

Review

Advances in Federated Learning: Applications and Challenges in Smart Building Environments and Beyond

Mohamed Rafik Aymene Berkani ¹, Ammar Chouchane ², Yassine Himeur ^{3,*}, Abdelmalik Ouamane ⁴, Sami Miniaoui ³, Shadi Atalla ³, Wathiq Mansoor ³ and Hussain Al-Ahmad ³

¹ Research Laboratory in Advanced Electronics Systems (LSEA), University Yahia Fares of Medea, Medea 26000, Algeria; berkani.aymene@univ-medea.dz

² University Center of Barika, Amdoukal Road, Barika 05001, Algeria; chouchane_ammam@yahoo.com

³ College of Engineering and Information Technology, University of Dubai, Dubai 14143, United Arab Emirates; sminiaoui@ud.ac.ae (S.M.); stalla@ud.ac.ae (S.A.); wmansoor@ud.ac.ae (W.M.); halahmad@ud.ac.ae (H.A.-A.)

⁴ Laboratory of LI3C, University of Biskra, Biskra 07000, Algeria; ouamaneabdealmaalik@univ-biskra.dz

* Correspondence: yhimeur@ud.ac.ae

Abstract: Federated Learning (FL) is a transformative decentralized approach in machine learning and deep learning, offering enhanced privacy, scalability, and data security. This review paper explores the foundational concepts, and architectural variations of FL, prominent aggregation algorithms like FedAvg, FedProx, and FedMA, and diverse innovative applications in thermal comfort optimization, energy prediction, healthcare, and anomaly detection within smart buildings. By enabling collaborative model training without centralizing sensitive data, FL ensures privacy and robust performance across heterogeneous environments. We further discuss the integration of FL with advanced technologies, including digital twins and 5G/6G networks, and demonstrate its potential to revolutionize real-time monitoring, and optimize resources. Despite these advances, FL still faces challenges, such as communication overhead, security issues, and non-IID data handling. Future research directions highlight the development of adaptive learning methods, robust privacy measures, and hybrid architectures to fully leverage FL's potential in driving innovative, secure, and efficient intelligence for the next generation of smart buildings.

Keywords: federated Learning; deep learning; machine learning; Internet of Things; smart building; anomaly detection; thermal comfort; energy prediction; healthcare; privacy-preserving



Academic Editor: Wenbing Zhao

Received: 23 January 2025

Revised: 13 March 2025

Accepted: 19 March 2025

Published: 27 March 2025

Citation: Berkani, M.R.A.; Chouchane, A.; Himeur, Y.; Ouamane, A.; Miniaoui, S.; Atalla, S.; Mansoor, W.; Al-Ahmad, H. Advances in Federated Learning: Applications and Challenges in Smart Building Environments and Beyond. *Computers* **2025**, *14*, 124. <https://doi.org/10.3390/computers14040124>

Copyright: © 2025 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Artificial intelligence (AI) is a transformative field of computer science that aims to develop intelligent systems capable of performing tasks such as decision-making, learning, reasoning, problem-solving, perception, and language processing [1,2]. These tasks often require capabilities akin to human intelligence. AI encompasses various subfields, including machine learning (ML), deep learning (DL), natural language processing, computer vision, and robotics [3,4]. ML and DL, as subsets of AI, are expected to benefit significantly from the growing availability of data and advancements in computational power, algorithms, and statistical models [5,6].

Despite these advancements, challenges persist, particularly in safeguarding data privacy. Google introduced federated learning (FL) in 2016 to address privacy concerns [7,8]. FL enables model training while preserving privacy by keeping data localized, eliminating the need to share raw data with centralized servers [7]. This paradigm significantly

enhances privacy and reduces the risk of data breaches [9]. FL has also demonstrated potential in improving efficiency, scalability, and adaptability across various applications, including smart buildings [10–12].

FL operates by training local models on decentralized devices and aggregating their parameters to create a global model. Two approaches exist: centralized FL (CFL), which uses a central server for aggregation, and decentralized FL (DFL), which relies on peer-to-peer communication [13,14]. This process not only addresses privacy concerns but also minimizes communication costs, reduces latency, and enhances model performance by leveraging diverse data from multiple sources [15,16].

The integration of FL into smart buildings is particularly promising. Smart buildings equipped with Internet of Things (IoT) devices aim to optimize resource utilization, enhance occupant comfort, and promote sustainability [17,18]. IoT devices monitor and control various building parameters, such as temperature, air quality, energy consumption, and security, enabling intelligent and responsive environments [19,20]. However, traditional centralized ML approaches in smart buildings often face challenges related to data privacy, security, and adaptability to contextual data [21–23].

Figure 1 illustrates a smart building's interconnected system of devices, seamlessly communicating through wired connections and wireless Wi-Fi networks. This integration enables harmonious interactions, such as smart thermostats working with lighting and security systems to optimize climate control and enhance safety, particularly when residents are away. The diagram categorizes devices into functional systems: thermal comfort for climate regulation, smart lighting for adjustable illumination, gas detection for air quality monitoring, smart sensors for data collection, anomaly detection for security breach identification, monitoring for real-time surveillance, network communication for connectivity and remote control, energy efficiency for appliance management, and healthcare for monitoring health data and supporting medical emergencies [14]. Together, these systems transform buildings into safer, more efficient, and higher-quality environments, leveraging automation and data analysis to improve modern living through seamless information exchange and coordinated device functionality [24].

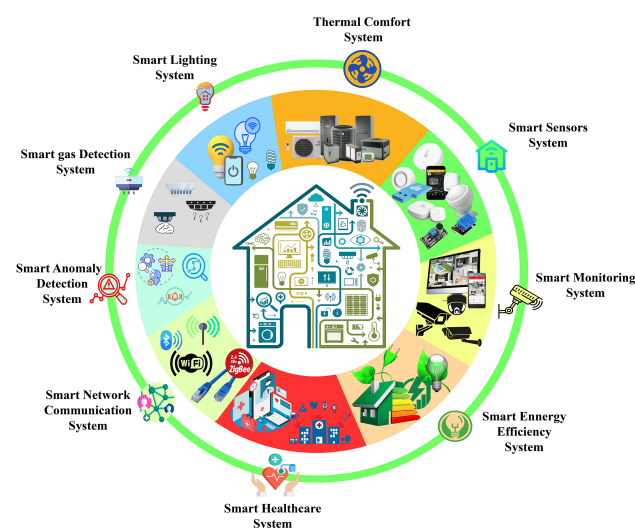


Figure 1. Smart Building and IoT.

FL offers a viable solution to the significant challenges faced in smart buildings, such as data privacy, security vulnerabilities, and data heterogeneity by enabling collaborative learning across devices without sharing raw data [25,26]. This decentralized approach enhances privacy, reduces data transfer costs, and allows for contextual learning, leading

to more accurate and efficient ML models tailored to individual building needs [27]. FL's ability to overcome data silos and integrate diverse data formats further supports its application in smart buildings [28].

1.1. Comparison with Existing FL Reviews

The proposed review article on federated learning (FL) in smart building environments introduces several novel contributions compared to existing FL surveys. While numerous studies have explored FL applications in various domains, such as smart cities [29], industrial engineering [30], intrusion detection [31], renewable energy [32], and industrial IoT [33], none have specifically focused on FL within smart building environments. This survey is the first to comprehensively analyze how FL enhances energy efficiency, thermal comfort, anomaly detection, and healthcare in smart buildings.

Existing surveys have covered FL applications in broader contexts. The study by Jiang et al. [29] focuses on FL applications in smart cities, highlighting data privacy and security issues in urban sensing. However, it does not provide insights into FL's specific role in smart buildings, leaving a gap in understanding how FL can optimize real-time monitoring and resource allocation in building environments. Similarly, Banabilah et al. [26] examine FL applications across various technology and market domains but their study lacks a dedicated discussion on its integration with smart buildings. Their survey emphasizes FL's market adoption but does not explore building-specific challenges such as energy optimization or thermal comfort.

Nguyen et al. [16] discuss FL for IoT services and applications, covering topics such as IoT data sharing and attack detection. While their work acknowledges the importance of FL for IoT-driven environments, it primarily focuses on general IoT frameworks without addressing the specific needs of smart buildings. In contrast, our review extends beyond general IoT applications to discuss building-specific FL implementations, such as anomaly detection and healthcare integration.

Li et al. [30] provide an overview of FL in industrial engineering, touching on energy systems and fault detection. However, their study does not extensively cover privacy concerns, security mechanisms, or digital twin integration in FL-based smart buildings. Similarly, Belenguer et al. [31] focus on FL for intrusion detection, providing valuable insights into cybersecurity applications. However, their work is limited to threat detection, without exploring broader FL applications in smart building environments.

Another relevant study is the study by Grataloup et al. [32], which examines FL applications in renewable energy, specifically focusing on energy efficiency and privacy-preserving techniques. However, while their review discusses smart grid optimization, it does not explore other critical smart building applications such as healthcare, thermal comfort, or real-time anomaly detection. Qian et al. [34] investigate FL for fault diagnosis in mechanical systems, addressing predictive maintenance and security in industrial settings. However, their study remains centered on machinery fault diagnosis, lacking a broader discussion of FL's role in smart buildings.

Vahabi et al. [33] analyze FL and edge computing in Industrial IoT (IIoT), emphasizing real-time monitoring and resource optimization. While their study shares some similarities with ours in terms of performance optimization, it primarily focuses on edge computing challenges rather than offering a comprehensive discussion of FL's role in smart building environments.

Our proposed review is the first dedicated study on FL in smart buildings, providing a structured discussion on privacy-preserving techniques, federated aggregation methods, and the challenges associated with FL deployment in smart buildings. It explores the integration of FL with digital twins and 5G/6G networks, optimizing real-time monitoring

and energy management. Moreover, our review highlights unique challenges such as data heterogeneity, communication overhead, security threats, and non-IID data issues, which have not been addressed comprehensively in prior works. Future research directions, including hybrid FL architectures and adaptive learning methods tailored for smart building environments, are also discussed, making this survey a foundational reference for advancing FL applications in smart buildings. Table 1 presents a comparative summary of our review with existing surveys.

Table 1. Comparison of the Proposed FL Review with Existing Surveys.

FL Review Study	Main Focus	Distinct Contributions of the Proposed FL Review	Limitations
[29]	FL for Smart Cities	First survey focused exclusively on FL for smart building environments.	Does not cover FL's role in smart building-specific applications.
[26]	FL applications across technology and market domains	Highlights FL integration with digital twins and 5G/6G for smart buildings.	Lacks in-depth discussion on FL's application in smart buildings.
[16]	FL for IoT services and applications	Focuses on smart buildings as a distinct application area rather than general IoT.	Primarily focuses on IoT without detailed coverage of smart building environments.
[30]	FL in Industrial Engineering	Explores smart building-specific challenges, such as thermal comfort and energy prediction.	Does not extensively discuss privacy, security, or digital twin integration.
[31]	FL for Intrusion Detection Systems	Discusses anomaly detection in smart buildings using FL.	Limited to intrusion detection without exploring broader smart building applications.
[32]	FL for Renewable Energy Applications	Covers smart building energy efficiency and privacy-preserving techniques.	Focuses only on energy applications, neglecting other smart building use cases.
[34]	FL for Fault Diagnosis in Mechanical Systems	Addresses smart building applications like predictive maintenance and security.	Primarily centered on fault diagnosis, lacking a broader discussion of FL applications in smart buildings.
[33]	FL and Edge Computing in Industrial IoT	Examines FL's role in real-time smart building monitoring and resource optimization.	Emphasizes edge computing but does not comprehensively cover smart building environments.
Our	FL in Smart Building Environments	First review dedicated to FL in smart buildings, covering thermal comfort, energy prediction, healthcare, and anomaly detection. Discusses FL's integration with digital twins and 5G/6G networks. Analyzes open challenges and future directions for FL in next-generation smart buildings.	Some cases explaining the implementation of FL in smart building environments are missing.

1.2. Paper's Contributions

This survey aims to provide a comprehensive review of FL in the context of smart buildings. Specifically, we discuss the current state of FL, its applications, and its significance in enhancing building automation, energy management, air quality monitoring, security, and maintenance optimization.

The main contributions of this survey are summarized as follows:

- The concept of FL and its relevance to smart buildings is explored.
- FL applications across various smart building domains, such as energy management, air quality, gas detection, healthcare monitoring, and maintenance optimization, are analyzed.
- Real-world smart building projects employing FL to enhance performance and efficiency are examined.
- Challenges and open issues in implementing FL for smart buildings are identified, and potential future research directions are outlined.

The remainder of the paper is organized and structured as follows: Section 2 presents a comprehensive overview of FL, encompassing its fundamental principles, architectural frameworks, and key protocols. Section 3 explores the real-world applications and implementations of FL in smart building environments, analyzing various use cases and their respective performance metrics. Section 4 critically evaluates the existing challenges in FL deployment and explores promising future research directions. Section 5 synthesizes the key findings and presents concluding remarks, along with implications for future research in this field.

2. Federated Learning

2.1. Federated Learning Concept

The artificial intelligence (AI) community faces significant challenges in acquiring, combining, and utilizing data from disparate sources due to strict privacy regulations, such as the General Data Protection Regulation (GDPR) [35]. To address these challenges, Google introduced federated learning (FL) in 2016, a groundbreaking and advanced technology [36,37]. FL has rapidly emerged as a compelling alternative to centralized systems, enabling the training of high-quality machine learning (ML) and deep learning (DL) models on decentralized datasets [38].

FL is a privacy-preserving decentralized learning technique that facilitates model training on local data without transferring it to a central server. Instead, only the updated model parameters are shared with a central server, ensuring data privacy [39]. This approach allows multiple devices, such as smartphones, wearable devices, and smart sensors, to collaboratively train models while keeping their data private. The central server aggregates the locally trained models, typically by averaging the received model parameters, to create a global model. The updated global model is then distributed back to each client to refine their local models. FL promotes faster, more efficient, and more accurate model development while upholding stringent privacy standards [38,40,41].

In smart building environments, FL can be applied to various domains, including smart lighting, energy efficiency, gas detection, healthcare, thermal comfort, anomaly detection, and camera monitoring [42,43]. Figure 2 illustrates FL's applications in smart buildings, showcasing its potential to enhance functionality and operational efficiency. Moreover, Figure 3 presents a comprehensive taxonomy of FL models based on several aspects.

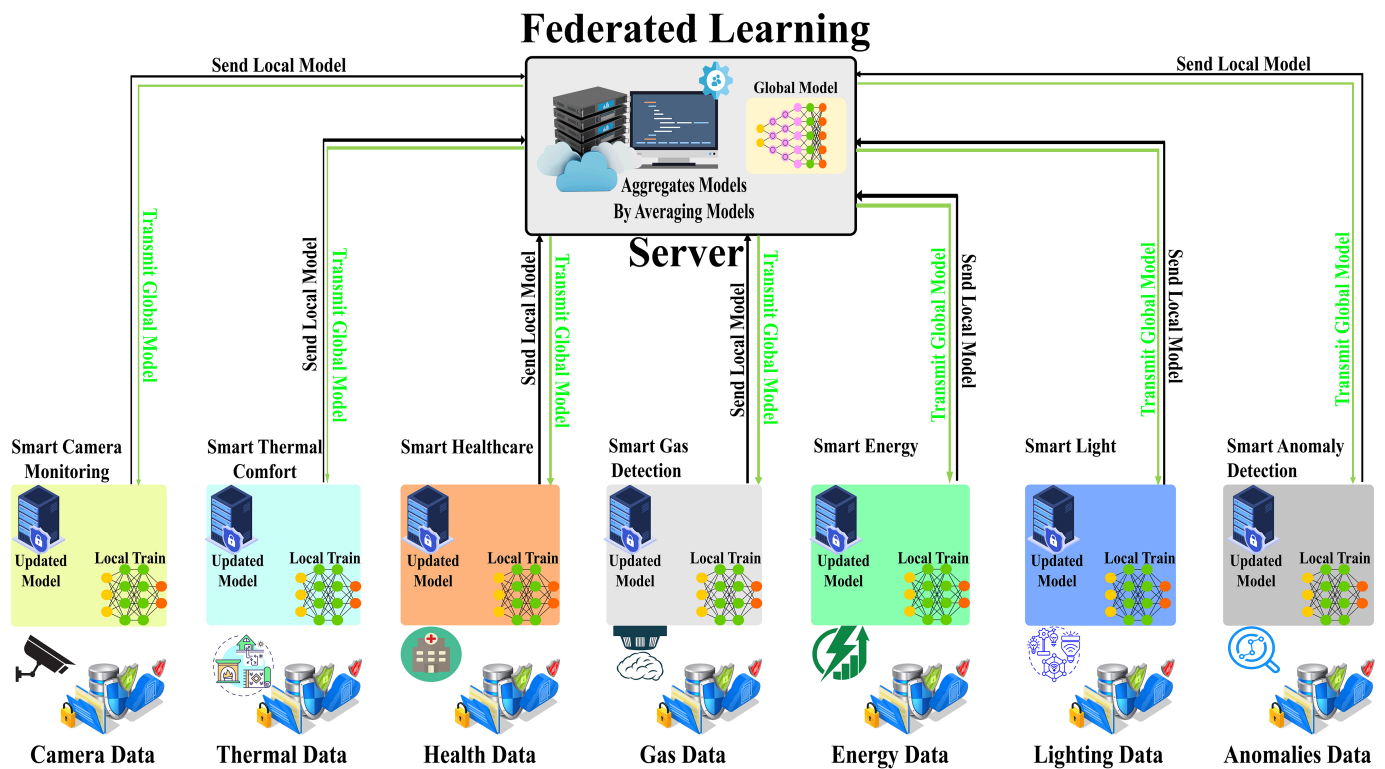


Figure 2. Federated Learning for Smart Building Applications.

2.2. Decentralized Data

Unlike traditional centralized approaches, FL keeps data distributed across individual devices or servers, addressing privacy and security concerns [44–46]. This decentralized approach enables models to train on sensitive localized data without direct sharing, thereby reducing the risks associated with data centralization [47]. The privacy-preserving nature of FL also minimizes communication overhead and allows secure and efficient model training and aggregation without direct access to the data, meeting privacy and security requirements [48].

2.3. Training Process

2.3.1. Data Preprocessing

Data preprocessing is a critical step in developing AI models, particularly in FL [49]. Real-world data, typically collected from diverse sources, often contain noise, missing values, and inconsistencies that must be addressed before analysis. Preprocessing tasks include transforming raw data into a refined format suitable for AI models through techniques such as:

- Data cleaning, integration, and reduction.
- Data transformation, feature extraction, and normalization.
- Specialized methods such as envelope detection, filtering, and sequence alignment [50–52].

These techniques improve data quality, enabling more accurate and efficient model training.

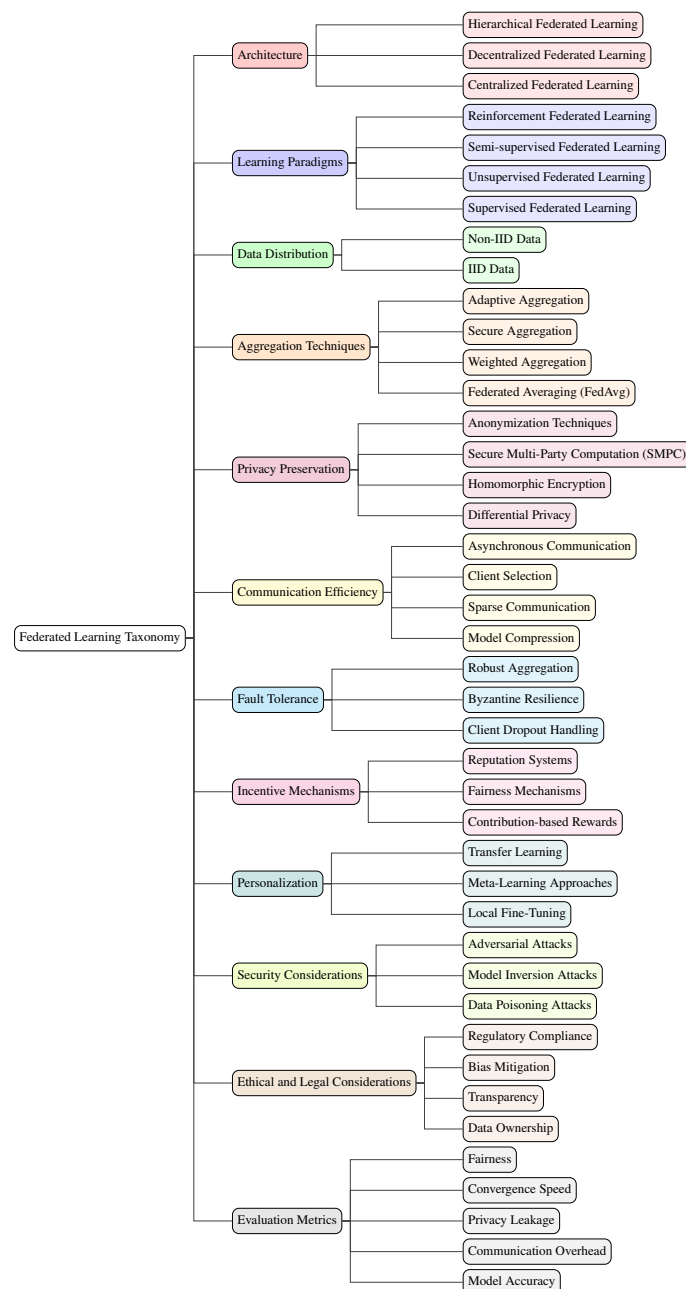


Figure 3. Taxonomy of Federated Learning in Smart Buildings [14].

2.3.2. Model Initialization

In FL protocols, the central server is responsible for initializing the model parameters or weights before commencing decentralized training across clients [53]. These initial weights are crucial for stabilizing optimization trajectories and ensuring efficient convergence of robust local models. Once initialized, the central server broadcasts the local models with initial weights to all clients, initiating the federated training process. Each client performs local training on its private data, and the resulting weight updates are iteratively aggregated by the server to enhance the global model [44,54,55].

2.3.3. Local Training

After initializing the initial model weights, denoted as W_G^0 , the central server distributes the local models to clients for decentralized training using their respective local

datasets. Each client, denoted as k , performs optimization on its private dataset D_k to compute updated weights W_k^* by minimizing the local loss function $F(W_k)$:

$$W_k^* = \arg \min F(W_k) \quad (1)$$

The specific form of the loss function depends on the FL algorithm employed. For example, in a federated linear regression model with input–output pairs $\{x_i, y_i\}$ for $i = 1 : k$, the loss function is expressed as:

$$F(W_k) = \frac{1}{2} (x_i^T W_k - y_i)^2 \quad (2)$$

After local optimization, client k uploads the updated model parameters to the central server. These parameters are aggregated to improve the global model, which is then redistributed to the clients for the next round of local training [16,54].

2.3.4. Model Aggregation

Model aggregation is a critical component of FL, consolidating parameters from clients during each communication round to create an updated global model. This process ensures privacy preservation by aggregating model parameters instead of raw data, thereby addressing privacy and security concerns.

Aggregation enables effective global model training while avoiding direct data transmission during the training process. Communication-efficient techniques and incentive mechanisms encourage widespread participation of devices, optimizing parameter exchange and model performance [56,57].

In addition to parameter aggregation, techniques such as fine-tuning, multi-task learning, and knowledge extraction enhance the performance of federated models while maintaining privacy and model integrity [57]. These approaches provide superior accuracy compared to standalone local models.

The most widely used aggregation technique is iterative model averaging, initially developed by McMahan et al. [47]. This method aggregates local models during each communication round to update the global model. Over time, this foundational strategy has inspired several advanced aggregation techniques, such as the **private aggregation of teacher ensembles (PATE)**. PATE aggregates knowledge from multiple teacher models into a student model while ensuring robust privacy guarantees for training data [57].

Further innovations include Bayesian nonparametric frameworks, which align neurons from local models to construct a coherent global model. These probabilistic methods improve adaptability to heterogeneous data distributions [58].

Another significant advancement is the integration of FL with multitask learning, enabling local models to be trained for various tasks simultaneously. This approach fosters more adaptable and efficient learning paradigms [59]. Additionally, the convergence of FL with blockchain technologies enhances secure model exchanges and weight updates across distributed devices. Blockchain-based FL ensures secure aggregation while facilitating transparent and verifiable updates in decentralized environments [60,61].

Model aggregation techniques in FL can be broadly categorized into two types:

- **Parameter-Based Aggregation**: Consolidates trainable parameters, such as weights and gradients, from local models.
- **Output-Based Aggregation**: Combines model outputs, such as logits or compressed representations. An example is **FedMask**, which aggregates binary masks on the server side to reduce communication and computational overhead [54,62].

Each aggregation method offers unique benefits, including improved communication efficiency, enhanced privacy preservation, and higher model performance, catering to various FL system requirements.

Aggregation can also follow two architectural forms:

- **Centralized Aggregation**: Performed by a central server.
- **Decentralized Aggregation**: Achieved through peer-to-peer communication [59].

The global weighted loss function, denoted as L_{wt}^G , aggregates the weighted losses from all clients' datasets and is computed as:

$$L_{wt}^G = \frac{1}{N} \sum_{i=1}^N L_{wt_i} \quad (3)$$

where:

- N : The total number of samples across all clients.
- L_{wt_i} : The weighted loss for the i -th sample.

Equation (3) provides a comprehensive metric for evaluating the global model's performance. The global weighted loss function serves as a critical tool for optimizing and assessing the overall effectiveness of the federated learning system.

3. Advanced Strategies for Federated Model Aggregation

In this analysis, we introduce recent advanced strategies for model aggregation that play a critical role in optimizing the performance of the global model in heterogeneous and non-IID (non-independent and identically distributed) data environments. These innovative approaches address challenges inherent in FL paradigms, including communication overhead and privacy preservation. Below, we outline several key algorithms that form the foundation of federated model aggregation, each offering unique solutions to the complexities of distributed learning scenarios:

- **FedAvg**: Federated averaging (FedAvg), proposed by McMahan et al. in 2017 [47], is one of the earliest and most widely adopted FL algorithms. It aggregates client parameters by weighting and averaging them based on the proportion of data each client contributes. The FL process begins with the server sharing a global model with a subset of clients. These clients perform local training using their private data and send updated model parameters to the server. The server then aggregates these updates using a weighted average:

$$w_{\text{global}}(t) = \sum_{i=1}^K \frac{n_i}{n} \cdot w_{\text{local}_i}(t) \quad (4)$$

where $w_{\text{global}}(t)$ represents the global model at round t , $w_{\text{local}_i}(t)$ denotes the local model update from client i , n_i is the number of data samples on client i , and n signifies the total number of data samples across all clients.

FedAvg allows clients to perform local computations while the server orchestrates global learning, ensuring data privacy, reducing communication costs, and enhancing performance on decentralized datasets.

- **FedProx**: Federated proximal (FedProx), introduced by Li et al. in 2020 [63], extends FedAvg by incorporating a proximal regularization term in the optimization objective. This term pulls local updates closer to the global model, addressing the challenges posed by heterogeneous data distributions. The global model update is defined as:

$$w_{\text{global}}(t) = \arg \min_w \left(\frac{\sum_{i=1}^K n_i L(w_{\text{local}_i}(t))}{n} + \frac{\mu}{2} \|w - w_{\text{global}}(t-1)\|^2 \right) \quad (5)$$

where μ is a regularization parameter controlling the influence of the proximal term. This approach improves convergence in settings where local updates diverge due to data or resource heterogeneity.

- **FedNova:** Federated novel averaging (FedNova), developed by Qi et al. in 2023 [54], enhances FedAvg by addressing statistical heterogeneity and variability in local optimization steps. FedNova normalizes local updates during aggregation to balance contributions from clients executing different numbers of local updates. The aggregation is defined as:

$$w_{\text{global}}(t) = \arg \min_w \left(\frac{\sum_i n_i \cdot L(w_{\text{local}_i}(t))}{\sum_i n_i} + \frac{\lambda}{2} \|w - w_{\text{global}}(t-1)\|^2 \right) \quad (6)$$

FedNova introduces lightweight modifications to FedAvg, incurring negligible overhead while improving accuracy and robustness in non-IID environments.

- **Scaffold:** The Scaffold algorithm, proposed by Karimireddy et al. [64], addresses client drift caused by data heterogeneity using control variates. These variates correct local updates by adjusting them toward the server's gradient direction, improving stability under non-IID conditions. While Scaffold introduces additional communication overhead, it significantly enhances performance in complex FL scenarios.
- **MOON:** MOON (Model-contrastive federated learning) mitigates model drift by aligning feature representations between global and local models while encouraging divergence from previous local models. This dual regularization approach reduces overfitting and improves performance on non-IID data [54,65].
- **Zeno:** Zeno is a Byzantine-resilient algorithm designed to handle malicious or faulty client updates. It evaluates client contributions using a stochastic oracle that scores updates based on their impact on the global loss function. High-scoring updates are prioritized for aggregation, enhancing robustness against adversarial attacks [54,66].
- **FedMA:** Federated matching and aggregation (FedMA), proposed by Wang et al. in 2020 [67], is a unified model aggregation algorithm designed for both CNN and LSTM models in federated learning (FL). FedMA performs aggregation on the central server by matching and averaging hidden elements, such as neurons and channels, within the neural architecture. Experimental results show that FedMA is particularly effective in heterogeneous and diverse client environments, outperforming algorithms like FedAvg and FedProx across multiple training rounds [67,68]. The core innovation of FedMA lies in its parameter-matching paradigm, which addresses the challenge of permutation invariance in federated models. In this approach, $w_{j,l}$ represents the l^{th} neuron derived from dataset j and connected to the primary weight matrix $W^{(1)}\Pi_j$, while θ_i denotes the i^{th} neuron in the global model. The similarity between individual neurons is quantitatively assessed using a similarity function, $c(\cdot, \cdot)$. The optimization problem in FedMA is formulated as:

$$\min_{\{\pi_j^l\}} \sum_{i=1}^L \sum_{j,l} \min_{\theta_i} \pi_j^l c(w_{j,l}, \theta_i) \text{ s.t. } \sum_i \pi_j^l = 1 \quad \forall j, l; \sum_l \pi_j^l = 1 \quad \forall i, j. \quad (7)$$

By appropriately defining $c(\cdot, \cdot)$ and solving this optimization problem, FedMA effectively aggregates permuted federated models, ensuring robust performance in diverse data settings.

- Per-FedAvg:** Personalized federated averaging (Per-FedAvg), proposed by Fallah et al. in 2020 [69], combines model-agnostic meta-learning (MAML) with FL to create personalized local models for each client. MAML is utilized to train a global model that can be fine-tuned on a small subset of each client's private data, enabling improved model adaptation and performance [69,70]. Per-FedAvg is explicitly designed for personalized FL (PFL), addressing the unique challenges of personalization. It begins by computing the gradient of each client's local function, defined as the average of meta-functions, where each meta-function evaluates the loss function on the client's data. The global model is then sent to a subset of clients, who perform local SGD iterations to personalize the model using their data. These personalized updates are returned to the server, which averages them to update the global model. This iterative process continues until convergence [69]. Empirical evaluations demonstrate the effectiveness of Per-FedAvg in achieving accurate personalized models in FL. It consistently outperforms other PFL algorithms in terms of both accuracy and client-specific adaptation [69].

Additionally, comparative analysis of the aggregation methods is illustrated in Table 2 and other aggregation methods and their applications are summarized in Figure 3. Moving forward, after collecting the local updated model parameters or weights w_{local_i} from the local clients, the server aggregates them to create a new version of the global model w_{global} using the aggregation method described in the model aggregation section.

Table 2. Comparative analysis of FL aggregation methods.

Aggregation Method	Handling Non-IID Data	Convergence Speed	Communication Overhead	Privacy	Model Robustness	Scalability	Accuracy	Applicability
FedAvg	Weak	Fast	Moderate	Standard	Moderate	High	Moderate	Suitable for energy management and anomaly detection where data is relatively homogeneous across buildings.
FedProx	Strong	Moderate	Moderate	Standard	Strong	High	High	Ideal for occupancy detection and thermal comfort optimization where sensor data varies across buildings.
FedNova	Strong	Moderate	Low	Standard	Moderate	Moderate	Moderate	Suitable for decentralized control systems and predictive maintenance in smart buildings.
Scaffold	Strong	Slow	High	Standard	Strong	Low	High	Useful for scenarios where sensor data distribution changes frequently, such as adaptive lighting and air quality monitoring.
MOON	Strong	Fast	High	Improved	Strong	High	High	Applicable for personalized user comfort models in smart buildings.
Zeno	Strong	Moderate	Moderate	Robust	Very Strong	Moderate	High	Suitable for security-sensitive applications, such as intrusion detection and anomaly detection in HVAC systems, where some clients might provide unreliable or malicious updates.
FedMA	Strong	Slow	High	Standard	Very Strong	Low	Very High	Effective for deep learning applications such as HVAC fault detection and smart security monitoring.
Per-FedAvg	Very Strong	Moderate	Moderate	Strong	Strong	High	Very High	Ideal for smart home automation and personalized thermal comfort control, where different buildings or rooms may have distinct environmental conditions and preferences.

3.1. Global Model

In FL, the global model serves as the central model that integrates updates from multiple local models trained across distributed client devices [71]. Unlike traditional centralized ML, where data is collected and processed on a central server, FL allows each

client to train a local model on its private data. This approach preserves data privacy and significantly reduces data transfer overhead.

During the FL process, clients train their local models and send only the model updates (e.g., weights or gradients) to the central server. The server aggregates these updates to improve the global model, which is then periodically shared back with clients to incorporate the latest aggregated knowledge into subsequent local training rounds. This iterative process continues until the global model achieves the desired level of performance or convergence [72,73].

The global model plays a crucial role in FL by encapsulating the collective learning from all participating clients while ensuring the privacy of individual client data.

3.2. Types of Federated Learning

3.2.1. Horizontal Federated Learning

Horizontal federated learning (HFL), also referred to as sample-based FL, involves collaborative training among clients with datasets that share the same feature space but differ in sample space. As illustrated in Figure 4a, clients collectively train a global FL model using their local datasets, which have identical features but vary in content due to differing samples [36,54].

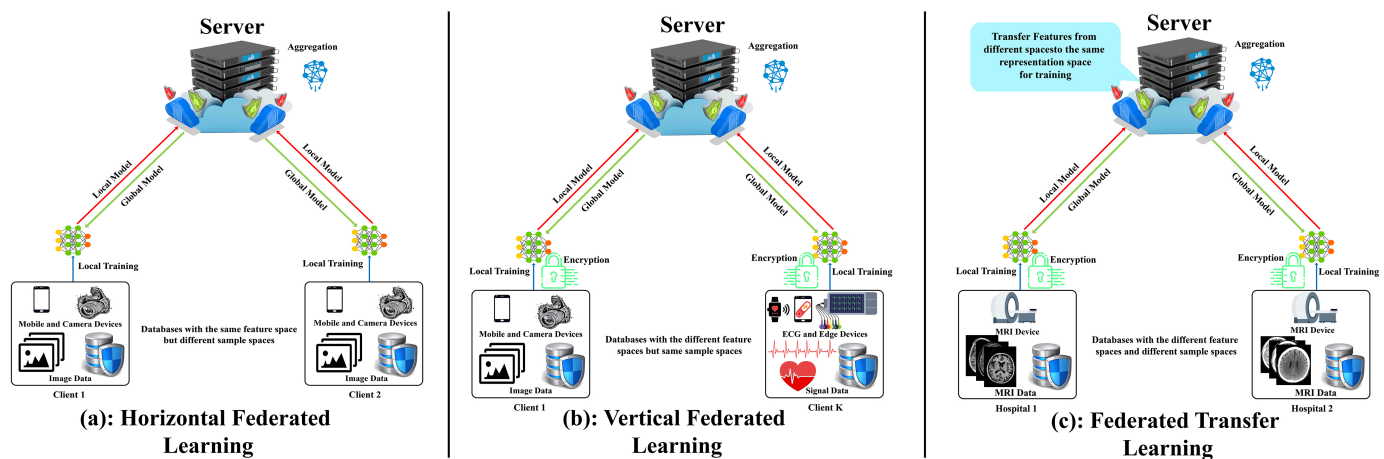


Figure 4. Types of Federated Learning.

For example, in an FL study on heart disease detection, electrocardiogram (ECG) signals were used as training data. These signals, collected from patients of different ages and genders, shared consistent feature attributes such as waveform characteristics. Local models can employ various AI techniques, including linear regression, support vector machines (SVMs), long short-term memory (LSTM), and convolutional neural networks (CNNs). To enhance security, local updates are often obfuscated using encryption or differential privacy techniques.

Once local models are trained, the server aggregates the updates into a global model, which is then redistributed to clients for predictive use. This approach ensures privacy, leverages distributed datasets, and enhances the efficiency of collaborative learning [16,54].

3.2.2. Vertical Federated Learning

Vertical federated learning (VFL), also known as feature-based FL, focuses on training models using datasets that share the same sample space but have different feature spaces, as depicted in Figure 4b. This method enables data owners to maintain control over their sensitive data while benefiting from collaborative training [36].

In VFL, datasets originate from the same objects, sensors, or devices but contain distinct types of features extracted from diverse sources, such as signals or images. An alignment mechanism is developed to identify overlapping data samples across clients, which are then aggregated to train a generalized FL model. Encryption techniques ensure privacy and security during this process [54,68].

For instance, in smart building IoT applications, entities with shared sample spaces but unique feature sets can collaborate through VFL to train local models for tasks like optimizing thermal comfort, detecting gas leaks, and identifying anomalies. This approach ensures privacy while enabling effective model training [16].

3.2.3. Federated Transfer Learning

Federated transfer learning (FTL), as shown in Figure 4c, expands the sample space within the VFL framework by enabling global model training using datasets from diverse clients without revealing sensitive information. FTL transforms distinct feature spaces into a unified representation for aggregating multi-client data, ensuring privacy and security [54,68].

FTL involves transferring features across disparate feature spaces into a common representation, which is then used to train a global model. During this process, local models are trained on private datasets, and the server aggregates these models to construct a robust global model by minimizing a loss function. This technique is particularly beneficial in IoT networks and healthcare applications [36,57].

For example, in healthcare, FTL enables collaboration among hospitals and countries with distinct patient datasets (sample spaces) and medical test results (feature spaces). By leveraging collective knowledge, FTL enhances diagnostic accuracy while preserving data privacy, significantly benefiting patient care and research.

FTL is a powerful approach that facilitates collaboration across disparate data sources while ensuring privacy and security. It improves model accuracy and supports applications in healthcare and other domains, particularly for tasks like disease diagnosis.

3.3. Architecture of the Federated Learning Network

From the networking perspective, depending on the network topology, FL can be divided into two categories: centralized FL and decentralized FL.

3.3.1. Centralized Federated Learning

Centralized FL (CFL) is the most prevalent FL architecture adopted in IoT systems. As depicted in Figure 5a, a CFL system comprises a central server and multiple clients that perform and execute the FL model. During the training phase, clients engage in the training of a local model utilizing their respective datasets [74,75]. Subsequently, they then transmit and share these local models to the central server, which aggregates them using aggregation methods such as FedAvg, FedProx, and FedNova, and disseminates the aggregated global model back to clients. In CFL, the server assumes the role of a pivotal network component, as it orchestrates the entire process of aggregating model updates and sharing the global model. This architecture facilitates collaborative training on decentralized data for tasks like anomaly detection while preserving client data privacy and security [16,59].

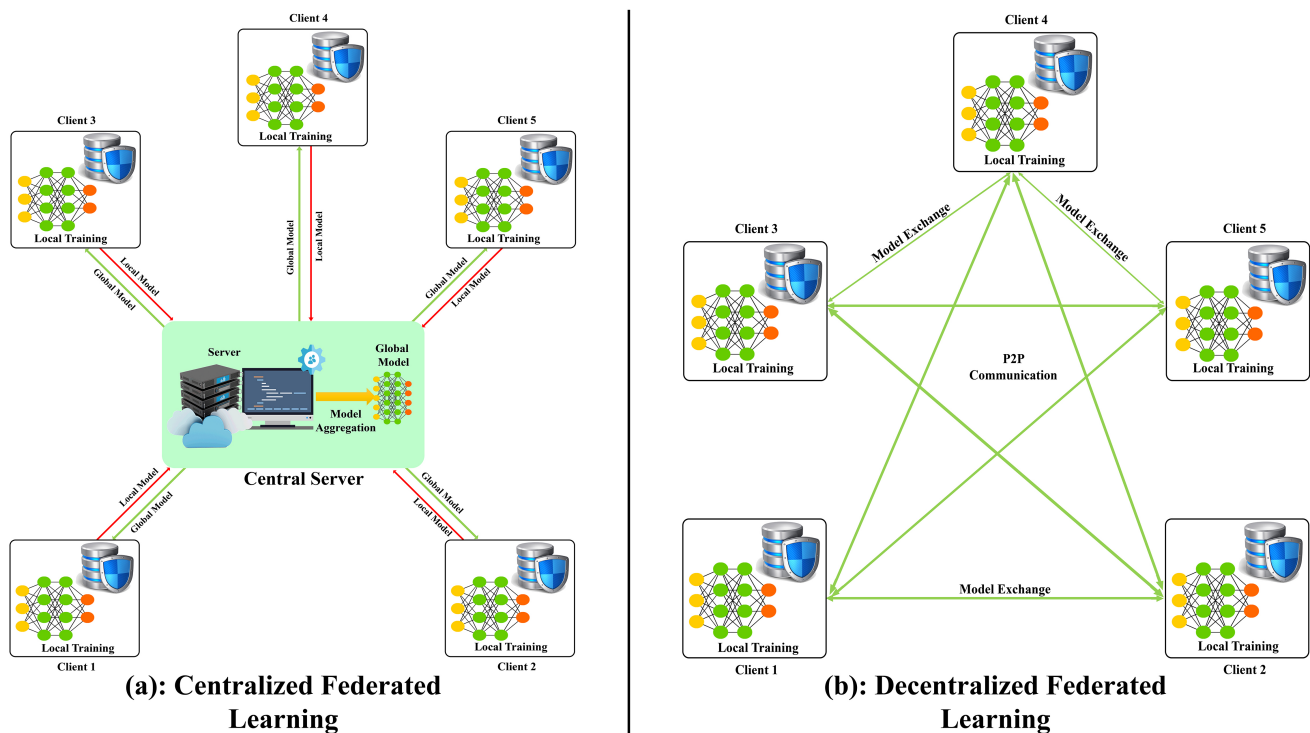


Figure 5. Network Structure of Federated Learning.

3.3.2. Decentralized Federated Learning

Decentralized FL (DFL) is a network topology that abandons the requirement for a central server to coordinate the training process, opting for a peer-to-peer (P2P) network topology where all clients are interconnected, as illustrated in Figure 5b. During each communication phase, clients engage in local training utilizing their respective datasets [16,76]. Subsequently, each client implements model aggregation using the local model updates received from neighboring clients via P2P communication, to achieve a globally aggregated model. DFL is designed to fully (completely) or partially replace central server-based FL (CFL) when communication with the central server is unavailable or when the network topology exhibits high scalability. Due to its contemporary features, DFL can be seamlessly integrated with P2P-based communication technologies such as blockchains to construct DFL systems. DFL clients can communicate through blockchain ledgers, where local model updates are offloaded for secure model exchange and aggregation [16,75].

3.4. Overview of Federated Learning Attacks

FL, due to its inherently distributed client participation, is exposed to a range of adversarial threats that target both the global model's integrity and the confidentiality of local data [77,78]. In particular, poisoning attacks involve injecting malicious data or gradient updates to degrade performance or embed backdoors in the global model [77,78], while inference attacks such as model inversion or membership inference analyze shared gradients or parameters to extract sensitive information about local training data [79,80]. Several studies have investigated how an adversary, serving as a legitimate client, can affect updates that survive the averaging procedure, thus overriding or biasing the global model.

C. Fung et al. [77] presented a defense method against Sybil-based adversarial attacks by comparing the similarity of user contributions during model averaging and filtering out the attacker's updates. Interestingly, some modifications to FedAvg such as FedProx or SCAFFOLD, which reduce the effect of individual client's updates, can incidentally mitigate these threats [81]. However, these methods alone may be insufficient, especially

against more sophisticated backdoor or byzantine attacks [82], as well as inference-based exploits. As a result, additional adversarial defenses, such as robust aggregation protocols, Byzantine-resilient algorithms, anomaly detection, and privacy-preserving techniques like differential privacy and homomorphic encryption are often employed to ensure that FL systems maintain both robust model performance and data confidentiality [83,84].

3.5. Privacy-Preserving Techniques in Federated Learning

In this section, we focus on methods such as differential privacy, cryptographic protocols, and blockchain-based frameworks—that chiefly counter inference attacks including model inversion or membership inference [81]. While these techniques can prevent adversaries from seeking to extract raw data from shared gradients or parameters, they offer limited protection against integrity-focused attacks like data poisoning or Byzantine faults. Consequently, robust aggregation and anomaly detection mechanisms remain critical for comprehensive FL security.

FL is a safe collaborative training approach for ML/DL models that ensures data privacy by keeping the local data unexposed to other users [80,85,86]. It involves exchanging model parameters between users while maintaining the confidentiality of individual data points. Although FL offers enhanced safety, the exchange of model parameters may still leak sensitive information about user data, making it vulnerable to many potential attacks that can occur against ML/DL models, including model inversion and membership inference attacks, which aim to extract raw data from shared models [10,79,84,87]. The importance of such measures is further emphasized by legal regulations such as the General Data Protection Regulation (GDPR) in the European Union [88], which guarantees the protection of personal data privacy. To mitigate these threats, privacy-preserving techniques, including differential privacy and k-anonymity, have been developed to provide different privacy guarantees. These techniques can be categorized into three main groups: cryptographic methods, differential privacy methods, and blockchain techniques, which enable a decentralized trust mechanism to leverage cryptographic consensus algorithms and immutable ledger structures to ensure tamper-resistant transaction records for enhancing security, data integrity, and fault tolerance in distributed systems.

3.5.1. Differential Privacy Method

Differential privacy (DP) techniques provide a principled and mathematically rigorous framework to measure the level of privacy afforded by a privacy-preserving mechanism. These techniques are based on probabilistic statistical models that quantify the degree of disclosure of private information about individual data instances [84]. Differential privacy techniques can be broadly categorized into two main approaches:

- **Global Differential Privacy Technique:** This technique aims to ensure that the effect of substituting an arbitrary sample in the dataset is sufficiently small, such that the query results cannot be utilized to explore more information about any specific samples in the data [89]. A key advantage of these methods is their greater accuracy compared to local differential privacy techniques, as they do not require the addition of a large amount of noise to the dataset [90].
- **Local Differential Privacy Technique:** Introduced to eliminate the requirement of the central trusted authority inherent (demanded) in global differential privacy [91–93]. Local differential privacy does not require a trusted third-party; however, a trade-off of this approach is that the total amount of noise required is substantially greater than that in a global differential privacy technique [90,91].

Differential privacy [89,94,95] guarantees that a single record does not significantly influence the output decision of the FL system, thereby obfuscating the ability to decrypt

the individual records from the decision. Several studies have proposed incorporating differential privacy FL to ensure that users do not gain knowledge about whether a specific individual's record is utilized in the learning process [96–98]. This is usually achieved by introducing random noise to the data or model weights [97,99], thus obfuscating and protecting individual records against inference model attacks, albeit at the potential cost of reduced accuracy in the generated results. To enhance confidentiality guarantees and improve performance, FL systems can adopt combinations of multiple differential privacy methods with other techniques, such as a trusted execution environment (TEE) or Intel SGX improving more security and mitigates information leakage risks [100,101]. At the same time, integration of TEEs introduces inherent hardware dependencies and potential exposure to side-channel attacks, necessitating robust supplementary security measures such as secure memory encryption and periodic attestation protocols to enhance system security and resilience.

Table 3 provides a summary of the privacy level and the distinct attack types of existing FL techniques that may occur at different stages of the learning process.

Table 3. Privacy level and Attack types in the FL system.

Level	Attacks Type	Description
Inputs [102,103]	Data Poisoning	Malicious alteration of training data labels to degrade model performance on specific classes
Learning Process [82,104,105]	Model Poisoning	Uploading of specific model parameters to decrease global model's accuracy.
	Byzantine Fault	Participant-behaving uploading of random updates.
The learned Model [85,86]	Inference Attacks	Server inferring sensitive data from exchanged model parameters during learning process.
		Membership inference attacks to identify training data usage.

3.5.2. Cryptographic Technique

Cryptographic techniques are widely employed in privacy-preserving ML/DL algorithms and primarily include homomorphic encryption, secret sharing, and secure multi-party computation (SMC). In these techniques, users must encrypt their data (messages) before transmission, perform operations on the encrypted data (messages), which are converted into a secret code, and decrypt the output to obtain the final result during communications [106,107]. Applying these methods to FL systems (FLSs) can significantly increase the level of protection. However, SMC does not provide perfect privacy guarantees for the final model, which remains vulnerable to inference attacks and model inversion attacks [84,107]. Due to the additional encryption and decryption operations, substantial computational overhead is imposed on such systems. For instance, SMC ensures that parties cannot learn anything except the output, facilitating the secure aggregation of transferred gradients. Furthermore, these methods can impose a significant computational burden on FLSs, depending on the employed cryptographic method [10,84,108].

Homomorphic encryption significantly enhances security and supports the decentralized nature of FL by enabling encrypted computations at the client level without decryption, enhancing data privacy and security. However, its practical implementation introduces challenges such as increased computational overhead, energy consumption for resource-constrained devices, scalability issues for large numbers of clients, and potential metadata

privacy leaks. Effective key management and governance mechanisms are crucial. For FL with varying computational capacities, new optimized homomorphic encryption algorithms are needed to balance privacy, accuracy, and computational efficiency across different ML models while considering scalability and resource constraints [109]. Additionally, advanced research in fully homomorphic encryption (FHE) aims to mitigate the high computational costs by reducing key sizes and improving encryption efficiency, thereby facilitating its deployment in real time FL applications.

3.5.3. Blockchain

Blockchain technology has several strengths and limitations when integrated into FLs. Its decentralized architecture, cryptographic algorithms, and immutability features enhance data privacy, security, and transparency. The transparency of blockchain allows all users to be visible in model updates, facilitating collaboration and trust. Smart contracts enable the automation of data usage policies. However, the blockchain does not provide complete privacy protection, and its transparency may expose sensitive information, necessitating additional privacy enhancement methods [110,111]. Its process in FL-chain systems requires significant computational resources, potentially impacting training speed, efficiency, and scalability. Moreover, maintaining the blockchain consumes substantial energy. Blockchain networks often face scalability limitations, slowing processing times as the number of participants increases. Integrating blockchains into FLs is complex, requiring the development of smart contracts, consensus mechanisms, and compatibility with existing FL protocols, increasing development time and budget [110,112,113]. From a governance perspective, reaching a consensus on system updates, protocol changes, or policy modifications may require extensive coordination among participants, potentially slowing decision-making processes. Using blockchains in FL healthcare systems involves trade-offs between decentralization and scalability, transparency and privacy, security and efficiency, implementation complexity, and governance control. These trade-offs must be carefully considered when designing an FL-chain healthcare system [110,112,113].

4. Real-World Applications of Federated Learning in Smart Building

FL is a DL/ML techniques that enables local training of FL models on decentralized datasets, without sharing the data or centralizing the data keeping it private on IoT devices. This makes FL a powerful tool for privacy preservation and reducing communication costs, with a wide range of real-world applications including the following:

4.1. Federated Learning-Based Anomaly Detection

The proliferation of IoT sensors in smart buildings has enhanced comfort, eco-friendliness, and sustainability. These sensors generate complex, time-based data crucial for identifying anomalies and improving energy forecasting. Traditional centralized anomaly detection systems often suffer from long response times, necessitating the adoption of FL frameworks. FL enables anomaly detection while preserving data privacy by training a global model without sharing individual device data, making it a promising solution for distributed IoT environments. Table 4 summarizes recent FL-based anomaly detection applications in smart buildings.

Wang et al. [44] proposed federated deep neural network (FDNNs) and federated multi-input DNNs (FMI-DNNs) for privacy-preserving anomaly detection in a centralized FL architecture. This approach achieved a remarkable accuracy of 99.4% and a mean absolute error (MAE) of 0.093 on the IoT-Botnet 2020 dataset, demonstrating state-of-the-art performance in secure anomaly detection. Building on privacy-centric frameworks, Abdel Sater et al. [38] introduced a federated stacked LSTM (FSLSTM)

model that converges twice as fast as a traditional LSTM while significantly reducing communication costs. Evaluated on datasets from General Electric’s IoT production system, their approach achieved 90% accuracy and an MAE of 0.162, outperforming baseline methods in both classification and regression tasks. To address the challenges of data imbalance in FL, Weinger et al. [114] explored data augmentation techniques for IoT anomaly detection. Their experiments on public IoT datasets revealed that augmentation improved performance by 22.9%, achieving 95.94% accuracy. However, the study also highlighted that increasing FL client numbers worsened class imbalance, necessitating oversampling strategies for improved training stability.

Table 4. Summary of FL-based anomaly detection works in smart building applications.

Ref.	Year	DL Model	FL Method	Dataset	Best Performance	Advantages	Limitations
[44]	2023	DNN	FDNN FMI-DNN	IoT-Botnet 2020	Acc = 99.4%	Robust model against adversarial attacks. Preserves and maintains the security of local data. Train DL model using FL with centralized structure	Potential for communication delays and computational overhead when aggregating model updates from numerous localized IoT devices in real-time federated learning environments.
[38]	2021	LSTM	FSLSTM	Sensors Event Log Energy Usage	Acc = 90%	The proposed model converges more than 2x faster during training than the LSTM model. Reduced communication costs	Challenge of maintaining consistent performance across diverse smart building environments while minimizing communication overhead.
[114]	2022	NN GAN	FL with NN	TON-IoT, DS2OS	Acc = 95.94%	The Modbus dataset and a neural network model were used to compare centralized learning and FL. FL with imbalanced data worsens as more clients join, reducing training progress and causing anomaly detection issues.	Challenges include generating realistic synthetic data for rare attack types, maintaining privacy with data augmentation techniques, and adapting to rapidly evolving IoT threat landscapes across diverse device ecosystems.
[115]	2022	Log FNN, Reg, 1D-CNN, AE, RNN, LSTM, GRU	DL models Trained Using FL	KDD99, NSL-KDD, CIDD5001	Acc = 98.9%	Challenges with FL such as requiring lightweight models for edge devices, handling device heterogeneity, improving communication efficiency, and addressing non-IID data distributions across devices.	Their framework has issues with novel anomaly detection, performance consistency across diverse hardware, and balancing accuracy with privacy in resource-constrained IoT environments.
[116]	2022	GRU	FL train GRU	Modbus	Acc = 99.5%	Federated approach requires additional communication and aggregation time compared to centralized training. Implement a decentralized communication efficient framework for anomaly detection in IoT networks. Ensure the privacy of data.	Their system may encounter difficulties in adapting to rapidly evolving attack patterns, balancing model complexity with device resource constraints, and maintaining detection accuracy across diverse network environments and device types.
[117]	2024	LSTM-AE	ADLA-FL	RTU synthetic industrial dataset	Acc = 98%	FL framework requires a promising solution for secure, privacy-preserving anomaly detection, balancing performance with data protection requirements.	Coordination complexity in FL, high computational costs on edge devices, limited generalizability from synthetic data, and significant overhead from homomorphic encryption.
[118]	2024	DT, LR	FedGroup-EL	UNSW IoT, Real-world	Acc = 99.64%, 99.89%	Enhanced privacy through FL, improved detection performance with FedGroup-EL models, robust security via homomorphic encryption, and comprehensive performance evaluation using simulations.	Potential challenges in distinguishing subtle attacks, complexity in accurately predicting detailed attack characteristics, limited generalizability to unseen attack types, and computational overhead in evaluating multiple algorithms on real-world datasets.
[119]	2024	ANN	FLDS	CICDDOS2019	Higher F1-score	Enhanced detection accuracy, resource efficiency, real-time monitoring, and improved scalability with reduced latency	Potential synchronization delays between digital twins and physical devices, high computational overhead associated with maintaining real-time digital twins, and challenges in scaling the system to larger networks or more complex attack scenarios.
[120]	2024	CNN-GRU-LSTM	Asynchronous FL-CNN-GRULSTM	Edge-IIoTset	Acc = 100%	Offers enhanced threat detection accuracy, improved data privacy, and increased real-world applicability for IIoT cybersecurity through its hybrid model, federated learning framework, and comprehensive validation.	Increased complexity, potential model divergence and increased vulnerability, and dataset limitations may impede real-world effectiveness across diverse IIoT environments and evolving threats.

Jithish et al. [115] proposed an FL-based smart grid anomaly detection system using 1D-CNN models trained locally on smart meters. Their approach ensured privacy by securing model updates with SSL/TLS protocols. Achieving 98.9% accuracy on standard datasets such as KDD99 and NSL-KDD, the system demonstrated efficient performance in memory, CPU usage, and bandwidth, making it suitable for edge-level anomaly detection. Similarly,

Mothukuri et al. [116] presented a Federated GRU model for IoT network intrusion detection. This decentralized approach periodically updated the global model by aggregating locally trained weights. When tested on the Modbus dataset, the method achieved 99.5% accuracy, showcasing its potential for practical IoT network security applications while preserving data privacy.

Shrestha et al. [117] introduced ADLA-FL, a privacy-preserving anomaly detection framework for smart grid systems. By integrating LSTM networks with homomorphic encryption, the system enabled secure, collaborative model training among energy providers. Evaluated on synthetic industrial datasets, ADLA-FL achieved a 97% F1-score and 98% accuracy while maintaining low computational overhead, demonstrating its viability for secure and efficient anomaly detection in critical infrastructure. Zhang et al. [118] proposed FedGroup, an FL method that leverages ensemble learning to enhance the detection of attack types in IoT devices. Evaluations on the UNSW IoT dataset showed an impressive 99.64% accuracy with minimal communication overhead, highlighting its effectiveness in improving IoT security through collaborative learning.

Incorporating advanced technologies, Salim et al. [119] developed a digital twin-integrated FL system for IoT networks. Their adaptive thresholding with Early stopping (ATES) method improved model aggregation efficiency, reducing latency by 14% compared to fog-based implementations. Evaluations on the CICDDoS 2019 dataset confirmed superior performance in cyberthreat detection, emphasizing the potential of digital twins in enhancing IoT network security. Finally, Bukhari et al. [120] introduced a hybrid asynchronous FL framework combining CNN, GRU, and LSTM models for IIoT anomaly detection. The approach achieved perfect scores (100% accuracy, precision, recall, and F1) on the Edge-IIoTset dataset, demonstrating unparalleled adaptability and robustness in addressing real-time industrial threats while ensuring data privacy.

4.2. Federated Learning-Based Thermal Comfort

In a 2001 survey, the National Human Activity Pattern Survey revealed that people spend 87% of their time indoors [121]. This has made identifying the thermal comfort of occupants inside buildings increasingly important. Since the 1970s, two main approaches have been developed to solve this problem: the steady-state model and the adaptive model. The IoT is a promising solution for thermal comfort control in smart homes. IoT-based systems can provide thermal control comfort and energy efficiency by actively considering the user's perspective.

FL is a promising new approach to thermal comfort control in smart buildings. It allows multiple devices to train a shared thermal comfort model without sharing their data, which protects the privacy of occupants. Federated learning can also be used to train personalized thermal comfort models, which can improve accuracy. Table 5 illustrates a specific recent real-world application for thermal comfort-based FL in smart buildings.

M. Khalil et al. [122] proposed a privacy-preserving FL-based neural network (Fed-NN) for thermal comfort prediction. Fed-NN departs from current centralized approaches, where a universal learning model is updated through a secure parameter aggregation process instead of sharing raw data across building IoT environments, preserving privacy and security. The authors designed a branch selection protocol to reduce communication overhead in FL. Their experimental studies on a real-world dataset revealed the robustness, accuracy 80.39%, and stability of their model compared to other ML models while taking privacy into consideration.

Table 5. Summary of FL-based thermal comfort optimization works.

Ref.	Year	DL Model	FL Method	Dataset	Best Performance	Limitations
[122]	2022	NN	Fed-NN	Real-World dataset	80.39%	This approach reduces the communication overhead but does not eliminate it completely.
[123]	2021	DNN	FDNN	CU-BEMS	Loss 0.01	Evaluation is limited to a simulation using the CU-BEMS dataset. Real-world performances differ.
[124]	2021	CNN	CSFDL	Real-World dataset	99.00%	The CSFDL technique faces challenges in adapting to highly diverse building types or energy consumption patterns, could be computationally intensive for resource-constrained devices, and its effectiveness against advanced cyber-attacks may require ongoing validation as new threats emerge.
[125]	2019	ANN	Federated ANN	Real-World dataset	/	The evaluation was performed on a small simulated environment. Future testing is needed on larger real-world building spaces.
[126]	2022	CNN	Fed-CNN	ASHRAE	96.86%	The framework struggles with heterogeneous HVAC systems, early-stage fault detection accuracy, and balancing privacy constraints against model performance across diverse building types.
[127]	2023	CNN-LSTM	FL-CNN-LSTM	NYSERDA NIST Energy	RMSE 66.91 improvement	The FDA-HeatFlex approach faces challenges in adapting to highly diverse building types or unconventional heat pump systems, and its performance could be limited by the quality and representativeness of the source domain data used for transfer learning.

Khalil et al. [123] proposed a privacy-preserving federated deep neural network (FDNN) model for thermal comfort control in smart buildings. Local model training occurs without sharing data, ensuring privacy. Their framework was evaluated on the CU-BEMS dataset, and it achieved good accuracy and 0.01 loss. The authors' experiments demonstrate FL are promising for smart building control because of their high prediction accuracy and ability to maintain thermal comfort. The results on a public dataset of a building in Bangkok demonstrate the effectiveness and privacy-preserving capabilities of the proposed approach for smart building control.

Moradzabeh et al. [124] proposed cyber-secure federated deep learning (CSFDL), a novel privacy preserving approach for heating load demand forecasting. By combining FL and convolutional neural network (CNN) models, CSFDL provides a global super-model for forecasting heating demand for different local clients without revealing their privacy. The authors trained and tested the CSFDL global server model on a real-world dataset of 10 clients in their building environment. Compared with other ML/DL models such as support vector regression (SVR), LSTM, and generalized regression neural network (GRNN), CSFDL achieved 99% performance, robustness, and stability. The evaluation indicates the effectiveness of CSFDL against other conventional techniques while preserving privacy.

Perry et al. [125] proposed a novel federated ANN configuration with two new architectural components: an agent ANN (A-ANN) operates autonomously, with some federated influence from the coordinating ANN (C-ANN) for thermal control in building environments. Their experiments show how the proposed approach can optimally control actuators to regulate heat flow and maintain desired temperatures in the different rooms of a building by coordinating a distributed and centralized AI-controlled simulated office environment. On a real-world collected dataset, they demonstrate their proposed system can effectively disperse heat and optimize temperature.

X. Wang et al. [126] proposed a privacy-preserving FL-based convolutional neural network (Fed-CNN) model for HVAC fault detection and diagnosis systems utilizing multiparty data for multi-scale joint modeling by combining FL and CNN models. Without sharing data, the Fed-CNN trained model locally, and achieved an F1-score of 96.86% on a real-world chiller dataset from ASHRAE. The Fed-CNN model can also perform cross-domain fault detection and diagnosis for chillers and air handling units (AHUs), outperforming CNN, LSTM, GRU, NLSTM, BILSTM, and LGBM models. The FL framework improved upon HVAC fault detection and diagnosis systems.

Khanal et al. [127] proposed an innovative federated domain adaptation heat pump flexibility (FDA-HeatFlex) framework that combines parameter-based transfer learning (TL), adaptive boosting (AdaBoost), and FL techniques to accurately predict indoor temper-

atures and drive flexible information for heat pumps in new buildings while preserving privacy. FDA-HeatFlex addresses two key challenges, namely, the data distribution discrepancy (data shift) between a known source building and new target buildings and derives their flexibility. They trained CNN and Bi-LSTM models locally by employing FL by aggregating weights using the FedAvg method. They conducted an extensive experimental evaluation on two widely used public real-world datasets, the New York State Energy Research and Development Authority (NYSERDA) and the Net-Zero Energy Residential Test Facility (NIST). FDA-HeatFlex significantly outperforms the other approaches, with a 66.91% RMSE and a 91.8% error in the average temperature and heat pump flexibility predictions, respectively, because the FTL approach enables accurate scaling to new buildings while preserving privacy.

Figure 6 illustrates the flowchart of a thermal comfort system based on FL used to detect different levels of temperature and humidity, and to optimize thermal comfort.

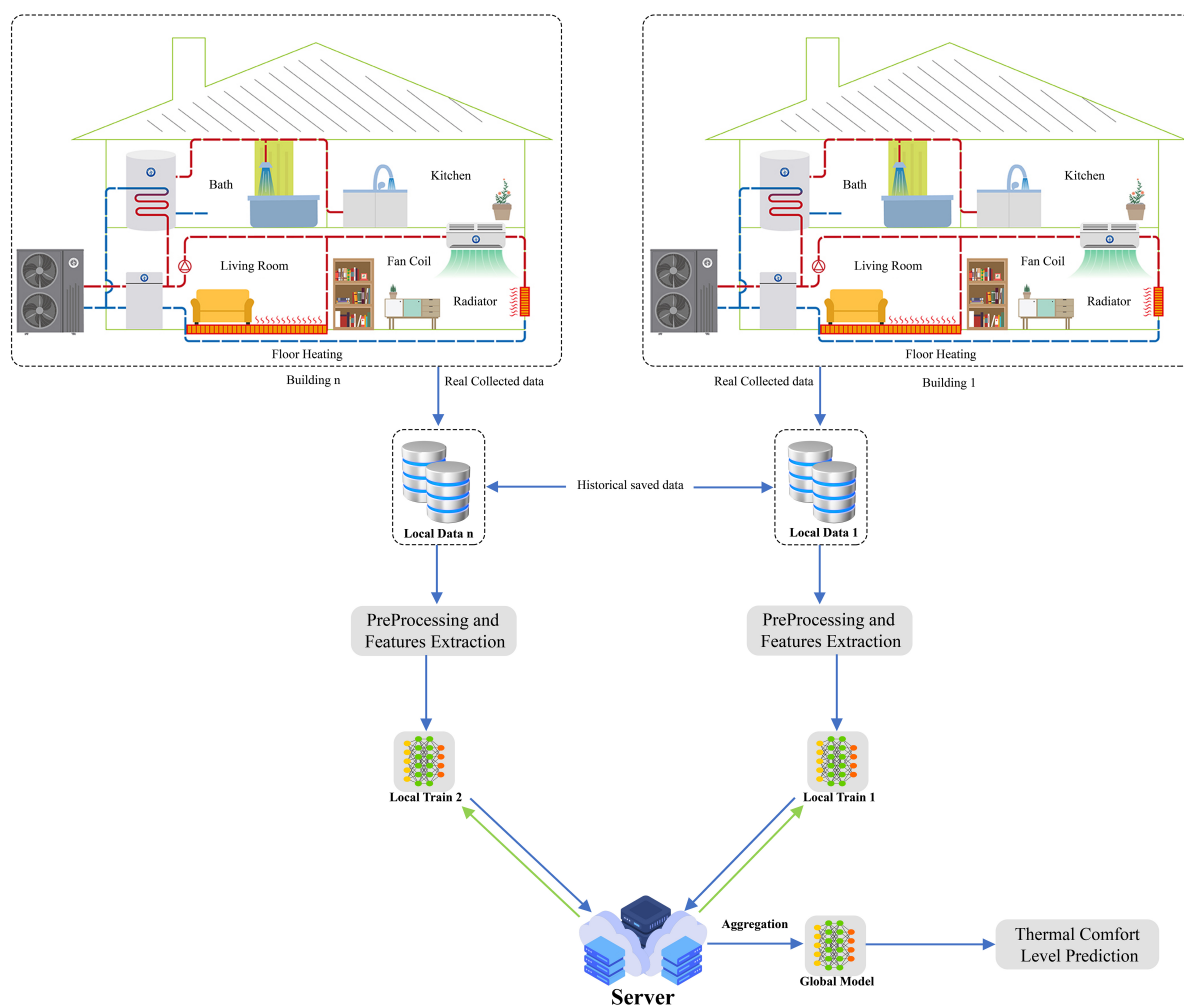


Figure 6. Thermal comfort monitoring and optimization system.

4.3. Federated Learning-Based Energy Prediction

The escalating trend of urbanization has resulted in a relentless surge in building energy consumption, contributing to a staggering 40% share of global energy utilization [128]. The quest for enhancing the efficiency of building energy consumption has prompted extensive investigations, with energy load forecasting taking center stage. Recent statistics highlight that the building sector alone accounted for 36% of the world's total final energy

consumption and was responsible for 37% of energy-related CO₂ emissions in the year 2020 [129]. This underscores the pivotal role played by building energy management systems (BEMS) in enhancing building energy efficiency and curbing energy consumption, ultimately fostering the development of net-zero energy structures with minimal carbon emissions. With the pursuit of more efficient and sustainable energy management strategies, FL has emerged as a cutting-edge approach harnessing the potential of distributed data and collaborative model training. This subsection offers a comprehensive overview of the innovative applications of FL in the realm of energy prediction. By seamlessly integrating data privacy and predictive accuracy, FL is poised to revolutionize the way we forecast and optimize energy consumption. Consequently, it has become a focal point of research and development in the energy management domain, holding the promise of reshaping how we approach this critical field. Table 6 illustrates a specific recent real-world applications for energy efficiency prediction based FL in smart buildings.

Table 6. Summary of FL-based energy prediction works.

Ref.	Year	DL Model	FL Method	Dataset	Best Performance	Limitations
[130]	2021	LSTM	FL with LSTM	Real-world data collected from London 2012–2014	RMSE 0.133	Edge computational constraints are ignored.
[131]	2023	CNN-LSTM	FL-based CNN-LSTM net-energy	AUSGRID	MSE MAE 0.32	This approach has limited generalizability to diverse global contexts, potential scalability issues with large user bases, and might require further validation against evolving attack methods and long-term energy consumption pattern changes.
[132]	2023	RNN-CNN	FL based RNN-CNN	Actual university campus dataset	Acc 97%	This framework has limited applicability across diverse building types, scalability challenges in large communities, and potential difficulties in adapting to rapidly changing energy consumption patterns or unforeseen anomalies.
[133]	2023	LSTM	FedSign-DP	Real-world dataset	68%	Their framework faces challenges in maintaining prediction accuracy with extreme quantization and differential privacy, particularly for highly imbalanced datasets, and the PowerSelection protocol could potentially introduce bias in model training.
[134]	2023	LSTM	FedraTrees	Tetouan Power Consumption	MAE 0.0168, MAPE% 3.54%	FedraTrees framework faces challenges in generalizing across diverse energy consumption patterns, could be sensitive to data quality variations among participants, and might struggle with capturing complex temporal dependencies that LSTM-based models excel at.
[129]	2023	LSTM	FL based LSTM	BDGP2	RMSE = 9.70% MAE = 7.40% CV = 0.0694 MAPE = 0.0557	Reliance on accurate local data distributions for effective clustering, which may not always be achievable in diverse or sparse datasets.
[135]	2022	LSTM	FL based LSTM	FUZZ-IEEE	RMSE 0.09–0.14	Per household FL performed worst due to having data from only one home.
[136]	2024	LSTM	FL-LSTM	NREL	RMSE = B 0.07056 – A 0.09386	Generalizability to diverse populations, computational demands of LSTMs and FL, and data integration challenges in real-world implementations.

M. Savi et al. [130] proposed a privacy-preserving approach exploiting federated LSTM models and edge computing capabilities for building energy consumption forecasting. Distinct users' LSTM models are locally trained on edge devices and aggregated using FedAvg to create a global model. The global model is then sent back for improved forecasting performance. Their approach collaboratively trains a global model without sharing data, reducing training time and communication overhead. They evaluated their approach on a real-world dataset collected in London, UK, from 2012 to 2014, and achieved 0.133 RMSE and 0.38 kWh performance, while preserving privacy and achieving a similar forecasting performance comparable to that of centralized solutions.

Badr et al. [131] introduced a privacy-preserving and communication-efficient FL-based energy predictor for net-metering systems. Using CNN-LSTM models, local training was performed on user devices without exposing raw data, while encrypted models were aggregated into a global predictor using an inner-product functional encryption (IPFE) cryptosystem. Communication efficiency was improved using a change-and-transmit (CAT) approach, significantly reducing the communication overhead by over 96% compared to Paillier cryptosystems. Their method, evaluated on a real power dataset, achieved

0.32 MSE/MAE, delivering state-of-the-art performance while preserving privacy and achieving 90% communication bandwidth savings.

Building on the theme of privacy preservation and efficient FL frameworks, Wang et al. [132] proposed a secure adaptive FL framework for load forecasting in community-building energy systems. Leveraging a hybrid RNN-CNN model, this approach demonstrated robustness in managing network faults while maintaining data security. Evaluations on a university campus dataset yielded a 10% error reduction, a 92% F1-score, and 97% accuracy, outperforming other models in accuracy and privacy preservation. Expanding on decentralized FL applications, Khalil et al. [133] developed the FedSign-DP framework for energy management in buildings. Utilizing LSTM models with differential privacy, their approach ensured secure data handling and bandwidth efficiency. Evaluations on the Pecan Street dataset demonstrated high accuracy with only a 10% decrease compared to centralized learning while reducing communication costs and bandwidth consumption to 1.56 Mb. The method outperformed protocols like FedStd and FedSign in privacy and communication efficiency, showcasing its practicality for real-world applications.

Adding to the discussion of lightweight FL models, Al-Quraan et al. [134] introduced FedraTrees, a framework leveraging ensemble learning for energy consumption prediction. This approach utilized a delta-based FL stopping algorithm to minimize unnecessary iterations, achieving an MAE of 0.0168 and MAPE of 3.54% on the Tetouan Power Consumption dataset. FedraTrees outperformed FedAvg while reducing computational and communication overheads to 2% and 13%, respectively, highlighting its suitability for privacy-preserving and cost-efficient energy prediction. To address data scarcity and heterogeneity in FL, Tang et al. [129] proposed a privacy-preserving framework for few-shot building energy prediction. By combining dynamic clustering and transfer learning, they enabled knowledge sharing among building clusters. Evaluations on the BDGP2 dataset demonstrated an RMSE of 9.70%, MAE of 7.40%, and MAPE of 0.0557, establishing their framework as a robust solution for improving energy prediction while safeguarding occupant privacy.

Further emphasizing the utility of FL for residential energy forecasting, Petrangeli et al. [135] proposed an approach tailored to edge computing environments. Their method employed local LSTM training to ensure data privacy and achieved an RMSE of 0.09–0.14 on the FUZZ-IEEE dataset. This work demonstrated a trade-off between privacy and accuracy, offering an effective solution for grid management and energy production planning while ensuring quality of service (QoS). Concluding the discussion, Mendes et al. [136] introduced an FL framework for predicting temporal net energy demand in transactive energy communities. Incorporating generation and demand forecasts with FTL, this hierarchical architecture supported collaborative learning while preserving data privacy. Evaluations on the NREL dataset showcased high adaptability, with Community B achieving an RMSE of 0.07056 compared to 0.09386 for Community A. Their innovative use of FTL highlighted its potential to enhance performance across diverse scenarios, supporting the growth of emerging energy communities.

Figure 7, illustrates the flowchart of an energy consumption monitoring system based on FL used to predict energy consumption and optimize the consumed energy.

4.4. Federated Learning-Based Healthcare Applications

The Internet of Medical Things (IoMT) has significantly revolutionized the healthcare sector, enhancing individual well-being through advanced data collection and analysis [137]. IoMT devices, particularly wearable sensors, play a crucial role in gathering medical data, which is then analyzed using AI techniques to enable innovative applications such as remote health monitoring and disease prediction [138]. Notably, DL has emerged as a powerful tool in biomedical image analysis, facilitating early detection of chronic diseases and improving healthcare service delivery.

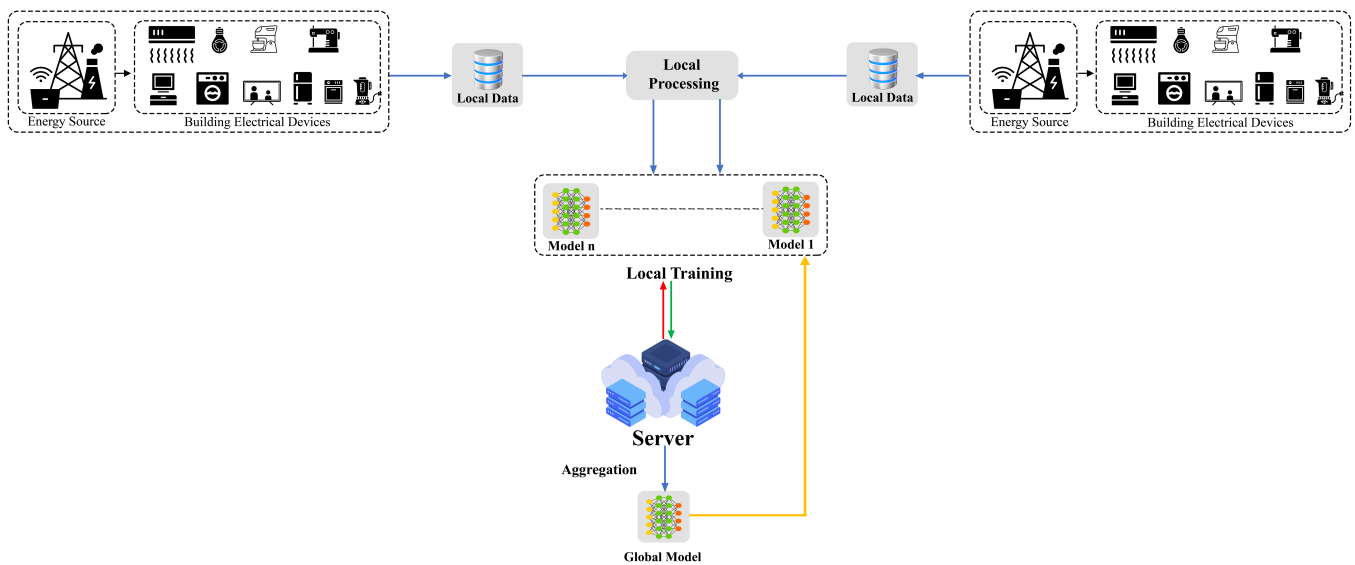


Figure 7. Energy prediction system based on FL.

FL offers a transformative approach in healthcare by enabling collaborative model training across decentralized devices while preserving patient privacy. By leveraging distributed data sources without centralized aggregation, FL ensures secure knowledge exchange, making it a vital solution for enhancing diagnostic and monitoring capabilities in smart healthcare systems. The applications of FL in healthcare, particularly in conjunction with the IoMT, have demonstrated significant promise in addressing privacy concerns while maintaining robust performance. Table 7 provides a summary of key FL-based healthcare applications. Building on these advancements, Li et al. [139] introduced ADDETECTOR, a privacy-preserving FL system for detecting Alzheimer’s disease (AD) using speech data collected via IoT devices in smart environments. The system employs a three-layer architecture to ensure data ownership, integrity, and confidentiality, leveraging differential privacy and encryption for enhanced security. Locally trained models (e.g., logistic regression, SVM-linear, and Naive Bayes) are aggregated asynchronously into a global model, ensuring robust privacy protection. Evaluations on the ADRes dataset of 1010 cases demonstrated an accuracy of 81.9% with a low time overhead of 0.7 s, showcasing the system’s effectiveness in AD detection while preserving privacy.

Expanding on privacy-preserving frameworks, Cai et al. [140] developed a skin cancer detection model combining FL with deep generative models to address challenges posed by limited and insufficient data. By employing dual generative adversarial networks (DualGANs) for data augmentation, they improved the quality and diversity of training data. Their FL-integrated DualGANs for skin cancer detection model (FDSCDM) used DualGANs for data augmentation and a CNN for classification, ensuring patient privacy through FL while minimizing communication costs. Evaluations on the ISIC 2018 dataset revealed that the FDSCDM achieved an accuracy of 91% and an AUC of 88%, significantly advancing medical IoT applications by addressing data scarcity and delivering excellent detection performance.

Table 7. Summary of FL-based healthcare applications.

Ref.	Year	DL Model	FL Method	Dataset	Best Performance	Limitations
[139]	2021	SVM Logistic Regression	ADDETECTOR	ADRes	81.9%	Evaluation on larger and diverse datasets would be needed.
[140]	2023	DualGAN CNN	FL-DualGAN CNN	ISIC 2018	ACC 91% AUC 88%	This approach may face challenges in generating diverse and clinically accurate synthetic images, struggle with rare skin cancer types or atypical presentations, and potentially introduce biases in the federated learning process due to data imbalances across participating institutions.
[141]	2022	Deep model	DFL	Dermatology Atlas	AUC 97% ACC 85%	This approach faces challenges in ensuring data quality across diverse IoT devices, adapting to varied skin conditions, and balancing privacy constraints with model performance in resource-limited healthcare settings.
[142]	2023	ANN-AE	FedSDM	ECG dataset	ACC 95% Loss 0.01	Uses an imbalanced dataset. Energy consumption for communication between devices/nodes should not be considered. Their mobility modeling may not accurately capture real user behaviors.
[143]	2022	CNN-AE	FL-CNN-AE	MIT-BIH Ar- rhythmia	Noisy 94.5% Clean 98.9%	The data privacy should be enhanced.
[144]	2022	VGG16 CNN	CFL	X-ray chest COVID-19 chest	improvement of 16% 11%	The performance degrades after a certain number of rounds due to overfitting.
[145]	2023	Resnet-9 CNN	FedECG	MIT-BIH	94.8%	Highly imbalanced ECG datasets, faces scalability challenges in large-scale IoT deployments, and potentially sacrifice some model accuracy for privacy and efficiency in resource-constrained environments.
[146]	2024	CNN-GAN	FedCSCD- GAN	Prostate Can- cer, Lung Cancer, Breast Cancer	ACC = 96.95%, 97.80%, 97%	Data quality variations, privacy-utility trade-offs, high computational demands, challenges in interpretability and compliance, struggles with rare cancer types, limited generalizability, and potential biases from non-diverse training data.
[147]	2024	CNN-AE	FL-CNN-AE	MIT-BIH, CinC2017, PTB-XL	Acc = 73.0%	Complex model training, data heterogeneity, limited generalizability, high computational requirements, and potential privacy risks.
[148]	2024	LSTM	FL-LSTM	MHealth	Acc = 87.5%	Higher energy consumption on smartphones with increasing training rounds, poor prediction accuracy for certain activities, and potential challenges in scaling the system to more devices and diverse activities.

Moving on, Elayan et al. [141] introduced deep FL (DFL), a privacy-preserving approach for healthcare data monitoring using IoT devices. Their framework ensures data confidentiality by training local models on participant devices for skin disease detection, which are then aggregated into a global model at a central server and redistributed. This decentralized approach reduces operational costs while safeguarding patient privacy. Evaluations on the dermatology atlas dataset demonstrated an AUC of 97% and accuracy of 85%, highlighting its potential for sustainable healthcare applications. Building on privacy-preserving healthcare solutions, Rajagopal et al. [142] developed FedSDM, an FL framework integrated within an edge-fog-cloud architecture for real-time ECG anomaly detection. This system employed an auto-encoder ANN to train local models, which were aggregated into a global model to ensure data safety. Tested on imbalanced ECG datasets and the EUA mobility dataset, FedSDM achieved a 95% accuracy with low loss (0.01) and outperformed fog and cloud deployments in terms of energy consumption, network usage, cost, execution time, and latency, demonstrating significant improvements in resource efficiency.

Raza et al. [143] introduced a novel FL framework for ECG-based healthcare applications incorporating explainable AI (XAI) to enhance interpretability. Their framework utilized a CNN-based autoencoder to denoise ECG signals, with the encoder employing TL to construct a CNN classifier. The XAI module provided insights into classification results, empowering clinical decision-making. Experiments on the MIT-BIH dataset yielded an accuracy of 94.5% on noisy data and 98.9% on clean data, with an 8.2% reduction in communication costs, advancing privacy-conscious decision support systems. Qayyum et al. [144] proposed clustered FL (CFL), a collaborative learning framework for COVID-19 diagnosis using multi-modal medical images, such as X-rays and ultrasound scans, sourced from various hospitals. By training local VGG16 CNN models and aggregating them into a shared multi-modal global model, CFL preserved privacy while improving diagnosis accuracy. Evaluations on benchmark datasets demonstrated F1-score improvements of 16% and

11% for multi-modal tasks compared to conventional FL, showcasing its effectiveness in privacy-sensitive applications.

Advancing FL for ECG abnormality prediction, Ying et al. [145] introduced a federated semi-supervised learning (FSSL) framework addressing non-IID data, labeling challenges, and privacy concerns. Their approach integrated pseudo-labeling, data augmentation, and a ResNet-9 model with FedAvg aggregation. Tested on the MIT-BIH dataset, the framework achieved 94.8% accuracy with only 50% labeled data, outperforming distributed methods by 3%. This study highlights the potential of FSSL in utilizing unlabeled data for robust healthcare applications. Raza et al. [146] proposed FedCSCD-GAN, an FL framework combining GANs and CNNs for collaborative cancer diagnosis across distributed institutions. Differential privacy and f-differential anonymization techniques safeguarded patient data, while GANs generated high-fidelity medical data. Evaluations on prostate, lung, and breast cancer datasets achieved accuracies of 96.95%, 97.80%, and 97%, respectively, demonstrating robust diagnostic performance and advancing secure collaborative medical data analysis.

Chorney et al. [147] developed a federated learning approach for training ECG classifiers under heterogeneous data distributions. Their study introduced novel techniques such as federated clustered hyperparameter tuning (FedCHT) and genetic federated clustered learning (CFL), alongside autoencoders for handling diverse ECG datasets. Evaluations on datasets such as MIT-BIH Arrhythmia achieved an F1 score of 69.7%, demonstrating the challenges of non-IID data in clinical settings while offering a flexible FL framework for real-world applications.

Finally, Dayakaran et al. [148] presented an FL-based human activity recognition (HAR) framework leveraging LSTM models for privacy-preserving training on distributed smartphone sensor data. Using FedAvg for model aggregation, the framework demonstrated a testing accuracy of 87.5% on the MHealth dataset while consuming energy comparable to traditional centralized models. This approach highlights the potential of FL for collaborative training across multiple devices while ensuring privacy in real-world applications involving sensitive personal data. Together, these studies highlight the transformative potential of FL in healthcare, addressing critical challenges such as data privacy, insufficient datasets, and communication efficiency while enabling robust and accurate diagnostic systems.

Figure 8, illustrates the flowchart of a healthcare monitoring system based on FL used to detect different diseases and elderly activities and optimize the health of occupants.

4.5. Real-World Federated Learning Implementation

This subsection represent real-world FL implementations in in different applications such as anomaly detection, healthcare, and energy consumption and their experimental results summarized in Table 8.

S. Becker et al. [149], developed a real-world FL prototype based on an autoencoder for anomaly detection in industrial IoT (IIoT) condition monitoring, their work preserves data privacy by enabling decentralized training on edge devices utilizing a real-world dataset. The experimental results demonstrated that their FL approach reduces overall network usage from up to 99.20% and achieves an average f1-score of 99.4%. (Anomaly-Detection-IIoT, <https://github.com/OliverStoll/Anomaly-Detection-IIoT/tree/master> (accessed on 21 December 2024)).

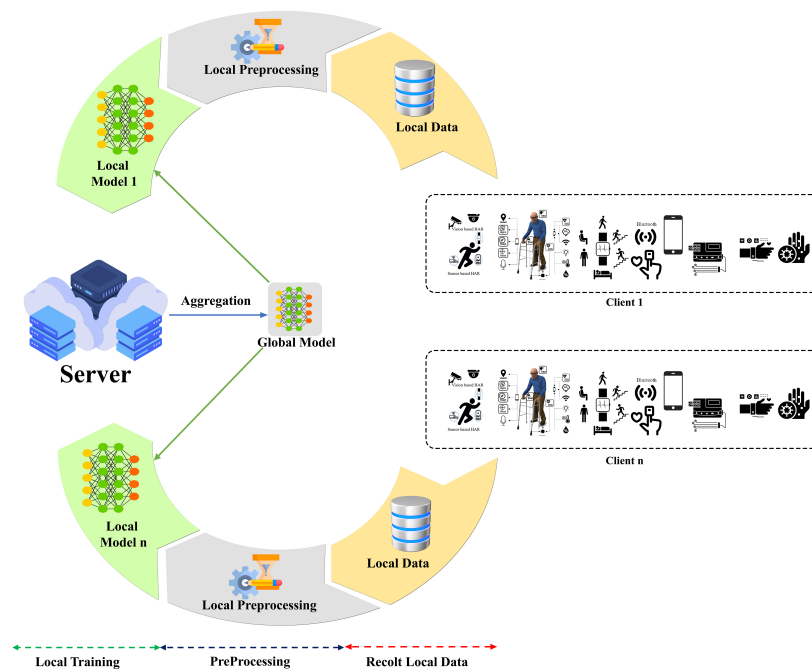


Figure 8. Healthcare application system based on FL.

Table 8. FL real-world implementation.

Authors	Year	Application	Dataset	FL Approach	Key Performance
S. Becker et al. [149]	2022	Anomaly detection	IIoT real-world dataset	FL Autoencoder	Network usage reduced by up to 99.20%. F1-score of 99.4%.
T. Zhang et al. [150]	2021	Anomaly detection	N-BaIoT and LANDER on physical Raspberry Pi devices	FedIoT FedDetect	Accuracy : 93.70%, Training under 1 h on Raspberry Pi.
X. Wang et al. [151]	2021	Anomaly detection	Real manufacturing setup	FLAD, Federated DRL, DDPG	FAR: 3–6%, MDR: 2–6%, System throughput: 165 tps, Latency: 9–13.5 s.
S.S. Tripathy et al. [152]	2024	Healthcare	Real-world health data	FedHealthFog	Communication latency reduced by 87.01%, 26.90%, and 71.74%. Energy consumption reduced by 57.98%, 34.36%, and 35.37%.
S.H. Alsamhi et al. [153]	2024	Healthcare	Real world medical data	Combine FL with blockchain	Improved patient data protection. Reduced data breaches. Real-world privacy mandates.
D. N. Sachin et al. [154]	2024	Healthcare	Real-world data diabetes monitoring, eye retinopathy classification, maternal health, remote health monitoring, and HAR	FedCure, personalized FL for IoMT	Accuracy: over 90%. Minimal communication overhead. Handles non-IID effectively. Confirms clinical feasibility.
M R A. Berkani et al. [155]	2024	Healthcare	SaYoPillow	FedWell	Accuracy: 99.95%. Loss: 0.0019%. Communication cost: 0.08 MB.
Khan et al. [156]	2025	Energy prediction	Real smart home energy data	FL with XAI for decision interpretability	MSE: 0.6655. Optimizes energy consumption.
I. Varlamis et al. [24]	2023	Energy consumption	Real-world sensor data	(EM) ³ , FL energy efficiency recommendation	Reduction in unnecessary monitor usage by 42%. Decrease in excessive lighting consumption by 75%. Accuracy: over 90%.
M R A. Berkani et al. [157]	2024	Energy and Smoke	Real-world smoke detection IoT	FL-CNN-1D	Accuracy: 99.97%. Communication cost: 0.4 MB.

T. Zhang et al. [150] implemented FedIoT, a full FL platform for IoT cybersecurity, integrating the FedDetect algorithm for anomaly detection. They benchmarked FedIoT in a real hardware setup on Raspberry Pi devices, using N-BaIoT and LANDER datasets. The FedDetect algorithm achieved 93.7% accuracy while preserving data privacy through FL. More importantly, their experiments on Raspberry Pi boards demonstrated efficient

resource usage, keeping training times under one hour, thus proving real-world deployment for edge-based FL. (FedIoT, <https://github.com/FedML-AI/FedML/tree/master/iot> (accessed 21 December 2024)).

In [151], X. Wang et al. introduced FLAD, a federated deep reinforcement learning (DRL) approach for IIoT anomaly detection that operates in a real manufacturing environment. FLAD integrates deep deterministic policy gradient (DDPG) with privacy leakage degree metrics, eliminating the need to centralize training data. Their experimental evaluations shows false alarm rates (FAR) between 3% and 6%, missing detection rate (MDR) between 2% and 6%, and system throughput reaching 165 transactions per second (tps), with latency of 9 to 13.5 s across various IIoT applications benchmarks that demonstrate practical system performance.

S S. Tripathy et al. [152], proposed FedHealthFog, an FL-based healthcare analytics system deployed on fog computing platforms to enhance privacy, reduce latency, and optimize resource usage. By running real data experiments in IoT-enabled healthcare settings, FedHealthFog showed significant improvements in communication latency reduced by 87.01%, 26.90%, and 71.74%, and energy consumption reduced by 57.98%, 34.36%, and 35.37% relative to benchmark algorithms, underscoring its practical effectiveness.

In [153], S H. Alsamhi et al. combined FL with the blockchain for decentralized healthcare data sharing, deploying their framework in a real world medical IoT setup to ensure privacy, security, and transparency. Their evaluations reported improved patient data protection and reduced data breaches, thereby demonstrating how FL supports real-world data privacy mandates and fosters patient trust.

In [154], D. N. Sachin et al., present FedCure, a heterogeneity-aware personalized FL approach for IoMT healthcare. Extensive tests on diverse real-world healthcare datasets such as diabetes monitoring, eye retinopathy classification, maternal health, remote health monitoring, and HAR, showed over 90% accuracy with minimal communication overhead. These results highlight the robustness of FedCure in handling real-world Non-IID data and confirm its clinical feasibility for personalized healthcare.

M R A. Berkani et al. [155], introduced FedWell, a privacy-preserving FL framework for occupant stress monitoring in smart buildings. They integrates SaYoPillow smart devices and wearable environmental sensors, leveraging a lightweight ANN trained using FedAvg aggregation. Experimental evaluations on the SaYoPillow dataset achieved 99.95% accuracy, with a minimal loss of 0.0019% and a low communication cost of 0.08 MB, ensuring real-time stress monitoring, data privacy, and scalability in smart building environments.

In [156], Khan et al. introduced an FL-driven explainable AI (XAI) framework for real-world smart energy management in smart buildings, focusing on data privacy, cybersecurity, and transparency. By combining FL for decentralized training with XAI to improve decision interpretability, they achieved superior performance on a real-world smart home energy dataset, with a random forest model reaching the lowest MSE of 0.6655 and outperforming other ML models. This approach effectively optimizes energy consumption while ensuring privacy, security, and user trust.

In [24], I. Varlamis et al. proposed (EM)³, an FL-based energy efficiency recommendation system that leverages big data analytics and edge computing to optimize energy consumption in smart buildings. They processes IoT sensor data locally to generate personalized, context-aware recommendations for reducing energy waste while preserving user privacy. Evaluations using real-world sensor data demonstrated a 42% reduction in unnecessary monitor usage and a 75% decrease in excessive lighting consumption, with FL achieving over 90% accuracy in predicting optimal energy saving actions.

In [157], M R A. Berkani et al., introduced an FL-based smoke and fire detection system for smart buildings, leveraging a CNN-1D model trained on wearable environmental sensor

data, enabling privacy preserving collaborative learning across clients. Evaluations on a real-world smoke detection IoT dataset achieved an accuracy of 99.97% with a minimal communication cost of 0.4 MB. This ensures real-time fire detection, reduces false alarm, and enhance safety while preserving data privacy in smart building environments.

5. Open Challenges

The AI community struggles to acquire, merge, and utilize decentralized data while safeguarding privacy and adhering to data protection regulations such as the GDPR. In response, Google introduced a groundbreaking technology known as FL in 2016 [47]. This innovative and advanced approach has undergone continuous evolution. However, FL presents various challenges and issues, including privacy concerns, security considerations, storage implications, communication overhead, and other pertinent factors. While providing solutions, FL introduces new challenges, presenting new opportunities to develop innovative methods and solutions that address the existing challenges and paves the way for advancements in privacy-preserving AI methodologies.

FL is an ML/DL technique based on collaborative model training under the control of a central server, where training occurs locally, with data remaining decentralized on the client/user to ensure privacy. FL leverages various DL/ML techniques and models with local models transferred to a central server for aggregation to create the global model, which is sent back to clients. Several research challenges are associated with FL in the context of smart buildings, can be categorized into six main areas as illustrated in Figure 9.

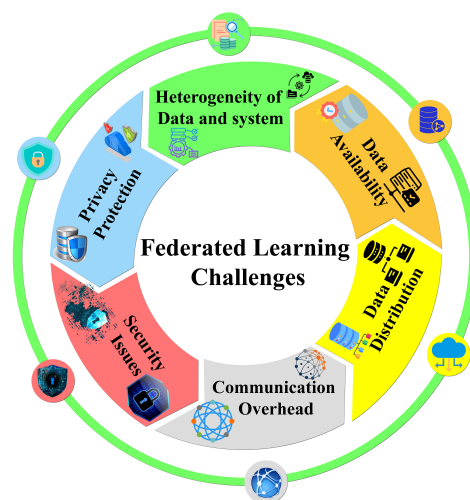


Figure 9. FL Challenges.

During training iterations, clients communicate frequently with a central server for model aggregation, underscoring the need for efficient protocols that minimize delays and optimize the FL process. System and data heterogeneity pose significant challenges for FL model training. Differences in hardware and software capabilities across devices highlight the need for a consistent, well coordinated FL environment

Privacy protection is a major challenge in FL. While decentralizing data can improve detection, it also increases the risk of unauthorized access to sensitive information during local training. Striking the right balance between privacy and security is vital to FL's success. Robust designs are needed to secure data and models against potential adversarial attacks from malicious clients/users, including encryption and authentication mechanisms.

The data distribution challenge is another noteworthy aspect of FL. Non-identical data distributions across devices may lead to potential model biases toward devices with more

data, requiring strategies to ensure the fairness and effectiveness of trained models across diverse sources. Finally, the data availability challenge is a critical consideration, as the effectiveness of training in FL depends on consistent data access and sufficient computing resources across decentralized devices. Advanced optimization techniques help address these needs and are vital for real-world FL deployments.

5.1. Privacy Protection Issues

Privacy concerns in FL stemming from the potential exposure of sensitive user and client data keep them locally on individual devices within federated settings. While this approach preserves privacy, sharing information during the training process poses a risk of disclosing sensitive data to third parties or a centralized server. Techniques such as SMC, DP, and model aggregation aim to address these concerns, but face challenges such as performance degradation, model efficiency issues, latency in model updates, and vulnerability to attacks. There is a balance between security trade-offs and privacy in FL systems [11,63,158]. Although FL stores data locally, privacy risks persist because sensitive information still resides on each device. Ensuring that data remain protected during both training and transmission is thus a central concern. The act of sharing gradients during training can inadvertently expose private information, posing a risk of data sharing to the central server or third parties.

In FL, only model updates, specifically gradient information, are shared, ensuring data protection for each device. However, the processing of these updates introduces the possibility of sensitive information exposure. Cryptography techniques like homomorphic encryption and secure multiparty computation and DP are commonly proposed strategies to enhance privacy and address this challenge by allow model updates to be computed on encrypted data, preventing unauthorized access while maintaining privacy; however, these methods present challenges such as performance impact, efficiency issues, latency in model updates, and vulnerability to attacks, prompting the need for innovative methodologies [158,159].

5.2. Security Issues

Despite the existence of various attacks, FL security systems often face limited evaluations of potential threats. Two prominent categories, data attacks and model attacks, including poisoning attacks, backdoor attacks, and adversarial assaults, pose significant risks to FL systems.

Data attacks occur during collaborative local training, where multiple clients contribute their training data. Detecting and preventing malicious clients can clandestinely introduce falsified data, compromising the training process and undermining the model's integrity. Model attacks involve a malicious client manipulating gradients or parameters, altering the model before integration into the centralized server for aggregation, and risking the integrity of the global model through invalid gradients. As model dimensionality increases, the susceptibility to attacks and backdoor attacks also increases [63,159]. Anomaly detection and robust aggregation for mitigating model attacks, techniques such as Zeno and Byzantine-resilient algorithms detect and filter out malicious updates to improve security of model aggregation. Digital twins provide an additional solution for security issues by creating FL environments to detect anomalies and ensure that FL models remain robust against security threats.

5.3. Communication Overhead

Communication is a pivotal element in FL-enabled smart building services, yet it poses a significant challenge due to the high communication overhead from local model updates. In smart buildings, having each client update the entire model at every epoch

can lead to high communication costs. One approach to mitigate this involves using a blockchain ledger on edge networks, which allows local computation and exchange of training updates without a central server. However, block mining introduces its own costs, so designing an FL–blockchain system must account for on-device training latency, update transmission time, and block mining latency, all while preserving sufficient model accuracy. Similar communication challenges have been observed in various FL-based systems across different fields such as healthcare, transportation, intrusion detection, anomaly detection, and digital twins in communication systems. Mitigating strategies involve reducing overall communications, message sizes, and quantities exchanged. In centralized settings with a server connecting to remote devices, communication issues can be alleviated. Conversely, decentralized topologies offer an alternative solution during communication bottlenecks, especially in low-bandwidth and high-latency networks [11,16,160]. Advanced techniques and methods to mitigate communication overhead challenges in FL include the following: Gradient compression and quantization, reducing and compressing the size of transmitted model updates by applying techniques such as count sketch (compresses gradient or weights), sparsification (transmit only important updates), and subsampling (reduces number of clients/updates per round). These methods help decrease the communication load while maintaining model accuracy [161,162]; a decentralized aggregation and blockchain technique based on a decentralized FL system that eliminates the need for a central server, enhancing distributed model updates more efficiently, security model updates without a central authority [163]; and integration of 5G/6G networks with FL, highlighting wireless communication technologies that promise higher speeds and lower latencies, significantly reducing communication delays in FL applications [164]. Unlike asynchronous FL, this allows clients to send updates at different times rather than waiting for synchronized updates, thus reducing bottlenecks and improving training efficiency [165].

5.4. Data Distribution

Data distribution plays a crucial role in the realm of AI, particularly within FL environments, where it is often categorized as independent and identically distributed (IID) data or non-IID data. The latter, arising from imbalances in data, features, and labels, introduces heightened complexity in both modeling and evaluation processes. FL commonly employs stochastic gradient descent, a prevalent optimization algorithm for training deep networks. However, with non-IID data, model convergence becomes more intricate, leading to challenges and significant performance degradation due to weight divergence caused by variations in the distribution of devices, classes, and population across the decentralized network [29,39].

5.5. Heterogeneity of the Data and System

Addressing system and data heterogeneity in FL is imperative, due to significant variations in device capabilities within the decentralized network, including computational power, storage capacities, and communication bandwidths, which are often influenced by hardware, network connections, and power supply disparities. Additionally, the intermittent reliability of edge computing devices, stemming from connectivity or energy limitations, further complicates the FL landscape. Strategies to address these challenges include asynchronous communication, parallelizing iterative optimization algorithms for minimizing stragglers and enhancing efficiency in heterogeneous environments. Active sampling of devices at each round, coupled with aggregating device updates within predefined windows, has emerged as a viable solution for managing heterogeneity. Moreover, addressing fault tolerance issues and incorporating algorithmic redundancy into code computations are crucial steps toward achieving robust FL with unreliable devices and

non-identically distributed data [158,160]. Recent advancements methods to mitigate this challenge include the following: FedProx and FedNova. These FL extensions improve the traditional FedAvg approach by adding a regularization term to have FedProx and normalizing updates to have FedNova to improve convergence under non-IID conditions and handling inconsistent client updates [166,167]; personalized FL that instead of training a single global model and tackles heterogeneous client by allowing each client to maintain a locally fine-tuned version of the model while sharing knowledge with the global model [168]; and adaptive learning algorithms that enhance FL robustness by dynamically adjusting updates to changing data distributions by continuously refining global model updates [169].

The non-identically distributed data collected from diverse devices significantly influence the performance of FL systems. Future research should explore adaptive FL models that dynamically adjust to changes in system and data heterogeneity. Continuous monitoring of device capabilities and data characteristics is needed for real-time adaptation, while standardization efforts should include guidelines for handling these complexities, ensuring interoperability and scalability across diverse environments.

5.6. Data Availability

Data availability is a pivotal factor in federated learning (FL), as it significantly influences the training efficacy of models across decentralized devices. Challenges in this domain often stem from variations in device connectivity, usage patterns, and privacy constraints, leading to intermittent data accessibility. Devices may be powered off, experience limited connectivity, or face privacy concerns that restrict data sharing or limit the duration for model updates, thereby impeding their active participation in the FL process [170]. A notable challenge in FL is the heterogeneity of data distributions across clients, commonly referred to as non-independent and identically distributed (non-IID) data. These non-IID data can adversely affect the convergence and accuracy of the global model. Moreover, the intermittent availability of clients, due to factors like varying device usage patterns and connectivity issues, further complicates the training process. Clients may become temporarily unavailable, leading to delays in model updates and potential biases in the aggregated model [171]. Privacy constraints add another layer of complexity, as they may limit the extent of data sharing or the duration for which data can be used for model updates, thereby hindering effective collaboration among clients [172].

To address these challenges, various strategies have been proposed. For instance, the federated graph-based sampling (FedGS) framework aims to stabilize global model updates and mitigate long-term biases arising from arbitrary client availability. By modeling data correlations among clients and employing a sampling strategy that ensures diversity and fairness, FedGS enhances the robustness and performance of FL systems [170]. Other approaches, such as clustered federated learning, attempt to group clients with similar data distributions to improve model accuracy and efficiency [173]. Additionally, advancements in differential privacy and secure multi-party computation help alleviate privacy-related constraints, enabling more robust participation from clients [174].

5.7. Federated Learning in Smart Buildings

The deployment of FL in smart buildings is further complicated by the heterogeneity of IoT devices, which exhibit significant variation in computational power, storage capacity, and communication bandwidth. Resource-limited edge devices may struggle to enable complex model training, while others may experience operational failures due to power constraints. Employing asynchronous FL has been proposed as a solution with lightweight models that can be deployed on constrained devices, while computationally intensive

training tasks are assigned to more capable clients, thereby optimizing resource utilization without compromising overall model performance [175]. Heterogeneous IoT ecosystems further complicate these challenges, as device capabilities like processing memory, and network bandwidth can vary widely. Resource-constrained edge nodes might not support the enabling of complex model training, while others may struggle with power or hardware failures. Asynchronous FL has emerged as one viable solution, deploying lightweight models on constrained devices while relegating heavier computations to more capable nodes. This approach optimizes system resources while maintaining global performance [175]. Large-scale implementations add another layer of complexity: more devices mean higher communication overhead and potential synchronization bottlenecks. Hierarchical FL, with intermediary nodes performing local aggregations before communicating to a central server, alleviates these issues by reducing both network traffic and round-trip latency, making FL more scalable [176].

5.8. Specific Federated Learning Application Challenges

FL deployment in smart buildings presents distinct challenges across energy prediction, anomaly detection, and thermal comfort optimization. These issues stem from data heterogeneity, system constraints, and security vulnerabilities. Smart building energy prediction is often influenced by non-stationary factors including occupancy dynamics, climatic variations, and seasonal effects. These factors create highly diverse, time dependent datasets collected from smart meters, HVAC systems, and lighting sensors. FL-based models must contend with this heterogeneity, as well as inconsistent or missing data caused by device malfunctions. Preprocessing strategies, data augmentation, and redundancy-aware fault tolerance can significantly improve data quality and model robustness [68]. In anomaly detection, FL enable real-time identification of security threats, device faults, and energy inefficiencies while maintaining local data privacy. However, incremental or asynchronous model updates can introduce communication delays, complicating timely responses to emerging threats. Adversarial attacks and Byzantine faults further heighten security concerns, demanding secure aggregation protocols, adversarial training, or SMC-based defenses to preserve both model fidelity and system integrity [177]. Thermal comfort optimization faces unique challenge, primarily due to occupant-specific preferences and limited, subjective data labels. Generic FL architectures can struggle with personalization when occupant feedback is sparse or highly variable. Techniques such as meta learning and client-adaptive FL are proving effective for tailoring HVAC setpoints to individual comfort profiles, thereby improving occupant satisfaction and energy efficiency. Transfer learning and synthetic data augmentation can help overcome data scarcity by leveraging external or simulated datasets, mitigating the lack of ground-truth labels and enabling more accurate comfort models.

6. Future Directions

Figure 10 shows into how FL optimizes online learning, resource usage, and data sharing in smart buildings through localized model training. This highlights the adaptive capacity of FL to efficiently manage dynamic and heterogeneous IoT data from various devices and sensors. Importantly, FL enhances privacy and security by limiting raw data sharing, increasing compatibility with digital twin architectures that require interoperability across operational and information systems. However, applying FL requires addressing the communication overhead due to potential bandwidth limitations, employing DP or encryption techniques to further improve privacy protections, and adapting solutions to varying data distributions across devices. While promising for handling evolving, distributed data in smart buildings, thoughtful system design is needed to ensure scalability

through efficient communication protocols, adjustable ML approaches, and suitable security measures.

Federated Learning Future Directions

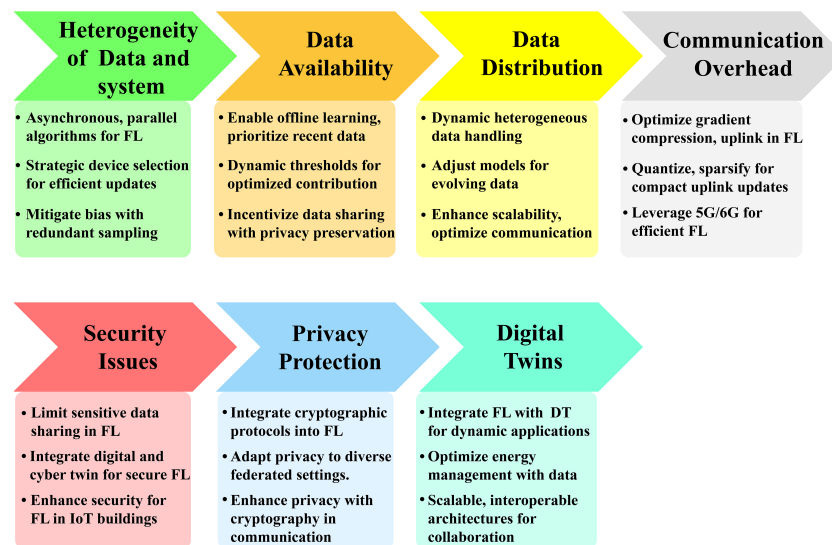


Figure 10. Future FL Directions.

6.1. Privacy Protection Issues

A possible solution and future direction of research is an emerging approach involving integrating cryptographic systems with FL models to enhance privacy protection while considering performance and computational cost reduction. Although exchanging only model updates can protect on-device data, vulnerabilities remain when updates are processed. Incorporating cryptographic safeguards provides an additional layer of security, ensuring data integrity throughout the FL process, ensuring sensitive information confidentiality, and offering a robust privacy solution with high accuracy [11,159]. The concept of privacy is evolving beyond the global or local levels to address variations in privacy constraints across devices and individual data points. Future research should aim to develop privacy techniques capable of handling mixed privacy restrictions [158].

6.2. Security Issues

To address privacy concerns, sharing less sensitive prediction results or information during the aggregation process has emerged as a viable solution, contributing to the development of a more robust and protected FL method that ensures optimal privacy. Additionally, combining FL with the concepts of cyber twins and digital twins (DTs) could offer enhanced security. These concepts involve virtual representations of physical systems or processes that enable better monitoring, analysis and prediction. Integrating these concepts with FL could provide a more comprehensive and secure approach to data handling and model training [39].

Furthermore, future research should focus on developing novel security approaches tailored to the unique challenges and requirements of FL-based systems in the context of smart building environments, safeguarding sensitive data and ensuring the integrity of FL systems is necessary in this context.

6.3. Communication Overhead

Researchers have aimed to introduce an efficient communication protocol capable of compressing uplink and downlink communication while remaining robust with an increased number of clients and diverse data distributions. The proposed algorithms allow

clients to compute gradients based on local data, compress these gradients using data structures such as Count Sketch, and transmit them to a central aggregator, reducing the amount of communication needed per round while meeting federated training quality requirements [29,160]. Additionally, model compression techniques, including quantization, subsampling, and sparsification, are employed to reduce the message size conveyed during update rounds. Finally, the utilization of 5G/6G networks is proposed to offer significantly higher speeds and lower latency compared to previous generations, enabling more efficient FL in various applications across different fields. These strategies collectively contribute and enhance FL performance and efficiency in diverse applications [14,160].

6.4. Data Distribution

To effectively address Non-IID data challenges in FL, a comprehensive set of solutions can be implemented. Initiating data preprocessing techniques is crucial, aiming to rectify imbalances in data, features, and labels across devices. Intelligent client sampling strategies, considering device diversity and computational capabilities, contribute to a more representative dataset. Personalization techniques tailor models to individual devices while maintaining a global perspective, proving effective for device-specific patterns. Addressing privacy concerns through DP or FL with homomorphic encryption is paramount for non-IID data [29]. Adaptive learning algorithms dynamically adjust to evolving data distributions, while communication-efficient techniques such as decentralized optimization or compressed model updates maintain efficiency in FL environments. Implementing transfer learning methodologies, incentivizing collaboration among devices, and introducing continuous monitoring and adaptation mechanisms further contribute to overcoming non-IID data challenges. Finally, the establishment of standardized evaluation metrics fosters fair comparisons between solutions, under varying data conditions. Integrating these strategies collectively enhances the robustness and adaptability of FL models, ensuring their efficacy in the face of non-IID data complexities [29,39,158].

6.5. Heterogeneity of the Data and System

To avoid system heterogeneity, asynchronous communication techniques are employed, and parallelizing iterative optimization algorithms is a highly promising approach for eliminating the possibilities of stragglers in heterogeneous environments. Another approach involves actively selecting participating devices at each round, aggregating updates within a pre-defined window, wherein only a small subset of devices participate in each training round. A plausible approach is preventing device failures leading to bias in the device sampling scheme when failed devices have specific data features. Additionally, introducing algorithmic redundancy as an element in coded computation techniques can achieve fault tolerance [39,158].

6.6. Data Availability

To address data availability challenges, several strategies can be implemented. Offline learning and caching mechanisms enable devices to learn during connected intervals and contribute to global model updates online. Time-weighted federated averaging prioritizes recent updates, minimizing stale or outdated data impacts. Dynamic participation thresholds based on data availability and quality give greater priority to devices with more relevant data. Privacy-preserving techniques such as DP can address and encourage more extensive data sharing. In addition, incentivization mechanisms, adaptive scheduling algorithms, and ongoing research in these areas are essential for optimizing data availability in FL. Striking a balance between optimizing model performance and accommodating intermittent device data contributes to resilient and adaptable FL systems for real-world applications.

6.7. Digital Twins

Key trajectories for FL in smart buildings include integration with digital twins enabling real-time and life-critical applications with dynamic adaptation based on FL updates and facilitating seamless maintenance and management in smart buildings. Another promising pathway involves an evolution toward predictive maintenance, where the combination of FL and digital twins analyzes sensor data, predict potential faults, and optimize maintenance strategies, ultimately reducing operational downtime [178,179].

Furthermore, future strategies include leveraging FL for energy management, optimizing energy consumption patterns through historical data and real-time adjustments based on factors such as building occupancy and weather conditions. Personalized environments with customized lighting, temperature, and other environmental factors are explored for individual occupant preferences and behaviors, thereby enhancing overall comfort and productivity [178]. Establishing robust security and privacy measures for FL models and data, especially in the integration with digital twins, remains paramount in future directions [159]. The development of scalability and interoperability concerns has driven research toward developing architectures capable of handling growing smart building data while ensuring seamless integration across diverse devices and platforms [179,180].

Regulatory compliance is a critical aspect of future directions for creating frameworks that align FL with evolving data privacy and security regulations. Finally, collaboration across smart cities has emerged as a visionary trajectory, extending FL beyond individual buildings to optimize energy usage and services across entire building ecosystems [178].

Future research should explore the adoption of FL technology in sensitive domains such as healthcare, thermal comfort, energy prediction, anomaly detection, and air quality for effective smart building implementation. Addressing security and privacy challenges is crucial for real-time deployment. Efforts should focus on developing frameworks seamlessly integrating digital twins and FL, especially for real-time and sensitive scenario applications. Additionally, establishing standards and frameworks tailored to 5G/6G and beyond network requirements is needed. The integration of FL and digital twins for deployment in real-time and life-critical scenarios, stands out as a key focus, significantly impacting daily lives by contributing to smarter and more intelligent buildings [178].

Moreover, investigating the impact of FL on smart buildings is complicated by local requirements and distributed learning can offer improved considerations for users' contexts and privacy, advancing the capabilities of smart buildings. The proposed federation framework, which orchestrates a group of autonomous learners distributed across smart buildings, represents an innovative approach to enhancing building intelligence and efficiency. These future research directions hold promise for creating more sophisticated and user-centric smart building applications [178,180].

7. Conclusions

This study provides a comprehensive exploration of FL, detailing its foundational concepts, architectural variations, and applications in domains such as anomaly detection, energy prediction, thermal comfort optimization, and healthcare. The contributions of this study are significant. FL's decentralized model training enables privacy-preserving collaboration across diverse datasets, ensuring compliance with regulations like GDPR. Its integration into smart building systems has demonstrated significant advancements in energy optimization, thermal comfort, and anomaly detection. Moreover, innovative model aggregation strategies like FedAvg, FedProx, and FedNova address challenges posed by data and system heterogeneity, enhancing model performance and convergence.

The findings reveal the performance gains of FL in distributed systems. FL frameworks outperform traditional centralized methods by effectively utilizing non-centralized data,

achieving state-of-the-art accuracy in multiple domains. FL's effectiveness in healthcare, thermal comfort, and energy prediction highlights its robust performance while addressing privacy and communication challenges. Efficient model aggregation techniques such as FedAvg and FedMA offer scalable solutions for combining distributed model updates, leading to improved global model accuracy. Furthermore, the incorporation of differential privacy (DP) and encryption techniques has proven effective in mitigating risks such as data leakage and adversarial attacks, bolstering FL's robustness to privacy concerns.

Despite these advances, several challenges require attention. Communication overhead remains a significant issue due to the iterative nature of FL, which demands substantial communication resources, particularly for non-IID data. Data heterogeneity across clients leads to performance disparities and increased convergence times. FL systems also remain vulnerable to various security threats, including poisoning, backdoor, and inference attacks, necessitating advancements in security mechanisms. Additionally, scalability issues arise as FL systems expand to accommodate numerous clients, introducing complexities in maintaining model efficiency and computational fairness. Resource constraints on edge devices further limit FL's potential due to their limited computational power, storage, and energy efficiency.

To address these challenges, several future directions are proposed. Enhanced privacy mechanisms, such as advanced cryptographic techniques and hybrid approaches combining DP with secure multi-party computation (SMPC), can offer improved data confidentiality. Adaptive learning strategies and personalized FL frameworks will enable better handling of non-IID data and system heterogeneity. Integration with emerging technologies such as 5G/6G for reduced communication latency and digital twins for real-time monitoring and predictive maintenance will further strengthen FL's applicability. Additionally, efforts to optimize model training for resource-constrained edge devices will enhance FL's feasibility in IoT environments. Robust security solutions to counteract emerging threats, such as adversarial and Byzantine attacks, are imperative. Expanding FL's applications across domains, including healthcare, transportation, and climate modeling, will unlock new opportunities for decentralized intelligence.

In conclusion, FL has emerged as a transformative approach in distributed machine learning, addressing the key challenges of data privacy and security. Its adoption across various domains showcases its versatility and potential. However, addressing existing challenges and exploring the proposed future directions will be pivotal in realizing FL's full potential and fostering its integration into critical applications.

Funding: This research received no external funding.

Data Availability Statement: No data were generated or used for this study as it is a review article.

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

References

1. Sayed, A.N.; Himeur, Y.; Varlamis, I.; Bensaali, F. Continual learning for energy management systems: A review of methods and applications, and a case study. *Appl. Energy* **2025**, *384*, 125458.
2. Sayed, A.N.; Bensaali, F.; Himeur, Y.; Dimitrakopoulos, G.; Varlamis, I. Enhancing building sustainability: A Digital Twin approach to energy efficiency and occupancy monitoring. *Energy Build.* **2025**, *328*, 115151. [[CrossRef](#)]
3. Theodosiou, A.A.; Read, R.C. Artificial intelligence, machine learning and deep learning: Potential resources for the infection clinician. *J. Infect.* **2023**, *87*, 287–294.
4. Yazici, İ.; Shayea, I.; Din, J. A survey of applications of artificial intelligence and machine learning in future mobile networks-enabled systems. *Eng. Sci. Technol. Int. J.* **2023**, *44*, 101455.
5. Himeur, Y.; Elnour, M.; Fadli, F.; Meskin, N.; Petri, I.; Rezgui, Y.; Bensaali, F.; Amira, A. AI-big data analytics for building automation and management systems: A survey, actual challenges and future perspectives. *Artif. Intell. Rev.* **2023**, *56*, 4929–5021.

6. Berkani, M.R.A.; Chouchane, A.; Himeur, Y.; Ouamane, A.; Amira, A. An Intelligent Edge-Deployable Indoor Air Quality Monitoring and Activity Recognition Approach. In Proceedings of the 2023 6th International Conference on Signal Processing and Information Security (ICSPIS), Dubai, United Arab Emirates, 8–9 November 2023; pp. 184–189. [\[CrossRef\]](#)
7. Truong, N.; Sun, K.; Wang, S.; Guitton, F.; Guo, Y. Privacy preservation in federated learning: An insightful survey from the GDPR perspective. *Comput. Secur.* **2021**, *110*, 102402.
8. Li, Y.; Tao, X.; Zhang, X.; Liu, J.; Xu, J. Privacy-preserved federated learning for autonomous driving. *IEEE Trans. Intell. Transp. Syst.* **2021**, *23*, 8423–8434.
9. Jagarlamudi, G.K.; Yazdinejad, A.; Parizi, R.M.; Pouriyeh, S. Exploring privacy measurement in federated learning. *J. Supercomput.* **2023**, *80*, 10511–10551.
10. Chronis, C.; Varlamis, I.; Himeur, Y.; Sayed, A.N.; Al-Hasan, T.M.; Nhlabatsi, A.; Bensaali, F.; Dimitrakopoulos, G. A survey on the use of Federated Learning in Privacy-Preserving Recommender Systems. *IEEE Open J. Comput. Soc.* **2024**, *5*, 227–247.
11. Pandya, S.; Srivastava, G.; Jhaveri, R.; Babu, M.R.; Bhattacharya, S.; Maddikunta, P.K.R.; Mastorakis, S.; Piran, M.J.; Gadekallu, T.R. Federated learning for smart cities: A comprehensive survey. *Sustain. Energy Technol. Assessments* **2023**, *55*, 102987.
12. Rahman, A.; Hossain, M.S.; Muhammad, G.; Kundu, D.; Debnath, T.; Rahman, M.; Khan, M.S.I.; Tiwari, P.; Band, S.S. Federated learning-based AI approaches in smart healthcare: Concepts, taxonomies, challenges and open issues. *Clust. Comput.* **2023**, *26*, 2271–2311. [\[CrossRef\]](#) [\[PubMed\]](#)
13. Bousbiat, H.; Himeur, Y.; Varlamis, I.; Bensaali, F.; Amira, A. Neural load disaggregation: Meta-analysis, federated learning and beyond. *Energies* **2023**, *16*, 991. [\[CrossRef\]](#)
14. Himeur, Y.; Varlamis, I.; Kheddar, H.; Amira, A.; Atalla, S.; Singh, Y.; Bensaali, F.; Mansoor, W. Federated learning for computer vision. *arXiv* **2023**, arXiv:2308.13558.
15. Zhang, Z.; Gao, Z.; Guo, Y.; Gong, Y. Scalable and low-latency federated learning with cooperative mobile edge networking. *IEEE Trans. Mob. Comput.* **2022**, *23*, 812–822.
16. Nguyen, D.C.; Ding, M.; Pathirana, P.N.; Seneviratne, A.; Li, J.; Poor, H.V. Federated learning for internet of things: A comprehensive survey. *IEEE Commun. Surv. Tutorials* **2021**, *23*, 1622–1658. [\[CrossRef\]](#)
17. Bechar, A.; Elmir, Y.; Himeur, Y.; Medjoudj, R.; Amira, A. Federated and Transfer Learning for Cancer Detection Based on Image Analysis. *arXiv* **2024**, arXiv:2405.20126.
18. Rafsanjani, H.N.; Nabizadeh, A.H. Towards human-centered artificial intelligence (ai) in architecture, engineering, and construction (aec) industry. *Comput. Hum. Behav. Rep.* **2023**, *11*, 100319.
19. Tagliabue, L.C.; Cecconi, F.R.; Rinaldi, S.; Ciribini, A.L.C. Data driven indoor air quality prediction in educational facilities based on IoT network. *Energy Build.* **2021**, *236*, 110782. [\[CrossRef\]](#)
20. Yang, B.; Liu, Y.; Liu, P.; Wang, F.; Cheng, X.; Lv, Z. A novel occupant-centric stratum ventilation system using computer vision: Occupant detection, thermal comfort, air quality, and energy savings. *Build. Environ.* **2023**, *237*, 110332.
21. Silva, L.; Bezzo, F.B.; van Ham, M. COVID-19 restrictions: An opportunity to highlight the effect of neighbourhood deprivation on individuals' health-related behaviours. *Soc. Sci. Med.* **2023**, *325*, 115917. [\[CrossRef\]](#)
22. Sun, Z.; Wang, Z.; Xu, Y. Privacy protection in cross-platform recommender systems: Techniques and challenges. *Wirel. Netw.* **2023**, *30*, 6721–6730.
23. Bousbiat, H.; Bousseldj, R.; Himeur, Y.; Amira, A.; Bensaali, F.; Fadli, F.; Mansoor, W.; Elmenreich, W. Crossing roads of federated learning and smart grids: Overview, challenges, and perspectives. *arXiv* **2023**, arXiv:2304.08602.
24. Varlamis, I.; Sardianos, C.; Chronis, C.; Dimitrakopoulos, G.; Himeur, Y.; Alsalemi, A.; Bensaali, F.; Amira, A. Using big data and federated learning for generating energy efficiency recommendations. *Int. J. Data Sci. Anal.* **2023**, *16*, 353–369.
25. Imteaj, A.; Mamun Ahmed, K.; Thakker, U.; Wang, S.; Li, J.; Amini, M.H. Federated learning for resource-constrained IoT devices: Panoramas and state of the art. *Fed. Transf. Learn.* **2022**, *27*, 7–27.
26. Banabilah, S.; Aloqaily, M.; Alsayed, E.; Malik, N.; Jararweh, Y. Federated learning review: Fundamentals, enabling technologies, and future applications. *Inf. Process. Manag.* **2022**, *59*, 103061.
27. Xu, C.; Qu, Y.; Xiang, Y.; Gao, L. Asynchronous federated learning on heterogeneous devices: A survey. *Comput. Sci. Rev.* **2023**, *50*, 100595.
28. Kheddar, H.; Dawoud, D.W.; Awad, A.I.; Himeur, Y.; Khan, M.K. Reinforcement-Learning-Based Intrusion Detection in Communication Networks: A Review. In *IEEE Communications Surveys & Tutorials*; IEEE: New York, NY, USA, 2024.
29. Jiang, J.C.; Kantarci, B.; Oktug, S.; Soyata, T. Federated learning in smart city sensing: Challenges and opportunities. *Sensors* **2020**, *20*, 6230. [\[CrossRef\]](#)
30. Li, L.; Fan, Y.; Tse, M.; Lin, K.Y. A review of applications in federated learning. *Comput. Ind. Eng.* **2020**, *149*, 106854.
31. Belenguer, A.; Pascual, J.A.; Navaridas, J. A review of federated learning applications in intrusion detection systems. *Comput. Netw.* **2025**, *258*, 111023.
32. Grataloup, A.; Jonas, S.; Meyer, A. A review of federated learning in renewable energy applications: Potential, challenges, and future directions. *Energy* **2024**, *17*, 100375.

33. Vahabi, M.; Fotouhi, H. Federated learning at the edge in Industrial Internet of Things: A review. *Sustain. Comput. Inform. Syst.* **2025**, *46*, 101087.
34. Qian, Q.; Zhang, B.; Li, C.; Mao, Y.; Qin, Y. Federated transfer learning for machinery fault diagnosis: A comprehensive review of technique and application. *Mech. Syst. Signal Process.* **2025**, *223*, 111837.
35. Wang, L. Application of information technology in judicial field: The development model of online litigation in China. *Comput. Law Secur. Rev.* **2024**, *52*, 105936.
36. Jatain, D.; Singh, V.; Dahiya, N. A contemplative perspective on federated machine learning: Taxonomy, threats & vulnerability assessment and challenges. *J. King Saud-Univ.-Comput. Inf. Sci.* **2022**, *34*, 6681–6698.
37. Rieyan, S.A.; News, M.R.K.; Rahman, A.M.; Khan, S.A.; Zaarif, S.T.J.; Alam, M.G.R.; Hassan, M.M.; Ianni, M.; Fortino, G. An advanced data fabric architecture leveraging homomorphic encryption and federated learning. *Inf. Fusion* **2024**, *102*, 102004.
38. Sater, R.A.; Hamza, A.B. A federated learning approach to anomaly detection in smart buildings. *ACM Trans. Internet Things* **2021**, *2*, 1–23.
39. Agrawal, S.; Sarkar, S.; Aouedi, O.; Yenduri, G.; Piamrat, K.; Alazab, M.; Bhattacharya, S.; Maddikunta, P.K.R.; Gadekallu, T.R. Federated learning for intrusion detection system: Concepts, challenges and future directions. *Comput. Commun.* **2022**, *195*, 346–361.
40. Doriguzzi-Corin, R.; Siracusa, D. FLAD: Adaptive federated learning for DDoS attack detection. *Comput. Secur.* **2024**, *137*, 103597.
41. Abdulla, N.; Demirci, M.; Ozdemir, S. Smart meter-based energy consumption forecasting for smart cities using adaptive federated learning. *Sustain. Energy Grids Netw.* **2024**, *38*, 101342.
42. Nguyen, H.; Nawara, D.; Kashef, R. Connecting the Indispensable Roles of IoT and Artificial Intelligence in Smart Cities: A Survey. *J. Inf. Intell.* **2024**, *2*, 261–285.
43. Ahmed, S.F.; Alam, M.S.B.; Afrin, S.; Rafa, S.J.; Rafa, N.; Gandomi, A.H. Insights into Internet of Medical Things (IoMT): Data fusion, security issues and potential solutions. *Inf. Fusion* **2024**, *102*, 102060. [\[CrossRef\]](#)
44. Wang, X.; Wang, Y.; Javaheri, Z.; Almutairi, L.; Moghadamnejad, N.; Younes, O.S. Federated deep learning for anomaly detection in the internet of things. *Comput. Electr. Eng.* **2023**, *108*, 108651. [\[CrossRef\]](#)
45. Beltrán, E.T.M.; Gómez, Á.L.P.; Feng, C.; Sánchez, P.M.S.; Bernal, S.L.; Bovet, G.; Pérez, M.G.; Pérez, G.M.; Celdrán, A.H. Fedstellar: A platform for decentralized federated learning. *Expert Syst. Appl.* **2024**, *242*, 122861. [\[CrossRef\]](#)
46. Truhn, D.; Arasteh, S.T.; Saldanha, O.L.; Müller-Franzes, G.; Khader, F.; Quirke, P.; West, N.P.; Gray, R.; Hutchins, G.G.; James, J.A.; et al. Encrypted federated learning for secure decentralized collaboration in cancer image analysis. *Med Image Anal.* **2024**, *92*, 103059. [\[CrossRef\]](#) [\[PubMed\]](#)
47. McMahan, B.; Moore, E.; Ramage, D.; Hampson, S.; Agüera y Arcas, B. Communication-efficient learning of deep networks from decentralized data. In Proceedings of the Artificial Intelligence and Statistics, PMLR, Ft. Lauderdale, FL, USA, 20–22 April 2017; pp. 1273–1282.
48. Gugueoth, V.; Safavat, S.; Shetty, S. Security of Internet of Things (IoT) using federated learning and deep learning-Recent advancements, issues and prospects. *ICT Express* **2023**, *9*, 941–960. [\[CrossRef\]](#)
49. Rodríguez-Barroso, N.; Stipcich, G.; Jiménez-López, D.; Ruiz-Millán, J.A.; Martínez-Cámara, E.; González-Seco, G.; Luzón, M.V.; Veganzones, M.A.; Herrera, F. Federated Learning and Differential Privacy: Software tools analysis, the Sherpa. ai FL framework and methodological guidelines for preserving data privacy. *Inf. Fusion* **2020**, *64*, 270–292.
50. Jain, D.; Ranjan, R.; Sharma, A.; Sharma, S.N.; Jain, A. Fast and accurate ECG signal peaks detection using symbolic aggregate approximation. *Multimed. Tools Appl.* **2024**, *83*, 75033–75059. [\[CrossRef\]](#)
51. Li, S. Image recognition algorithm of aerobics athletes' upper limb movements based on federated learning. *J. Radiat. Res. Appl. Sci.* **2024**, *17*, 100835. [\[CrossRef\]](#)
52. Ali, M.A.; Sharma, A.K.; Dhanaraj, R.K. Heterogeneous features and deep learning networks fusion-based pest detection, prevention and controlling system using IoT and pest sound analytics in a vast agriculture system. *Comput. Electr. Eng.* **2024**, *116*, 109146. [\[CrossRef\]](#)
53. Mora, A.; Bujari, A.; Bellavista, P. Enhancing generalization in federated learning with heterogeneous data: A comparative literature review. *Future Gener. Comput. Syst.* **2024**, *157*, 1–15. [\[CrossRef\]](#)
54. Qi, P.; Chiaro, D.; Guzzo, A.; Ianni, M.; Fortino, G.; Piccialli, F. Model aggregation techniques in federated learning: A comprehensive survey. *Future Gener. Comput. Syst.* **2023**, *150*, 272–293. [\[CrossRef\]](#)
55. Ma, X.; Zhang, J.; Guo, S.; Xu, W. Layer-wised model aggregation for personalized federated learning. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, New Orleans, LA, USA, 18–24 June 2022; pp. 10092–10101.
56. Pandey, S.R.; Tran, N.H.; Bennis, M.; Tun, Y.K.; Manzoor, A.; Hong, C.S. A Crowdsourcing Framework for On-Device Federated Learning. *IEEE Trans. Wirel. Commun.* **2020**, *19*, 3241–3256. [\[CrossRef\]](#)
57. Zhang, C.; Xie, Y.; Bai, H.; Yu, B.; Li, W.; Gao, Y. A survey on federated learning. *Knowl.-Based Syst.* **2021**, *216*, 106775. [\[CrossRef\]](#)
58. Wang, J.; Liu, Q.; Liang, H.; Joshi, G.; Poor, H.V. Tackling the objective inconsistency problem in heterogeneous federated optimization. *Adv. Neural Inf. Process. Syst.* **2020**, *33*, 7611–7623.

59. Xu, J.; Glucksberg, B.S.; Su, C.; Walker, P.; Bian, J.; Wang, F. Federated learning for healthcare informatics. *J. Healthc. Inform. Res.* **2021**, *5*, 1–19. [\[CrossRef\]](#)
60. Kim, H.; Park, J.; Bennis, M.; Kim, S.L. Blockchain On-Device Federated Learning. *IEEE Commun. Lett.* **2020**, *24*, 1279–1283. [\[CrossRef\]](#)
61. Zheng, Z.; Xie, S.; Dai, H.N.; Chen, X.; Wang, H. Blockchain challenges and opportunities: A survey. *Int. J. Web Grid Serv.* **2018**, *14*, 352–375. [\[CrossRef\]](#)
62. Li, A.; Sun, J.; Zeng, X.; Zhang, M.; Li, H.; Chen, Y. Fedmask: Joint computation and communication-efficient personalized federated learning via heterogeneous masking. In Proceedings of the 19th ACM Conference on Embedded Networked Sensor Systems, Coimbra, Portugal, 15–17 November 2021; pp. 42–55.
63. Li, T.; Sahu, A.K.; Talwalkar, A.; Smith, V. Federated learning: Challenges, methods, and future directions. *IEEE Signal Process. Mag.* **2020**, *37*, 50–60. [\[CrossRef\]](#)
64. Karimireddy, S.P.; Kale, S.; Mohri, M.; Reddi, S.; Stich, S.; Suresh, A.T. Scaffold: Stochastic controlled averaging for federated learning. In Proceedings of the International Conference on Machine Learning, PMLR, Virtual, 13–18 July 2020; pp. 5132–5143.
65. Shi, Y.; Zhang, Y.; Xiao, Y.; Niu, L. Optimization Strategies for Client Drift in Federated Learning: A review. *Procedia Comput. Sci.* **2022**, *214*, 1168–1173. [\[CrossRef\]](#)
66. Shi, J.; Wan, W.; Hu, S.; Lu, J.; Zhang, L.Y. Challenges and approaches for mitigating byzantine attacks in federated learning. In Proceedings of the 2022 IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Wuhan, China, 9–11 December 2022; pp. 139–146.
67. Wang, H.; Yurochkin, M.; Sun, Y.; Papailiopoulos, D.; Khazaeni, Y. Federated learning with matched averaging. *arXiv* **2020**, arXiv:2002.06440.
68. Cheng, X.; Li, C.; Liu, X. A review of federated learning in energy systems. In Proceedings of the 2022 IEEE/IAS Industrial and Commercial Power System Asia (I&CPS Asia), Shanghai, China, 8–11 July 2022; pp. 2089–2095.
69. Fallah, A.; Mokhtari, A.; Ozdaglar, A. Personalized federated learning with theoretical guarantees: A model-agnostic meta-learning approach. *Adv. Neural Inf. Process. Syst.* **2020**, *33*, 3557–3568.
70. Liu, F.; Li, M.; Liu, X.; Xue, T.; Ren, J.; Zhang, C. A Review of Federated Meta-Learning and Its Application in Cyberspace Security. *Electronics* **2023**, *12*, 3295. [\[CrossRef\]](#)
71. Ji, S.; Tan, Y.; Saravirta, T.; Yang, Z.; Liu, Y.; Vasankari, L.; Pan, S.; Long, G.; Walid, A. Emerging trends in federated learning: From model fusion to federated x learning. *Int. J. Mach. Learn. Cybern.* **2024**, *15*, 3769–3790.
72. Xu, S.; Xia, H.; Zhang, R.; Liu, P.; Fu, Y. FedNor: A robust training framework for federated learning based on normal aggregation. *Inf. Sci.* **2024**, *684*, 121274.
73. Wang, J.; Wang, R.; Xu, G.; He, D.; Pei, X.; Zhang, F.; Gan, J. FedPKR: Federated Learning With Non-IID Data Via Periodic Knowledge Review in Edge Computing. *IEEE Trans. Sustain. Comput.* **2024**, *9*, 902–912.
74. Gupta, R.; Alam, T. Survey on federated-learning approaches in distributed environment. *Wirel. Pers. Commun.* **2022**, *125*, 1631–1652.
75. Boobalan, P.; Ramu, S.P.; Pham, Q.V.; Dev, K.; Pandya, S.; Maddikunta, P.K.R.; Gadekallu, T.R.; Huynh-The, T. Fusion of federated learning and industrial Internet of Things: A survey. *Comput. Netw.* **2022**, *212*, 109048.
76. Hiwale, M.; Walambe, R.; Potdar, V.; Kotecha, K. A systematic review of privacy-preserving methods deployed with blockchain and federated learning for the telemedicine. *Healthc. Anal.* **2023**, *3*, 100192.
77. Fung, C.; Yoon, C.J.; Beschastnikh, I. Mitigating sybils in federated learning poisoning. *arXiv* **2018**, arXiv:1808.04866.
78. Bhagoji, A.N.; Chakraborty, S.; Mittal, P.; Calo, S. Analyzing federated learning through an adversarial lens. In Proceedings of the International Conference on Machine Learning, PMLR, Long Beach, CA, USA, 9–15 June 2019; pp. 634–643.
79. Fredrikson, M.; Jha, S.; Ristenpart, T. Model inversion attacks that exploit confidence information and basic countermeasures. In Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, Denver, CO, USA, 12–16 October 2015; pp. 1322–1333.
80. Shokri, R.; Stronati, M.; Song, C.; Shmatikov, V. Membership inference attacks against machine learning models. In Proceedings of the 2017 IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, 22–26 May 2017; pp. 3–18.
81. Briggs, C.; Fan, Z.; Andras, P. A review of privacy-preserving federated learning for the Internet-of-Things. In *Federated Learning Systems Towards Next-Generation AI*; Springer: Cham, Switzerland, 2021; pp. 21–55.
82. Xie, C.; Huang, K.; Chen, P.Y.; Li, B. Dba: Distributed backdoor attacks against federated learning. In Proceedings of the International Conference on Learning Representations, New Orleans, LA, USA, 6–9 May 2019.
83. Bonawitz, K.; Ivanov, V.; Kreuter, B.; Marcedone, A.; McMahan, H.B.; Patel, S.; Ramage, D.; Segal, A.; Seth, K. Practical secure aggregation for privacy-preserving machine learning. In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, Dallas, TX, USA, 30 October–3 November 2017; pp. 1175–1191.
84. Yin, X.; Zhu, Y.; Hu, J. A comprehensive survey of privacy-preserving federated learning: A taxonomy, review, and future directions. *ACM Comput. Surv. (CSUR)* **2021**, *54*, 1–36.

85. Nasr, M.; Shokri, R.; Houmansadr, A. Comprehensive privacy analysis of deep learning: Passive and active white-box inference attacks against centralized and federated learning. In Proceedings of the 2019 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 19–23 May 2019; pp. 739–753.
86. Melis, L.; Song, C.; De Cristofaro, E.; Shmatikov, V. Exploiting unintended feature leakage in collaborative learning. In Proceedings of the 2019 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 19–23 May 2019; pp. 691–706.
87. Li, Q.; Wen, Z.; Wu, Z.; Hu, S.; Wang, N.; Li, Y.; Liu, X.; He, B. A survey on federated learning systems: Vision, hype and reality for data privacy and protection. *IEEE Trans. Knowl. Data Eng.* **2021**, *35*, 3347–3366.
88. Voigt, P.; Von dem Bussche, A. *The Eu General Data Protection Regulation (GDPR). A Practical Guide*, 1st ed.; Springer International Publishing: Cham, Switzerland, 2017; Volume 10.
89. Dwork, C.; Roth, A. The algorithmic foundations of differential privacy. *Found. Trends® Theor. Comput. Sci.* **2014**, *9*, 211–407.
90. Hassan, M.U.; Rehmani, M.H.; Chen, J. Differential privacy techniques for cyber physical systems: A survey. *IEEE Commun. Surv. Tutorials* **2019**, *22*, 746–789. [[CrossRef](#)]
91. Xiong, X.; Liu, S.; Li, D.; Cai, Z.; Niu, X. A comprehensive survey on local differential privacy. *Secur. Commun. Netw.* **2020**, *2020*, 8829523.
92. Yang, M.; Guo, T.; Zhu, T.; Tjuawinata, I.; Zhao, J.; Lam, K.Y. Local differential privacy and its applications: A comprehensive survey. *Comput. Stand. Interfaces* **2023**, *89*, 103827.
93. Cormode, G.; Jha, S.; Kulkarni, T.; Li, N.; Srivastava, D.; Wang, T. Privacy at scale: Local differential privacy in practice. In Proceedings of the 2018 International Conference on Management of Data, Houston, TX, USA, 10–15 June 2018; pp. 1655–1658.
94. Dwork, C.; McSherry, F.; Nissim, K.; Smith, A. Calibrating noise to sensitivity in private data analysis. In Proceedings of the Theory of Cryptography: Third Theory of Cryptography Conference, TCC 2006, New York, NY, USA, 4–7 March 2006; Proceedings 3; Springer: Berlin/Heidelberg, Germany, 2006; pp. 265–284.
95. Dwork, C.; McSherry, F.; Nissim, K.; Smith, A. Calibrating noise to sensitivity in private data analysis. *J. Priv. Confidentiality* **2016**, *7*, 17–51.
96. Abadi, M.; Chu, A.; Goodfellow, I.; McMahan, H.B.; Mironov, I.; Talwar, K.; Zhang, L. Deep learning with differential privacy. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, 24–28 October 2016; pp. 308–318.
97. Andrew, G.; Thakkar, O.; McMahan, B.; Ramaswamy, S. Differentially private learning with adaptive clipping. *Adv. Neural Inf. Process. Syst.* **2021**, *34*, 17455–17466.
98. Zhao, Y.; Zhao, J.; Yang, M.; Wang, T.; Wang, N.; Lyu, L.; Niyato, D.; Lam, K.Y. Local differential privacy-based federated learning for internet of things. *IEEE Internet Things J.* **2020**, *8*, 8836–8853. [[CrossRef](#)]
99. Li, Q.; Wu, Z.; Wen, Z.; He, B. Privacy-preserving gradient boosting decision trees. In Proceedings of the AAAI Conference on Artificial Intelligence, New York, NY, USA, 7–12 February 2020; Volume 34, pp. 784–791.
100. Aziz, R.; Banerjee, S.; Bouzeffrane, S.; Le Vinh, T. Exploring homomorphic encryption and differential privacy techniques towards secure federated learning paradigm. *Future Internet* **2023**, *15*, 310. [[CrossRef](#)]
101. Wu, X.; Zhang, Y.; Shi, M.; Li, P.; Li, R.; Xiong, N.N. An adaptive federated learning scheme with differential privacy preserving. *Future Gener. Comput. Syst.* **2022**, *127*, 362–372. [[CrossRef](#)]
102. Li, B.; Wang, Y.; Singh, A.; Vorobeychik, Y. Data poisoning attacks on factorization-based collaborative filtering. *Adv. Neural Inf. Process. Syst.* **2016**, *29*.
103. Mothukuri, V.; Parizi, R.M.; Pouriyeh, S.; Huang, Y.; Dehghantanha, A.; Srivastava, G. A survey on security and privacy of federated learning. *Future Gener. Comput. Syst.* **2021**, *115*, 619–640.
104. Bagdasaryan, E.; Veit, A.; Hua, Y.; Estrin, D.; Shmatikov, V. How to backdoor federated learning. In Proceedings of the International Conference on Artificial Intelligence and Statistics, PMLR, Palermo, Italy, 26–28 August 2020; pp. 2938–2948.
105. Blanchard, P.; El Mhamdi, E.M.; Guerraoui, R.; Stainer, J. Machine learning with adversaries: Byzantine tolerant gradient descent. *Adv. Neural Inf. Process. Syst.* **2017**, *30*.
106. Wagner, I.; Eckhoff, D. Technical privacy metrics: A systematic survey. *ACM Comput. Surv. (Csur)* **2018**, *51*, 1–38.
107. Hardy, S.; Henecka, W.; Ivey-Law, H.; Nock, R.; Patrini, G.; Smith, G.; Thorne, B. Private federated learning on vertically partitioned data via entity resolution and additively homomorphic encryption. *arXiv* **2017**, arXiv:1711.10677.
108. Pfützner, B.; Steckhan, N.; Arnrich, B. Federated learning in a medical context: A systematic literature review. *ACM Trans. Internet Technol. (TOIT)* **2021**, *21*, 1–31.
109. Gu, X.; Sabrina, F.; Fan, Z.; Sohail, S. A review of privacy enhancement methods for federated learning in healthcare systems. *Int. J. Environ. Res. Public Health* **2023**, *20*, 6539. [[CrossRef](#)]
110. Ali, M.; Karimipour, H.; Tariq, M. Integration of blockchain and federated learning for Internet of Things: Recent advances and future challenges. *Comput. Secur.* **2021**, *108*, 102355.
111. Qu, Y.; Uddin, M.P.; Gan, C.; Xiang, Y.; Gao, L.; Yearwood, J. Blockchain-enabled federated learning: A survey. *ACM Comput. Surv.* **2022**, *55*, 1–35.

112. Chang, Y.; Fang, C.; Sun, W. A blockchain-based federated learning method for smart healthcare. *Comput. Intell. Neurosci.* **2021**, *2021*, 4376418.
113. Issa, W.; Moustafa, N.; Turnbull, B.; Sohrabi, N.; Tari, Z. Blockchain-based federated learning for securing internet of things: A comprehensive survey. *ACM Comput. Surv.* **2023**, *55*, 1–43.
114. Weinger, B.; Kim, J.; Sim, A.; Nakashima, M.; Moustafa, N.; Wu, K.J. Enhancing IoT anomaly detection performance for federated learning. *Digit. Commun. Netw.* **2022**, *8*, 314–323.
115. Jithish, J.; Alangot, B.; Mahalingam, N.; Yeo, K.S. Distributed Anomaly Detection in Smart Grids: A Federated Learning-Based Approach. *IEEE Access* **2023**, *11*, 7157–7179.
116. Mothukuri, V.; Khare, P.; Parizi, R.M.; Pouriyeh, S.; Dehghantanha, A.; Srivastava, G. Federated-learning-based anomaly detection for IoT security attacks. *IEEE Internet Things J.* **2021**, *9*, 2545–2554.
117. Shrestha, R.; Mohammadi, M.; Sinaei, S.; Salcines, A.; Pampliega, D.; Clemente, R.; Sanz, A.L.; Nowroozi, E.; Lindgren, A. Anomaly detection based on lstm and autoencoders using federated learning in smart electric grid. *J. Parallel Distrib. Comput.* **2024**, *193*, 104951.
118. Zhang, Y.; Suleiman, B.; Alibasa, M.J.; Farid, F. Privacy-Aware Anomaly Detection in IoT Environments using FedGroup: A Group-Based Federated Learning Approach. *J. Netw. Syst. Manag.* **2024**, *32*, 20.
119. Salim, M.M.; Camacho, D.; Park, J.H. Digital Twin and federated learning enabled cyberthreat detection system for IoT networks. *Future Gener. Comput. Syst.* **2024**, *161*, 701–713.
120. Bukhari, S.M.S.; Zafar, M.H.; Abou Houran, M.; Qadir, Z.; Moosavi, S.K.R.; Sanfilippo, F. Enhancing cybersecurity in Edge IIoT networks: An asynchronous federated learning approach with a deep hybrid detection model. *Internet Things* **2024**, *27*, 101252.
121. Klepeis, N.E.; Nelson, W.C.; Ott, W.R.; Robinson, J.P.; Tsang, A.M.; Switzer, P.; Behar, J.V.; Hern, S.C.; Engelmann, W.H. The National Human Activity Pattern Survey (NHAPS): A resource for assessing exposure to environmental pollutants. *J. Expo. Sci. Environ. Epidemiol.* **2001**, *11*, 231–252.
122. Khalil, M.; Esseghir, M.; Merghem-Boulahia, L. A federated learning approach for thermal comfort management. *Adv. Eng. Inform.* **2022**, *52*, 101526. [\[CrossRef\]](#)
123. Khalil, M.; Esseghir, M.; Merghem-Boulahia, L. Federated learning for energy-efficient thermal comfort control service in smart buildings. In Proceedings of the 2021 IEEE Global Communications Conference (GLOBECOM), Madrid, Spain, 7–11 December 2021; pp. 01–06.
124. Moradzadeh, A.; Moayyed, H.; Mohammadi-Ivatloo, B.; Aguiar, A.P.; Anvari-Moghaddam, A. A secure federated deep learning-based approach for heating load demand forecasting in building environment. *IEEE Access* **2021**, *10*, 5037–5050. [\[CrossRef\]](#)
125. Perry, R.; Fallon, E. A federated learning system for optimised environmental control of consecutive areas. In Proceedings of the International Conferences, ICT, Society and Human Beings 2019, Connected Smart Cities 2019, Web Based Communities and Social Media 2019, IADIS, Porto, Portugal, 16–19 July 2019.
126. Wang, X.; Yan, K. Fault Detection and Diagnosis of HVAC System Based on Federated Learning. In Proceedings of the 2022 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech), Falerna, Italy, 12–15 September 2022; pp. 1–8.
127. Khanal, S.; Ho, N.; Pedersen, T.B. FDA-HeatFlex: Scalable Privacy-Preserving Temperature and Flexibility Prediction for Heat Pumps using Federated Domain Adaptation. In Proceedings of the 14th ACM International Conference on Future Energy Systems, Orlando, FL, USA, 20–23 June 2023; pp. 172–183.
128. IEA. *Buildings—Energy System*; IEA: Paris, France, 2023.
129. Tang, L.; Xie, H.; Wang, X.; Bie, Z. Privacy-preserving knowledge sharing for few-shot building energy prediction: A federated learning approach. *Appl. Energy* **2023**, *337*, 120860.
130. Savi, M.; Olivadese, F. Short-term energy consumption forecasting at the edge: A federated learning approach. *IEEE Access* **2021**, *9*, 95949–95969.
131. Badr, M.M.; Mahmoud, M.; Fang, Y.; Abdulaal, M.; Aljohani, A.J.; Alasmay, W.; Ibrahim, M.I. Privacy-preserving and communication-efficient energy prediction scheme based on federated learning for smart grids. *IEEE Internet Things J.* **2023**, *10*, 7719–7736.
132. Wang, R.; Yun, H.; Rayhana, R.; Bin, J.; Zhang, C.; Herrera, O.E.; Liu, Z.; Mérida, W. An adaptive federated learning system for community building energy load forecasting and anomaly prediction. *Energy Build.* **2023**, *295*, 113215.
133. Khalil, M.; Esseghir, M.; Boulahia, L.M. Privacy-Preserving federated learning: An application for big data load forecast in buildings. *Comput. Secur.* **2023**, *131*, 103211. [\[CrossRef\]](#)
134. Al-Quraan, M.; Khan, A.; Centeno, A.; Zoha, A.; Imran, M.A.; Mohjazi, L. FedraTrees: A novel computation-communication efficient federated learning framework investigated in smart grids. *Eng. Appl. Artif. Intell.* **2023**, *124*, 106654.
135. Petrangeli, E.; Tonello, N.; Vallati, C. Performance evaluation of federated learning for residential energy forecasting. *IoT* **2022**, *3*, 381–397. [\[CrossRef\]](#)

136. Mendes, N.; Mendes, J.; Mohammadi, J.; Moura, P. Federated learning framework for prediction of net energy demand in transactive energy communities. *Sustain. Energy Grids Netw.* **2024**, *40*, 101522.
137. Dwivedi, R.; Mehrotra, D.; Chandra, S. Potential of Internet of Medical Things (IoMT) applications in building a smart healthcare system: A systematic review. *J. Oral Biol. Craniofacial Res.* **2022**, *12*, 302–318.
138. Manickam, P.; Mariappan, S.A.; Murugesan, S.M.; Hansda, S.; Kaushik, A.; Shinde, R.; Thipperudraswamy, S. Artificial intelligence (AI) and internet of medical things (IoMT) assisted biomedical systems for intelligent healthcare. *Biosensors* **2022**, *12*, 562. [[CrossRef](#)] [[PubMed](#)]
139. Li, J.; Meng, Y.; Ma, L.; Du, S.; Zhu, H.; Pei, Q.; Shen, X. A federated learning based privacy-preserving smart healthcare system. *IEEE Trans. Ind. Inform.* **2021**, *18*.
140. Cai, X.; Lan, Y.; Zhang, Z.; Wen, J.; Cui, Z.; Zhang, W. A many-objective optimization based federal deep generation model for enhancing data processing capability in IoT. *IEEE Trans. Ind. Inform.* **2021**, *19*, 561–569.
141. Elayan, H.; Aloqaily, M.; Guizani, M. Sustainability of healthcare data analysis IoT-based systems using deep federated learning. *IEEE Internet Things J.* **2021**, *9*, 7338–7346.
142. Rajagopal, S.M.; Supriya, M.; Buyya, R. FedSDM: Federated learning based smart decision making module for ECG data in IoT integrated Edge-Fog-Cloud computing environments. *Internet Things* **2023**, *22*, 100784.
143. Raza, A.; Tran, K.P.; Koehl, L.; Li, S. Designing ecg monitoring healthcare system with federated transfer learning and explainable ai. *Knowl.-Based Syst.* **2022**, *236*, 107763.
144. Qayyum, A.; Ahmad, K.; Ahsan, M.A.; Al-Fuqaha, A.; Qadir, J. Collaborative federated learning for healthcare: Multi-modal COVID-19 diagnosis at the edge. *IEEE Open J. Comput. Soc.* **2022**, *3*, 172–184.
145. Ying, Z.; Zhang, G.; Pan, Z.; Chu, C.; Liu, X. FedECG: A federated semi-supervised learning framework for electrocardiogram abnormalities prediction. *J. King Saud-Univ.-Comput. Inf. Sci.* **2023**, *35*, 101568.
146. Rehman, A.; Xing, H.; Feng, L.; Hussain, M.; Gulzar, N.; Khan, M.A.; Hussain, A.; Saeed, D. FedCSCD-GAN: A secure and collaborative framework for clinical cancer diagnosis via optimized federated learning and GAN. *Biomed. Signal Process. Control.* **2024**, *89*, 105893.
147. Chorney, W.; Wang, H. Towards federated transfer learning in electrocardiogram signal analysis. *Comput. Biol. Med.* **2024**, *170*, 107984.
148. Dayakaran, D.; Kadiresan, N. Federated Learning Framework for Human Activity Recognition Using Smartphones. *Procedia Comput. Sci.* **2024**, *235*, 2069–2078.
149. Becker, S.; Styp-Rekowski, K.; Stoll, O.V.L.; Kao, O. Federated learning for autoencoder-based condition monitoring in the industrial internet of things. In Proceedings of the 2022 IEEE International Conference on Big Data (Big Data), Osaka, Japan, 17–20 December 2022; pp. 5424–5433.
150. Zhang, T.; He, C.; Ma, T.; Gao, L.; Ma, M.; Avestimehr, S. Federated learning for internet of things. In Proceedings of the 19th ACM Conference on Embedded Networked Sensor Systems, Coimbra, Portugal, 15–17 November 2021; pp. 413–419.
151. Wang, X.; Garg, S.; Lin, H.; Hu, J.; Kaddoum, G.; Piran, M.J.; Hossain, M.S. Toward accurate anomaly detection in industrial internet of things using hierarchical federated learning. *IEEE Internet Things J.* **2021**, *9*, 7110–7119.
152. Tripathy, S.S.; Beborrtta, S.; Chowdhary, C.L.; Mukherjee, T.; Kim, S.; Shafi, J.; Ijaz, M.F. FedHealthFog: A federated learning-enabled approach towards healthcare analytics over fog computing platform. *Heliyon* **2024**, *10*, e26416. [[PubMed](#)]
153. Alsamhi, S.H.; Myrzashova, R.; Hawbani, A.; Kumar, S.; Srivastava, S.; Zhao, L.; Wei, X.; Guizan, M.; Curry, E. Federated learning meets blockchain in decentralized data-sharing: Healthcare use case. *IEEE Internet Things J.* **2024**, *11*, 19602–19615.
154. Annappa, B.; Hegde, S.; Abhijit, C.S.; Ambesange, S. Fedcure: A heterogeneity-aware personalized federated learning framework for intelligent healthcare applications in iomt environments. *IEEE Access* **2024**, *12*, 15867–15883.
155. Berkani, M.R.A.; Chouchane, A.; El Ouanas Belabbaci, A.O. FedWell: A Federated Framework for Privacy-Preserving Occupant Stress Monitoring in Smart Buildings. *Preprints* **2024**. [[CrossRef](#)]
156. Khan, M.A.; Farooq, M.S.; Saleem, M.; Shahzad, T.; Ahmad, M.; Abbas, S.; Abu-Mahfouz, A.M. Smart buildings: Federated learning-driven secure, transparent and smart energy management system using XAI. *Energy Rep.* **2025**, *13*, 2066–2081.
157. Berkani, M.R.A.; Chouchane, A.; Himeur, Y.; Abdennebi, A.; Sagiroglu, S.; Amira, A. Federated Learning-Based Intelligent Indoor Smoke and Fire Detection System for Smart Buildings. In Proceedings of the 2024 International Conference on Telecommunications and Intelligent Systems (ICTIS), Djelfa, Algeria, 14–15 December 2024; pp. 1–7.
158. Gadekallu, T.R.; Pham, Q.V.; Huynh-The, T.; Bhattacharya, S.; Maddikunta, P.K.R.; Liyanage, M. Federated learning for big data: A survey on opportunities, applications, and future directions. *arXiv* **2021**, arXiv:2110.04160.
159. Rasha, A.H.; Li, T.; Huang, W.; Gu, J.; Li, C. Federated learning in smart cities: Privacy and security survey. *Inf. Sci.* **2023**, *632*, 833–857.
160. Bharati, S.; Mondal, M.; Podder, P.; Prasath, V. Federated learning: Applications, challenges and future directions. *Int. J. Hybrid Intell. Syst.* **2022**, *18*, 19–35.
161. Liang, K.; Zhong, H.; Chen, H.; Wu, Y. Wyner-Ziv gradient compression for federated learning. *arXiv* **2021**, arXiv:2111.08277.

162. Albasyoni, A.; Safaryan, M.; Condat, L.; Richtárik, P. Optimal gradient compression for distributed and federated learning. *arXiv* **2020**, arXiv:2010.03246.
163. Dirir, A.; Salah, K.; Svetinovic, D.; Jayaraman, R.; Yaqoob, I.; Kanhere, S.S. Blockchain-based decentralized federated learning. In Proceedings of the 2022 Fourth International Conference on Blockchain Computing and Applications (BCCA), San Antonio, TX, USA, 5–7 September 2022; pp. 99–106.
164. Sun, H.; Ma, X.; Hu, R.Q. Adaptive federated learning with gradient compression in uplink NOMA. *IEEE Trans. Veh. Technol.* **2020**, *69*, 16325–16329. [\[CrossRef\]](#)
165. Wang, Z.; Zhang, Z.; Tian, Y.; Yang, Q.; Shan, H.; Wang, W.; Quek, T.Q. Asynchronous federated learning over wireless communication networks. *IEEE Trans. Wirel. Commun.* **2022**, *21*, 6961–6978.
166. Hu, K.; Xiang, L.; Tang, P.; Qiu, W. Feature norm regularized federated learning: Utilizing data disparities for model performance gains. In Proceedings of the Thirty-Third International Joint Conference on Artificial Intelligence, Jeju, Republic of Korea, 3–9 August 2024; pp. 4136–4146.
167. Yu, X.; He, Z.; Sun, Y.; Xue, L.; Li, R. The Effect of Personalization in FedProx: A Fine-grained Analysis on Statistical Accuracy and Communication Efficiency. *arXiv* **2024**, arXiv:2410.08934.
168. Hanzely, F.; Hanzely, S.; Horváth, S.; Richtárik, P. Lower bounds and optimal algorithms for personalized federated learning. *Adv. Neural Inf. Process. Syst.* **2020**, *33*, 2304–2315.
169. Huang, T.; Shen, L.; Sun, Y.; Lin, W.; Tao, D. Fusion of global and local knowledge for personalized federated learning. *arXiv* **2023**, arXiv:2302.11051.
170. Zhang, K.; Fan, X.; Qi, J.; Jin, H.; Yang, P.; Shen, S.; Wang, C. FedGS: Federated Graph-based Sampling with Arbitrary Client Availability. *arXiv* **2022**, arXiv:2211.13975.
171. Siomos, V.; Siomos, V.; Naval-Marimont, S.; Passerat-Palmbach, J.; Tarroni, G. Addressing Data Heterogeneity in Federated Learning with Adaptive Normalization-Free Feature Recalibration. *arXiv* **2024**, arXiv:2410.02006.
172. Chen, H.; Wang, H.; Long, Q.; Jin, D.; Li, Y. Advancements in federated learning: Models, methods, and privacy. *ACM Comput. Surv.* **2024**, *57*, 1–39.
173. Sattler, F.; Muller, K.R.; Samek, W. Clustered federated learning: Model-agnostic distributed multitask optimization under privacy constraints. *IEEE Trans. Neural Netw. Learn. Syst.* **2020**, *32*, 3710–3722. [\[CrossRef\]](#) [\[PubMed\]](#)
174. Wang, Y.; Wang, Q.; Zhao, L.; Wang, C. Differential privacy in deep learning: Privacy and beyond. *Future Gener. Comput. Syst.* **2023**, *148*, 408–424. [\[CrossRef\]](#)
175. Mammen, P.M. Federated learning: Opportunities and challenges. *arXiv* **2021**, arXiv:2101.05428.
176. Yang, Z.; Chen, M.; Wong, K.K.; Poor, H.V.; Cui, S. Federated learning for 6G: Applications, challenges, and opportunities. *Engineering* **2022**, *8*, 33–41. [\[CrossRef\]](#)
177. Wen, J.; Zhang, Z.; Lan, Y.; Cui, Z.; Cai, J.; Zhang, W. A survey on federated learning: Challenges and applications. *Int. J. Mach. Learn. Cybern.* **2023**, *14*, 513–535. [\[CrossRef\]](#)
178. Ramu, S.P.; Boopalan, P.; Pham, Q.V.; Maddikunta, P.K.R.; Huynh-The, T.; Alazab, M.; Nguyen, T.T.; Gadekallu, T.R. Federated learning enabled digital twins for smart cities: Concepts, recent advances, and future directions. *Sustain. Cities Soc.* **2022**, *79*, 103663. [\[CrossRef\]](#)
179. Mihai, S.; Yaqoob, M.; Hung, D.V.; Davis, W.; Towakel, P.; Raza, M.; Karamanoglu, M.; Barn, B.; Shetve, D.; Prasad, R.V.; et al. Digital twins: A survey on enabling technologies, challenges, trends and future prospects. *IEEE Commun. Surv. Tutorials* **2022**, *24*, 2255–2291. [\[CrossRef\]](#)
180. Jamil, S.; Rahman, M.; Fawad. A comprehensive survey of digital twins and federated learning for industrial internet of things (IIoT), internet of vehicles (IoV) and internet of drones (IoD). *Appl. Syst. Innov.* **2022**, *5*, 56. [\[CrossRef\]](#)

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.