., Ryu, M., & Rodriguez, A. (2024). Advances in privacy preserving federated learning to realize a truly learning healthcare system. In *2024 IEEE 6th International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications*, 273–279. https://doi.org/10.1109/TPS-ISA62245.2024.00039

[48] Silva, I., & Soto, M. (2022). Privacy-preserving data sharing in healthcare: An in-depth analysis of big data solutions and regulatory compliance. *International Journal of Applied Health Care Analytics*, *7*(1), 14–23.

[49] Chernyshev, M., Zeadally, S., & Baig, Z. (2019). Healthcare data breaches: Implications for digital forensic readiness. *Journal of Medical Systems*, *43*(1), 7. https://doi.org/10.1007/s10916-018-1123-2

[50] Iroju, O., Soriyan, A., Gambo, I., & Olaleke, J. (2013). Interoperability in healthcare: Benefits, challenges and resolutions. *International Journal of Innovation and Applied Studies*, *3*(1), 262–270.

[51] AlSalman, H., Al-Rakhami, M. S., Alfakih, T., & Hassan, M. M. (2024). Federated learning approach for breast cancer detection based on DCNN. *IEEE Access*, *12*(1), 40114–40138. https://doi.org/10.1109/ACCESS.2024.3374650

[52] Lee, E. K., Atallah, H. Y., Wright, M. D., Post, E. T., Thomas, C., Wu, D. T., & Haley, L. L. (2015). Transforming hospital emergency department workflow and patient care. *Interfaces*, *45*(1), 58–82. https://doi.org/10.1287/inte.2014.0788

[53] Dove, E. S., & Phillips, M. (2015). Privacy law, data sharing policies, and medical data: A comparative perspective. In A. Gkoulalas-Divanis & G. Loukides (Eds.), *Medical data privacy handbook* (pp. 639–678). Springer.

[54] Díaz, J. S. P., & García, Á. L. (2023). Study of the performance and scalability of federated learning for medical imaging with intermittent clients. *Neurocomputing*, *518*, 142–154. https://doi.org/10.1016/j.neucom.2022.11.011

[55] Hutchings, E., Loomes, M., Butow, P., & Boyle, F. M. (2020). A systematic literature review of health consumer attitudes towards secondary use and sharing of health administrative and clinical trial data: A focus on privacy, trust, and transparency. *Systematic Reviews*, *9*(1), 235. https://doi.org/10.1186/s13643-020-01481-9

[56] Rahman, A. U., Saqia, B., Alsenani, Y. S., & Ullah, I. (2024). Data quality, bias, and strategic challenges in reinforcement learning for healthcare: A survey. *International Journal of Data Informatics and Intelligent Computing*, *3*(3), 24–42. https://doi.org/10.59461/ijdiic.v3i3.128

[57] Smith, R. G., & Davis, R. (1981). Frameworks for cooperation in distributed problem solving. *IEEE Transactions on Systems, Man, and Cybernetics*, *11*(1), 61–70. https://doi.org/10.1109/TSMC.1981.4308579

[58] Rahman, K. J., Ahmed, F., Akhter, N., Hasan, M., Amin, R., Aziz, K. E., . . . , & Islam, A. N. (2021). Challenges, applications and design aspects of federated learning: A survey. *IEEE Access*, *9*, 124682–124700. https://doi.org/10.1109/ACCESS.2021.3111118

[59] Javaid, M., Haleem, A., Singh, R. P., & Suman, R. (2023). Towards insighting cybersecurity for healthcare domains: A comprehensive review of recent practices and trends. *Cyber Security and Applications*, *1*, 100016. https://doi.org/10.1016/j.csa.2023.100016

[60] Li, H., Li, C., Wang, J., Yang, A., Ma, Z., Zhang, Z., & Hua, D. (2023). Review on security of federated learning and its application in healthcare. *Future Generation Computer Systems*, *144*, 271–290. https://doi.org/10.1016/j.future.2023.02.021

[61] Keshta, I., & Odeh, A. (2021). Security and privacy of electronic health records: Concerns and challenges. *Egyptian Informatics Journal*, *22*(2), 177–183. https://doi.org/10.1016/j.eij.2020.07.003

[62] Azad, M. A., Arshad, J., Mahmoud, S., Salah, K., & Imran, M. (2022). A privacy-preserving framework for smart context-aware healthcare applications. *Transactions on Emerging Telecommunications Technologies*, *33*(8), e3634. https://doi.org/10.1002/ett.3634

[63] Determann, L. (2020). Healthy data protection. *Michigan Telecommunications and Technology Law Review*, *26*(2), 229–278. https://doi.org/10.36645/mtlr.26.2.healthy

[64] Sharma, S. (2019). *Data privacy and GDPR handbook*. USA: Wiley. https://doi.org/10.1002/9781119594307

[65] Lynöe, N., Sandlund, M., Dahlqvist, G., & Jacobsson, L. (1991). Informed consent: Study of quality of information given to participants in a clinical trial. *British Medical Journal*, *303*, 610–613. https://doi.org/10.1136/bmj.303.6803.610

[66] Cheung, A. S. Y. (2018). Moving beyond consent for citizen science in big data health and medical research. *Northwestern Journal of Technology and Intellectual Property*, *16*(1), 2. https://doi.org/10.2139/ssrn.2943185

[67] Meisel, A. (1979). The "exceptions" to the informed consent doctrine: Striking a balance between competing values in medical decisionmaking. *Wisconsin Law Review*, *1979*(2), 413–488.

[68] Yi, X., Paulet, R., & Bertino, E. (2014). Homomorphic encryption. In X. Yi, R. Paulet & E. Bertino (Eds.), *Homomorphic encryption and applications* (pp. 27–46). Springer.

[69] Goldreich, O. (1998). *Secure multi-party computation* [Manuscript in preparation]. Department of Computer Science and Applied Mathematics, Weizmann Institute of Science.

[70] Dwork, C. (2008). Differential privacy: A survey of results. In *Theory and Applications of Models of Computation: 5th International Conference*, 1–19. https://doi.org/10.1007/978-3-540-79228-4_1

[71] Zhu, H., Zhang, H. & Jin, Y. (2021). From federated learning to federated neural architecture search: A survey. *Complex & Intelligent Systems*, *7*(2), 639–657. https://doi.org/10.1007/s40747-020-00247-z

[72] Wei, K., Li, J., Ma, C., Ding, M., Wei, S., Wu, F., & Chen, G. (2021). Vertical federated learning: Challenges, methodologies and experiments. *arXiv Preprint: 2202.04309*.

[73] Liu, Y., Kang, Y., Xing, C., Chen, T., & Yang, Q. (2020). A secure federated transfer learning framework. *IEEE Intelligent Systems*, *35*(4), 70–82. https://doi.org/10.1109/MIS.2020.2988525

[74] Wirth, F. N., Meurers, T., Johns, M., & Prasser, F. (2021). Privacy-preserving data sharing infrastructures for medical research: Systematization and comparison. *BMC Medical Informatics and Decision Making*, *21*(1), 242. https://doi.org/10.1186/s12911-021-01602-x

[75] Gostin, L. (1991). Genetic discrimination: The use of genetically based diagnostic and prognostic tests by employers and insurers. *American Journal of Law & Medicine*, *17*(1–2), 109–144. https://doi.org/10.1017/S0098858800007942

[76] Capron, A. M. (2000). Genetics and insurance: Accessing and using private information. *Social Philosophy and Policy*, *17*(2), 235–275. https://doi.org/10.1017/S0265052500002181

[77] Dasaradharami Reddy, K., & Gadekallu, T. R. (2023). A comprehensive survey on federated learning techniques for healthcare informatics. *Computational Intelligence and Neuroscience*, *2023*(1), 8393990. https://doi.org/10.1155/2023/8393990

[78] 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. https://doi.org/10.1109/COMST.2021.3075439

[79] Imteaj, A., Thakker, U., Wang, S., Li, J., & Amini, M. H. (2022). A survey on federated learning for resource-constrained IoT devices. *IEEE Internet of Things Journal*, *9*(1), 1–24. https://doi.org/10.1109/JIOT.2021.3095077

[80] Sobel, B. L. W. (2018). Artificial intelligence's fair use crisis. *The Columbia Journal of Law & The Arts*, *41*(1), 45–97. https://doi.org/10.7916/jla.v41i1.2036

[81] Zhang, P., & Kamel Boulos, M. N. (2022). Privacy-by-design environments for large-scale health research and federated

learning from data. *International Journal of Environmental Research and Public Health*, *19*(19), 11876.https://doi.org/10.3390/ijerph191911876

[82] McMahan, H. B., Moore, E., Ramage, D., Hampson, S., & Aguera y Arcas, B. (2017). Communication-efficient learning of deep networks from decentralized data. In *Proceedings of the 20th International Conference on Artificial Intelligence and Statistics*, *54*, 1273–1282.

[83] Shiranthika, C., Saeedi, P., & Bajić, I. V. (2023). Decentralized learning in healthcare: a review of emerging techniques. *IEEE Access*, *11*, 54188–54209. https://doi.org/10.1109/ACCESS.2023.3281832

[84] Rehman, A., Abbas, S., Khan, M. A., Ghazal, T. M., Adnan, K. M., & Mosavi, A. (2022). A secure healthcare 5.0 system based on blockchain technology entangled with federated learning technique. *Computers in Biology and Medicine*, *150*, 106019. https://doi.org/10.1016/j.compbiomed.2022.106019

[85] Ahmed, Z., Mohamed, K., Zeeshan, S., & Dong, X. Q. (2020). Artificial intelligence with multi-functional machine learning platform development for better healthcare and precision medicine. *Datebase*, *2020*, baaa010. https://doi.org/10.1093/database/baaa010

[86] Rieke, N., Hancox, J., Li, W., Milletarì, F., Roth, H. R., Albarqouni, S., . . . , & Cardoso, M. J. (2020). The future of digital health with federated learning. *npj Digital Medicine*, *3*(1), 119. https://doi.org/10.1038/s41746-020-00323-1

[87] Antunes, R. S., André da Costa, C., Küderle, A., Yari, I. A., & Eskofier, B. (2022). Federated learning for healthcare: Systematic review and architecture proposal. *ACM Transactions on Intelligent Systems and Technology (TIST)*, *13*(4), 1–23. https://doi.org/10.1145/3501813

[88] Kaye, J., Whitley, E. A., Lund, D., Morrison, M., Teare, H., & Melham, K. (2015). Dynamic consent: A patient interface for twenty-first century research networks. *European Journal of Human Genetics*, *23*(2), 141–146. https://doi.org/10.1038/ejhg.2014.71

[89] Lu, Y., Huang, X., Zhang, K., Maharjan, S., & Zhang, Y. (2020). Blockchain empowered asynchronous federated learning for secure data sharing in internet of vehicles. *IEEE Transactions on Vehicular Technology*, *69*(4), 4298–4311. https://doi.org/10.1109/TVT.2020.2973651

[90] Sheller, M. J., Edwards, B., Reina, G. A., Martin, J., Pati, S., Kotrotsou, A., . . . , & Bakas, S. (2020). Federated learning in medicine: Facilitating multi-institutional collaborations without sharing patient data. *Scientific Reports*, *10*(1), 12598. https://doi.org/10.1038/s41598-020-69250-1

[91] Wang, Y., Kung, L., & Byrd, T. A. (2018). Big data analytics: Understanding its capabilities and potential benefits for healthcare organizations. *Technological Forecasting and Social Change*, *26*, 3–13. https://doi.org/10.1016/j.techfore.2015.12.019

How to Cite: Karamat, F., Rahman, A. U., Saqia, B., Zafar, A., & Khan, W. A. (2025). Addressing Privacy-Preservation in Healthcare Using Federated Learning: A Survey. *Artificial Intelligence and Applications*. https://doi.org/10.47852/bonviewAIA52023976