Smart Health 40 (2026) 100663

Contents lists available at ScienceDirect

Smart Health

journal homepage: www.elsevier.com/locate/smhl

Federated Artificial Intelligence approaches for wearables and health devices

Golshid Ranjbaran [a], Sergio Consoli [b], Gabriele Leoni [b], Diego Reforgiato Recupero [c,*], Chanchal K. Roy [a]

[a] Department of Computer Science, University of Saskatchewan, Thorvaldson 176 110 Science Place Saskatoon, SK CanadaS7N 5C9
[b] European Commission, Joint Research Centre (JRC), Via E. Fermi 2749, 21027 Ispra, Italy
[c] Department of Mathematics and Computer Science, University of Cagliari, Via Ospedale 72, 09124, Cagliari, Italy

ARTICLE INFO

Keywords:
Federated Learning (FL)
Wearable health devices
Privacy data preservation
Sensor technology
Cloud computing
Blockchain integration
Remote patient monitoring
Personalized healthcare

ABSTRACT

This review paper explores the integration of Federated Learning (FL) with wearable health devices, emphasizing its transformative potential in healthcare applications. The study systematically examines key criteria influencing the implementation and effectiveness of FL, particularly focusing on privacy data preservation, sensor technology, cloud computing, and blockchain integration. By comparing existing literature, our work highlights FL's ability to enhance data security and privacy while enabling real-time health monitoring and personalized treatment plans. The analysis includes a comprehensive examination of technical frameworks, emphasizing the use of wearable sensors and IoT devices in remote patient monitoring and chronic disease management. Additionally, the review addresses the challenges of scalability, interoperability, and regulatory compliance, proposing innovative strategies to overcome these barriers. Through this effort, the paper contributes to the expanding research on decentralized healthcare solutions, offering insights into the future directions and practical implications of FL in wearable health technologies.

1. Introduction

The integration of Artificial Intelligence (AI) in healthcare has led to significant advancements in disease prediction, patient monitoring, and personalized medicine. One of the emerging paradigms in AI-driven healthcare is Federated Learning (FL), a decentralized Machine Learning (ML) approach that facilitates model training across multiple devices by allowing data to remain on local devices, thus enhancing data privacy and security. This approach is particularly relevant for wearable health devices, which continuously collect physiological and behavioral data from users, providing real-time insights into their health status (Baucas et al., 2023a; Orzikulova et al., 2024).

Wearable health devices, including smartwatches, fitness trackers, and medical-grade sensors, generate vast amounts of data that can be leveraged for predictive analytics and early disease detection (Haghayegh et al., 2024). These devices continuously monitor various physiological parameters such as heart rate, blood oxygen levels, sleep patterns, body temperature, and physical activity (Alam et al., 2024). The collected data is processed using advanced algorithms to detect anomalies, assess overall health trends, and provide actionable insights to both users and healthcare professionals (Abbas et al., 2024). Wearable health devices are

* Corresponding author.
E-mail addresses: golshid.ranjbaran@usask.ca (G. Ranjbaran), sergio.consoli@ec.europa.eu (S. Consoli), gabriele.leoni@ec.europa.eu (G. Leoni), diego.reforgiato@unica.it (D.R. Recupero).

https://doi.org/10.1016/j.smhl.2026.100663
Received 15 May 2025; Received in revised form 14 April 2026; Accepted 25 April 2026
Available online 27 April 2026

widely used in chronic disease management, post-surgical recovery monitoring, and fitness tracking (Tongnian Wang et al., 2023). Moreover, their integration with mobile applications and cloud-based platforms enables remote monitoring, facilitating telemedicine and personalized treatment plans (Zhao et al., 2024). However, the large-scale deployment of these devices also introduces challenges such as data heterogeneity, sensor calibration issues, energy constraints, and interoperability concerns (Ali et al., 2022a). Traditional centralized machine learning methods pose significant risks related to privacy, data security, and regulatory compliance (Waqar, 2024). FL mitigates these concerns by ensuring that data remains on local devices while only model updates are shared, thereby enhancing patient privacy and reducing cybersecurity risks (Odera, 2023).

FL has also demonstrated significant benefits in various other domains. In finance, it has been employed to detect fraudulent transactions without exposing sensitive customer data (Rieke et al., 2020). In the telecommunications sector, FL has contributed in optimizing network performance while safeguarding user privacy (Pokhrel & Choi, 2020). Furthermore, in the context of smart cities, FL has improved traffic management and resource allocation by allowing decentralized data processing. These successes highlight FL's versatility and effectiveness across different industries, reinforcing its potential in healthcare applications (Ghadi et al., 2023).

The relevance of FL is further underscored by the upcoming European Health Data Space (EHDS), whose regulation came into force in March 2025.[1] The EHDS aims to create a harmonized framework for health data management across EU member states. Within the EHDS framework, federated AI models offer significant potential. Federated learning allows for decentralized AI model training, hence supporting cross-border collaborations without sharing or moving of raw data.

Several studies in the literature address FL in healthcare applications, yet none specifically focus on wearable health devices with our chosen criteria: Privacy, Sensors, Cloud Computing, and Blockchain Abbas et al. (2024). While existing works provide valuable insights into the broader applications of FL in healthcare, they often overlook the unique challenges posed by wearable devices, including their reliance on real-time data acquisition, limited computational power, and the need for seamless connectivity (Baucas et al., 2023a). The increasing adoption of wearable technologies highlights the urgent need for targeted research that explores how FL can enhance privacy, improve data efficiency, optimize sensor integration, leverage cloud computing, and employ blockchain for secure, decentralized data management in wearable health technologies (Shahsavari et al., 2024).

While several surveys address FL in healthcare and Internet of Medical Things (IoMT), they typically adopt a system-agnostic perspective, treating devices as generic data sources within distributed infrastructures. However, wearable health devices introduce a distinct set of constraints that fundamentally affect the design and operation of FL systems.

In particular, wearable environments are characterized by: (i) strict energy and computational limitations, (ii) high-frequency and noisy physiological data streams, (iii) intermittent connectivity and user-driven availability, and (iv) strong requirements for real-time responsiveness and personalization. These constraints lead to non-trivial trade-offs between privacy, communication efficiency, model convergence, and device sustainability, which are not adequately captured in general FL-in-healthcare surveys.

Therefore, this work adopts a wearable-centric perspective, focusing on how these constraints shape the design and evaluation of FL systems in this context.

These characteristics motivate the selection of four key dimensions, Privacy, Sensors, Cloud Computing, and Blockchain, which jointly capture the primary system-level challenges of federated learning in wearable environments. Privacy is central due to the sensitive and continuously collected nature of physiological data. Sensor technologies influence data quality and heterogeneity, directly affecting model performance. Cloud computing supports scalable coordination and aggregation under resource constraints. Blockchain provides mechanisms to enhance trust, security, and traceability in decentralized settings.

Together, these dimensions provide a structured lens through which federated learning systems can be analyzed and optimized under wearable-specific constraints.

This review aims to explore the role of FL in healthcare applications, with a particular focus on wearable health devices. A terminological clarification is necessary before proceeding. Throughout this review, privacy and security are treated as distinct but interdependent dimensions. Privacy governs which parties may legitimately access or infer information from health data — a concern directly served by FL's architectural property of retaining raw data on local devices. Security, by contrast, refers to the technical, administrative, and physical safeguards that protect data and systems from unauthorized access, manipulation, or breach. This distinction is consequential because regulatory frameworks such as the Health Insurance Portability and Accountability Act (HIPAA)[2] Security Rule and the General Data Protection Regulation (GDPR)[3] impose requirements on both dimensions in ways that are not interchangeable. A system may preserve privacy at the algorithmic level while remaining exposed to security vulnerabilities at the device, communication, or infrastructure level. These four dimensions not only reflect the core system-level challenges of wearable federated learning, but also collectively span both privacy and security concerns. Privacy-preserving mechanisms such as differential privacy and secure aggregation address data confidentiality, while encryption, authentication, and blockchain-based audit controls engage system-level security. Where the reviewed literature conflates these concepts or addresses one at the expense of the other, this review explicitly identifies such gaps.

Building on these four dimensions, the study systematically examines how FL can be effectively designed and deployed under wearable constraints, as follows:

- *Privacy*: Ensuring compliance with health data regulations (e.g., HIPAA and GDPR) while maintaining data confidentiality across decentralized systems.

[1] European Health Data Space Regulation: https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space-regulation-ehds_en.

[2] https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html

[3] https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

- *Sensors*: Evaluating how sensor technologies embedded in wearables affect data quality, heterogeneity, and FL model performance.
- *Cloud Computing*: Investigating the role of cloud-based aggregation and computational offloading to improve scalability and efficiency in FL frameworks.
- *Blockchain*: Exploring blockchain-based solutions to enhance security, trust, and traceability in federated learning implementations.

By reviewing recent advancements and case studies, this paper provides a comprehensive analysis of how FL can be optimized for wearable healthcare applications while addressing existing challenges and future research directions.

In particular, this paper makes the following contributions:

- We provide a wearable-centric review of federated learning in healthcare, highlighting how device-level constraints fundamentally influence FL design.
- We synthesize a structured analytical framework to systematically examine FL systems in wearable environments.
- We perform a dual-level analysis combining review papers and technical implementations, supported by a feature-based taxonomy of 11 dimensions.
- We identify key system-level trade-offs specific to wearable FL, including energy vs. accuracy, personalization vs. generalization, and decentralization vs. convergence.
- We conceptualize federated learning in wearables as a multi-objective system design problem.

The remainder of this paper is structured as follows. Section 2 reviews the state of the art on FL in healthcare applications, highlighting how our work differentiates from existing studies. Section 3 outlines the methodology used for paper selection, detailing the inclusion and exclusion criteria. Section 4 presents an analysis of relevant review studies, discussing their insights into the integration of wearable health devices with federated AI models. Section 5 classifies and examines technical studies on wearables and health devices, focusing on key distinguishing features. Section 6 synthesizes the main findings, identifying emerging trends and critical challenges. Section 7 translates these insights into practical design guidelines for optimizing FL systems in wearable healthcare contexts. Finally, Section 8 concludes the paper by summarizing the key takeaways and outlines potential directions for future research.

2. Related work

2.1. Literature

Several studies address FL in healthcare applications, yet none specifically focus on wearable health devices with our chosen criteria (i.e., privacy, sensing, cloud-based processing, and blockchain mechanisms). While comprehensive reviews of FL in smart healthcare discuss various designs, including privacy-aware FL, resource-aware FL, and incentive mechanisms, they take a broad perspective rather than focusing exclusively on wearable health devices, as highlighted in several works, such as in Nguyen et al. (2022).

FL is noted for its potential in privacy-preserving healthcare analytics (Pfitzner et al., 2021), yet these surveys often do not deeply delve into wearable health technologies or our specific criteria. The pipeline, applications, and challenges of FL in healthcare — such as data heterogeneity, security risks, and model training inefficiencies — are analyzed in other studies (Joshi et al., 2022), though they remain focused on general healthcare applications rather than wearables.

Further, reviews of FL applications in healthcare, particularly in medical imaging and expert diagnosis, often center on improving data-sharing efficiency while preserving privacy, without extensively discussing sensor-based wearable health monitoring (Chaddad et al., 2023). Explorations of privacy preservation in smart healthcare systems emphasize the role of IoMT devices (Ali et al., 2022b); however, they lack specific insights into wearable health sensors.

Mobile health applications utilize FL for remote monitoring and diagnosis, showing potential for handling sensitive, heterogeneous data (Tongnian Wang et al., 2023), but do not directly explore cloud computing and blockchain integration in wearable health devices.

Recent studies have begun addressing relevant aspects. For instance, (Putra et al., 2024) emphasizes a cloud–edge AI framework and the role of Edge Federated Learning (EFL) in handling large-scale medical data analytics in wearable personal health monitoring. Although this work highlights security and computational constraints of IoMT, it does not directly focus on FL in wearable health devices. Similarly, a comprehensive survey explores privacy-preserving FL for smart healthcare, discussing security challenges in IoMT networks and proposing advanced FL architectures (Ali et al., 2022a). However, it does not specifically investigate the intersection of FL, wearable devices, and blockchain for secure health monitoring.

These contributions offer valuable insights into FL's application in healthcare but underscore the need for targeted research on its role in wearable health devices, particularly concerning Privacy, Sensors, Cloud Computing, and Blockchain.

Table 1
Topics comparison between our paper and the state of the art (sorted chronologically).

Paper	Year	Privacy	Sensors	Cloud Computing	Blockchain
Pfitzner et al. (2021)	2021	✓			
Nguyen et al. (2022)	2022	✓	✓		
Joshi et al. (2022)	2022	✓		✓	
Ali et al. (2022a)	2022	✓		✓	✓
Chaddad et al. (2023)	2023	✓	✓		
Tongnian Wang et al. (2023)	2023	✓	✓	✓	
Putra et al. (2024)	2024	✓	✓	✓	
Our paper	2025	✓	✓	✓	✓

2.2. Comparison against the state of the art

In Table 1, we compare the existing literature reviews against our paper in terms of the topics covered. Specifically, in Section 1, we outlined the purpose of this paper: a survey on FL in wearable health devices, focusing on four main criteria: Privacy, Sensors, Cloud Computing, and Blockchain. Therefore, the comparison in Table 1 illustrates which of these criteria are addressed by each state-of-the-art paper.

Several prior works provide broad reviews of FL in healthcare. For instance, (Pfitzner et al., 2021) offers a systematic literature review on FL applications in the medical domain, focusing on privacy preservation and regulatory compliance. However, it does not specifically cover wearable health devices, sensors, cloud computing, or blockchain. Similarly, (Nguyen et al., 2022) discusses privacy-aware and resource-aware FL applications in smart healthcare, incorporating insights into sensor usage. Despite its contributions, it does not explore cloud computing and blockchain integration for wearable health monitoring.

Additional studies investigate FL's applicability to specific healthcare applications. For example, (Joshi et al., 2022) examines FL's pipeline, applications, and challenges, addressing issues such as data heterogeneity and training inefficiencies. While it considers cloud computing aspects, it does not provide a structured evaluation of FL for wearable health sensors. Similarly, (Chaddad et al., 2023) focuses on FL models for medical imaging and expert diagnosis, incorporating sensor-based data processing but without discussing cloud computing or blockchain integration.

Recent surveys have attempted to bridge this gap. Tongnian Wang et al. (2023) reviews FL applications in mobile health (mHealth), emphasizing remote health monitoring and diagnostic support. While it addresses privacy and sensor-based applications, it lacks a comprehensive discussion on blockchain and its role in secure wearable health monitoring. Likewise, (Putra et al., 2024) highlights the role of IoMT in wearable health monitoring, with a strong focus on cloud–edge AI integration but without an in-depth exploration of blockchain technology.

Additionally, (Ali et al., 2022a) provides a detailed survey on privacy-preserving FL in smart healthcare, incorporating advanced architectures such as deep reinforcement learning and generative adversarial networks (GANs) to enhance security. While it discusses blockchain applications, it does not cover wearable health sensors extensively.

In contrast, our paper uniquely contributes to the literature by:

1. Providing a targeted review of FL in wearable health devices, structured around Privacy, Sensors, Cloud Computing, and Blockchain.
2. Offering a comparative assessment of existing FL frameworks in the context of wearable health monitoring.
3. Highlighting the specific role of blockchain in enhancing privacy and security in FL-based wearable health technologies.

This work, therefore, fills a crucial research gap by offering a structured and comparative analysis of FL approaches tailored to wearable health devices, emphasizing their practical implications and technological constraints.

3. Papers retrieval

This section outlines the method used to identify relevant papers for our research. The search was conducted in November 2024 using the Scopus database. We employed a keyword-based search strategy, focusing on terms such as Health, Federated, Model, Learning, and Wearable. To ensure comprehensive coverage, we used the wildcard operator * (e.g., health includes terms such as healthcare and e-health).

We searched for papers with our defined search string in at least one of the title, keywords, and abstract fields. The search was further refined by restricting the domain to Computer Science and Engineering, and we limited the publication date to papers released after 2020. The search string that we have defined is the following:

TITLE-ABS-KEY (health AND federated* AND (learning OR model) AND wearable*) AND PUBYEAR > 2020 AND (LIMIT-TO (SUBJAREA, "COMP") OR LIMIT-TO (SUBJAREA, "ENGI"))*

With these criteria applied, we retrieved a total of 136 eligible papers, as indicated in Table 2.

To narrow down the selection, two experts carefully reviewed each paper and excluded those that did not primarily focus on wearable health and federated models/learning. Our review process involved a thorough examination of titles and abstracts. We identified 38 papers relevant to our research.

Table 2
Number of eligible papers after each stage.

Papers found in the research	136
Papers relevant to our study	38

Regarding the other 98 papers that were excluded, the reasons for their exclusion varied. Some lacked a clear focus on either wearable devices or health applications, making them less relevant to the scope of this study. Others did not incorporate FL approaches or models, which is a core aspect of our research objective. Additionally, some papers were too broad in scope, such as review articles that did not delve into practical implementations or specific case studies relevant to wearable health devices. Furthermore, a few of the excluded papers were books rather than research articles, which did not align with the criteria for inclusion in this study. The breakdown of excluded papers is as follows:

- 48 papers were only marginally related to wearable devices or health applications. For example, the paper (Li et al., 2022) focused on generic data privacy issues within FL but did not specifically address wearable devices or health applications.
- 31 papers were excluded as they did not explore federated models or learning directly related to health or wearables. For example, (Mahanipour & Khamfroush, 2024) discussed feature selection techniques but did not apply or discuss wearable health data.
- 13 papers were reviews or surveys on FL that did not have a clear focus on wearable or health-related implementations. While informative, these entries lacked practical models or methodologies for the specified domain, like (Gupta et al., 2024).
- 6 papers were book chapters rather than research articles and therefore did not meet the inclusion criteria, as they typically lacked experimental results or direct applications to wearable health devices, such as (Babu et al., 2024a).

To identify the most important features among the identified papers, we conducted a topic modeling exercise using BERTopic (Grootendorst, 2022) on the full set of extracted documents. BERTopic is a topic modeling technique that leverages the powerful language representations from transformers, specifically BERT (Bidirectional Encoder Representations from Transformers) (Devlin et al., 2019) and its variants like SBERT (Sentence-BERT) (Reimers & Gurevych, 2019) or MPNet (Masked and Permuted Pre-training for Language Understanding) (Song et al., 2020). Unlike traditional topic modeling approaches such as Latent Dirichlet Allocation (LDA) (Jelodar et al., 2019), which are based on the statistical properties of the words in documents (such as TF-IDF) (Kim & Gil, 2019), BERTopic utilizes contextual embeddings to understand the semantic meanings of words within their context. In brief, BERTopic performs topic modeling by undertaking the following steps:

- **Document Embedding**: BERTopic starts by converting documents into embeddings using a pre-trained transformer model. In particular, we used the 'all-mpnet-base-v2' model, publicly available via Hugging Face.[4] The produced embeddings are high-dimensional vectors that capture the semantic meaning of the entire documents.
- **Dimensionality Reduction**: To manage the complexity of these high-dimensional vectors and to improve the interpretability of the resulting topics, BERTopic applies dimensionality reduction techniques. We used UMAP (Allaoui et al., 2020) to reduce the embedding dimensions while preserving as much of the original topological structure as possible.
- **Clustering**: After dimensionality reduction, BERTopic clusters the reduced embeddings to group together documents that are semantically similar. We employed HDBSCAN (McInnes & Healy, 2017) given its robustness to noise in the data. Indeed, HDBSCAN is designed to identify and group dense regions of data points while being less influenced by data points that do not fit well into any cluster, which are considered noise. This characteristic makes HDBSCAN particularly suitable for complex datasets where the presence of noise could otherwise lead to less accurate clustering results.
- **Topic Creation and Interpretation**: Each cluster is interpreted as a topic. To describe each topic, BERTopic identifies the most representative words based on the cluster's content. This is typically done by examining the words that have the highest frequency or that are most central within the cluster's embedding space.
- **Evaluation**: Finally, to evaluate the quality of the topics generated, the coherence score (C_v) is calculated (RRöder et al., 2015). This score measures the degree of semantic similarity between the high-scoring words within the topic. The topic coherence measure is based on a sliding window, one-set segmentation of the top words and an indirect confirmation measure that uses normalized pointwise mutual information (NPMI) and the cosine similarity (Mifrah & Benlahmar, 2022). A higher coherence score suggests that the words are more meaningfully related to each other, and the topic is more interpretable to humans (C_v is between 0 and 1).

To ensure the reliability and interpretability of the BERTopic-based thematic extraction, we complemented the coherence score with additional validation steps. First, following standard practices in topic modeling (RRöder et al., 2015), automated clustering was combined with expert-driven validation. The generated topics were mapped to higher-level survey themes through a human-in-the-loop procedure: each topic was represented by its top keywords and most representative documents, which were independently reviewed by domain experts and iteratively grouped into semantically coherent categories. Disagreements were resolved through discussion, ensuring consistent and interpretable theme definitions.

[4] https://huggingface.co/sentence-transformers/all-mpnet-base-v2

Second, we assessed the robustness of the clustering pipeline with respect to key modeling choices. In particular, we examined the stability of the resulting topics under variations of the sentence embedding model, as well as the hyperparameters of UMAP (e.g., number of neighbors and minimum distance) and HDBSCAN (e.g., minimum cluster size). The main thematic structures remained stable across configurations, with only minor variations in topic granularity, which is expected for unsupervised methods.

Finally, qualitative evaluation was conducted to verify intra-topic semantic consistency and alignment with the assigned survey themes. This hybrid validation approach, combining quantitative metrics with expert-driven assessment, follows established practices in large-scale document clustering and topic modeling, where interpretability and domain relevance are critical for downstream analysis.

This approach proved instrumental in uncovering the latent thematic structures embedded within the body of literature. Specifically, we employed this procedure in two distinct phases. First, we applied it to the set of review papers, which facilitated the identification of 4 thematic elements. Subsequently, we applied the same method to the corpus of technical papers, leading to the emergence of 11 more granular thematic axes.

4. Reviews

Among the papers most relevant to our topic, we identified ten review papers, namely: Ali et al. (2022a), Badidi (2023), Haque et al. (2024), Moshawrab et al. (2023), Mosaiyebzadeh et al. (2023), Putra et al. (2024), Qureshi et al. (2023), Schulte et al. (2024), Shaik et al. (2023), and Upreti et al. (2024). This section provides an overview of the content of these ten review papers, the features analyzed within them, and how each work aligns with these features.

We searched for papers that address the integration of wearables and health devices with Federated AI models, focusing on four critical subtopics: privacy, sensors, cloud computing, and blockchain. These subtopics were selected due to their pivotal role in addressing key challenges and opportunities in smart healthcare systems. Table 3 illustrates the compliance of each reviewed paper with the selected subtopics, highlighting their relevance. Checkmarks identify papers where the corresponding subtopic has high importance, while the checkmarks in brackets identify papers where the subtopic has marginal importance, but is still mentioned. We will now provide a brief explanation of how we chose these topics.

Privacy data preservation is a critical challenge in applying ML techniques, especially in healthcare. FL has emerged as a promising solution by enabling collaborative model training across distributed devices without sharing raw data. This decentralized approach ensures data confidentiality by sharing model parameters instead of user data, significantly reducing privacy risks (Moshawrab et al., 2023; Upreti et al., 2024). Papers such as (Moshawrab et al., 2023) and Schulte et al. (2024) emphasize privacy-preserving techniques like differential privacy and homomorphic encryption, which mitigate risks such as data leakage and model inversion. Additionally, frameworks like Secure Hierarchical Federated Learning (SHFL) and blockchain-based systems have demonstrated strong capabilities in anonymizing data and securing sensitive transactions (Mosaiyebzadeh et al., 2023; Shaik et al., 2023).

The IoMT ecosystem introduces unique challenges, including real-time data acquisition risks and potential breaches during transmission. Federated cloud–edge AI architectures have been proposed to ensure sensitive data remains localized while supporting high-quality diagnostics and personalized healthcare (Putra et al., 2024; Upreti et al., 2024). Papers like (Badidi, 2023) discuss advanced techniques such as secure aggregation and digital twin technologies to address privacy risks, though challenges like efficient resource management and adversarial threats persist.

Sensors, including biosensors, are integral to wearables and healthcare devices. They play a crucial role in real-time monitoring of vital signs and continuous health data acquisition, enabling early detection and improved treatment plans. Papers such as (Putra et al., 2024) and Shaik et al. (2023) highlight innovations like RFID-enabled garments and epidermal tattoos, which enhance patient comfort and diagnostic accuracy. Despite these advancements, challenges such as sensor interoperability and data security remain areas for future research.

Cloud computing is another key enabler in healthcare systems, providing scalable data processing, real-time monitoring, and centralized storage. Papers like (Haque et al., 2024) and Badidi (2023) explore its applications in managing large datasets generated by IoMT devices and wearable sensors. However, limitations such as latency and privacy concerns are noted. Hybrid cloud–edge computing models, as discussed in Putra et al. (2024), address these issues by processing data locally before transmission to the cloud, enabling real-time analytics while maintaining scalability.

Blockchain technology is increasingly recognized as a critical component for securing healthcare systems. Works such as (Mosaiyebzadeh et al., 2023) and Ali et al. (2022a) discuss blockchain's role in ensuring data immutability and traceability within FL frameworks. Applications such as Ethereum-based data repositories demonstrate the potential for decentralized healthcare management. However, challenges such as computational demands and scalability trade-offs remain, as highlighted in Badidi (2023).

Following the cluster analysis we described earlier, for the review papers we identified four prominent thematic clusters, each reflecting a distinct area of focus. For each cluster, we selected a representative candidate feature that encapsulates its core focus, serving as a basis for our subsequent analysis and comparison. These candidate features are:

- **Importance**: FL plays a transformative role in securing decentralized healthcare data and enhancing IoMT systems, as extensively highlighted in Moshawrab et al. (2023) and Upreti et al. (2024).
- **Devices**: IoMT devices, including wearable biosensors and health monitors, play a pivotal role in enabling secure, scalable, and patient-centric healthcare, as highlighted by Shaik et al. (2023) and Badidi (2023).

Table 3
Compliance of each review paper to the four subtopics from Section 1 (sorted chronologically).

Paper	Year	Privacy Data	Sensors	Cloud Computing	Blockchain
Ali et al. (2022a)	2022				✓
Badidi (2023)	2023			✓	
Mosaiyebzadeh et al. (2023)	2023	(✓)			✓
Moshawrab et al. (2023)	2023	✓			
Qureshi et al. (2023)	2023				
Shaik et al. (2023)	2023	(✓)	(✓)		✓
Haque et al. (2024)	2024			(✓)	
Putra et al. (2024)	2024		✓	✓	
Schulte et al. (2024)	2024	✓			
Upreti et al. (2024)	2024	✓		(✓)	

- **Domains**: Federated AI models and wearable health devices demonstrate versatility across residential, clinical, and public health domains, enabling personalized care and secure data management, as emphasized in Moshawrab et al. (2023) and Upreti et al. (2024).
- **Use cases**: Federated AI models and wearable devices address diverse healthcare challenges, from home-based monitoring and hospital diagnostics to public health interventions and workplace health management, as highlighted in Moshawrab et al. (2023) and Upreti et al. (2024).

Table 4 describes, for each retrieved review paper, its compliance with each feature. The meaning of each abbreviation is described in Table 13. In the following, we will detail and comment on how each feature is adhered to by the papers, and identify patterns that emerge from this analysis. Specifically, we will examine whether the papers comply with the features all in the same way, or not, showing the differences among them.

4.1. Importance

The significance of FL and wearable health devices varies across the reviewed papers. Moshawrab et al. (2023) focuses extensively on privacy preservation in FL, showcasing its potential to secure sensitive healthcare data while enabling collaborative AI model training. Similarly, (Upreti et al., 2024) highlights the transformative role of FL in managing decentralized healthcare data, emphasizing its pivotal role in IoMT systems. On the other hand, (Qureshi et al., 2023) and Ali et al. (2022a) discuss privacy and FL as part of broader healthcare informatics topics, where these aspects are secondary to other considerations such as AI architectures and data processing. Meanwhile, (Shaik et al., 2023) primarily emphasizes wearable sensors, with only marginal attention to the integration of FL, and Putra et al. (2024) explores privacy-enhancing technologies in IoMT, with FL discussed as a supporting framework rather than a central theme.

4.2. Devices

The reviewed papers highlight a range of devices central to healthcare advancements, particularly in IoMT and wearable health systems. Shaik et al. (2023) focuses on wearable biosensors such as ECG patches, smartwatches, and fitness trackers, emphasizing their role in chronic disease monitoring, vital signs measurement, and non-invasive diagnostics. Similarly, (Badidi, 2023) explores advanced biosensor technologies like epidermal electronic tattoos and flexible bioelectronics, which enhance patient comfort and accuracy in monitoring.

Works such as (Moshawrab et al., 2023) and Qureshi et al. (2023) broadly discuss IoMT devices, including wearable health monitors, smart medical implants, and connected health hubs, highlighting their integration into FL frameworks for secure data sharing and analysis. Upreti et al. (2024) examines IoMT-enabled devices used in healthcare systems, such as mobile health devices and clinical monitoring tools, which facilitate real-time data acquisition and transmission.

Another work, (Haque et al., 2024), emphasizes the importance of multi-sensor setups, including RFID-enabled garments and non-invasive glucose monitors, which provide continuous data collection for AI-driven diagnostics. Authors in Putra et al. (2024) discuss IoMT devices from a privacy perspective, addressing the risks associated with data transmission from these devices without specifying particular types.

In addition to wearable devices, researchers in Ali et al. (2022a) explore edge-AI-driven IoMT devices, such as intelligent stethoscopes and point-of-care diagnostic tools, which combine cloud computing capabilities for real-time health management. Two more works, (Mosaiyebzadeh et al., 2023) and Schulte et al. (2024), focus on traditional healthcare IoT devices like blood pressure monitors and remote patient monitoring systems, emphasizing their scalability and adaptability in different healthcare settings.

Across all papers, these devices are critical to the success of IoMT ecosystems, enabling secure, scalable, and patient-centric healthcare delivery while leveraging FL and AI technologies to optimize data use and privacy.

Table 4
Classification of the review papers according to the four defined features (sorted chronologically). Full description of the acronyms can be found in Table 13.

Paper	Year	Importance	Devices	Domains	Use Cases
Ali et al. (2022a)	2022	Whole paper	Intelligent stethoscopes, point-of-care diagnostic tools	Ind.	Employee health monitoring, federated health solutions in industrial workplaces
Badidi (2023)	2023	One section	Epidermal electronic tattoos, flexible bioelectronics	PH	Pandemic response, scalable health interventions
Mosaiyebzadeh et al. (2023)	2023	Whole paper	IoT-enabled wearable health sensors, smart meters	PH	Data privacy in IoMT ecosystems, federated cloud–edge solutions
Moshawrab et al. (2023)	2023	Whole paper	Smart medical implants, wearable biosensors	Res.	Chronic disease monitoring, decentralized healthcare data management
Qureshi et al. (2023)	2023	One subs	EEG patches, fitness trackers, non-invasive glucose monitors	Res., Clin.	Home-based health monitoring, fitness and chronic condition management
Shaik et al. (2023)	2023	One subs	Wearable vital sign monitors, AI-enhanced IoT sensors	Res.	Remote patient monitoring, elderly care
Haque et al. (2024)	2024	One subs	AI-integrated biosensors, RFID-enabled garments	Res., Clin.	Early diagnostics, personalized health monitoring
Putra et al. (2024)	2024	One section	IoMT wearable devices, health monitoring hubs	PH	Real-time diagnostics, large-scale health interventions
Schulte et al. (2024)	2024	One section	Remote patient monitoring devices, traditional IoT devices	Clin., PH	AI-driven diagnostics, disease outbreak monitoring, privacy-preserving health analytics
Upreti et al. (2024)	2024	Whole paper	Mobile health devices, clinical diagnostic tools	Clin., PH	Multi-institution health collaboration, privacy-preserving diagnostics

4.3. Domains

The reviewed papers address diverse healthcare areas, with a range of specific use cases that highlight the adaptability of federated AI models and wearable health devices.

Residential Healthcare: Papers such as (Moshawrab et al., 2023; Qureshi et al., 2023), and Haque et al. (2024) emphasize home-based health monitoring systems that leverage wearable biosensors for chronic disease management and real-time vital sign tracking. These applications enable patients to receive personalized care in non-clinical settings, reducing hospital visits.

Clinical and Hospital Settings: In papers like (Schulte et al., 2024) and Upreti et al. (2024), FL is integrated into hospital systems to manage sensitive patient data while maintaining privacy. Use cases include AI-driven diagnostics, treatment optimization, and collaborative healthcare initiatives across multiple institutions.

Public Health Applications: Papers (Putra et al., 2024) and Badidi (2023) explore the use of edge computing and federated AI for large-scale health interventions, such as monitoring and controlling infectious diseases. These works emphasize applications in epidemiology and pandemic response, where secure, decentralized data management is critical.

Rehabilitation and Precision Medicine: Specialized use cases are detailed in Mosaiyebzadeh et al. (2023) and Shaik et al. (2023), focusing on wearable devices that support rehabilitation tracking and AI-driven models for personalized treatment plans. These studies highlight the potential of federated learning to adapt to condition-specific requirements, such as recovery monitoring or genetic data analysis.

Industrial and Organizational Health: The work in Ali et al. (2022a) investigates the application of federated AI in workplace health monitoring, showcasing use cases such as employee wellness tracking and occupational health management. These implementations often integrate blockchain technologies for secure, scalable data handling.

By spanning residential, clinical, public health, specialized, and industrial domains, the reviewed papers underscore the versatility of federated AI models and wearable devices in addressing diverse healthcare challenges.

4.4. Use cases

The reviewed papers highlight a diverse range of use cases that demonstrate the adaptability and effectiveness of FL and wearable health devices across various domains.

In residential settings, FL and wearable biosensors play a crucial role in managing chronic diseases and enabling decentralized healthcare data management. For example, (Moshawrab et al., 2023) demonstrates how smart medical implants and wearable biosensors reduce the need for frequent hospital visits while ensuring patient privacy. Similarly, (Qureshi et al., 2023) explores the use of ECG patches, fitness trackers, and non-invasive glucose monitors for home-based health monitoring, chronic condition management, and fitness tracking, facilitating personalized care in non-clinical environments.

In clinical and public health domains, FL enhances AI-driven diagnostics and supports large-scale health interventions. Papers such as (Schulte et al., 2024) focus on remote patient monitoring devices and traditional IoT systems to enable accurate diagnostics and real-time disease outbreak monitoring, ensuring privacy-preserving analytics. Authors in Putra et al. (2024) further expand on this by exploring IoMT wearable devices and health monitoring hubs to support real-time diagnostics and pandemic response efforts, offering scalable and secure solutions. Moreover, the work performed in Badidi (2023) discusses the application of advanced technologies such as epidermal electronic tattoos and flexible bioelectronics for scalable health interventions and pandemic response, demonstrating the potential of FL to address public health crises effectively.

Personalized health monitoring is another significant use case highlighted in the reviewed papers. AI-integrated biosensors and RFID-enabled garments are used for early diagnostics and tailored healthcare interventions. For instance, (Haque et al., 2024) underscores their effectiveness in providing continuous and personalized health monitoring in residential and clinical domains.

FL also finds applications in industrial and workplace health monitoring. In Ali et al. (2022a), intelligent stethoscopes and point-of-care diagnostic tools are employed to monitor employee health and safety in industrial settings, integrating federated health solutions to maintain data security and privacy.

Additionally, wearable vital sign monitors and AI-enhanced IoT sensors support remote patient monitoring and elderly care. The work in Shaik et al. (2023) emphasizes their role in continuous health tracking and promoting patient independence, particularly in residential environments. Beyond this, (Upreti et al., 2024) explores FL's role in facilitating multi-institution health collaboration using mobile health devices and clinical diagnostic tools, ensuring privacy-preserving diagnostics and seamless cooperation across healthcare institutions.

Lastly, (Mosaiyebzadeh et al., 2023) addresses privacy challenges in IoMT ecosystems, focusing on data privacy frameworks and federated cloud–edge solutions that enable secure data sharing in public health applications. These efforts demonstrate the scalability and adaptability of FL in maintaining data confidentiality across diverse healthcare use cases.

The reviewed papers illustrate how FL and wearable health devices are transforming healthcare across residential, clinical, public health, and industrial domains. By enabling chronic disease monitoring, personalized care, large-scale interventions, and secure data management, these technologies address pressing healthcare needs while maintaining scalability, privacy, and adaptability.

4.5. Cross-review synthesis and emerging patterns

A comparative examination of the reviewed surveys reveals not only thematic overlaps but also important conceptual differences in how FL is positioned within wearable healthcare ecosystems.

Privacy is consistently identified as the primary motivation for FL adoption in healthcare (Ali et al., 2022a; Moshawrab et al., 2023; Upreti et al., 2024). However, the mechanisms proposed to ensure privacy vary substantially. Works such as Moshawrab et al. (2023) and Schulte et al. (2024) emphasize cryptographic techniques including differential privacy and homomorphic encryption, which provide strong theoretical guarantees. In contrast, Putra et al. (2024) and Badidi (2023) advocate architectural solutions such as cloud–edge hierarchies that keep raw data localized while sharing aggregated parameters. Meanwhile, Mosaiyebzadeh et al. (2023) and Ali et al. (2022a) explore blockchain-based trust reinforcement mechanisms to enhance traceability and accountability.

These approaches embody distinct trade-offs. Cryptographic solutions (Moshawrab et al., 2023; Schulte et al., 2024) strengthen formal privacy guarantees but introduce computational overhead, which may be problematic for resource-constrained wearable devices. Architectural solutions (Badidi, 2023; Putra et al., 2024) improve scalability and latency management but require reliable edge infrastructure. Blockchain-based approaches (Ali et al., 2022a; Mosaiyebzadeh et al., 2023) enhance auditability and tamper resistance; however, their suitability for wearable FL systems depends critically on the underlying architecture. Permissionless chains such as Ethereum — referenced implicitly in Mosaiyebzadeh et al. (2023) through decentralized data repository designs — rely on probabilistic consensus mechanisms (PoW/PoS) that introduce block confirmation latencies ranging from seconds to minutes and impose substantial energy overhead, rendering them largely incompatible with real-time physiological monitoring. In contrast, permissioned chains such as Hyperledger Fabric, which underlie the lightweight and fog-integrated designs in Baucas et al. (2023b) and Farooq et al. (2022), employ deterministic consensus protocols such as PBFT that achieve sub-second finality at significantly lower energy cost, making them considerably more viable for battery-constrained wearable deployments. These

architectural distinctions are rarely made explicit in the reviewed literature, representing a gap in how blockchain is currently evaluated within wearable FL frameworks.

Regarding sensing technologies, several reviews highlight innovations such as RFID-enabled garments (Haque et al., 2024), epidermal electronic tattoos (Badidi, 2023), and wearable biosensors (Shaik et al., 2023). Nevertheless, sensor characteristics are rarely connected to federated optimization dynamics. Broader healthcare FL surveys (Joshi et al., 2022; Pfitzner et al., 2021) acknowledge challenges such as data heterogeneity and non-IID distributions, yet the interaction between wearable signal variability and convergence behavior remains underexplored in wearable-specific reviews.

Finally, an evolution in domain focus is observable. Earlier perspectives emphasize cross-institutional collaboration and regulatory compliance (Schulte et al., 2024; Upreti et al., 2024), whereas more recent works move toward patient-centric and edge-centric intelligence (Putra et al., 2024; Shaik et al., 2023). This transition reflects a broader shift from institution-level data sharing toward adaptive personalization at the device level.

Overall, although Privacy, Sensors, Cloud Computing, and Blockchain are consistently discussed as independent pillars, their systemic interaction is seldom synthesized. A unified systems perspective that jointly evaluates privacy guarantees, computational efficiency, device constraints, and regulatory compliance remains insufficiently developed in the current literature.

A recurring limitation across the reviewed survey papers is the conflation of privacy-preserving mechanisms with security safeguards. Works such as (Moshawrab et al., 2023) and Schulte et al. (2024) explicitly discuss differential privacy and homomorphic encryption, yet frame these exclusively as privacy techniques without evaluating their coverage of security requirements such as those mandated by the HIPAA Security Rule. The distinction matters practically: differential privacy noise injection protects against statistical inference attacks on model outputs (a privacy concern under 45 CFR §164.502[5]), but does not address transmission security requirements under §164.312(e), device authentication under §164.312(d), or audit logging requirements under §164.312(b).[6] Among the reviewed surveys, only Ali et al. (2022a) and Mosaiyebzadeh et al. (2023) engage with security mechanisms — specifically blockchain-based audit trails — in ways that partially address HIPAA Security Rule technical safeguard categories. However, neither paper provides a systematic mapping between proposed mechanisms and regulatory requirements. Administrative safeguards (workforce training, contingency planning, risk analysis) and physical safeguards (device and media controls) are entirely absent from all reviewed surveys — a significant gap given that wearable devices are physically mobile, loss-prone, and frequently operated outside controlled clinical environments. With respect to GDPR, the reviewed surveys acknowledge data minimization and purpose limitation principles but rarely evaluate how specific FL architectures satisfy them technically. The right to erasure (Article 17)[7] remains particularly problematic for FL systems: if model weights encode individual-level information — a risk demonstrated empirically by gradient inversion attacks — selective data removal from a trained global model is currently an open technical problem not addressed in any reviewed survey. Similarly, data portability (Article 20)[8] and the requirement for documented legal basis for secondary use of health data are compliance dimensions entirely unaddressed in the wearable FL literature.

5. Technical papers

This section presents an analysis of the identified papers focusing on the integration of Federated AI models in wearables and health devices, namely: Alahmadi et al. (2024), Alferaidi et al. (2024), Aminifar et al. (2024), Antona and Stephanidis (2022), Arya et al. (2023), Avdan and Onal (2024), Babu et al. (2024b), Baucas et al. (2023b), Bhatt et al. (2024), Birari et al. (2023), Can and Ersoy (2021), Elayan et al. (2021), Fang et al. (2021), Farooq et al. (2022), Ghosh and Ghosh (2023), Hu et al. (2023), El Jaouhari (2023), Kaur et al. (2024), Kotiyal et al. (2023), Lakhan et al. (2024), Pham et al. (2023), Rahmany et al. (2023), Ravi Shanker Reddy and Beena (2022), Sachin et al. (2023), Shae and Tsai (2021), Wang et al. (2023), Yu et al. (2022), and Zhang et al. (2021). We will highlight the relevance of these studies in the areas and explore a novel set of features developed as part of this research.

We focused on papers discussing Federated AI models in wearables and health devices, emphasizing at least one of the following subtopics from Section 1: Privacy, Sensors, Cloud Computing, or Blockchain. Table 6 outlines which subtopics each paper addresses. Like in Table 3, the checkmarks refer to papers where the corresponding subtopic has high relevance, while the checkmarks in brackets refer to papers where the subtopic is still mentioned, but with less relevance.

The most recurring theme is Privacy, which is the primary focus in several papers (Alahmadi et al., 2024; Alferaidi et al., 2024; Aminifar et al., 2024; Antona & Stephanidis, 2022; Babu et al., 2024b; Baucas et al., 2023b; Bhatt et al., 2024; Birari et al., 2023; Can & Ersoy, 2021; El Jaouhari, 2023; Elayan et al., 2021; Ghosh & Ghosh, 2023; Hu et al., 2023; Kaur et al., 2024; Lakhan et al., 2024; Pham et al., 2023; Rahmany et al., 2023; Sachin et al., 2023; Wang et al., 2023). Specifically, (Babu et al., 2024b) and Lakhan et al. (2024) feature models that integrate privacy mechanisms with sensor data collection, (Baucas et al., 2023b) explores privacy within blockchain systems, while the remaining cited papers (Alahmadi et al., 2024; Alferaidi et al., 2024; Aminifar et al., 2024; Antona & Stephanidis, 2022; Bhatt et al., 2024; Birari et al., 2023; El Jaouhari, 2023; Elayan et al., 2021; Ghosh & Ghosh, 2023; Hu et al., 2023; Kaur et al., 2024; Pham et al., 2023; Rahmany et al., 2023; Sachin et al., 2023; Wang et al., 2023) address privacy more implicitly in different contexts.

[5] https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-E/section-164.502
[6] https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-C/section-164.312
[7] https://gdpr-info.eu/art-17-gdpr/
[8] https://gdpr-info.eu/art-20-gdpr/

Sensors are another central aspect, explicitly highlighted in Kotiyal et al. (2023) and Fang et al. (2021), where physiological data collection is the main focus. Sensors also play a critical, albeit secondary, role in papers like (Babu et al., 2024b; Can & Ersoy, 2021; Lakhan et al., 2024; Rahmany et al., 2023), supporting broader privacy or monitoring frameworks.

Additionally, Blockchain appears in a select set of works, most notably in Baucas et al. (2023b) and Farooq et al. (2022), where decentralized security frameworks are detailed. Similarly, (Ravi Shanker Reddy & Beena, 2022) and Shae and Tsai (2021) address blockchain as a supportive feature for privacy-preserving systems. Finally, Cloud Computing is the focus in papers like (Avdan & Onal, 2024; Sachin et al., 2023; Yu et al., 2022), which detail cloud-based aggregation for data processing or federated learning models.

Flexibility in combining these features is evident, but Privacy remains the dominant focus across the majority of the cited works.

In the following, we will briefly describe the content of these papers. Babu et al. (2024b) explores a federated learning framework integrating privacy-preserving methods with wearable sensors for secure and effective health monitoring. Similarly, (Lakhan et al., 2024) builds on federated models, focusing on enhancing privacy while utilizing wearable devices to monitor physiological data. In contrast, (Kotiyal et al., 2023) centers primarily on sensor technologies, emphasizing the role of physiological data from wearables for activity and health monitoring.

Unlike the previous works, (Bhatt et al., 2024) and Alferaidi et al. (2024) focus exclusively on privacy mechanisms, proposing cryptographic solutions to secure sensitive health data. Avdan and Onal (2024) and Sachin et al. (2023) address cloud-based frameworks for managing and aggregating distributed data in healthcare systems, optimizing resource use and scalability. Meanwhile, (Baucas et al., 2023b) integrates blockchain into privacy-focused healthcare solutions, establishing a decentralized mechanism for secure and transparent data sharing.

The scenario in Farooq et al. (2022) and Ravi Shanker Reddy and Beena (2022) centers on blockchain technologies, highlighting their role in securing distributed medical data and ensuring data integrity. Conversely, (Fang et al., 2021) and Pham et al. (2023) prioritize sensors, detailing their applications in smart health systems for real-time abnormal health detection and stress monitoring.

It is important to note that while privacy-preserving techniques are central to most models, stakeholders like healthcare providers, device manufacturers, and patients are frequently implicit. For instance, (Babu et al., 2024b) and Lakhan et al. (2024) focus on privacy for individual users, while (Baucas et al., 2023b) introduces blockchain to ensure trust among multiple parties. Similarly, (Avdan & Onal, 2024) includes cloud providers as key actors in managing distributed models, whereas (Fang et al., 2021) focuses solely on sensor-based systems with minimal external stakeholders.

Flexibility in combining these features is evident across the works, but Privacy remains the dominant focus, with Sensors often playing a supportive role in facilitating secure and effective healthcare solutions.

As in Section 4, we have established a set of features to classify the papers describing the novel frameworks and approaches, which are outlined below.

- **Granularity**: Describes the data granularity at which the proposed framework or approach operates. For instance, some frameworks focus on real-time data from wearable sensors, often measured in milliseconds or seconds, while others use aggregated health records analyzed daily or weekly.
- **Vector**: Describes the main focus or data type involved in the framework. Many works are centered on health-related data, such as physiological signals (e.g., heart rate, oxygen levels), but some extend to environmental or contextual data from IoT devices.
- **Devices**: Describes the devices utilized in the framework, including wearable sensors, smartphones, edge devices, or dedicated health-monitoring equipment. Examples include electrocardiogram (ECG) monitors, fitness bands, and smartphones with in-built sensors.
- **Domains**: Describes the domain for which the framework or approach has been designed or tested. Many frameworks are tailored for healthcare applications, focusing on areas like personalized medicine, stress detection, or remote patient monitoring.
- **Use case**: Describes the use case to which the framework is applied. For example, some frameworks target individual users for stress monitoring, while others address broader entities, such as community health programs or hospital networks. The number in parentheses indicates the dataset size or population studied, where available.
- **Customer type**: Describes the type of customer or end-user to which the framework refers. These can include individual patients, healthcare providers, or large-scale organizations, such as hospitals or research institutions.
- **Provider type**: Describes the type of provider implementing the framework, such as technology providers (e.g., IoT platform developers), healthcare service providers, or data aggregators working with hospitals.
- **Benefits**: Describes the type of utility the framework provides. Common aims include improving health outcomes, ensuring privacy, enabling real-time monitoring, and reducing operational costs for healthcare providers.
- **Constraints**: Describes the types of constraints under which the framework operates. This may include limitations like battery life of wearable devices, network bandwidth for data transfer, or compliance with privacy regulations.
- **Market readiness**: Describes whether the framework has been implemented in real-world settings or remains in the experimental stage. Some works detail fully deployed systems, while others are limited to prototype testing.
- **Methods**: Describes the methods used in building the federated learning framework, such as blockchain integration, statistical modeling, or machine learning techniques. Some frameworks emphasize hybrid approaches combining these methods to achieve multiple objectives.

Table 5
Reference Table for the "Extracted Features".

Table Name	Reference
Granularity, Vector, Devices, Domains	Table 7
Use Case, Customer Type, Provider Type, Benefits	Table 8
Constraints, Market Readiness, Methods	Table 9
Acronym Description	Table 13

Table 6
Relevance of features for each technical paper.

Paper	Year	Privacy	Sensors	Cloud Computing	Blockchain
Can and Ersoy (2021)	2021	✓	(✓)		
Elayan et al. (2021)	2021	✓		(✓)	
Fang et al. (2021)	2021		✓		
Shae and Tsai (2021)	2021	(✓)			✓
Zhang et al. (2021)	2021	(✓)	✓		
Yu et al. (2022)	2022			✓	
Farooq et al. (2022)	2022				✓
Ravi Shanker Reddy and Beena (2022)	2022	(✓)			✓
Antona and Stephanidis (2022)	2022	✓		(✓)	
Baucas et al. (2023b)	2023	✓			✓
Birari et al. (2023)	2023	✓			
Ghosh and Ghosh (2023)	2023	✓			
Kotiyal et al. (2023)	2023		✓		
El Jaouhari (2023)	2023	✓			
Sachin et al. (2023)	2023	✓		(✓)	
Wang et al. (2023)	2023	✓	(✓)		
Rahmany et al. (2023)	2023	✓	(✓)		✓
Pham et al. (2023)	2023	✓	✓		
Arya et al. (2023)	2023	(✓)			✓
Alahmadi et al. (2024)	2024	✓			
Alferaidi et al. (2024)	2024	✓			
Aminifar et al. (2024)	2024	✓			
Avdan and Onal (2024)	2024			✓	
Bhatt et al. (2024)	2024	✓			
Kaur et al. (2024)	2024	✓			
Babu et al. (2024b)	2024	✓	✓		
Lakhan et al. (2024)	2024	✓	✓		

This study is an extensive and in-depth examination of this field, with numerous terms used across different papers. The papers have been analyzed based on the 11 distinct features just outlined, and the total of 28 technical papers have been meticulously reviewed accordingly. The results of this analysis are presented in Table 5, which includes a list of 4 tables: Tables 7, 8, and 9 summarize the papers based on the 11 features. Full terms for the acronyms can be found in the Appendix (Table 13). In order to improve the reader's comprehension, we have provided as a supplementary online material, a comprehensive summary table featuring all the papers and their classification features. The table is accessible via the Joint Research Centre Data Catalogue[9] at the following permanent link: http://data.europa.eu/89h/46d2d46f-8006-4b9c-81a0-2bda83b4fc58. This catalog contains a complete list of both the technical and review papers, organized according to the features considered in our analysis. Including this extensive table within the manuscript would have been impractical.

Looking at Table 6, we can note a dominant emphasis on privacy-preserving mechanisms, while comparatively fewer works prioritize sensor optimization or cloud efficiency as primary contributions. Privacy-centric federated models are central in works such as Babu et al. (2024b), Lakhan et al. (2024), Bhatt et al. (2024), Alferaidi et al. (2024), Alahmadi et al. (2024), and Baucas et al. (2023b). In contrast, sensor-driven innovation is more explicitly foregrounded in Kotiyal et al. (2023) and Fang et al. (2021). This imbalance suggests that FL in wearable healthcare is currently framed primarily as a privacy-preserving paradigm rather than a holistic system optimization strategy.

Furthermore, three major technical strategies can be identified:

1. *Model-centric privacy enhancement*, where secure aggregation, differential privacy, or modified federated optimizers are introduced (e.g., Bhatt et al. (2024), Can and Ersoy (2021), Aminifar et al. (2024), Pham et al. (2023), Wang et al., 2023).

[9] Joint Research Centre Data Catalogue: https://data.jrc.ec.europa.eu/.

Table 7
Extracted Features: Granularity, Vector, Devices, Domain. Full description of the acronyms can be found in Table 13.

Paper	Year	Granularity	Vector	Devices	Domains
Can and Ersoy (2021)	2021	RT	PS	SW, SB, CS	H
Elayan et al. (2021)	2021	RT	PS	FT, SW, CSI, CS	H
Fang et al. (2021)	2021	RT	PS	SW, CS	H
Shae and Tsai (2021)	2021	RT	PS, EMR_D	WD, EMR_S	H
Zhang et al. (2021)	2021	RT	PS, VD	WS, ED, CS	SH
Yu et al. (2022)	2022	RT	PS, CD	HMD, CS	eH
Farooq et al. (2022)	2022	RT	PS, AD	FT, SW, CS	H
Ravi Shanker Reddy and Beena (2022)	2022	RT	PS	SB, BC, FM, CL	H
Antona and Stephanidis (2022)	2022	RT	PS, PS	SW, CS	H, E
Baucas et al. (2023b)	2023	RT	PS, ES, PI	BS, EMS	H
Birari et al. (2023)	2023	RT	PS	MS, ARS	H
Ghosh and Ghosh (2023)	2023	RT	PS	WS, ED	H
Kotiyal et al. (2023)	2023	20HZ	A	WD, ED, CS	SE, Ind., H
El Jaouhari (2023)	2023	RT	PS	SW, CS	H, E
Sachin et al. (2023)	2023	RT	PS	IoMT_S, CS	RH
Wang et al. (2023)	2023	RT	PS	WD, SP, SS, AS	SH
Rahmany et al. (2023)	2023	RT	AD, PS	SW, CS, SP, ARS	H
Pham et al. (2023)	2023	RT	AD, PS	WS, SW	H, MH
Arya et al. (2023)	2023	RT	A, PS	FT, SW, ED	H
Hu et al. (2023)	2023	RT	PS, ES, CP	PM, A, CS	H
Alahmadi et al. (2024)	2024	RT	PS	SW, FT, CS	H
Alferaidi et al. (2024)	2024	RT	PS, ES, AD	ESS, EGP, SW, HR, D	H, RH
Aminifar et al. (2024)	2024	256HZ	PS	EEG_S, eWS, CS	MH
Avdan and Onal (2024)	2024	RT	PS, AD, ES	WS, SP, CS	H
Bhatt et al. (2024)	2024	RT	PS	SW, FT	H
Kaur et al. (2024)	2024	RT	PS	SW, FT, BS, ED, CS	H
Babu et al. (2024b)	2024	RT	PS, AD, ES	SW, FT, EEGM, SHS	H
Lakhan et al. (2024)	2024	RT	PS	W, SW, BS, IoMT_S	H

2. *Architecture-centric optimization*, where cloud–edge or hierarchical aggregation structures are designed to reduce latency and computational burden (e.g., Avdan and Onal (2024), Yu et al. (2022), Sachin et al., 2023).
3. *Ledger-centric trust reinforcement*, where blockchain mechanisms ensure data integrity and decentralized governance (e.g., Baucas et al. (2023b), Farooq et al. (2022), (Ravi Shanker Reddy & Beena, 2022), Shae & Tsai, 2021).

These strategies involve distinct performance trade-offs. Model-centric approaches (Aminifar et al., 2024; Bhatt et al., 2024) often maintain scalability but may introduce gradient perturbations or additional communication overhead, potentially affecting convergence stability. Architecture-centric designs (Avdan & Onal, 2024; Yu et al., 2022) improve responsiveness through distributed edge processing, yet increase infrastructure complexity and synchronization requirements. Blockchain-integrated systems (Baucas et al., 2023b; Farooq et al., 2022) strengthen transparency and tamper resistance; however, consensus mechanisms and ledger maintenance introduce computational and energy overhead that may not align with low-power wearable constraints.

Sensor granularity further influences performance. High-frequency EEG-based systems such as Aminifar et al. (2024) (256 Hz sampling) and accelerometer-driven activity recognition frameworks such as Kotiyal et al. (2023) (20 Hz sampling) achieve fine-grained anomaly detection but increase communication cost and energy consumption. Conversely, aggregated physiological monitoring approaches (Babu et al., 2024b; Lakhan et al., 2024) reduce transmission overhead yet may sacrifice early detection sensitivity.

Therefore, performance differences across frameworks are frequently shaped not only by algorithmic design but also by assumptions regarding data resolution, device capability, and communication topology. A systematic co-design between sensing granularity and federated optimization remains largely unexplored.

5.1. Granularity

The reviewed papers exhibit diverse data granularity levels, largely influenced by the specific domain, use case, and computational requirements. A significant portion of the studies operates in real-time, processing physiological signals, activity data, and environmental signals captured from various wearable and IoT devices such as smartwatches, fitness trackers, biosensors, and IoMT sensors. These systems are predominantly employed in healthcare for applications such as chronic disease monitoring, stress detection, and remote patient supervision (Alahmadi et al., 2024; Alferaidi et al., 2024; Babu et al., 2024b; Birari et al., 2023; El Jaouhari, 2023; Farooq et al., 2022; Kaur et al., 2024; Lakhan et al., 2024; Rahmany et al., 2023; Shae & Tsai, 2021; Yu et al., 2022; Zhang et al., 2021). The real-time nature of these frameworks ensures immediate responsiveness, which is particularly crucial for emergency detection and continuous health tracking.

Beyond real-time systems, some studies define granularity based on sampling frequency. For instance, certain frameworks leverage accelerometer signals sampled at 20 Hz for human activity recognition and group activity monitoring (Avdan & Onal,

Table 8
Extracted Features: Use Case, Customer Type, Provider Type, Benefits. Full description of the acronyms can be found in Table 13..

Paper	Year	Use Case	Customer Type	Provider Type	Benefits
Can and Ersoy (2021)	2021	SD, PP, SM	SMI, HP, R	WDM, CSP, HP	PP, ASD, S, R
Elayan et al. (2021)	2021	SDD, HM, PP	P, HP, R	IoMT_DM, CSP, HL	PP, AD, DA, S
Fang et al. (2021)	2021	RHP, PP, PR	FE, HP, R	WDM, HI	PP, AP, S
Shae and Tsai (2021)	2021	PP, IDS	P, HP, PC	D, HL, HI	PP, S
Zhang et al. (2021)	2021	SD, MD, PP	SMI, HP	IoT_DM, CSP, HI	PP, EE, R, S
Yu et al. (2022)	2022	MCC, D, PP, R	P, HP, R	WDM, CSP, H, HL	E, PP, S, R
Farooq et al. (2022)	2022	RM, PP, SD	EI, P, HP	W_IoT_DM, CSP, WDM	PP, S, R, RCL, PO
Ravi Shanker Reddy and Beena (2022)	2022	CIP, PP, LE	I, PP	BN, CSP	PP, EDD, DC
Antona and Stephanidis (2022)	2022	RM, PP	I, HP, HL	D, HI	PT, PP
Baucas et al. (2023b)	2023	MCC, DAB, EDI	P, HP	IoT_DM, R, HP	PP, S, R, HA
Birari et al. (2023)	2023	CIM, EDD, ER	P, PP, R	WDM, CSP, HI	PO, EDI, RS
Ghosh and Ghosh (2023)	2023	HM	P, HP, D	IoMT_DM, HP	PP, PO, RP
Kotiyal et al. (2023)	2023	S, HAR	E, A, IoT_S	HL, IoMT_DM, D	MDD, PP, LRC, AD
El Jaouhari (2023)	2023	RM, PP	I, HP, HL	D, HI	HD, PP, S, F
Sachin et al. (2023)	2023	MCD, HAR, PP, PR	P, HP, HI	WDM, CSP, WDM	PP, AD, S, EE, RCL
Wang et al. (2023)	2023	MCD, DM, SD, PP	P, HP, R	WDM, CSP, H	PP, S, E, PO
Rahmany et al. (2023)	2023	RM, MCC	I, HP, HL	CSP, HP	PT, PP, RP, HM
Pham et al. (2023)	2023	MD	I	HP, HL, R	PP, ASD
Arya et al. (2023)	2023	RM, PP, PR	FI, HP, R	WDM, CSP, HI	PP, RCC
Hu et al. (2023)	2023	RM, FD, ER, HM, LE, PR	EI, HP	WDM, IoMT_D, HP	PP, G, EDD
Alahmadi et al. (2024)	2024	HM, EDD, PP	P, HP, D	IoT_DM, IP, HP	LRC, PP, E, S
Alferaidi et al. (2024)	2024	RM, ER, EDD	P, HP	HL, D, R	PC, A, E, DS, ES
Aminifar et al. (2024)	2024	RM, ESD, PP, DHA	P, HP, R	IoT_DM, CSP, HP	PP, S, PO, RCC
Avdan and Onal (2024)	2024	SD, SD	SMI, HP	IoMT_DM, D, HP	PC, A, E, ES, DS
Bhatt et al. (2024)	2024	HM, PP, RM	P, HP, R	MDM, HP	AP, PP, LRC, RCL
Kaur et al. (2024)	2024	RM	P, HP, R	WDM, CSP, WDM	S, PE, PP
Babu et al. (2024b)	2024	MCD, DAB, PP, HA	P, HP, R	HP, IoT_DM	PP, S, LRC, EDD, PT, A
Lakhan et al. (2024)	2024	MWU, DAB, OD, ER	WU, HP, R	HL, H, IoT_DM	HA, DS, LRC, DP, HM

2024; Kotiyal et al., 2023), while others process EEG signals at 256 Hz for detecting neurological conditions such as epileptic seizures (Aminifar et al., 2024). These high-resolution approaches enable the extraction of fine-grained insights, allowing for early anomaly detection and precise health monitoring.

In contrast, other research efforts focus on hierarchical granularity, combining real-time data with aggregated or batched processing through edge computing and cloud-based architectures. Such multi-tiered systems process continuous sensor data at the edge for immediate insights while periodically transferring aggregated information to cloud platforms for deeper analysis (Arya et al., 2023; Baucas et al., 2023b; Bhatt et al., 2024; Can & Ersoy, 2021; Elayan et al., 2021; Fang et al., 2021; Hu et al., 2023; Pham et al., 2023; Sachin et al., 2023; Wang et al., 2023). This strategy optimizes computational efficiency, balancing responsiveness with scalability.

Several studies also incorporate contextual and behavioral data alongside physiological signals, refining granularity beyond traditional biometric monitoring. For instance, frameworks integrating environmental monitoring sensors and contextual parameters provide a holistic perspective on health, considering external factors influencing physiological conditions (Birari et al., 2023; Ghosh & Ghosh, 2023; Ravi Shanker Reddy & Beena, 2022). Similarly, behavioral signals such as motion patterns and stress indicators offer personalized insights, enabling adaptive and proactive interventions (Alahmadi et al., 2024; Antona & Stephanidis, 2022).

Table 9
Extracted Features: Constraints, Market Readiness, Methods. Full description of the acronyms can be found in Table 13.

Paper	Year	Constraints	Market Readiness	Methods
Can and Ersoy (2021)	2021	DQ, HCC, P	RDV	FL, MLP, TFF
Elayan et al. (2021)	2021	HCC, CL	TP	FL, TL, DL
Fang et al. (2021)	2021	HCC, DQ, S	RDV	BFL, ARX
Shae and Tsai (2021)	2021	HCC, DO, S	PP	B, FL, NFT
Zhang et al. (2021)	2021	ID, HCC	PP	FL, EIDR, AGUC
Yu et al. (2022)	2022	HCC	RDV	MFL, MLSGD, ECI
Farooq et al. (2022)	2022	HCC	TP	B, FL
Ravi Shanker Reddy and Beena (2022)	2022	HCC, DQ	RP	FL, B
Antona and Stephanidis (2022)	2022	ID, HCC, P	TP	XAI, PPFL, RL
Baucas et al. (2023b)	2023	HCC, BC, IL	PCP	FL, CI, ML
Birari et al. (2023)	2023	HCC, DS	TP	FedERF, FedIERF
Ghosh and Ghosh (2023)	2023	DQ, HCC, S, R	TP	FL, SAT, M_MSS
Kotiyal et al. (2023)	2023	S, HCC	PCP	FSN, FGO, AMA, EC, CI
El Jaouhari (2023)	2023	HCC, R, DS, S	TP	XAI, PPFL, RL
Sachin et al. (2023)	2023	HCC, P, DS	RDV	FL, CNN-LSTM, HE, IL
Wang et al. (2023)	2023	HCC, S	PP	FL, RS, BV, LR, GD
Rahmany et al. (2023)	2023	P, DQ, IL	P	FL, B, ML
Pham et al. (2023)	2023	P, DQ	TP	FL, Fed_Avg
Arya et al. (2023)	2023	DQ, HCC	TP	FL
Hu et al. (2023)	2023	HCC, P, DS, R	TP	FSFD, LG, DNN, H_fog
Alahmadi et al. (2024)	2024	HCC, V, EC, MC	P	FL, B, Fog-IoT, ANN
Alferaidi et al. (2024)	2024	CC, SS, HCC	RP	FL, B, AR/VR, 6G, M_IoMT_S
Aminifar et al. (2024)	2024	HCC, CL, P	RDV	FL, SMC, ANN
Avdan and Onal (2024)	2024	HCC, DS, IL	SP	FL, FedAvg, FL_LDA, FL_ANN, FL_ADA, FL_CNN
Bhatt et al. (2024)	2024	CC, SS, HCC	SP	FedAagrad, SMOTE, ANN, 5G
Kaur et al. (2024)	2024	HCC, SI, F, B	PP	FL, SAT, DNN, B
Babu et al. (2024b)	2024	HCC, DS	P	FL, C
Lakhan et al. (2024)	2024	HCC, EC, P, DS, RD, SQ	SP	FL, DCNN, AES, DF

Overall, the granularity of data processing across these studies ranges from ultra-fine-grained real-time measurements to aggregated, context-aware insights, ensuring adaptability to diverse computational constraints and application-specific demands. The choice of granularity is often a trade-off between accuracy, computational cost, and real-time responsiveness, dictated by the nature of the application and the available infrastructure.

5.2. Vector

The notion of "Vector" in the reviewed works primarily refers to the type of data involved in the proposed frameworks. A significant number of studies focus on health-related data, particularly physiological signals such as heart rate, oxygen saturation, EEG, and ECG readings. These data vectors are extensively used for real-time monitoring, medical diagnosis, and predictive analytics in healthcare applications (Antona & Stephanidis, 2022; Babu et al., 2024b; Birari et al., 2023; Ghosh & Ghosh, 2023; Lakhan et al., 2024; Ravi Shanker Reddy & Beena, 2022). Some studies emphasize the role of biosignals in detecting anomalies, facilitating early disease diagnosis, and personalizing healthcare solutions (Baucas et al., 2023b; Can & Ersoy, 2021; Sachin et al., 2023).

Beyond physiological data, several frameworks extend their scope to environmental and contextual data collected from IoT devices. These include data streams from wearable sensors, ambient temperature, humidity, and geolocation-based information, providing a more comprehensive situational awareness in smart environments (Alferaidi et al., 2024; Farooq et al., 2022; Kaur et al., 2024; Pham et al., 2023; Shae & Tsai, 2021). The integration of such diverse vectors enhances the adaptability and efficiency of various machine learning and deep learning models applied in healthcare, industrial automation, and smart city applications (Elayan et al., 2021; Zhang et al., 2021). Additionally, some works explore the impact of sensor fusion on improving accuracy in anomaly detection systems by aggregating data from multiple sources (Fang et al., 2021).

Moreover, multi-modal data fusion is a key area of exploration, combining different types of vectors to improve model accuracy and robustness. Some works integrate ECG data with motion sensor readings to distinguish between physical activity and potential cardiac anomalies (Alahmadi et al., 2024; Aminifar et al., 2024; Yu et al., 2022). Others leverage a fusion of textual, numerical, and categorical vectors to enhance predictive capabilities in medical, industrial, and security applications (Arya et al., 2023; Bhatt et al., 2024; El Jaouhari, 2023; Rahmany et al., 2023; Wang et al., 2023).

Furthermore, a few studies focus on the role of vector representation in natural language processing and graph-based models, utilizing embeddings to transform textual or structured information into feature-rich numerical representations for downstream tasks (Avdan & Onal, 2024; Hu et al., 2023; Kotiyal et al., 2023). This trend highlights the expanding role of vectors beyond structured sensor data, incorporating knowledge graphs, symbolic AI, and multimodal learning.

In summary, the definition and utilization of Vector in these frameworks highlight the increasing importance of diverse data types in modern AI-driven applications. Whether focusing on physiological signals, environmental sensors, or multi-modal fusion, the reviewed studies underscore the pivotal role of vector selection in achieving accurate and reliable outcomes.

5.3. Devices

The reviewed works employ a diverse range of devices, including wearable sensors, smartphones, edge computing devices, and dedicated health-monitoring equipment. These devices facilitate real-time data collection, enabling various health and environmental monitoring applications.

Wearable sensors such as smartwatches, fitness trackers, and biosensors are prominently used for physiological data collection. These devices continuously monitor biometric signals like heart rate, oxygen saturation, and movement patterns, which are crucial for applications like chronic disease monitoring, stress detection, and early anomaly detection (Alahmadi et al., 2024; El Jaouhari, 2023; Kotiyal et al., 2023; Pham et al., 2023). For instance, smartwatches and fitness bands are widely integrated into healthcare frameworks, allowing for seamless tracking of physical activities and cardiovascular health (Alferaidi et al., 2024; Aminifar et al., 2024; Baucas et al., 2023b). Additionally, specialized sensors such as EEG monitors and e-glass wearable systems have been utilized for detecting neurological conditions like epileptic seizures (Birari et al., 2023; Elayan et al., 2021; Yu et al., 2022).

Beyond individual wearables, edge computing devices such as Raspberry Pi and Jetson Nano play a crucial role in decentralized health-monitoring frameworks. These devices enable low-latency processing of sensor data, reducing dependency on cloud infrastructure while maintaining privacy (Ghosh & Ghosh, 2023; Kaur et al., 2024; Lakhan et al., 2024). Wearable biosensors and accelerometers also integrate with edge devices to enhance mobility and efficiency in healthcare applications (Avdan & Onal, 2024; Rahmany et al., 2023; Sachin et al., 2023; Wang et al., 2023).

Smartphones serve as another pivotal component in data acquisition and processing. Equipped with in-built sensors, they facilitate real-time health assessments and emergency response systems (Bhatt et al., 2024; Farooq et al., 2022; Hu et al., 2023). Some frameworks leverage smartphone cameras for capturing skin images, aiding in remote dermatological diagnosis (Babu et al., 2024b; Ravi Shanker Reddy & Beena, 2022; Zhang et al., 2021). Additionally, smartphones often act as intermediaries, aggregating data from multiple wearable and IoT sensors before transmitting it to cloud servers for further analysis (Antona & Stephanidis, 2022; Can & Ersoy, 2021; Shae & Tsai, 2021).

IoT-enabled smart home devices such as smart home sensors and environmental monitoring units are also incorporated into monitoring frameworks. These systems capture contextual data, such as ambient temperature, humidity, and air quality, to provide a holistic view of an individual's health (Arya et al., 2023; Birari et al., 2023; Fang et al., 2021; Kaur et al., 2024). The integration of such environmental data with physiological signals enhances the predictive accuracy of health-monitoring models (Alahmadi et al., 2024; El Jaouhari, 2023; Yu et al., 2022).

In summary, the selected studies emphasize a multi-device ecosystem for comprehensive health and environmental monitoring. By leveraging wearable sensors, smartphones, edge computing, and smart home devices, these frameworks enhance real-time analytics, improve accuracy, and ensure privacy-preserving health assessments.

Beyond functional diversity, device selection introduces structural constraints that directly influence federated learning performance. Wearable-centric architectures, as explored in Alahmadi et al. (2024), Kotiyal et al. (2023), and Pham et al. (2023), maximize data locality and minimize privacy exposure but are constrained by limited battery capacity and computational resources. Such constraints often restrict local training epochs or model complexity, potentially slowing global convergence.

Smartphone-assisted or intermediary aggregation models, such as those in Can and Ersoy (Can & Ersoy, 2021), Shae and Tsai (Shae & Tsai, 2021), and Antona and Stephanidis (Antona & Stephanidis, 2022), alleviate on-device computation but introduce additional communication layers that may increase latency and synchronization challenges.

Edge–cloud hybrid architectures, including Avdan and Onal (Avdan & Onal, 2024), Yu et al. (2022), and Sachin et al. (2023), demonstrate improved scalability and aggregation efficiency through more powerful edge servers. However, increased infrastructure complexity may enlarge the attack surface, a concern highlighted in privacy-oriented frameworks such as Lakhan et al. (2024) and Bhatt et al. (2024).

Device heterogeneity further affects algorithmic stability. Connectivity fluctuations, energy limitations, and client dropouts — common in wearable deployments — may bias model updates and slow convergence, particularly under non-IID conditions discussed in broader healthcare FL analyses (Joshi et al., 2022; Pfitzner et al., 2021).

Consequently, frameworks that report strong experimental performance often operate under controlled device conditions (e.g., Aminifar et al. (2024), Kotiyal et al., 2023), rather than demonstrating robustness under realistic heterogeneous wearable environments. Addressing energy-aware participation and adaptive aggregation remains an open challenge in federated wearable systems.

5.4. Domains

The reviewed studies span a variety of domains, with a predominant focus on healthcare applications. Many frameworks are designed for personalized medicine, remote patient monitoring, and early disease detection, leveraging wearable sensors, IoT devices, and machine learning models to improve healthcare outcomes (Avdan & Onal, 2024; Hu et al., 2023; Kotiyal et al., 2023). These systems aim to provide continuous health assessment, enabling early diagnosis and timely intervention for chronic conditions like cardiovascular diseases, diabetes, and neurological disorders (Aminifar et al., 2024; Baucas et al., 2023b; Lakhan et al., 2024). For instance, some frameworks use biosensors and real-time monitoring platforms to track physiological parameters such as heart rate variability and blood glucose levels (Alferaidi et al., 2024; Can & Ersoy, 2021; Ghosh & Ghosh, 2023). Others focus on stress detection by analyzing multi-modal data, including biometric signals and behavioral indicators (Bhatt et al., 2024; Birari et al., 2023; El Jaouhari, 2023).

Beyond individual health tracking, remote patient monitoring (RPM) systems have been widely adopted to support elderly care, post-surgery recovery, and chronic disease management. These systems integrate wearable sensors and cloud-based analytics to facilitate remote consultations, reducing the need for in-person hospital visits (Alahmadi et al., 2024; Babu et al., 2024b; Yu et al., 2022). Some frameworks specifically address mental health monitoring, utilizing physiological and contextual data to detect early signs of depression and anxiety (Kaur et al., 2024; Ravi Shanker Reddy & Beena, 2022; Zhang et al., 2021).

While healthcare remains the dominant domain, several studies extend their focus to industrial applications, including predictive maintenance and workplace safety. Frameworks in this category use sensor-based monitoring to detect mechanical failures, worker fatigue, or hazardous environmental conditions, thereby preventing accidents and equipment failures (Pham et al., 2023; Sachin et al., 2023; Shae & Tsai, 2021; Wang et al., 2023). In addition, smart home and environmental monitoring systems leverage IoT-based solutions to track air quality, temperature fluctuations, and energy consumption, ensuring optimized living conditions (Elayan et al., 2021; Fang et al., 2021; Farooq et al., 2022).

Another emerging application area is sports and fitness tracking, where wearable technology is employed to enhance athletic performance and injury prevention. Some frameworks focus on motion analysis using accelerometer and gyroscope data to optimize training regimens for athletes (Birari et al., 2023; El Jaouhari, 2023; Yu et al., 2022). Additionally, fitness monitoring solutions are increasingly integrated into consumer applications, providing real-time feedback on physical activities and caloric expenditure (Alferaidi et al., 2024; Arya et al., 2023; Ghosh & Ghosh, 2023; Rahmany et al., 2023).

In summary, the reviewed studies highlight the diverse applicability of these frameworks across multiple domains, with a strong emphasis on healthcare, industrial safety, smart environments, and fitness tracking. By leveraging advanced data collection and analysis techniques, these systems improve decision-making, enhance personalized monitoring, and contribute to safer and more efficient environments.

5.5. Use case

The reviewed frameworks are applied to various use cases, ranging from individual-level monitoring to broader community health programs and hospital networks. Many studies focus on individual users, particularly for stress detection, mental health assessment, and personalized health monitoring. These frameworks leverage physiological signals such as heart rate variability and electrodermal activity to evaluate stress levels and emotional well-being (Alahmadi et al., 2024; El Jaouhari, 2023; Fang et al., 2021; Farooq et al., 2022; Kotiyal et al., 2023; Pham et al., 2023). Some studies incorporate smartphone-based data, including activity tracking, sleep patterns, and digital biomarkers, to enhance accuracy in personalized health assessments (Alferaidi et al., 2024; Birari et al., 2023; Ravi Shanker Reddy & Beena, 2022).

Beyond individual monitoring, several frameworks are designed for workplace wellness programs and employee stress management. These solutions integrate wearable sensors and digital platforms to analyze employee health trends, providing organizations with insights into workplace stressors and productivity correlations (Hu et al., 2023; Kaur et al., 2024; Lakhan et al., 2024; Rahmany et al., 2023; Shae & Tsai, 2021). Some studies extend their focus to community-level health monitoring, utilizing IoT-enabled solutions to track environmental and behavioral factors affecting public health (Arya et al., 2023; Avdan & Onal, 2024; Babu et al., 2024b; Can & Ersoy, 2021). These frameworks often integrate data from smart city infrastructure, public health surveys, and large-scale sensor networks to monitor collective well-being.

In hospital and clinical settings, several frameworks support RPM and disease management for conditions such as cardiovascular diseases and chronic illnesses. These studies employ ECG-based wearable devices, continuous glucose monitors, and cloud-based platforms to enable real-time intervention and reduce hospital visits (Antona & Stephanidis, 2022; Baucas et al., 2023b; Bhatt et al., 2024; Ghosh & Ghosh, 2023; Sachin et al., 2023; Wang et al., 2023). Some frameworks also focus on predictive analytics, leveraging multi-modal patient data to anticipate health deterioration and recommend timely interventions (Aminifar et al., 2024; Elayan et al., 2021; Yu et al., 2022; Zhang et al., 2021).

In summary, the reviewed frameworks demonstrate diverse applications, addressing individual users, workplace environments, community health programs, and hospital networks. The scalability of these solutions underscores their potential in enhancing both personalized and population-wide health interventions.

5.6. Customer type

The reviewed frameworks cater to a diverse range of end-users, spanning from individual patients to healthcare providers and large-scale organizations such as hospitals and research institutions. Many studies focus on individual customers, particularly patients who require personalized healthcare solutions. These frameworks leverage wearable devices, smartphone applications, and remote monitoring technologies to assist individuals in tracking their health metrics, such as stress levels, heart rate variability, and activity patterns (Avdan & Onal, 2024; Babu et al., 2024b; Birari et al., 2023; Kaur et al., 2024; Pham et al., 2023; Wang et al., 2023). Some frameworks are tailored for chronic disease patients, providing real-time health monitoring and alerts for conditions such as diabetes, cardiovascular diseases, and mental health disorders (Alahmadi et al., 2024; El Jaouhari, 2023; Fang et al., 2021; Farooq et al., 2022; Kotiyal et al., 2023).

Beyond individual users, several frameworks are designed for healthcare providers, including physicians, nurses, and clinical specialists. These systems integrate real-time patient data, predictive analytics, and decision-support tools to enhance diagnosis, treatment planning, and remote patient monitoring (Baucas et al., 2023b; Bhatt et al., 2024; Can & Ersoy, 2021; Ghosh & Ghosh, 2023; Sachin et al., 2023; Zhang et al., 2021). Some studies specifically address telemedicine platforms, allowing healthcare

professionals to monitor patients remotely through IoT-enabled devices and AI-driven analytics (Alferaidi et al., 2024; Aminifar et al., 2024; Hu et al., 2023; Rahmany et al., 2023). These frameworks facilitate early intervention, improve patient outcomes, and optimize clinical workflows.

Additionally, some frameworks cater to large-scale organizations, such as hospitals, research institutions, and public health agencies. These implementations focus on big-data-driven healthcare analytics, integrating electronic health records (EHRs), population health data, and AI-powered predictive modeling to enhance decision-making at institutional levels (Antona & Stephanidis, 2022; Arya et al., 2023; Elayan et al., 2021; Lakhan et al., 2024; Yu et al., 2022). Hospitals leverage these frameworks for patient management, resource optimization, and operational efficiency, ensuring seamless integration of real-time health monitoring with hospital information systems (Birari et al., 2023; Ravi Shanker Reddy & Beena, 2022; Shae & Tsai, 2021).

In summary, the reviewed studies demonstrate a multi-tiered approach to customer engagement, addressing individual patients, healthcare professionals, and institutional stakeholders. These frameworks highlight the scalability of AI-driven healthcare solutions, ensuring improved patient care, clinical decision support, and large-scale health management.

5.7. Provider type

The reviewed frameworks are implemented by a diverse range of providers, including technology developers, healthcare service providers, and data aggregators. These entities play a crucial role in designing, deploying, and maintaining AI-driven solutions for healthcare, smart monitoring, and data analytics.

A significant number of studies highlight the role of technology providers, particularly IoT platform developers, AI engineers, and software companies that design and implement hardware–software solutions for real-time health monitoring, predictive analytics, and decision support systems (Alahmadi et al., 2024; Babu et al., 2024b; Bhatt et al., 2024; Farooq et al., 2022; Ghosh & Ghosh, 2023; Shae & Tsai, 2021). These providers develop wearable sensors, cloud-based analytics platforms, and AI-powered healthcare applications, enabling the seamless integration of machine learning models with smart devices for remote health monitoring and diagnostics (Avdan & Onal, 2024; Kaur et al., 2024; Kotiyal et al., 2023; Rahmany et al., 2023; Wang et al., 2023; Zhang et al., 2021).

Additionally, healthcare service providers, including hospitals, clinics, and telemedicine companies, are key stakeholders in deploying these frameworks for patient monitoring, chronic disease management, and remote diagnostics (Alferaidi et al., 2024; Elayan et al., 2021; Lakhan et al., 2024; Sachin et al., 2023; Yu et al., 2022). These providers utilize IoT-enabled medical devices, cloud-based electronic EHRs, and AI-driven clinical decision support systems to improve patient outcomes, operational efficiency, and medical interventions (Aminifar et al., 2024; Antona & Stephanidis, 2022; Baucas et al., 2023b; El Jaouhari, 2023; Fang et al., 2021). Some frameworks are directly embedded into hospital infrastructure, enabling healthcare professionals to monitor patients in real time, optimize resource allocation, and facilitate early disease detection through predictive analytics (Arya et al., 2023; Can & Ersoy, 2021; Hu et al., 2023).

Another crucial category includes data aggregators, such as research institutions, public health agencies, and health-tech companies, which focus on data collection, integration, and large-scale analysis of health records, wearable sensor data, and population health trends (Alferaidi et al., 2024; Birari et al., 2023; Kaur et al., 2024; Shae & Tsai, 2021). These providers work closely with hospitals, government organizations, and technology firms to ensure that AI-driven frameworks are trained on diverse, high-quality datasets, improving the accuracy and generalizability of healthcare applications (Avdan & Onal, 2024; El Jaouhari, 2023; Farooq et al., 2022; Ravi Shanker Reddy & Beena, 2022).

In conclusion, technology providers, healthcare service providers, and data aggregators collectively drive the implementation of AI-based healthcare solutions. Their contributions ensure the development, deployment, and scalability of frameworks that enhance health monitoring, predictive diagnostics, and data-driven decision-making across multiple domains.

5.8. Benefits

The reviewed frameworks provide a wide range of benefits, addressing healthcare efficiency, patient outcomes, data privacy, real-time monitoring, and cost reduction. These benefits are crucial drivers behind the adoption of AI-powered and IoT-enabled healthcare solutions, demonstrating their impact across different applications.

One of the most prominent benefits is improving health outcomes through early diagnosis, personalized treatment plans, and continuous patient monitoring (Aminifar et al., 2024; Babu et al., 2024b; Hu et al., 2023; Ravi Shanker Reddy & Beena, 2022; Zhang et al., 2021). Many frameworks leverage machine learning models and wearable sensor data to detect abnormalities in physiological signals, such as heart rate fluctuations, oxygen saturation changes, or stress indicators, enabling timely interventions for patients at risk (Baucas et al., 2023b; Kotiyal et al., 2023; Pham et al., 2023; Yu et al., 2022). Some studies focus on chronic disease management, where AI-driven solutions provide long-term monitoring and predictive analytics to help patients with diabetes, cardiovascular diseases, and mental health conditions (Avdan & Onal, 2024; Fang et al., 2021; Farooq et al., 2022).

Another critical advantage is ensuring privacy and security, particularly in frameworks handling sensitive health data. Many approaches incorporate privacy-preserving mechanisms, such as differential privacy and blockchain-based data sharing, to protect patient information while maintaining model performance (Alahmadi et al., 2024; Antona & Stephanidis, 2022; Ghosh & Ghosh, 2023; Kaur et al., 2024; Lakhan et al., 2024; Rahmany et al., 2023; Wang et al., 2023). These methods enable secure data exchange between healthcare providers, research institutions, and technology firms, ensuring compliance with regulatory requirements while maintaining trust in AI-driven healthcare solutions (Bhatt et al., 2024; Can & Ersoy, 2021).

Furthermore, real-time monitoring and decision-making capabilities significantly enhance healthcare efficiency and responsiveness. Several studies emphasize IoT-integrated frameworks that enable continuous health tracking, emergency alert systems, and remote patient management (Alferaidi et al., 2024; Aminifar et al., 2024; Arya et al., 2023; Ravi Shanker Reddy & Beena, 2022). These systems allow clinicians to receive instant notifications about critical patient conditions, improving response times and reducing the risk of life-threatening complications (El Jaouhari, 2023; Fang et al., 2021; Yu et al., 2022). Additionally, frameworks leveraging edge computing facilitate low-latency decision-making, ensuring that processing is done locally rather than relying on cloud servers (Baucas et al., 2023b; Shae & Tsai, 2021).

Lastly, cost reduction is a notable benefit, particularly in hospital management, resource allocation, and telemedicine services. AI-driven solutions optimize hospital workflows, automate administrative tasks, and enhance predictive maintenance for medical equipment, leading to lower operational costs for healthcare institutions (Alahmadi et al., 2024; Sachin et al., 2023). Moreover, remote patient monitoring solutions reduce the need for frequent hospital visits, allowing patients to receive quality care from home, ultimately minimizing healthcare expenses for both individuals and organizations (Birari et al., 2023; Farooq et al., 2022).

In summary, the benefits of these frameworks are multi-faceted, ranging from improving patient health and privacy protection to enabling real-time monitoring and reducing costs. The reviewed studies collectively highlight the transformative potential of AI and IoT in revolutionizing healthcare delivery, enhancing efficiency, accuracy, and accessibility across diverse applications.

5.9. Constraints

The reviewed frameworks operate under various constraints that impact their performance, feasibility, and scalability. These constraints primarily involve hardware limitations, network bandwidth, computational efficiency, and regulatory compliance, all of which must be carefully addressed to ensure the effectiveness of AI-driven and IoT-enabled healthcare solutions.

One of the most common challenges is the battery life of wearable devices used for continuous health monitoring. Many frameworks rely on low-power sensors, ECG monitors, and fitness bands to track physiological signals, but energy efficiency remains a critical limitation (Lakhan et al., 2024; Pham et al., 2023). Studies propose power-aware algorithms and optimized data transmission methods to minimize energy consumption while maintaining real-time data collection (Bhatt et al., 2024; Shae & Tsai, 2021). Additionally, edge computing techniques have been introduced to reduce reliance on cloud processing, thereby extending the operational time of battery-powered devices (Alferaidi et al., 2024; Farooq et al., 2022; Ghosh & Ghosh, 2023).

Another significant constraint is network bandwidth and latency, which affect the real-time transmission of health data. Many frameworks operate in resource-constrained environments, where limited connectivity, unstable internet access, or high-latency networks can hinder data synchronization between wearable devices, mobile applications, and cloud servers (Alahmadi et al., 2024; Antona & Stephanidis, 2022; Kotiyal et al., 2023; Rahmany et al., 2023; Ravi Shanker Reddy & Beena, 2022; Sachin et al., 2023). To address this, several approaches implement data compression techniques, adaptive sampling rates, and edge computing frameworks to optimize bandwidth utilization and reduce network congestion (Aminifar et al., 2024; Baucas et al., 2023b; Elayan et al., 2021).

Computational limitations also pose a major challenge, particularly in resource-constrained devices like smartphones and embedded IoT systems. Running complex AI models on such devices requires efficient inference mechanisms that balance model accuracy with computational overhead (Babu et al., 2024b; Birari et al., 2023; Can & Ersoy, 2021; El Jaouhari, 2023). Several studies incorporate lightweight deep learning architectures, quantization techniques, and federated learning approaches to enable real-time analysis without overwhelming local hardware resources (Alferaidi et al., 2024; Sachin et al., 2023; Shae & Tsai, 2021; Wang et al., 2023).

Additionally, compliance with privacy regulations such as HIPAA, GDPR, and other national data protection laws introduces legal and ethical constraints on how data is collected, stored, and processed. Many frameworks must adhere to strict encryption standards, anonymization techniques, and access control policies to ensure patient data confidentiality and security (Avdan & Onal, 2024; Zhang et al., 2021). Some studies explore blockchain-based solutions and secure multiparty computation as innovative methods to enhance privacy and regulatory compliance without sacrificing performance (Alahmadi et al., 2024; Kaur et al., 2024; Kotiyal et al., 2023; Yu et al., 2022).

Moreover, scalability constraints arise when frameworks transition from small-scale pilot studies to large-scale real-world deployments. Many approaches require significant infrastructure investment, including high-performance computing resources, secure cloud storage, and reliable communication networks (Baucas et al., 2023b; Farooq et al., 2022; Hu et al., 2023; Lakhan et al., 2024). To tackle these issues, researchers propose modular architectures and distributed learning models that can dynamically scale based on the availability of computing resources (Bhatt et al., 2024).

In summary, the effectiveness of these frameworks is shaped by a range of hardware, software, network, and regulatory constraints. By addressing battery life, bandwidth limitations, computational efficiency, privacy concerns, and scalability challenges, the reviewed studies highlight innovative strategies to enhance the practicality and reliability of AI-driven healthcare solutions.

5.10. Market readiness

The market readiness of the reviewed frameworks varies significantly, ranging from fully deployed solutions to experimental prototypes still undergoing validation. While some studies detail real-world implementations, others remain at the conceptual or laboratory testing stage, requiring further refinements before they can be commercially viable.

Several frameworks have already been deployed in real-world settings, particularly in remote patient monitoring, personalized medicine, and healthcare analytics. These systems leverage wearable devices, cloud-based platforms, and AI-driven analytics to

provide real-time health insights, enabling practical use by hospitals, research institutions, and healthcare providers (Aminifar et al., 2024; Babu et al., 2024b; Hu et al., 2023; Ravi Shanker Reddy & Beena, 2022; Zhang et al., 2021). Studies reporting successful deployment often include clinical trials, hospital collaborations, or integration with existing healthcare infrastructures, demonstrating their practical feasibility (Baucas et al., 2023b; Fang et al., 2021; Kaur et al., 2024; Kotiyal et al., 2023; Pham et al., 2023; Wang et al., 2023).

However, a significant number of studies remain in the prototype phase, focusing on algorithmic validation, small-scale pilot studies, or synthetic data experiments. These works typically assess model accuracy, computational efficiency, and robustness in controlled environments, but lack the necessary scalability and regulatory approvals for immediate deployment (Birari et al., 2023; Can & Ersoy, 2021; El Jaouhari, 2023; Elayan et al., 2021; Lakhan et al., 2024; Rahmany et al., 2023). Many such frameworks require further optimization in terms of energy efficiency, security, and interoperability before they can be adopted in practical applications (Bhatt et al., 2024; Sachin et al., 2023; Shae & Tsai, 2021; Yu et al., 2022).

Key challenges preventing full-scale deployment include privacy regulations, data-sharing restrictions, and technical scalability. Many frameworks handling sensitive patient data must comply with HIPAA, GDPR, or similar legal frameworks, which imposes strict encryption, anonymization, and data ownership requirements before deployment is possible (Antona & Stephanidis, 2022; Arya et al., 2023; Avdan & Onal, 2024; Farooq et al., 2022; Ghosh & Ghosh, 2023). Additionally, hardware constraints — such as battery life limitations in wearable sensors and real-time processing demands — further delay market readiness (Alahmadi et al., 2024; Wang et al., 2023).

To bridge the gap between experimental research and real-world applications, several studies propose edge computing integration and adaptive AI models to enhance practical feasibility (Birari et al., 2023; Kotiyal et al., 2023; Ravi Shanker Reddy & Beena, 2022). Some works also emphasize collaborations between academia and industry, ensuring that proposed solutions align with market demands and regulatory standards (Alferaidi et al., 2024; Hu et al., 2023; Shae & Tsai, 2021).

While several frameworks have reached real-world deployment, many remain at the experimental or prototype stage, requiring further validation, regulatory approval, and performance optimizations. Addressing scalability, privacy, and hardware limitations is crucial for advancing these frameworks toward full market adoption.

5.11. Methods

The reviewed frameworks employ a diverse set of methods, including blockchain integration, statistical modeling, and machine learning techniques. Many works combine multiple methods in hybrid approaches to enhance security, efficiency, and interpretability, ensuring robustness in healthcare and IoT-based applications.

A significant number of studies leverage machine learning and deep learning techniques for data classification, anomaly detection, and predictive analytics. Commonly used ML models include Support Vector Machines, Decision Trees, Random Forest, and Neural Networks, applied to tasks such as stress detection, disease prediction, and biometric signal analysis (Alferaidi et al., 2024; Birari et al., 2023; Kaur et al., 2024; Shae & Tsai, 2021; Yu et al., 2022). In some frameworks, reinforcement learning is introduced to optimize resource allocation and adaptive decision-making in healthcare systems (Elayan et al., 2021; Farooq et al., 2022; Hu et al., 2023).

Several studies adopt federated learning to address data privacy and decentralized model training challenges. By enabling local model training on edge devices without sharing raw data, FL frameworks ensure compliance with privacy regulations like GDPR and HIPAA while still benefiting from global model improvements (Alahmadi et al., 2024; Arya et al., 2023; Lakhan et al., 2024; Ravi Shanker Reddy & Beena, 2022; Sachin et al., 2023). These frameworks are particularly useful for collaborative healthcare systems, remote patient monitoring, and multi-institutional research studies (Bhatt et al., 2024; Zhang et al., 2021).

To further enhance security and trust, some works incorporate blockchain technology for tamper-proof data storage, access control, and secure transactions. Blockchain-based frameworks ensure integrity and transparency in healthcare records and IoT device communications, mitigating risks related to data manipulation and unauthorized access (Antona & Stephanidis, 2022; Avdan & Onal, 2024; Can & Ersoy, 2021; El Jaouhari, 2023; Fang et al., 2021). Hybrid frameworks often integrate blockchain with federated learning, ensuring both privacy-preserving model training and secure decentralized data sharing (Baucas et al., 2023b; Wang et al., 2023).

In addition to AI-driven techniques, several works employ statistical and rule-based modeling to develop interpretable decision-making frameworks. Bayesian models, Markov chains, and heuristic-based methods are used for predictive modeling, patient monitoring, and anomaly detection in medical datasets (Alferaidi et al., 2024; Birari et al., 2023; Rahmany et al., 2023; Shae & Tsai, 2021; Yu et al., 2022). These methods are particularly useful in resource-constrained settings where computational efficiency is critical (Alahmadi et al., 2024; Babu et al., 2024b; Ghosh & Ghosh, 2023).

Hybrid approaches integrating AI, statistical methods, and decentralized architectures are gaining prominence, enabling frameworks to achieve multiple objectives such as privacy preservation, real-time decision-making, and computational efficiency. For example, some works combine deep learning with blockchain for secure medical data analytics, while others integrate federated learning with IoT-based edge computing for low-latency healthcare monitoring (Aminifar et al., 2024; Kotiyal et al., 2023; Pham et al., 2023; Ravi Shanker Reddy & Beena, 2022).

The methods employed in these frameworks highlight a shift toward privacy-aware, scalable, and AI-enhanced solutions. While machine learning and federated learning remain dominant approaches, emerging trends such as blockchain integration, reinforcement learning, and hybrid AI techniques are driving advancements in healthcare, IoT, and smart environments.

Table 10
Mapping of federated learning security mechanisms to HIPAA Security Rule safeguard categories. Gaps indicate requirements unaddressed in the reviewed literature.

HIPAA Sec. Rule Safeguard Categ.	Specific Standard CFR Reference	FL Mechanism Addressing It	Representative Papers
Technical — Access Control	Section 164.312(a)(1): Unique user identification, emergency access, automatic log-off	Blockchain-based identity and access management; secure aggregation preventing server access to raw gradients	Baucas et al. (2023b); Farooq et al. (2022); Can and Ersoy (2021)
Technical — Audit Controls	Section 164.312(b): Hardware, software, and procedural mechanisms to record and examine activity	Immutable blockchain ledger for logging model update provenance and access events	Baucas et al. (2023b); Farooq et al. (2022); Shae and Tsai (2021)
Technical — Transmission Security	Section 164.312(e)(2): Encryption of ePHI in transit	AES encryption of model updates; homomorphic encryption preserving confidentiality during aggregation	Lakhan et al. (2024); Bhatt et al. (2024); Aminifar et al. (2024)
Technical — Integrity Controls	Section 164.312(c)(1): Protect ePHI from improper alteration or destruction	Cryptographic signing of model updates; blockchain-enforced immutability of health records	Farooq et al. (2022); Ravi Shanker Reddy and Beena (2022); Wang et al. (2023)
Administrative — Risk Analysis	Section 164.308(a)(1): Conduct accurate and thorough assessment of potential risks	Threat modeling for FL attack surfaces (gradient inversion, model poisoning); largely unaddressed in reviewed literature	Gap identified across reviewed frameworks
Administrative — Workforce Training	Section 164.308(a)(5): Security awareness and training programme	Not addressed in any reviewed technical paper	Gap identified across reviewed frameworks
Physical — Device and Media Controls	Section 164.310(d)(1): Disposal, re-use, and accountability for hardware containing ePHI	Not addressed; wearable device loss/theft poses unmitigated ePHI exposure risk	Gap identified across reviewed frameworks

To assess regulatory alignment more precisely, Table 10 maps the security-relevant methods identified in the reviewed technical papers to the corresponding HIPAA Security Rule safeguard categories (45 CFR Part 164, Subpart C[10]). This mapping reveals both the coverage and the gaps in how current wearable FL frameworks address regulatory security requirements.

The mapping in Table 10 reveals a systematic imbalance: technical safeguards related to encryption and access control are partially addressed through cryptographic FL mechanisms, while administrative and physical safeguards remain entirely outside the scope of the reviewed literature. This gap is not merely academic. Under HIPAA, covered entities and business associates are required to implement all three safeguard categories. A federated learning framework that achieves strong cryptographic privacy guarantees but does not address audit logging, workforce access controls, or physical device security does not constitute a compliant implementation. Future work should therefore extend security evaluation in wearable FL systems beyond algorithmic privacy mechanisms to encompass the full HIPAA Security Rule safeguard taxonomy.

5.12. Performance-oriented evaluation dimensions

While the proposed 11-feature taxonomy enables a structured description of existing approaches, it does not fully capture how these systems perform under the constraints of wearable federated learning. To complement the descriptive analysis, we introduce a set of performance-oriented evaluation dimensions that reflect key challenges in wearable FL environments. The qualitative ratings were derived from each study's reported architectural choices, communication patterns, model design, and stated deployment constraints, rather than from a standardized cross-paper benchmark; they should therefore be interpreted as comparative synthesis indicators rather than absolute performance measurements:

- *Communication Cost*: The amount of data exchanged between clients and server, particularly relevant in bandwidth-constrained and energy-limited wearable settings.
- *Convergence Speed*: The number of communication rounds or time required for the model to reach acceptable performance.
- *Personalization Strategy*: The extent to which models are adapted to individual users versus maintaining a global model.

[10] https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-C/

Table 11
Qualitative comparison of federated learning approaches for wearable healthcare across performance-oriented evaluation dimensions.

Study	Comm.Cost	Conv.Speed	Person-		
alization	Non-IIDRobustn.	EnergyEfficiency			
Can and Ersoy (2021)	Medium	Medium	Low	Medium	Medium
Elayan et al. (2021)	High	Medium	Medium	Low	Low
Fang et al. (2021)	Low	High	Medium	Medium	High
Shae and Tsai (2021)	High	Low	Low	Low	Low
Zhang et al. (2021)	Medium	High	Low	Medium	Medium
Yu et al. (2022)	Medium	High	Low	Medium	Medium
Farooq et al. (2022)	Medium	Low	Low	Low	Medium
Ravi Shanker Reddy and Beena (2022)	Medium	Medium	Medium	Low	Medium
Antona and Stephanidis (2022)	Medium	Medium	High	Medium	Low
Baucas et al. (2023b)	Medium	Medium	Low	Medium	Medium
Birari et al. (2023)	Low	High	Medium	High	High
Ghosh and Ghosh (2023)	Low	Medium	Medium	Medium	High
Kotiyal et al. (2023)	Low	High	High	High	High
El Jaouhari (2023)	Medium	Medium	High	Medium	Low
Sachin et al. (2023)	High	Medium	Medium	Medium	Low
Wang et al. (2023)	Medium	Medium	Low	Low	Medium
Rahmany et al. (2023)	Medium	Low	Low	Low	Medium
Pham et al. (2023)	Low	Medium	High	Medium	High
Arya et al. (2023)	Low	Medium	Low	Low	High
Hu et al. (2023)	Low	High	High	High	Medium
Alahmadi et al. (2024)	Medium	Medium	Medium	Medium	Medium
Alferaidi et al. (2024)	High	Medium	Low	Medium	Low
Aminifar et al. (2024)	High	Low	High	Medium	Low
Avdan and Onal (2024)	Medium	High	Medium	Medium	Medium
Bhatt et al. (2024)	Low	High	Low	Medium	High
Kaur et al. (2024)	Medium	Medium	Low	Low	Medium
Babu et al. (2024b)	Medium	Medium	Low	Low	Medium
Lakhan et al. (2024)	High	Medium	High	Medium	Low

- *Robustness to Non-IID Data*: The ability of the FL approach to handle heterogeneous and user-specific data distributions.
- *Energy Efficiency*: The computational and communication overhead imposed on resource-constrained wearable devices.

Table 11 provides a qualitative comparison of the analyzed technical studies across these dimensions. The comparison is intended to highlight relative strengths and limitations of different approaches, enabling a more evaluative perspective beyond the structural characteristics captured by the taxonomy. These dimensions provide a complementary perspective to the feature-based taxonomy and also inform the design guidelines presented in Section 7, where system-level trade-offs are translated into actionable recommendations.

6. Discussion

This section synthesizes the findings across both review and technical papers to identify structural trends, recurring design patterns, and unresolved tensions in federated AI for wearable health systems. Rather than reiterating individual contributions, this section abstracts higher-level insights regarding efficiency, scalability, privacy guarantees, and personalization capacity.

Unlike general FL-in-healthcare or IoMT surveys, our analysis shows that wearable-constrained environments require a co-design of sensing, communication, and learning processes, where system performance is shaped as much by device limitations (e.g., energy, connectivity, and sensing granularity) as by algorithmic choices.

6.1. Cross-framework comparative analysis: Structural performance patterns and architecture choices

In Section 2, we compared our work against current literature and identified significant gaps. Indeed, our review paper highlights the distinct approaches used in various studies, particularly emphasizing advanced methodologies like blockchain for secure data aggregation (Shae & Tsai, 2021), federated learning for privacy-preserving healthcare analytics (Can & Ersoy, 2021), and deep learning for activity recognition (Aminifar et al., 2024). Unlike prior works such as (Shaik et al., 2023; Upreti et al., 2024), which concentrate primarily on human activity recognition, our study provides a broader perspective, integrating use cases across chronic illness management, mental health, and personalized care.

In Section 5, we analyzed multiple technical frameworks and their distinguishing features. For instance, (Wang et al., 2023) emphasized hierarchical edge-cloud architectures to enhance scalability, while (Zhang et al., 2021) focused on real-time stress and drowsiness detection using adaptive global update control. Similarly, (Sachin et al., 2023) showcased the use of hybrid CNN-LSTM models for activity recognition, providing robust performance in diverse environments. These frameworks often leverage wearable devices for real-time data collection, including physiological metrics such as ECG, heart rate, and glucose levels (El Jaouhari, 2023;

Kaur et al., 2024), ensuring granular monitoring. Applications like (Yu et al., 2022) go further by integrating clinical data with wearable devices, enabling collaborative diagnostics and privacy-preserving training.

While the reviewed studies report improvements in accuracy, latency, or scalability, a closer inspection reveals that performance gains appear not to be solely attributable to federated learning itself, but to specific architectural and algorithmic choices. Hierarchical edge–cloud designs (e.g., Wang et al., 2023) tend to outperform flat federated topologies in scalability-sensitive scenarios because they reduce communication rounds and localize aggregation. In contrast, frameworks such as (Zhang et al., 2021) that emphasize adaptive global update control prioritize responsiveness and stability over raw scalability.

A recurring pattern across high-performing systems is the integration of task-specific model architectures (e.g., CNN-LSTM hybrids in Sachin et al., 2023) with communication-aware optimization strategies. This suggests that effectiveness in wearable federated AI is not determined by the federated paradigm alone, but by the co-design of (i) model architecture, (ii) aggregation strategy, and (iii) system-level constraints (latency, bandwidth, and energy). Studies that treat these components jointly demonstrate more robust improvements compared to those optimizing only one dimension.

Regarding devices and domains, most reviewed studies prioritize wearable sensors, edge devices, and federated learning-enabled IoT setups. For instance, (Can & Ersoy, 2021) utilized edge devices and wearable biosensors to address energy and latency constraints during mental stress detection. Similarly, (Ravi Shanker Reddy & Beena, 2022) implemented federated learning with blockchain for decentralized health monitoring, ensuring enhanced privacy and security. Notably, (Birari et al., 2023) explored integrating environmental data alongside physiological metrics to assess comprehensive patient well-being.

Although many frameworks report competitive accuracy, fewer explicitly evaluate system-level efficiency metrics such as communication cost, memory footprint, and long-term device sustainability. For instance, blockchain-enhanced federated systems (e.g., Ravi Shanker Reddy & Beena, 2022) improve auditability and trustworthiness, yet introduce additional computational layers that may not scale under high-frequency physiological data streams. Similarly, edge-centric stress detection systems (e.g., Can & Ersoy, 2021) successfully reduce latency, but shift computational burden to battery-constrained devices.

This comparison highlights a critical insight: in wearable healthcare, the most "effective" technique is not necessarily the one achieving the highest accuracy, but the one that optimally balances predictive performance with communication efficiency, energy sustainability, and deployment feasibility. Future evaluations should therefore adopt multi-objective benchmarking rather than single-metric comparisons.

The studies also reveal varied levels of market readiness. While many frameworks, such as (Avdan & Onal, 2024), remain in early prototype stages, promising advancements have been demonstrated in controlled environments. For example, (Can & Ersoy, 2021) validated stress monitoring with federated learning, achieving 87.55% accuracy. On the other hand, (Hu et al., 2023) introduced scalable decentralized frameworks with incremental updates to optimize real-time predictions, addressing the computational constraints of IoT devices.

A comparative assessment indicates that most frameworks remain validation-driven rather than deployment-driven. Only a limited subset reports real-world or clinically anchored deployment scenarios, whereas the majority remains at prototype, simulation, or controlled validation stage. Experimental validations are typically conducted under controlled data distributions and stable connectivity assumptions, which do not fully reflect real-world wearable usage characterized by intermittent connectivity, device heterogeneity, and highly skewed non-IID data.

Frameworks such as (Hu et al., 2023) that incorporate incremental or adaptive updates represent a shift toward deployment-aware design. However, the literature still lacks longitudinal studies evaluating robustness over extended periods. Bridging this gap requires moving beyond proof-of-concept implementations toward stress-tested, real-world pilot deployments with heterogeneous user populations.

Finally, key benefits and constraints were discussed. Enhanced privacy and decentralized data handling are prominent benefits highlighted by Farooq et al. (2022) and Arya et al. (2023). Meanwhile, challenges like computational limitations on edge devices (Elayan et al., 2021), non-uniform data distributions (Yu et al., 2022), and the high costs associated with integrating advanced IoMT systems (Shae & Tsai, 2021) continue to hinder large-scale deployment. Notably, some frameworks, such as (Aminifar et al., 2024), addressed the granularity challenge by leveraging high-frequency data streams like EEG signals at 256 Hz, enabling applications like epilepsy detection. Moreover, (Birari et al., 2023) combined physiological data with environmental metrics for a holistic view of health, while (Zhang et al., 2021) highlighted stress detection through advanced signal processing on biosensors. These examples underscore the adaptability of IoMT systems to address varied healthcare scenarios with precision and efficiency.

6.2. *Five fundamental trade-offs in wearable federated AI systems*

Our comparative analysis reveals five fundamental trade-offs that shape the design of federated learning systems for wearable health devices:

- *Privacy vs. Model Accuracy:* Stronger privacy mechanisms (e.g., differential privacy noise injection, encryption) can degrade model precision, particularly in small-sample wearable datasets.
- *Decentralization vs. Convergence Speed:* Increased decentralization enhances privacy and regulatory compliance but may slow convergence due to non-IID data and asynchronous updates.

- *Transparency (Blockchain) vs. Latency and Energy:* Blockchain improves auditability and trust but its impact on latency and energy consumption varies substantially by architecture. Permissionless chains introduce multi-second to multi-minute confirmation delays and high energy overhead that directly conflict with real-time monitoring requirements and battery-constrained wearable devices. Permissioned chains with deterministic consensus (e.g., PBFT) offer sub-second finality and lower energy costs, but introduce infrastructure and governance complexity. Critically, consensus latency is not merely an operational concern, it constrains the minimum feasible synchronization interval at the aggregation layer, forcing longer local epochs and increasing the risk of client drift under non-IID data distributions.
- *Edge Processing vs. Energy Consumption:* On-device learning reduces cloud dependence but significantly increases battery consumption and device wear.
- *Personalization vs. Global Generalization:* Personalized federated models improve individual health predictions but may reduce robustness across diverse populations.

Importantly, these trade-offs are not independent dimensions but interdependent design axes. For example, increasing personalization often exacerbates convergence challenges in non-IID environments, which in turn may require more frequent communication rounds, affecting energy consumption. Similarly, stronger privacy guarantees through differential privacy can amplify the personalization–generalization tension by reducing the statistical signal available for minority user groups.

Therefore, future federated AI frameworks for wearable health should be conceptualized as multi-objective optimization problems, where privacy, efficiency, fairness, and personalization are jointly optimized under explicit constraints. This perspective shifts research away from isolated algorithmic enhancements toward principled system-level co-design.

6.3. Current challenges and future directions

This review contributes to bridging several gaps in the existing literature by providing a wearable-centric synthesis of federated learning applications, constraints, and design trade-offs. The collective evidence across review and technical papers suggests that federated learning in wearable healthcare should not be evaluated as a single algorithmic innovation, but rather as a systems-level paradigm integrating sensing, communication, computation, and governance layers. Frameworks that explicitly co-design these layers, aligning sensor granularity with aggregation frequency, privacy guarantees with energy budgets, and personalization strategies with convergence stability, demonstrate more balanced performance profiles than approaches optimizing isolated components. Thus, the central insight emerging from this review is that the effectiveness of federated AI in wearable health systems depends less on the choice of a specific optimization algorithm and more on principled architectural alignment with device constraints, data heterogeneity, and clinical requirements. This systems-oriented perspective provides the conceptual foundation upon which future methodological and deployment-oriented advancements can build.

Regarding interoperability and scalability specifically, this survey does not provide a quantitative benchmarking comparison of solution strategies; however, the reviewed technical literature does surface several concrete approaches that can be qualitatively synthesized. For scalability, hierarchical edge-cloud architectures — as demonstrated in Wang et al. (2023) and Putra et al. (2024) — reduce communication rounds and localize aggregation, showing measurable improvements in deployment feasibility across large device populations. Modular and distributed learning designs, such as those proposed in Bhatt et al. (2024), allow frameworks to dynamically scale computational load based on available resources. For interoperability, edge computing integration across heterogeneous device types — evidenced in Kotiyal et al. (2023) and Lakhan et al. (2024) — represents an emerging evaluated approach, enabling data exchange across devices with differing sensor modalities and computational capacities. However, standardized FL communication protocols and cross-platform model sharing remain largely unevaluated in the wearable health context, representing a critical gap for future work.

6.4. Toward a co-design view of the wearable FL pipeline

The trade-offs identified in the preceding sections are not independent concerns but manifestations of a single underlying co-design problem. In wearable FL systems, four coupled layers form a constraint pipeline: the sensing layer (sampling frequency, signal modality, sensor fusion), the communication layer (transmission frequency, payload size, network topology), the local learning layer (model complexity, local epochs, privacy mechanisms), and the global aggregation layer (optimizer choice, convergence rate, aggregation frequency). Constraints imposed at any one layer propagate, often non-linearly, through all downstream layers. Consider the sensing-to-communication link. A framework operating at 256 Hz EEG sampling (Aminifar et al., 2024) generates substantially higher data volumes per unit time than one using 20 Hz accelerometer signals (Kotiyal et al., 2023). This difference is not merely a storage concern: it forces either aggressive local preprocessing (increasing computational load on the device) or higher-bandwidth transmission (increasing energy consumption and latency). Both paths affect the local learning layer, the former by reducing available compute cycles for model training, the latter by depleting battery faster and shortening the device's active participation window. Shorter participation windows, in turn, introduce client dropout patterns that bias global aggregation under non-IID conditions, directly affecting optimizer stability and convergence speed. A symmetric constraint flows from the learning layer back toward sensing. Frameworks employing differential privacy noise injection (Aminifar et al., 2024; Bhatt et al., 2024) require sufficient gradient signal to maintain model utility, which in practice demands a minimum data volume per local update. This creates a lower bound on sensing frequency and local batch size, meaning privacy budget decisions implicitly constrain how aggressively a designer can reduce sensing granularity to save energy. Similarly, blockchain-based aggregation (Baucas et al., 2023b; Farooq et al.,

Table 12
Mapping of representative wearable healthcare use cases to recommended FL architectures, privacy mechanisms, and aggregation strategies based on the reviewed literature.

Use Case	Representative Papers	Recommended Architecture	Privacy Mechanism	Aggregation Strategy
Chronic Disease Monitoring	Babu et al. (2024a), Lakhan et al. (2024), Birari et al. (2023)	Edge-cloud hybrid; hierarchical aggregation	Differential privacy; secure aggregation	FedAvg with adaptive weighting
Stress Detection & Mental Health	Can and Ersoy (2021), Alahmadi et al. (2024), Pham et al. (2023)	On-device FL with smartphone intermediary	Differential privacy; homomorphic encryption	Asynchronous FedAvg
Remote Patient Monitoring	Ghosh and Ghosh (2023), Kaur et al. (2024), Shaik et al. (2023)	Cloud-edge FL; IoMT-enabled hubs	Secure aggregation; anonymization	Synchronous FedAvg with dropout tolerance
Epileptic Seizure Detection	Aminifar et al. (2024)	On-device FL with edge offloading	Secure multiparty computation	High-frequency synchronization with SMC
Activity Recognition & Fitness	Kotiyal et al. (2023), Arya et al. (2023)	Lightweight on-device FL	Federated Siamese networks; local DP	Periodic aggregation with energy-aware scheduling
Multi-institutional Health Collaboration	Upreti et al. (2024), Schulte et al. (2024)	Permissioned blockchain-integrated FL	Homomorphic encryption; PBFT consensus	Ledger-verified aggregation
Elderly Care & Fall Detection	Ghosh and Ghosh (2023), Hu et al. (2023)	Edge-IoMT FL with incremental updates	Secure aggregation	Incremental federated learning (FedIERF)
Industrial & Workplace Health	Ali et al. (2022b), Kotiyal et al. (2023)	Distributed edge FL	Local differential privacy	Modular distributed aggregation

2022; Shae & Tsai, 2021) introduces consensus latency that is effectively a constraint on the global aggregation layer, limiting how frequently model updates can be synchronized. In high-frequency physiological monitoring scenarios, this may force larger local epochs between synchronization events, increasing the risk of client drift and reducing convergence stability, precisely the tension identified in Section 6.2. This pipeline perspective reframes the design guidelines in Section 7 as layer-specific interventions with cross-layer consequences. Hierarchical aggregation (Guideline 1) reduces communication layer load but increases synchronization complexity at the aggregation layer. Energy-aware client participation (Guideline 3) manages the battery constraint at the sensing and communication layers but introduces statistical bias at the aggregation layer if participation is non-uniform. Sensor-aware model design (Guideline 4) explicitly links the sensing and local learning layers by adapting model architecture to signal resolution. Critically, none of the reviewed technical papers appears to explicitly co-optimize across all four layers simultaneously; rather, most optimize only a subset of the pipeline. Frameworks such as Aminifar et al. (2024) and Kotiyal et al. (2023) achieve strong performance within their sensing and learning layers but operate under stable connectivity assumptions that do not reflect realistic wearable deployment conditions. This gap between layer-specific optimization and true pipeline co-design represents the most significant open challenge in wearable federated AI, and should be a primary target for future work.

7. Design guidelines for wearable federated learning systems

While the previous sections provided a structured analysis of challenges and trade-offs, practitioners require actionable guidance to translate these insights into system design choices. Table 12 synthesizes the reviewed literature into a mapping of representative wearable healthcare use cases to recommended FL architectures, privacy mechanisms, and aggregation strategies, providing practitioners with a structured starting point for system design.

To this end, this section synthesizes a set of prescriptive guidelines derived from the reviewed literature that map key wearable constraints and application requirements to concrete federated learning design strategies.

1. Hierarchical aggregation for scalability and latency. When dealing with large-scale deployments or high-frequency physiological data, hierarchical or edge-cloud aggregation architectures should be preferred over flat federated topologies. These architectures reduce communication rounds and latency by performing intermediate aggregation at edge nodes, making them suitable for real-time monitoring scenarios.

2. Adaptive privacy mechanisms based on use case sensitivity. Privacy-preserving techniques should be selected according to the clinical context. For highly sensitive applications (e.g., mental health or chronic disease monitoring), stronger guarantees such as differential privacy or secure multiparty computation should be applied, potentially at the cost of reduced model accuracy. For less sensitive applications (e.g., fitness tracking), lighter mechanisms such as secure aggregation may provide a better trade-off between privacy and performance.

3. Energy-aware client participation. Given the limited battery capacity of wearable devices, client selection strategies should prioritize devices based on energy availability and communication conditions. Techniques such as partial participation or asynchronous updates can reduce energy consumption while maintaining acceptable convergence performance.

4. Sensor-aware model design. Model architectures and training strategies should account for the characteristics of the underlying sensor data. High-frequency signals (e.g., EEG) may require local preprocessing or feature extraction to reduce communication overhead, whereas lower-frequency aggregated signals may allow for more frequent model updates.

5. Blockchain integration for auditability-critical scenarios. Blockchain mechanisms should be employed when data traceability, auditability, and trust across multiple stakeholders are required (e.g., multi-institutional healthcare systems). However, blockchain architecture selection is a critical design decision for wearable FL systems. Permissionless chains (e.g., Ethereum) should be avoided in real-time monitoring scenarios due to probabilistic consensus latency and energy overhead incompatible with battery-constrained devices. Permissioned chains employing deterministic consensus protocols such as PBFT (e.g., Hyperledger Fabric) should be preferred, as they provide sub-second finality at substantially lower energy cost. Furthermore, consensus latency must be treated as a pipeline constraint — it sets a hard lower bound on aggregation frequency, which must be factored jointly into optimizer selection and local epoch design.

6. Hybrid personalization strategies. To balance personalization and generalization, federated models should combine global training with local fine-tuning. This approach improves individual-level performance while maintaining robustness across heterogeneous user populations.

Overall, these guidelines highlight that the optimal design of wearable federated learning systems depends on jointly considering device constraints, data characteristics, and application requirements, rather than optimizing individual components in isolation.

8. Conclusions

In this review, we explored the intersection of FL and wearable health devices, highlighting the transformative potential of this integration in healthcare applications. Our analysis systematically examined key criteria, including privacy, sensor technology, cloud computing, and blockchain, to assess the current state and future directions of FL in this domain. The review of the considered technical papers in topic from the literature revealed several innovative approaches and applications, from early disease detection and chronic disease management to mental stress detection and personalized healthcare. These studies underscore FL's ability to enhance data privacy, enable real-time monitoring, and support decentralized healthcare systems.

This review is particularly relevant given the upcoming adoption of the EHDS, whose regulation came into force on March 25, 2025. The EHDS aims to create a harmonized framework for managing health data across EU member states, enabling both primary and secondary use of data. Federated AI models have significant potential within the EHDS, as Federated Learning enhances privacy by enabling AI model training across devices without the need to share raw data.

Federated technologies align well with EHDS objectives by enhancing interoperability, standardization, and secure access to health data, fostering innovation in healthcare through ethical and efficient data use. By integrating federated AI models into wearable and health device ecosystems, this paper underscores their potential to revolutionize healthcare delivery and research under the EHDS framework.

Despite the advancements, challenges remain. The reviewed literature also suggests several promising directions for interoperability and scalability, including hierarchical edge-cloud aggregation, modular distributed learning, and integration across heterogeneous device types. However, standardized communication protocols and cross-platform model sharing remain largely unevaluated in the wearable FL context and should be prioritized in future work.

A critical gap in the existing literature concerns the treatment of regulatory compliance beyond data privacy. The HIPAA Security Rule (45 CFR Part 164, Subpart C) imposes requirements across three safeguard categories — technical, administrative, and physical — yet the reviewed literature engages almost exclusively with technical safeguards, and even then only partially. As documented in Table 10 (Section 5.11), encryption of model updates and blockchain-based audit logging address transmission security and audit control requirements respectively, but risk analysis, workforce training, contingency planning, and physical device controls are entirely unaddressed across the reviewed corpus. This is particularly significant for wearable deployments, where devices are routinely carried in uncontrolled environments, creating physical security exposure that no FL algorithm can mitigate. GDPR compliance presents similarly unresolved challenges. While FL's on-device data retention architecture directly supports the data minimization principle (Article 5(1)(c)) and purpose limitation (Article 5(1)(b)),[11] several GDPR rights create structural tensions with federated model training. The right to erasure (Article 17) — colloquially the 'right to be forgotten' — requires that an individual's personal data be deleted upon request. In a centralized system, this means deleting database records. In a federated system, personal data is encoded in model weights through the training process, and no current method reliably guarantees complete removal of an individual's contribution from a trained global model without retraining from scratch. Machine unlearning techniques represent a nascent research direction toward addressing this, but none of the reviewed works engage with it. Similarly, GDPR's requirement for a documented legal basis for processing (Article 6)[12] and for secondary use of health data (Article 9(2)(j))[13] impose governance obligations not addressed at the system design level in any reviewed framework. A further dimension absent from the reviewed literature is the medical device regulatory pathway. Wearable health devices that incorporate AI-driven decision support — including FL-based diagnostic and monitoring frameworks — may qualify as Software as a Medical Device (SaMD) under the FDA's digital health regulatory framework (21 CFR Part 880[14]; FDA AI/ML-Based SaMD 2021 Action Plan Singh

[11] https://gdpr-info.eu/art-5-gdpr/
[12] https://gdpr-info.eu/art-6-gdpr/
[13] https://gdpr-info.eu/art-9-gdpr/
[14] https://www.ecfr.gov/current/title-21/chapter-I/subchapter-H/part-880

et al., 2025) or as medical device software under the EU MDR 2017/745.[15] SaMD classification triggers pre-market submission requirements, clinical validation standards, and post-market surveillance obligations. The FDA's Predetermined Change Control Plan (PCCP) framework[16] is particularly relevant for adaptive FL systems, as it requires manufacturers to prospectively document the types of model updates permissible during deployment without requiring a new submission. None of the reviewed technical papers address SaMD classification, pre-market validation, or PCCP design — a gap that represents one of the most significant barriers to clinical deployment of wearable FL systems in practice. Addressing these regulatory gaps will require interdisciplinary collaboration between machine learning researchers, clinical informaticians, regulatory scientists, and legal experts. Specifically, future work should pursue:

- Formal mapping of FL system architectures to HIPAA Security Rule safeguard categories and GDPR Articles, producing compliance coverage matrices analogous to Table 10 but extended to cover administrative and physical safeguards.
- Development and evaluation of machine unlearning techniques tailored to federated models, enabling verifiable satisfaction of GDPR Article 17 without full model retraining.
- Systematic assessment of wearable FL frameworks against SaMD classification criteria and pre-market validation requirements, including prospective PCCP design for continuously updated federated models.
- Integration of privacy-by-design and security-by-design principles into federated learning system specifications from the outset, rather than as post-hoc additions.

Scalability, regulatory compliance, and security concerns also require robust solutions to facilitate widespread adoption. Future research should also shift from isolated feature enhancements toward co-optimization frameworks that simultaneously address privacy, device heterogeneity, sensor reliability, and regulatory compliance. Specifically:

- Adaptive federated algorithms that dynamically adjust privacy budgets based on clinical risk levels.
- Sensor-aware federated optimization that accounts for sampling frequency, signal quality, and calibration drift.
- Lightweight blockchain alternatives tailored for low-power wearables.
- Energy-aware client selection mechanisms that optimize participation based on battery constraints.
- Hybrid personalization strategies combining global federated models with local fine-tuning.
- Standardized interoperability frameworks for heterogeneous wearable devices, including unified data schemas and cross-platform FL communication protocols, to enable robust large-scale deployment.

Moreover, there is a need for standardized benchmarking protocols for wearable federated systems, incorporating metrics beyond accuracy, such as energy consumption, convergence time, and regulatory compliance readiness.

By reframing federated learning as a multi-objective system design challenge rather than solely a privacy-preserving technique, the field can move toward scalable, clinically viable deployments.

CRediT authorship contribution statement

Golshid Ranjbaran: Writing – review & editing, Writing – original draft, Project administration, Methodology, Investigation, Formal analysis, Data curation, Conceptualization. **Sergio Consoli:** Writing – review & editing, Writing – original draft, Validation, Supervision, Project administration, Methodology, Investigation, Conceptualization. **Gabriele Leoni:** Writing – review & editing, Writing – original draft, Validation, Formal analysis, Data curation, Conceptualization. **Diego Reforgiato Recupero:** Writing – review & editing, Writing – original draft, Validation, Supervision, Project administration, Methodology, Investigation, Funding acquisition, Conceptualization. **Chanchal K. Roy:** Writing – review & editing, Validation, Supervision, Funding acquisition.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

This research is supported in part by the Natural Sciences and Engineering Research Council of Canada (NSERC) Discovery Grants program, the Canada Foundation for Innovation's John R. Evans Leaders Fund (CFI-JELF), and by the industry-stream NSERC CREATE in Software Analytics Research (SOAR). Moreover, we would like to thank the colleagues of the Digital Health Unit (JRC.F7) at the Joint Research Centre of the European Commission for helpful guidance and support. The views expressed are purely those of the authors and may not in any circumstance be regarded as stating an official position of the European Commission.

Appendix

This appendix provides the full list of abbreviations used in Tables 7, 8, and 9.
See Table 13.

[15] http://data.europa.eu/eli/reg/2017/745/2026-01-01

[16] https://www.fda.gov/regulatory-information/search-fda-guidance-documents/predetermined-change-control-plans-medical-devices

Table 13
Acronyms grouped by field.

Acronyms used in the Manuscript	
AI	Artificial Intelligence
BERT	Bidirectional Encoder Representations from Transformers
EFL	Edge Federated Learning
EHDS	European Health Data Space
FL	Federated Learning
GANs	Generative Adversarial Networks
GDPR	General Data Protection Regulation
HIPAA	Health Insurance Portability and Accountability Act
IoMT	Internet of Medical Things
LDA	Latent Dirichlet Allocation
mHealth	Mobile Health
ML	Machine Learning
MPNET	Masked and Permuted Pre-Training
NPMI	Normalized Pointwise Mutual Information
SBERT	Sentence Bidirectional Encoder Representations from Transformers
SHFL	Secure Hierarchical Federated Learning
Benefits	
A	Accessibility
AD	Anomalies Detection
AP	Accurate Prediction
ASD	Accurate Stress Detection
DA	Decentralized Architecture
DC	Decentralized Control
DP	Disease Prediction
DS	Data Security
E	Efficiency
EDD	Early Disease Detection
EDI	Environmental Data Integration
EE	Energy-Efficient
ES	Environmental Sustainability
F	Flexibility
G	Generalization
HA	Healthcare Accessibility
HD	Health Detection
HM	Health Monitoring
LRC	Low Resource Consumption
MDD	Minimal Data Dependency
PC	Patient Care
PE	Patient Engagement
PO	Patient Outcomes
PP	Privacy Preservation
PT	Personalized Treatment
R	Robustness
RCC	Reduction in Computational Costs
RCL	Reduced Communication Latency
RP	Real-time Processing
RS	Reduced Strain
S	Scalability
Constraints	
B	Bias
BC	Blockchain complexity
CC	Configuration Consistency
CL	Communication Latency
DQ	Data Quality
DO	Data Ownership
DS	Data Security
EC	Energy Consumption
F	Fairness
HCC	High Computational Cost
ID	Imbalanced Datasets
IL	Infrastructure Limitations
MC	Maintaining Cost
P	Privacy

(*continued on next page*)

Table 13 (*continued*).

Acronyms used in the Manuscript	
R	Robustness
RD	Real-time Delays
S	Scalability
SI	Standardization issues
SQ	Service Quality
SS	Security Servers
V	Vulnerability
Customer Type	
D	Developers
EI	Elderly Individuals
FE	Fitness Enthusiasts
FI	Fitness Enthusiasts
HP	Healthcare Providers
I	Individuals
IoMT_S	IoMT Stakeholders
PC	Pharma Companies
P	Patients
R	Researchers
WU	Wheelchair Users
Devices	
A	Accelerometer
ARS	Activity Recognition Sensors
AS	Aggregation Servers
BC	Bio-Chips
BS	Biosensors
CL	Contact Lenses
CSI	Capturing Skin Images
CS	Cloud Servers
D	Drones
ED	Edge Devices
EGP	Epidermal Glucose Patches
EEG	Electroencephalography
EEG_S	EEG Sensors
ECGM	ECG Monitors
eWS	e-Glass Wearable Systems
EMR_S	EMR Systems
EMS	Environmental Monitoring Sensors
ESS	Enzyme-Free Sweat Sensors
FT	Fitness Trackers
FM	Facemasks
HR	Humanoid Robots
HMD	Health Monitoring Devices
IoT	Internet of Things
IoMT	Internet of Medical Things
IoMT_S	IoMT Sensors
MS	Movement Sensors
PM	Pulse Meter
RFID	Radio-Frequency Identification
SHS	Smart Home Sensors
SB	Smartbands
SP	Smartphones
SS	Signature Servers
SW	Smartwatches
WD	Wearable Devices
WS	Wearable Sensors
W	Wheelchairs
Domains	
Clin.	Clinical
E	Education
eH	E-Health
H	Healthcare
Ind.	Industrial
MH	Mobile-Healthcare
PH	Public Health
Res.	Residential
RH	Rural Healthcare

(*continued on next page*)

Table 13 (*continued*).

Acronyms used in the Manuscript	
SE	School Environment
SH	Smart Healthcare
Granularity	
20HZ	Accelerometer sampling at 20 Hz
256HZ	EEG sampling at 256 Hz
RT	Real Time
Market Readiness	
P	Prototype
PCP	Proof-of-concept Phase
RDV	Real-world Dataset Validation
RP	Research Phase
SP	Simulation Phase
TP	Testing Phase
Methods	
5G	5G Networks
6G	6G Networks
AGUC	Adaptive Global Update Control
AMA	Accelerometer-based Motion Analysis
ANN	Artificial Neural Networks
AR/VR	Augmented Reality/Virtual Reality Technologies
ARX	Autoregression with Exogenous Variables
AES	Advanced Encryption Standards
B	Blockchain
BFL	Bayesian Federated Learning
BV	Batch Verification
C	Cryptographic Techniques
CI	Cloud Infrastructure
CNN-LSTM	Convolutional Neural Network-Long Short-Term Memory
DCNN	Deep Convolutional Neural Networks
DF	Decision Forests
DNN	Deep Learning Models
EC	Edge Computing
EIDR	Intrinsic-Extrinsic Deep Reinforcement Learning
FedAagrad	Federated Adaptive Gradient Algorithm
FedAvg	Federated Averaging
FedERF	Federated Extremely Random Forest
FedIERF	Federated Incremental Extremely Random Forest
FGO	Fano Geometry to Optimize
FL	Federated Learning
FL_ADA	Federated Learning with Adaptive Algorithms
FL_ANN	Federated Learning with Artificial Neural Networks
FL_CNN	Federated Learning with Convolutional Neural Networks
FL_LDA	Federated Learning with Latent Dirichlet Allocation
FSFD	Few-shot-enabled Federated Learning
FSN	Federated Siamese Networks
Fog-IoT	Fog Computing for Internet of Things Architecture
GD	Gradient Descent
H_fog	Hierarchical Edge-Fog-Cloud
HE	Homomorphic Encryption
IL	Incremental Learning
KG	Knowledge Graph
LR	Logistic Regression
M_IoMT_S	Modular Internet of Medical Things Systems
M_MSS	Modular MSS
ML	Machine Learning
MLP	Multi-layer Perceptron
PPFL	Privacy-Preserving Federated Learning
RL	Reinforcement Learning
RS	Ring Signature
SAT	Secure Aggregation Techniques
SMC	Secure Multiparty Computation
SMOTE	Synthetic Minority Oversampling Technique
TFF	TensorFlow Federated
XAI	Explainable AI Techniques
Provider type	
BN	Blockchain-based Networks
CSP	Cloud Service Providers

(*continued on next page*)

Table 13 (*continued*).

Acronyms used in the Manuscript	
D	Developers
DN	Decentralized Networks
EI	Educational Institutions
H	Hospitals
HL	Healthcare Laboratories
HP	Healthcare Providers
IoMT_D	IoMT Developers
IoMT_DM	IoMT Device Manufacturers
IoT_DM	IoT Device Manufacturers
IP	Infrastructure Providers
MDM	Medical Device Manufacturers
R	Researchers
W_IoT_DM	Wearable IoT Device Manufacturers
WDM	Wearable Device Manufacturers
Use Cases	
CIM	Cognitive Impairment Monitoring
CIP	COVID-19 Infection Prediction
D	Diagnostics
DAB	Detecting Abnormal Biometric Values
DHA	Decentralized Health Analytics
DM	Decision-Making
EDD	Early Detection of Diseases
EDI	Environmental Data Integration
ER	Emergency Response
ESD	Epileptic Seizure Detection
FD	Fall Detection
HA	Healthcare Accessibility
HAR	Human Activity Recognition
IDS	Incentivized Data Sharing
LE	Location Estimating
MCC	Monitoring Chronic Conditions
MCD	Monitoring Chronic Diseases
MD	Monitoring Drivers
MWU	Monitoring Wheelchair Users
OD	Offloading Data
PP	Privacy-Preserving
PR	Personalized Recommendations
RHP	Real-time Heart Rate Prediction
RM	Remote Monitoring
S	Students
SD	Stress Detection
SM	Stress Monitoring
SDD	Skin Disease Detection
Vector	
A	Accelerometers
AD	Activity Data
CD	Clinical Data
CP	Contextual Parameters
EMR_D	EMR Data
ES	Environmental Signals
PI	Predictive Insights
PS	Physiological Signals
VD	Vehicular Data

Data availability

No data was used for the research described in the article.

References

Abbas, Syed Raza, Abbas, Zeeshan, Zahir, Arifa, & Lee, Seung Won (2024). Federated learning in smart healthcare: A comprehensive review on privacy, security, and predictive analytics with IoT integration. *Healthcare*, *12*(24), 2587.

Alahmadi, Abdulrahman, Khan, Haroon Ahmed, Shafiq, Ghufran, Ahmed, Junaid, Ali, Bakhtiar, Javed, Muhammad Awais, Khan, Mohammad Zubair, Alsisi, Rayan Hamza, & Alahmadi, Ahmed H (2024). A privacy-preserved iomt-based mental stress detection framework with federated learning. *Journal of Supercomputing*, *80*(8), 10255–10274.

Alam, Md Ashraful, Nabil, Ashrafur Rahman, Uddin, Mohammed Majbah, Sarker, Md Takbir Hossen, & Mahmud, Shaiful (2024). The role of predictive analytics in early disease detection: A data-driven approach to preventive healthcare. *Frontiers in Applied Engineering and Technology*, *1*(01), 105–123a.

Alferaidi, Ali, Yadav, Kusum, Alharbi, Yasser, Alreshidi, Eissa Jaber, Alreshidi, Abdulrahman, Aboshosha, Bassam W, Sharma, Rohit, Alkhayyat, Ahmed, & Aray, Daniel Gavilanes (2024). A novel hybrid, BERT and deep learning model network intrusion detection system for healthcare electronics. *IEEE Transactions on Consumer Electronics*.

Ali, Mansoor, Naeem, Faisal, Tariq, Muhammad, & Kaddoum, Georges (2022a). Federated learning for privacy preservation in smart healthcare systems: A comprehensive survey. *IEEE Journal of Biomedical and Health Informatics*, *27*(2), 778–789.

Ali, Mansoor, Naeem, Faisal, Tariq, Muhammad, & Kaddoum, Georges (2022b). Federated learning for privacy preservation in smart healthcare systems: A comprehensive survey. *IEEE Journal of Biomedical and Health Informatics*, *27*(2), 778–789.

Allaoui, Mebarka, Kherfi, Mohammed Lamine, & Cheriet, Abdelhakim (2020). Considerably improving clustering algorithms using umap dimensionality reduction technique: A comparative study. *Lecture Notes in Computer Science*, *12119 LNCS*, 317–325.

Aminifar, Amin, Shokri, Matin, & Aminifar, Amir (2024). Privacy-preserving edge federated learning for intelligent mobile-health systems. arXiv preprint arXiv:2405.05611.

Antona, Margherita, & Stephanidis, Constantine (2022). *vol. 13309, Universal access in human-computer interaction. User and context diversity: 16th international conference, UAHCI 2022, held as part of the 24th HCI international conference, HCII 2022, virtual event, June 26–July 1, 2022, Proceedings, Part II*. Springer Nature.

Arya, Karm Veer, Tripathi, Vipin Kumar, Rodriguez, Ciro, & Yusuf, Eddy (2023). *vol. 685, Proceedings of 7th ASRES international conference on intelligent technologies: ICIT 2022, Jakarta, Indonesia*. Springer Nature.

Avdan, Goksu, & Onal, Sinan (2024). Resilient healthcare 5.0: Advancing human-centric and sustainable practices in smart healthcare systems. In *IISE annual conference. proceedings* (pp. 1–6). Institute of Industrial and Systems Engineers (IISE).

Babu, CV Suresh, Surendar, V, Dheepak, N, Shiraj, S, & Praveen, K (2024a). Revolutionizing healthcare harnessing IoT-integrated federated learning for early disease detection and patient privacy preservation. In *Federated learning and privacy-preserving in healthcare AI* (pp. 195–216). IGI Global Scientific Publishing.

Babu, CV Suresh, Surendar, V, Dheepak, N, Shiraj, S, & Praveen, K (2024b). Revolutionizing healthcare harnessing IoT-integrated federated learning for early disease detection and patient privacy preservation. In *Federated learning and privacy-preserving in healthcare AI* (pp. 195–216). IGI Global.

Badidi, Elarbi (2023). Edge AI for early detection of chronic diseases and the spread of infectious diseases: opportunities, challenges, and future directions. *Future Internet*, *15*(11), 370.

Baucas, Marc Jayson, Spachos, Petros, & Plataniotis, Konstantinos N (2023a). Federated learning and blockchain-enabled fog-IoT platform for wearables in predictive healthcare. *IEEE Transactions on Computational Social Systems*, *10*(4), 1732–1741.

Baucas, Marc Jayson, Spachos, Petros, & Plataniotis, Konstantinos N (2023b). Federated learning and blockchain-enabled fog-IoT platform for wearables in predictive healthcare. *IEEE Transactions on Computational Social Systems*, *10*(4), 1732–1741.

Bhatt, Harsh, Jadav, Nilesh Kumar, Kumari, Aparna, Gupta, Rajesh, Tanwar, Sudeep, Polkowski, Zdzislaw, Tolba, Amr, & Hassanein, Azza S (2024). Artificial neural network-driven federated learning for heart stroke prediction in healthcare 4.0 underlying 5G. *Concurrency and Computation: Practice and Experience*, *36*(3), Article e7911.

Birari, Dipika R, Bamane, Kalyan Devappa, Kamble, Pratik Bibhishan, Dhaigude, Tanaji Anandrao, Shendge, Ravindra B, & Dandavate, Aarti (2023). Towards a holistic approach to chronic disease management: Integrating federated learning and IoT for personalized health care.. *Journal of Electrical Systems*, *19*(3).

Can, Yekta Said, & Ersoy, Cem (2021). Privacy-preserving federated deep learning for wearable IoT-based biomedical monitoring. *ACM Transactions on Internet Technology (TOIT)*, *21*(1), 1–17.

Chaddad, Ahmad, Wu, Yihang, & Desrosiers, Christian (2023). Federated learning for healthcare applications. *IEEE Internet of Things Journal*.

Devlin, Jacob, Chang, Ming-Wei, Lee, Kenton, & Toutanova, Kristina (2019). BERT: Pre-training of deep bidirectional transformers for language understanding. *vol. 1*, In *NAACL HLT 2019 - 2019 conference of the North American chapter of the association for computational linguistics: human language technologies - proceedings of the conference* (pp. 4171–4186).

El Jaouhari, Saad (2023). Collaborative medical smart spaces for an enhanced health issues detection. In *2023 IEEE globecom workshops* (pp. 2109–2112). IEEE.

Elayan, Haya, Aloqaily, Moayad, & Guizani, Mohsen (2021). Deep federated learning for IoT-based decentralized healthcare systems. In *2021 international wireless communications and mobile computing* (pp. 105–109). IEEE.

Fang, Lei, Liu, Xiaoli, Su, Xiang, Ye, Juan, Dobson, Simon, Hui, Pan, & Tarkoma, Sasu (2021). Bayesian inference federated learning for heart rate prediction. In *Wireless mobile communication and healthcare: 9th EAI international conference, mobiHealth 2020, virtual event, November 19, 2020, proceedings 9* (pp. 116–130). Springer.

Farooq, Komal, Syed, Hassan Jamil, Alqahtani, Samar Othman, Nagmeldin, Wamda, Ibrahim, Ashraf Osman, & Gani, Abdullah (2022). Blockchain federated learning for in-home health monitoring. *Electronics*, *12*(1), 136.

Ghadi, Yazeed Yasin, Mazhar, Tehseen, Shah, Syed Faisal Abbas, Haq, Inayatul, Ahmad, Wasim, Ouahada, Khmaies, & Hamam, Habib (2023). Integration of federated learning with IoT for smart cities applications, challenges, and solutions. *PeerJ Computer Science*, *9*, Article e1657.

Ghosh, Shreya, & Ghosh, Soumya K. (2023). Feel: Federated learning framework for elderly healthcare using edge-iomt. *IEEE Transactions on Computational Social Systems*, *10*(4), 1800–1809.

Grootendorst, Maarten (2022). Bertopic: Neural topic modeling with a class-based TF-IDF procedure. arXiv preprint arXiv:2203.05794.

Gupta, Mansi, Kumar, Mohit, & Dhir, Renu (2024). Unleashing the prospective of blockchain-federated learning fusion for IoT security: A comprehensive review. *Computer Science Review*, *54*, Article 100685.

Haghayegh, Fatemeh, Norouziazad, Alireza, Haghani, Elnaz, Feygin, Ariel Avraham, Rahimi, Reza Hamed, Ghavamabadi, Hamidreza Akbari, Sadighbayan, Deniz, Madhoun, Faress, Papagelis, Manos, Felfeli, Tina, et al. (2024). Revolutionary point-of-care wearable diagnostics for early disease detection and biomarker discovery through intelligent technologies. *Advanced Science*, *11*(36), Article 2400595.

Haque, Benazeer, Siddiqui, Ebtasam Ahmad, & Jha, Saurabh Kumar (2024). Considering the clinical significance of artificial intelligence and biosensors in the healthcare sector: A review. In *2024 IEEE international students' conference on electrical, electronics and computer science* (pp. 1–5). IEEE.

Hu, Chun-Yu, Hu, Li-Sha, Yuan, Lin, Lu, Dian-Jie, Lyu, Lei, & Chen, Yi-Qiang (2023). FedIERF: Federated incremental extremely random forest for wearable health monitoring. *Journal of Computer Science and Technology*, *38*(5), 970–984.

Jelodar, Hamed, Wang, Yongli, Yuan, Chi, Feng, Xia, Jiang, Xiahui, Li, Yanchao, & Zhao, Liang (2019). Latent Dirichlet allocation (LDA) and topic modeling: models, applications, a survey. *Multimedia Tools and Applications*, *78*(11), 15169–15211.

Joshi, Madhura, Pal, Ankit, & Sankarasubbu, Malaikannan (2022). Federated learning for healthcare domain-pipeline, applications and challenges. *ACM Transactions on Computing for Healthcare*, *3*(4), 1–36.

Kaur, Amandeep, Kaushal, Chetna, Hassan, Md Mehedi, & Aung, Si Thu (2024). *Federated deep learning for healthcare: A practical guide with challenges and opportunities*. Boca Raton, US: CRC Press.

Kim, Sang-Woon, & Gil, Joon-Min (2019). Research paper classification systems based on TF-IDF and LDA schemes. *Human-Centric Computing and Information Sciences*, *9*(1).

Kotiyal, Vaibhav, Gupta, Anshita, Deb, Pallav Kumar, Misra, Subhas Chandra, Das, Debanjan, & Udutalapally, Venkanna (2023). Skipper: A federated siamese network-based group activity segregator for IoMT systems. *IEEE Transactions on Computational Social Systems*, *10*(4), 1770–1779.

Lakhan, Abdullah, Hamouda, Hassen, Abdulkareem, Karrar Hameed, Alyahya, Saleh, & Mohammed, Mazin Abed (2024). Digital healthcare framework for patients with disabilities based on deep federated learning schemes. *Computers in Biology and Medicine*, *169*, Article 107845.

Li, Zhaohua, Wang, Le, Chen, Guangyao, Zhang, Zhiqiang, Shafiq, Muhammad, & Gu, Zhaoquan (2022). E2EGI: End-to-end gradient inversion in federated learning. *IEEE Journal of Biomedical and Health Informatics*, *27*(2), 756–767.

Mahanipour, Afsaneh, & Khamfroush, Hana (2024). FMLFS: A federated multi-label feature selection based on information theory in IoT environment. arXiv preprint arXiv:2405.00524.

McInnes, Leland, & Healy, John (2017). Accelerated Hierarchical Density Based Clustering. *vol. 2017-November*, In *IEEE international conference on data mining workshops, ICDMW* (pp. 33–42).

Mifrah, Sara, & Benlahmar, El Habib (2022). Topic Modeling with Transformers for Sentence-Level Using Coronavirus Corpus. *International Journal of Interactive Mobile Technologies (IJIM)*, *16*(17), pp. 50–59.

Mosaiyebzadeh, Fatemeh, Pouriyeh, Seyedamin, Parizi, Reza M, Sheng, Quan Z, Han, Meng, Zhao, Liang, Sannino, Giovanna, Ranieri, Caetano Mazzoni, Ueyama, Jó, & Batista, Daniel Macêdo (2023). Privacy-enhancing technologies in federated learning for the internet of healthcare things: a survey. *Electronics*, *12*(12), 2703.

Moshawrab, Mohammad, Adda, Mehdi, Bouzouane, Abdenour, Ibrahim, Hussein, & Raad, Ali (2023). Reviewing federated machine learning and its use in diseases prediction. *Sensors*, *23*(4), 2112.

Nguyen, Dinh C, Pham, Quoc-Viet, Pathirana, Pubudu N, Ding, Ming, Seneviratne, Aruna, Lin, Zihuai, Dobre, Octavia, & Hwang, Won-Joo (2022). Federated learning for smart healthcare: A survey. *ACM Computing Surveys (Csur)*, *55*(3), 1–37.

Odera, David (2023). Federated learning and differential privacy in clinical health: Extensive survey. *World J. Adv. Eng. Technol. Sci*, *8*, 305–329.

Orzikulova, Adiba, Kwak, Jaehyun, Shin, Jaemin, & Lee, Sung-Ju (2024). Federated learning for time-series healthcare sensing with incomplete modalities. arXiv preprint arXiv:2405.11828.

Pfitzner, Bjarne, Steckhan, Nico, & Arnrich, Bert (2021). Federated learning in a medical context: a systematic literature review. *ACM Transactions on Internet Technology (TOIT)*, *21*(2), 1–31.

Pham, Vinh, Lee, Yongho, & Chung, Tai-Myoung (2023). Personalized stress detection system using physiological data from wearable sensors. In *International conference on future data and security engineering* (pp. 433–441). Springer.

Pokhrel, Shiva Raj, & Choi, Jinho (2020). Federated learning with blockchain for autonomous vehicles: Analysis and design challenges. *IEEE Transactions on Communications*, *68*(8), 4734–4746.

Putra, Karisma Trinanda, Arrayyan, Ahmad Zaki, Hayati, Nur, Damarjati, Cahya, Bakar, Abu, Chen, Hsing-Chung, et al. (2024). A review on the application of internet of medical things in wearable personal health monitoring: A cloud-edge artificial intelligence approach. *IEEE Access*.

Qureshi, Rizwan, Irfan, Muhammad, Ali, Hazrat, Khan, Arshad, Nittala, Aditya Shekhar, Ali, Shawkat, Shah, Abbas, Gondal, Taimoor Muzaffar, Sadak, Ferhat, Shah, Zubair, et al. (2023). Artificial intelligence and biosensors in healthcare and its clinical relevance: A review. *IEEE Access*, *11*, 61600–61620.

Rahmany, Ines, Saidi, Rihab, Moulahi, Tarek, & Almutiq, Mutiq (2023). Reliable framework for digital forensics in medical internet of things. In *International conference on computational collective intelligence* (pp. 470–480). Springer.

Ravi Shanker Reddy, T., & Beena, B. M. (2022). AI integrated blockchain technology for secure health care—Consent-based secured federated transfer learning for predicting COVID-19 on wearable devices. In *International conference on innovative computing and communications: proceedings of ICICC 2022, volume 1* (pp. 345–356). Springer.

Reimers, Nils, & Gurevych, Iryna (2019). Sentence-BERT: Sentence embeddings using siamese BERT-networks. In *EMNLP-IJCNLP 2019 - 2019 conference on empirical methods in natural language processing and 9th international joint conference on natural language processing, proceedings of the conference* (pp. 3982–3992).

Rieke, Nicola, Hancox, Jonny, Li, Wenqi, Milletari, Fausto, Roth, Holger R, Albarqouni, Shadi, Bakas, Spyridon, Galtier, Mathieu N, Landman, Bennett A, Maier-Hein, Klaus, et al. (2020). The future of digital health with federated learning. *NPJ Digital Medicine*, *3*(1), 119.

RRöder, Michael, Both, Andreas, & Hinneburg, Alexander (2015). Exploring the space of topic coherence measures. In *WSDM 2015 - proceedings of the 8th ACM international conference on web search and data mining* (pp. 399–408).

Sachin, D. N., Annappa, B., & Ambesenge, Satheesh (2023). Fedrh: Federated learning based remote healthcare. In *2023 IEEE international conference on blockchain and distributed systems security* (pp. 1–7). IEEE.

Schulte, Jennifer, Engebretson, Patrick, & Spanier, Mark (2024). Artificial intelligence usage and data privacy discoveries within mhealth. *vol. 98*, In *Proceedings of 39th international conference on computers and their applications* (pp. 61–68).

Shae, Zon-Yin, & Tsai, Jeffrey J. P. (2021). On the design of medical data ecosystem for improving healthcare research and commercial incentive. In *2021 IEEE third international conference on cognitive machine intelligence* (pp. 124–131). IEEE.

Shahsavari, Yahya, Dambri, Oussama A, Baseri, Yaser, Hafid, Abdelhakim Senhaji, & Makrakis, Dimitrios (2024). Integration of federated learning and blockchain in healthcare: A tutorial. arXiv preprint arXiv:2404.10092.

Shaik, Thanveer, Tao, Xiaohui, Higgins, Niall, Li, Lin, Gururajan, Raj, Zhou, Xujuan, & Acharya, U Rajendra (2023). Remote patient monitoring using artificial intelligence: Current state, applications, and challenges. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, *13*(2), Article e1485.

Singh, Vidhi, Cheng, Susan, Kwan, Alan C., & Ebinger, Joseph (2025). United States Food and Drug Administration Regulation of Clinical Software in the Era of Artificial Intelligence and Machine Learning. *Mayo Clinic Proceedings: Digital Health*, *3*(3), Article 100231.

Song, Kaitao, Tan, Xu, Qin, Tao, Lu, Jianfeng, & Liu, Tie-Yan (2020). MPNet: masked and permuted pre-training for language understanding. In *Proceedings of the 34th international conference on neural information processing systems*. Red Hook, NY, USA: Curran Associates Inc..

Upreti, Deepak, Yang, Eunmok, Kim, Hyunil, & Seo, Changho (2024). A comprehensive survey on federated learning in the healthcare area: Concept and applications.. *CMES. Computer Modeling in Engineering & Sciences*, *140*(3).

Wang, Tongnian, Du, Yan, Gong, Yanmin, Choo, Kim-Kwang Raymond, & Guo, Yuanxiong (2023). Applications of federated learning in mobile health: scoping review. *Journal of Medical Internet Research*, *25*, Article e43006.

Wang, Wenshuo, Li, Xu, Qiu, Xiuqin, Zhang, Xiang, Brusic, Vladimir, & Zhao, Jindong (2023). A privacy preserving framework for federated learning in smart healthcare systems. *Information Processing & Management*, *60*(1), Article 103167.

Waqar, Ayaan (2024). Privacy considerations in medical technology: Role of federated learning and differential privacy in wearable devices. *International Journal of Healthcare Security and Regulations* *, Retrieved from [Link](https://Terra-Docs.S3.Us-East-2.Amazonaws.Com/IJHSR/Articles/Volume6-Issue4/IJHSR_2024_64_17.Pdf).

Yu, Chong, Shen, Shuaiqi, Wang, Shiqiang, Zhang, Kuan, & Zhao, Hai (2022). Efficient multi-layer stochastic gradient descent algorithm for federated learning in e-health. In *ICC 2022-IEEE international conference on communications* (pp. 1263–1268). IEEE.

Zhang, Daniel Yue, Kou, Ziyi, & Wang, Dong (2021). Fedsens: A federated learning approach for smart health sensing with class imbalance in resource constrained edge computing. In *IEEE INFOCOM 2021-IEEE conference on computer communications* (pp. 1–10). IEEE.

Zhao, Liutao, Xie, Haoran, Zhong, Lin, & Wang, Yujue (2024). Explainable federated learning scheme for secure healthcare data sharing. *Health Information Science and Systems*, *12*(1), 49.