



## Review

# Federated Learning for IoT: A Survey of Techniques, Challenges, and Applications

Elias Dritsas \*  and Maria Trigka 

Industrial Systems Institute (ISI), Athena Research and Innovation Center, 26504 Patras, Greece; trigka@isi.gr

\* Correspondence: dritsas@isi.gr

**Abstract:** Federated Learning (FL) has emerged as a pivotal approach for decentralized Machine Learning (ML), addressing the unique demands of the Internet of Things (IoT) environments where data privacy, bandwidth constraints, and device heterogeneity are paramount. This survey provides a comprehensive overview of FL, focusing on its integration with the IoT. We delve into the motivations behind adopting FL for IoT, the underlying techniques that facilitate this integration, the unique challenges posed by IoT environments, and the diverse range of applications where FL is making an impact. Finally, this submission also outlines future research directions and open issues, aiming to provide a detailed roadmap for advancing FL in IoT settings.

**Keywords:** federated learning; Internet of Things; machine learning; privacy-preserving; communication efficiency

## 1. Introduction

The advent of the IoT has essentially transformed the landscape of data generation, leading to a massive influx of data from billions of interconnected devices. These devices, ranging from sensors in smart cities to wearable health monitors, continuously generate vast amounts of data that hold significant potential for ML applications. However, traditional centralized ML approaches face inherent limitations in IoT environments, primarily due to the need for data centralization, which raises concerns over privacy, security, and data sovereignty. Moreover, the bandwidth and latency constraints in IoT networks further exacerbate these challenges, making it impractical to transfer all data to a central location for processing [1–3].

FL has emerged as a viable alternative to centralized ML, offering a decentralized approach that is particularly well-suited to the distributed and heterogeneous nature of IoT systems. In FL, the training process is distributed across multiple devices, allowing each device to update a local model independently using its own data. These local updates are then aggregated at a central server to form a global model without sharing raw data between devices [4]. This paradigm addresses privacy and security concerns by keeping data localized and significantly reduces the communication overhead associated with data transfer, making it an attractive solution for IoT applications [5,6].

The integration of FL into IoT systems is motivated by several key factors [7]. First, the heterogeneity of IoT devices, in terms of both hardware capabilities and data characteristics, necessitates a flexible learning framework that can adapt to varying conditions. FL inherently supports such flexibility by allowing devices to participate in the learning process according to their capabilities, making it possible to include a wide range of devices in the model training process. Second, the decentralized nature of FL aligns with the need



Academic Editor: Stefan Fischer

Received: 28 August 2024

Revised: 9 January 2025

Accepted: 19 January 2025

Published: 22 January 2025

**Citation:** Dritsas, E.; Trigka, M. Federated Learning for IoT: A Survey of Techniques, Challenges, and Applications. *J. Sens. Actuator Netw.* **2025**, *14*, 9. <https://doi.org/10.3390/jsan14010009>

**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/>).

for data sovereignty, particularly in scenarios where data are sensitive or subject to regulatory constraints. By enabling local model training, FL ensures that data remains under the control of the data owner, thus adhering to principles of data minimization and privacy by design [8–10].

Furthermore, the non-IID (Independent and Identically Distributed) nature of data in IoT environments presents a unique challenge for traditional ML algorithms, which typically assume that data are identically distributed across all nodes. In contrast, FL is inherently designed to handle such non-IID data distributions, as it allows each device to contribute updates based on its own data, thereby capturing the diverse characteristics of the underlying data sources. This capability is particularly important in IoT scenarios, where data from different devices can vary significantly due to factors such as location, usage patterns, and device-specific characteristics [11–13].

The potential of FL in IoT is not just theoretical; it has already begun to make an impact across various application domains. In healthcare, FL enables the development of predictive models using data from wearable devices, ensuring patient privacy while leveraging the collective intelligence of multiple data sources. In smart cities, FL can optimize traffic management systems by analyzing data from a network of sensors without compromising individual privacy. Similarly, in industrial IoT (IIoT), FL facilitates predictive maintenance by allowing machines to collaboratively learn from operational data, enhancing the accuracy of fault detection while maintaining data confidentiality [14–16].

This survey differentiates itself from the existing surveys summarized in Table 1 by addressing a unique confluence of challenges and applications within FL for IoT. Unlike prior works that primarily focus on specific aspects such as privacy, resource constraints, or integration with blockchain, this survey provides a holistic perspective, bridging gaps between foundational FL techniques and their tailored adaptations for IoT environments. It emphasizes emerging challenges like handling dynamic IoT networks, energy efficiency, and ensuring robust scalability while also exploring diverse applications ranging from healthcare to smart cities and industrial automation. Moreover, the survey offers a forward-looking analysis by identifying open issues and proposing actionable research directions, positioning it as a comprehensive resource for advancing FL's adoption in IoT ecosystems. This depth and breadth of analysis set the survey apart as a critical contribution to the field. More specifically, the primary contributions of this survey are as follows:

- Offers an in-depth analysis of FL techniques specifically tailored for IoT, addressing the unique demands of decentralized learning in heterogeneous environments.
- It systematically identifies the critical challenges in deploying FL in the IoT, including communication overhead, device heterogeneity, and privacy concerns.
- Examines diverse application domains, such as healthcare and smart cities, showcasing how FL enhances IoT applications while ensuring data privacy.
- It highlights key open issues and proposes future research directions, focusing on efficient communication, enhanced privacy techniques, and scalable FL architectures for IoT.

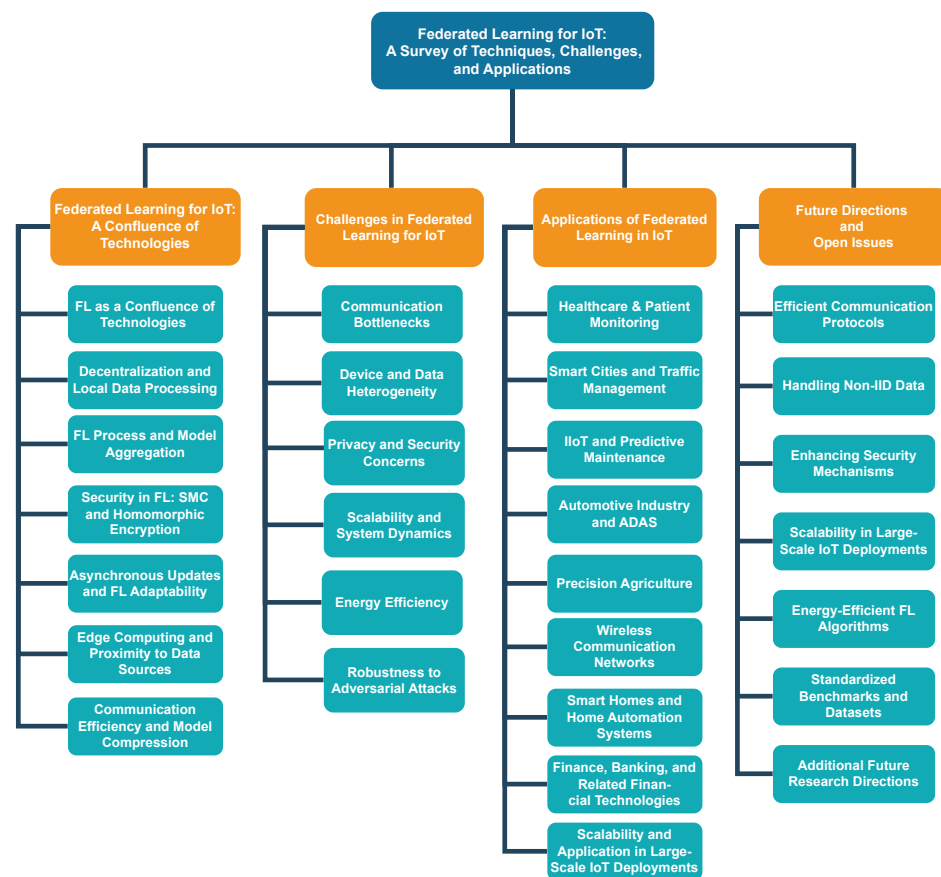
**Table 1.** Descriptive summary of surveys related to FL aspects in the IoT domain.

| Survey | Description  |
|--------|--|
| [17]   | Discusses the potential of FL for IoT applications, addressing challenges like data privacy, scalability, and distributed computing while proposing FL as a decentralized solution to enable smart IoT systems with privacy-preserving capabilities. |

**Table 1.** *Cont.*

| Survey | Description   |
|--------|---|
| [18]   | Explores FL for resource-constrained IoT devices, emphasizing the challenges like low computational power and high energy consumption. Discusses strategies to optimize FL for IoT devices with limited resources while maintaining privacy and security.   |
| [19]   | Surveys FL in IoT contexts, analyzing its use in applications like smart healthcare and transportation. Highlights challenges like heterogeneity, communication costs, and privacy risks in FL deployments. Provides insights into the integration of FL with IoT for privacy-enhanced artificial intelligence (AI).  |
| [20]   | Discusses the challenges of implementing FL in IoT platforms, including resource constraints, data heterogeneity, and privacy concerns. Highlights opportunities for FL to enhance IoT security, scalability, and model performance.  |
| [21]   | Explores blockchain-integrated FL for IoT applications, focusing on enhanced security and privacy through decentralization. Discusses application areas like industrial IoT, healthcare, and vehicular networks while addressing challenges such as compatibility and efficiency.   |
| [22]   | Examines advancements in FL and deep learning (DL) for IoT security, addressing privacy concerns, computational overhead, and vulnerabilities in centralized systems. Advocates for FL's potential in overcoming IoT security challenges while maintaining data privacy.  |
| [23]   | Highlights challenges and solutions in ensuring trustworthiness in FL systems. Discusses pillars like security, robustness, and privacy alongside practical implementation strategies for FL in sensitive fields such as healthcare and finance.  |
| [24]   | Proposes a comprehensive taxonomy for Trustworthy FL, focusing on interpretability, fairness, and privacy. Discusses vulnerabilities in FL processes and solutions for building reliable and secure FL systems.   |
| [25]   | Discusses client/server-related security and privacy issues on local and central servers, FL-related attacks in IoT and security measures, the available security measures (cryptographic and non-cryptographic), and FL-related vulnerabilities in the IoT domain and countermeasures to mitigate them. Proposes a framework, suggestions, recommendations, and the lessons learned.   |
| [26]   | Explores basics in FL, types of FL (horizontal, vertical, (de)centralized, cross-silo, cross-device), types of attacks in FL (data, model, privacy), FL defence strategies (pre/in/post-aggregation), defence frameworks against data and model attacks (e.g., blockchain, adversarial training, model pruning) and defences against privacy attacks (e.g., differential privacy (DP), homomorphic encryption (HE)). Also, it discusses the challenges and future directions. |
| [27]   | Focuses on combining blockchain with FL to address issues like trust, security, and efficiency in IoT systems. Highlights challenges such as overhead and compatibility while providing case studies on IoT applications like smart transportation and personal IoT.  |

The remaining paper is illustrated in Figure 1 and structured as follows. Section 2 describes the technologies of FL on IoT. Next, Section 3 analyzes the challenges in FL for IoT. Section 4 refers to applications of FL in the IoT. Moreover, Section 5 discusses future directions and open Issues. Finally, Section 6 summarizes the findings of this survey.



**Figure 1.** An illustrative diagram of the paper’s structure.

## 2. Federated Learning for IoT: A Confluence of Technologies

As IoT devices generate vast amounts of decentralized, sensitive data, FL offers a scalable, privacy-preserving solution by enabling local training and global model aggregation without transferring raw data. To adapt to the diverse demands of IoT, FL encompasses various types based on data partitioning, system architecture, and operational strategies [25,26]. These classifications (as picturized and detailed in Figure 2) reflect its flexibility in addressing challenges such as data heterogeneity, privacy preservation, resource constraints, and scalability, ensuring robust and efficient model training across diverse IoT applications.

FL stands at the intersection of advanced distributed computing, edge AI, and secure data processing, making it uniquely suited for complex and resource-constrained environments in IoT. This synergy between FL and IoT addresses several key technical challenges while unlocking new opportunities for decentralized intelligence [28–30].

At the heart of this confluence is the ability of FL to harness the computational power of edge devices—ranging from sensors and smart meters to more sophisticated devices like smartphones and autonomous vehicles—without centralizing data. This decentralization is crucial in IoT environments where data are abundant and sensitive. By keeping data on the local devices where they are generated, FL mitigates the risk of data breaches and reduces the latency associated with transferring large volumes of data to a central server for processing. This approach also aligns with regulatory frameworks like the General Data Protection Regulation (GDPR), which impose strict controls on data transfer and storage, making FL not just a technical solution but a compliance enabler [31–33].

## Types of FL

| Data Partitioning  | System Architecture   |
|--|---|
| <p><b>Horizontal FL:</b> Data across participants share similar features but belong to different users. This approach is suitable for scenarios like healthcare, where datasets have similar structures but different owners.</p> <p><b>Vertical FL:</b> Participants share the same users but have different features, common in cross-domain collaborations such as between banks and e-commerce platforms.</p> <p><b>Federated Transfer Learning:</b> Useful when participants have little overlap in both data features and users. This approach leverages transfer learning to bridge these gaps and improve model performance.</p> <p><b>Split FL:</b> It is a hybrid approach that combines horizontal and vertical data partitioning by splitting the model across client devices and central servers. Local training handles horizontally partitioned data (similar features, different users) while the server processes complementary vertical data (different features, same users) or aggregated outputs.</p> | <p><b>Centralized FL:</b> A central server orchestrates the process, collecting and aggregating model updates from client devices.</p> <p><b>Decentralized FL:</b> Eliminates the need for a central server, allowing devices to collaborate directly. This approach enhances resilience to single-point failures.</p> <p><b>Hierarchical FL:</b> Introduces intermediate aggregation layers at edge nodes (e.g., gateways) before updates are sent to the central server. This hierarchical structure improves scalability and reduces communication overhead, making it suitable for large-scale IoT deployments.</p> |
|  | Operational Strategies  |
|  | <p><b>Cross-Silo FL:</b> Designed for a small number of reliable and resourceful clients, such as institutions or organizations, which often have consistent participation in training.</p> <p><b>Cross-Device FL:</b> Involves a large number of resource-constrained and unreliable devices, such as smartphones or IoT devices, contributing to a global model.</p>  |

**Figure 2.** Types of FL based on data partitioning, system architecture, and operational strategies.

FL involves multiple phases, each optimized for the IoT landscape. Initially, the central server distributes a global model to all participating devices. These devices then perform local training using their data, which is inherently reflective of their unique operational environments. For instance, in a smart home system, each device might generate data influenced by its specific location, user behaviour, and usage patterns. The local models are then updated and only these updates, typically in the form of model gradients or weights, are transmitted back to the central server. This server aggregates the updates to refine the global model. This cyclical process continues until the global model converges, effectively enabling collective intelligence without requiring raw data sharing [34–36].

Moreover, the implementation of FL in IoT leverages the concept of edge computing, where computation is performed close to the data source. This proximity reduces the dependency on cloud infrastructure, thereby alleviating network congestion and ensuring real-time processing capabilities, which are critical in applications like autonomous driving or industrial automation. The use of edge devices in FL also allows for scalability in IoT networks, enabling millions of devices to participate in the learning process without overwhelming central servers [37–39].

The integration of FL with IoT is further bolstered by advances in communication technologies. Techniques such as model compression and sparse updates reduce the communication overhead, making FL feasible even in bandwidth-constrained IoT environments. Additionally, protocols like Federated Averaging (FedAvg) have been refined to efficiently aggregate model updates from a large number of devices while accounting for the varying quality and quantity of local data. This ensures that the global model remains robust and accurate despite the heterogeneous nature of IoT data [40–42].

Furthermore, FL for IoT is increasingly incorporating secure multiparty computation (SMPC) and HE techniques to enhance the security of model updates during transmission. These techniques ensure that even if the model updates are intercepted, the underlying data remains protected, thereby addressing one of the most significant security concerns in distributed learning [43–45].

Finally, the adaptability of FL algorithms to the dynamic nature of IoT networks—where devices frequently join and leave the network—ensures that learning can continue uninterrupted. This adaptability is crucial in IoT, where devices are often mobile, such as in vehicular networks, or subject to power constraints, as in sensor networks. By allow-

ing for asynchronous updates and flexible participation, FL accommodates the inherent volatility of IoT networks, ensuring that even transient data contributions are harnessed effectively [46–48].

This section highlights the strength of FL in addressing data privacy and communication latency challenges. However, it also reveals the inherent trade-off between scalability and the computational burden imposed on edge devices. The decentralization model ensures regulatory compliance but necessitates further advancements in efficient model aggregation techniques to cater to resource-constrained IoT settings. In Table 2, we briefly list the technologies leveraged for using FL in IoT.

**Table 2.** A summary of the technologies in the synergy of FL with IoT.

| Topic  | References | Description   |
|--|------------|---|
| FL as a Confluence of Technologies             | [28–30]    | Discusses the intersection of FL with advanced distributed computing, edge AI, and secure data processing, highlighting how FL is suited for IoT.                           |
| Decentralization and Local Data Processing     | [31–33]    | Explores the benefits of keeping data on local devices to mitigate risks of data breaches and reduce latency, which aligns with regulatory frameworks like GDPR.            |
| FL Process and Model Aggregation               | [34–36]    | Describes the FL process where a global model is distributed to devices, local training is conducted, and updates are aggregated to refine the global model.                |
| Edge Computing and Proximity to Data Sources   | [37–39]    | Examines the implementation of FL in IoT, leveraging edge computing to reduce dependency on cloud infrastructure and improve real-time processing.                          |
| Communication Efficiency and Model Compression | [40–42]    | Focuses on techniques like model compression and sparse updates to reduce communication overhead, making FL feasible in bandwidth-constrained IoT environments.             |
| Security in FL: SMPC and HE                    | [43–45]    | Address the incorporation of SMPC and HE in FL to enhance the security of model updates during transmission.  |
| Asynchronous Updates and FL Adaptability       | [46–48]    | Discusses the adaptability of FL algorithms to the dynamic nature of IoT networks, including asynchronous updates and hierarchical learning to accommodate network changes. |

### 3. Challenges in Federated Learning for IoT

The deployment of FL in IoT environments presents a set of complex challenges, rooted in the unique characteristics of IoT networks. These challenges extend beyond the conventional issues faced in centralized ML, requiring tailored approaches that consider the decentralized, resource-constrained, and dynamic nature of IoT systems. The following sections provide a deeper exploration of these challenges, highlighting the specific hurdles and the ongoing research efforts aimed at overcoming them.

#### 3.1. Communication Bottlenecks

Communication in IoT networks is a critical constraint when implementing FL. Unlike traditional networks, IoT environments often operate with limited bandwidth and intermit-



tent connectivity. The process of FL involves multiple iterations of communication between the central server and a vast number of IoT devices. Each iteration requires the transmission of model updates, which, although smaller than raw data, can still be significant in size, especially when scaled across millions of devices. In dense IoT deployments, such as smart cities or large industrial environments, the cumulative communication load can saturate the network, leading to delays, packet loss, and increased energy consumption [18,49–51].

To mitigate these communication bottlenecks, research has focused on various strategies, including model compression techniques like pruning and quantization. These methods reduce the size of the model updates that need to be transmitted, thereby decreasing the overall communication load. Additionally, techniques such as Federated Dropout, where only a subset of the model parameters is updated and communicated, can further alleviate network congestion. Another promising approach is the use of sparse communication protocols, which reduce the frequency of updates by allowing devices to communicate only when their local models have undergone significant changes. However, these techniques must be carefully balanced to ensure that the reduction in communication does not come at the expense of model accuracy or convergence speed [52–55].

Moreover, asynchronous communication protocols are gaining traction as a means to address the inherent variability in IoT networks. Unlike synchronous FL, where all devices must complete their local updates before aggregation, asynchronous FL allows devices to send updates at different times based on their network conditions and availability. This reduces the waiting time for devices with slower connectivity but introduces challenges in model consistency and aggregation. The central server must be capable of handling updates that arrive out of sync, which can complicate the aggregation process and potentially lead to model divergence if not properly managed. Therefore, ongoing research is focused on developing robust aggregation algorithms that can effectively integrate asynchronous updates while maintaining model integrity [56–59].

### 3.2. Device and Data Heterogeneity

IoT environments are characterized by a high degree of heterogeneity, both in terms of device capabilities and the nature of the data they generate. Devices in an IoT network can range from powerful edge servers with substantial computational resources to low-power sensors with minimal processing capacity. This disparity poses significant challenges for FL, expecting that all participating devices contribute to the model training process. In reality, devices with limited resources may struggle to perform even a single iteration of local training, leading to imbalances in the contributions to the global model. High-end devices might dominate the training process, skewing the model towards the data they hold, which can result in a model that does not generalize well across the network [60–63].

The heterogeneity of IoT devices also extends to the data they generate, which is often non-IID. In an IoT network, different devices are likely to observe different subsets of the overall data distribution, leading to local datasets not representative of the global data distribution. For instance, in a smart city, traffic sensors in different locations may observe vastly different traffic patterns, resulting in local models that are highly specialized to their specific context but not necessarily applicable elsewhere. This non-IID nature of data complicates the training process, as the aggregated global model might struggle to converge or exhibit poor performance when applied across the entire network [64–67].

Addressing device and data heterogeneity in FL for IoT requires innovative algorithmic solutions. One approach is the development of Personalized FL, where the global model serves as a baseline, and each device fine-tunes a local model that is better suited to its specific data. This approach, however, raises concerns about the trade-off between personalization and the overall generalizability of the model. Another strategy, often

referred to as Adaptive FL, involves the use of adaptive learning rates or dynamic aggregation techniques that weight updates based on the quality and relevance of the local data. These methods can help ensure that contributions from devices with non-IID data do not disproportionately skew the global model, thus maintaining a balance between generalization and specialization [68–72].

### 3.3. Privacy and Security Concerns

Privacy and security are paramount concerns in FL, particularly in IoT environments where devices often handle sensitive data, such as health information from wearable devices or operational data from industrial systems. While FL offers a privacy-preserving framework by keeping raw data on local devices, it does not fully eliminate the risks associated with data privacy. The model updates transmitted during the FL process, if not adequately protected, can leak sensitive information through techniques like model inversion attacks. In such attacks, an adversary could potentially reconstruct aspects of the original data by analyzing the gradients or model parameters shared by the devices [73–76].

Various cryptographic techniques are being integrated into the FL framework to enhance privacy in IoT. DP is one such technique which protects sensitive data in FL by adding noise to gradients, weights, or model parameters before they are shared with the central server, making it difficult for adversaries to infer the underlying data. The noise, sampled from distributions like Gaussian or Laplace, ensures individual data points remain indistinguishable within aggregated updates. The noise magnitude is captured by a parameter called privacy budget; a smaller budget offers stronger privacy but reduces model accuracy [26,77]. In IoT, this trade-off is critical, especially in applications like healthcare, where excessive noise can impair predictive model accuracy. Ensuring strong privacy may result in predictions or classifications that deviate significantly from true values, reducing the model's reliability.

However, the heterogeneity of devices and data in IoT environments poses significant challenges for implementing DP. Resource-constrained devices often struggle to manage the computational demands of advanced noise-scaling algorithms, and the added noise can further degrade model accuracy, particularly in non-IID data settings. These issues are amplified in scenarios where devices have limited computational or energy resources. Addressing these challenges necessitates the development of adaptive and efficient privacy-preserving techniques that balance noise addition with IoT-specific constraints, ensuring robust privacy protection without compromising model utility [25].

SMPC and HE provide robust privacy guarantees in FL by ensuring that computations occur on encrypted data, protecting sensitive information during model updates. However, their feasibility in constrained IoT environments faces significant challenges due to computational overhead and resource demands. HE involves complex mathematical operations, which significantly increase processing time and energy consumption, making it impractical for low-power devices. SMPC, requiring multiple rounds of secure communication, adds bandwidth and latency overhead, which is particularly problematic in IoT networks where devices often operate under strict power and connectivity constraints. These limitations hinder their application in latency-sensitive scenarios like industrial automation or real-time monitoring [78–80].

To mitigate these issues, lightweight HE techniques and optimized SMPC protocols have been developed to reduce computational complexity and communication overhead. Hybrid approaches, combining these methods with techniques like DP, aim to balance security and resource constraints by selectively applying stronger encryption where necessary. Additionally, resource-aware solutions, such as offloading intensive computations to



capable edge or cloud nodes, and hardware accelerators like GPUs or encryption-specific chips, offer pathways to improve feasibility in IoT environments.

The physical security of IoT devices also poses a significant challenge. Many IoT devices are deployed in unsecured or remote locations, making them vulnerable to physical tampering. An attacker could potentially compromise a device and alter its model updates, injecting malicious data into the FL process. This could lead to a corrupted global model, particularly if the attacker controls a significant number of devices. To mitigate such threats, researchers are exploring robust aggregation techniques that can identify and isolate potentially malicious updates. Byzantine-resilient algorithms, which are designed to tolerate a certain proportion of adversarial or faulty devices, are also being developed to enhance the security of FL in IoT environments [81–84].

### 3.4. Scalability and System Dynamics

Scalability is a critical issue in FL for IoT, particularly as IoT networks continue to grow in size and complexity. The challenge lies not only in managing the sheer number of devices but also in handling the dynamic nature of these networks. IoT devices frequently join and leave the network, experience changes in connectivity, or fail due to power constraints. These dynamics can disrupt the FL process, leading to inconsistent model updates and making it difficult to maintain a stable and accurate global model [85–88].

To address scalability, FL frameworks must be designed to handle large-scale networks with potentially millions of devices efficiently. This involves optimizing the communication protocols and aggregation algorithms to ensure that the system can scale without significant degradation in performance. One approach is Hierarchical FL, where devices are organized into clusters based on their geographic location, connectivity, or other factors. Each cluster performs local aggregation before sending updates to the central server, reducing the communication load and improving scalability. However, this approach introduces additional complexity in managing the clusters and ensuring that the global model remains consistent across the network [89–92].

The dynamic nature of IoT networks also requires FL systems to be adaptive and resilient. This involves developing algorithms that can dynamically adjust to changes in the network, such as devices dropping out or new devices joining. Adaptive device selection strategies, where devices are chosen for participation based on their current availability, reliability, and relevance of their data, are crucial for maintaining system stability. Additionally, techniques such as FedAvg with momentum or other adaptive aggregation methods can help smooth out the variations caused by the dynamic nature of IoT environments, ensuring that the global model converges despite the fluctuations in device participation [93–96].

### 3.5. Energy Efficiency

Energy efficiency is a critical concern in IoT, where many devices operate on limited power sources such as batteries or energy harvesting systems. The iterative nature of FL, which involves repeated rounds of local training and communication, can be particularly taxing on these devices, leading to the rapid depletion of energy reserves. This not only limits the participation of energy-constrained devices but also risks causing them to drop out of the network, which can disrupt the FL process and reduce the representativeness of the global model [97–100].

To address energy efficiency in FL for IoT, researchers are exploring various strategies to minimize the energy consumption associated with local training and communication. One approach is to use model compression techniques to create lightweight models that require fewer computational resources and, consequently, less energy to train. Techniques

such as model pruning, where unnecessary parameters are removed from the model, and knowledge distillation, where a smaller model is trained to mimic the behaviour of a larger model, are being explored to reduce the computational load on IoT devices. Additionally, adaptive training strategies, where the number of local iterations is dynamically adjusted based on the device's current energy levels, can help balance the trade-off between energy consumption and model accuracy [101–104].

On the communication side, energy-efficient protocols are being developed to reduce the power required for transmitting model updates. These include techniques such as compressing the model updates before transmission or using opportunistic communication, where devices transmit updates only when they have sufficient energy or favourable network conditions. Moreover, energy-aware scheduling algorithms, which prioritize devices with higher energy reserves for participation in the FL process, can help extend the overall lifespan of the network. However, these approaches must be carefully designed to ensure that energy savings do not come at the expense of reduced participation or biased model updates, which could undermine the overall effectiveness of the FL process [105–108].

Energy optimization in FL for IoT is crucial due to the limited power of many IoT devices. Adaptive training strategies, such as reducing local iterations or adjusting communication frequency based on energy levels, enable resource-constrained devices to participate without excessive energy drain. Techniques like model pruning and quantization reduce computational complexity and the size of model updates, ensuring energy efficiency while maintaining model performance. These approaches make FL more practical for IoT environments with stringent energy constraints [109,110].

Energy-efficient communication protocols further enhance sustainability. Sparse communication, where updates are transmitted only after significant local changes, and Federated Dropout, which updates a subset of parameters, minimize energy consumption during training. Hierarchical FL, with intermediate aggregation at edge nodes, reduces communication overhead on devices by limiting interactions with the central server. Integrating these strategies with energy-harvesting technologies, like solar or kinetic power, could sustain devices and address long-term energy challenges in FL for IoT [111–113].

### 3.6. Robustness to Adversarial Attacks

IoT networks are particularly vulnerable to adversarial attacks due to their distributed and often unsecured deployment. In the context of FL, adversarial attacks can take various forms, including data poisoning, where malicious devices send corrupted model updates with the intent of degrading the performance of the global model. The distributed nature of FL makes it challenging to detect and mitigate these attacks, as the central server relies on the assumption that the majority of devices are honest and that their updates are representative of the true data distribution [114–117].

Several strategies are being explored to enhance the robustness of FL in IoT against adversarial attacks. One approach uses robust aggregation techniques, such as Krum or median-based aggregation, to filter out outliers or malicious updates. These techniques work by analyzing the received updates from all devices and selecting the most consistent ones with the majority, effectively filtering out potentially adversarial contributions. However, these methods should be computationally efficient to be viable in IoT environments, where resources are limited [118–121].

Another critical area of research is the detection and isolation of Byzantine devices, which behave erratically or maliciously. ML-based anomaly detection techniques are being applied to identify patterns of behaviour that deviate from the norm, flagging devices that may be compromised. Once identified, these devices can be excluded from the FL process, reducing the risk of model corruption. Additionally, federated defence mechanisms, such

as federated adversarial training, are being developed to improve the resilience of the global model by training it to be robust against adversarial examples. This involves incorporating adversarially perturbed data during the training process, helping the model to learn to resist such perturbations in the future [122–125].

The previously discussed challenges in FL when this is applied to IoT are presented in Table 3. Also, a comprehensive and comparative view of the discussed FL techniques and their applicability to IoT environments is presented in Table 4. The purpose of the latter table is to evaluate key FL methods based on critical metrics, including scalability, communication efficiency, privacy preservation, robustness to attacks, energy efficiency, ability to handle non-IID data, and real-world applicability. These metrics were selected to address the unique challenges posed by IoT environments, such as device heterogeneity, limited resources, and data privacy concerns. Table 4 serves as a concise summary for researchers and practitioners to identify the most suitable FL techniques based on their specific IoT use cases. For instance, Hierarchical FL stands out for large-scale deployments, while DP FL is ideal for applications where privacy preservation is paramount. Similarly, model compression techniques like Federated Dropout and pruning-based (Pruned FL) excel in energy-constrained environments. This analysis also highlights the inherent trade-offs in each approach, such as the balance between energy efficiency and robustness to attacks or privacy preservation and communication overhead.

**Table 3.** An overview of challenges in FL for IoT.

| Topic                             | References | Description   |
|-----------------------------------|------------|---|
| Communication Bottlenecks         | [18,49–59] | Discusses challenges related to communication in FL within IoT, including bandwidth limitations, model update transmission, and strategies like model compression and sparse communication.   |
| Device and Data Heterogeneity     | [60–72]    | Explores the impact of heterogeneity in IoT devices and data on FL, addressing issues like non-IID data distribution, device capability variations, and strategies such as adaptive learning and dynamic aggregation.   |
| Privacy and Security Concerns     | [73–84]    | Focuses on privacy and security challenges in FL for IoT, covering methods like DP, HE, secure aggregation, and protection against adversarial attacks.   |
| Scalability and System Dynamics   | [85–96]    | Addresses scalability and system dynamics in FL for IoT, including hierarchical models, adaptive aggregation, and handling the dynamic nature of IoT networks where devices frequently join or leave.   |
| Energy Efficiency                 | [97–113]   | Discusses energy efficiency in FL, crucial for IoT devices with limited power resources, and examines techniques like lightweight models, energy-aware communication, and adaptive resource management. Efficient strategies reduce energy use for IoT devices in FL. Sparse updates and energy harvesting enhance FL sustainability. |
| Robustness to Adversarial Attacks | [114–125]  | Covers the robustness of FL models against adversarial attacks in IoT, including Byzantine-resilient aggregation methods, adversarial training, and the detection of compromised devices.   |

In the context of IoT environments, each method is characterized by strengths offering unique benefits and trade-offs that make them suitable for particular use cases while posing challenges and limitations in others. Below, we provide a focused analysis of key FL techniques to highlight their effectiveness in addressing IoT-specific constraints and their practical implications:

- FedAvg is a simple and widely used baseline method for FL. It offers broad applicability in general IoT deployments due to its simplicity. However, it struggles with non-IID data distributions, which can reduce model performance across diverse IoT devices.
- Asynchronous FL excels in scalability and adaptability to dynamic IoT networks where devices frequently join or leave. While it supports large-scale IoT systems, its complexity increases, and it risks model divergence due to asynchronous updates.
- Model compression techniques are effective in reducing communication and computational overhead, making them ideal for resource-constrained IoT devices. However, these methods may result in a trade-off with model accuracy, especially in scenarios requiring high precision.
- Personalized FL tailors models to the specific data and conditions of individual devices, ensuring better performance in heterogeneous IoT environments. Nonetheless, this approach may compromise the generalizability of the global model, particularly in networks with diverse data distributions.
- Blockchain enhances security and trust in FL by enabling secure collaboration in decentralized systems through its immutable ledger capabilities (cryptographic techniques, and consensus mechanism). This makes it highly suitable for privacy-sensitive IoT applications (e.g., in financial systems to enhance fraud detection while maintaining user privacy). However, it requires significant computational and energy resources, which can limit its feasibility in resource-constrained devices.

**Table 4.** Comparative analysis of FL techniques for IoT.

| Technique                | Scalability | Communication Efficiency | Privacy Preservation | Robustness to Attacks | Energy Efficiency | Handle Non-IID Data | Real-World Applicability            |
|--------------------------|-------------|--------------------------|----------------------|-----------------------|-------------------|---------------------|-------------------------------------|
| <b>FedAvg</b>            | High        | Moderate                 | Moderate             | Low                   | Moderate          | Low                 | Widely used, baseline for IoT       |
| <b>Asynchronous FL</b>   | Very High   | High                     | Moderate             | Low                   | High              | Moderate            | Suitable for dynamic IoT networks   |
| <b>DP FL</b>             | Moderate    | Moderate                 | High                 | High                  | Low               | Low                 | Effective for privacy-critical IoT  |
| <b>Hierarchical FL</b>   | Very High   | High                     | Moderate             | High                  | High              | High                | Ideal for large-scale IoT systems   |
| <b>Pruned FL</b>         | High        | Very High                | Low                  | Low                   | Very High         | Low                 | Energy-constrained IoT devices      |
| <b>Personalized FL</b>   | Moderate    | Low                      | Moderate             | Moderate              | Low               | Very High           | Useful for diverse IoT environments |
| <b>Federated Dropout</b> | High        | Very High                | Low                  | Low                   | Very High         | Low                 | Resource-limited IoT scenarios      |
| <b>Blockchain</b>        | High        | Low                      | Very High            | Very High             | Low               | Moderate            | Privacy/security-sensitive IoT      |
| <b>HE FL</b>             | Moderate    | Low                      | Very High            | Very High             | Low               | Low                 | Highly secure IoT applications      |
| <b>Adaptive FL</b>       | High        | High                     | Moderate             | Moderate              | High              | Moderate            | Dynamic IoT with varying resources  |

Addressing challenges such as communication bottlenecks and heterogeneity requires tailored solutions like model compression and adaptive aggregation. The exploration of these strategies underlines the necessity for balancing model accuracy with the operational realities of IoT environments. It also reinforces the critical role of robust algorithms to counter adversarial threats and ensure system integrity.

#### 4. Applications of Federated Learning in IoT

FL is poised to transform various IoT-driven sectors by enabling collaborative intelligence while preserving data privacy and minimizing communication overhead. One of the most compelling applications is in healthcare, where FL can be leveraged to enhance patient-monitoring systems. For instance, data from diverse wearable devices such as smartwatches and fitness trackers can be used to develop predictive models for chronic disease management, enabling real-time monitoring and personalized treatment plans without compromising patient data confidentiality. FL allows for the development of these models by aggregating insights across a wide demographic, ensuring that the models are robust and generalizable while still being tailored to individual health profiles [126–130].

In the realm of smart cities, FL can optimize traffic management systems by utilizing data from distributed sensors embedded in traffic lights, vehicles, and roads. By locally processing data and sharing only model parameters, cities can develop adaptive traffic control algorithms that reduce congestion and improve safety. Additionally, energy management within smart grids can be enhanced through FL by integrating data from distributed energy resources (DERs) like solar panels and battery storage systems. This enables predictive maintenance and demand–response strategies that optimize energy distribution and reduce outages [131–135].

IIoT is another critical domain where FL is making significant inroads. In manufacturing, FL can facilitate the creation of predictive maintenance models across a network of factories. For example, machinery equipped with sensors can locally process operational data to predict failures and share insights across the network without exposing proprietary data. This approach not only improves the accuracy of maintenance schedules but also extends equipment lifespan, reduces downtime, and optimizes operational efficiency [136–140].

In the automotive industry, FL can be utilized for developing advanced driver-assistance systems (ADAS) and autonomous vehicle technologies. Vehicles equipped with various sensors generate vast amounts of data, which can be used to improve navigation, object detection, and collision avoidance systems. FL enables these vehicles to collaboratively learn from each other's experiences, refining their algorithms while ensuring that sensitive data about routes or driving habits remain secure on each vehicle [141–145].

Agriculture is another sector where FL can drive innovation, particularly in precision farming. IoT devices such as drones, soil sensors, and weather stations collect data on crop health, soil moisture, and environmental conditions. FL allows for the aggregation of these insights to develop more accurate models for yield prediction, pest management, and irrigation scheduling. By leveraging local data, farmers can optimize inputs, reduce waste, and improve crop quality, all while keeping sensitive agricultural data secure [146–150].

In telecommunications, FL can optimize network management and service delivery. Mobile devices and base stations generate vast amounts of operational data that can be used to enhance network performance. FL enables the development of models for optimizing bandwidth allocation, reducing latency, and improving user experience by aggregating data across different network segments without the need for centralized data collection [151–155].

Finance and banking also stand to benefit from FL, particularly in fraud detection and risk management. IoT devices such as point-of-sale terminals, automated teller machines (ATMs), and mobile banking apps generate transaction data that can be locally processed to detect suspicious activities. FL allows financial institutions to share insights from these decentralized sources to improve fraud detection algorithms while keeping customer data encrypted and secure. This decentralized approach enhances security and reduces the risk of data breaches, making it an attractive solution for financial institutions operating in diverse regulatory environments [156–160].

In the context of smart homes, FL can enhance the security and efficiency of IoT-enabled devices. Smart appliances, lighting systems, and thermostats generate data that can be used to optimize energy consumption and improve user convenience. FL enables these devices to learn from each other, creating adaptive algorithms that respond to user behaviour patterns while ensuring that personal data remains private [161–165].

The application of FL in IoT spans a wide array of domains (as analyzed above and captured in Table 5), each benefiting from the cooperative training of ML models in a decentralized manner. The ability of FL to enhance model accuracy while preserving data privacy and reducing communication overhead positions it as a critical technology for the future of IoT [166–170].

**Table 5.** Summary of FL application domains in IoT.

| Topic  | References | Description   |
|--|------------|---|
| Healthcare & Patient Monitoring                            | [126–130]  | Discusses the application of FL in healthcare, particularly in patient monitoring systems, enabling predictive models without compromising privacy.   |
| Smart Cities and Traffic Management                        | [131–135]  | Explores the use of FL in optimizing traffic management systems within smart cities, focusing on adaptive control algorithms and the reduction of traffic congestion.   |
| IIoT and Predictive Maintenance                            | [136–140]  | Focuses on the application of FL in industrial IoT, specifically for predictive maintenance, enhancing operational efficiency and reducing equipment downtime.  |
| Automotive Industry and ADAS                               | [141–145]  | Discusses FL's role in the automotive industry, particularly in developing ADAS and autonomous vehicle technologies.  |
| Precision Agriculture                                      | [146–150]  | Examines the application of FL in agriculture, with a focus on improving crop management, disease detection, and yield prediction while ensuring data privacy through decentralized learning techniques.  |
| Wireless Communication Networks                            | [151–155]  | FL within wireless communication networks, particularly in the context of 6G and Mobile Edge Computing to enhance communication efficiency, manage bandwidth, and address network variability to support decentralized data processing in advanced wireless environments. |
| Finance, Banking, and Related Financial Technologies       | [156–160]  | Addresses FL in the financial sector, with a focus on enhancing security, privacy, and efficiency in processes.   |
| Smart Homes and Home Automation Systems                    | [161–165]  | FL to improve various aspects of smart home systems, including security, energy management, personalization, predictive maintenance, and overall efficiency.  |
| Scalability and Application in Large-Scale IoT Deployments | [166–170]  | Focuses on the scalability and effective deployment of FL in large and dynamic IoT environments.  |



The diverse applications across domains like healthcare, smart cities, and industrial IoT underscore FL's transformative potential. However, the variations in application-specific constraints emphasize the need for flexible frameworks that can adapt to unique data characteristics and regulatory requirements. This adaptability ensures that FL remains practical and impactful across varied IoT use cases.

## 5. Future Directions and Open Issues

The future of FL in IoT environments hinges on addressing several critical challenges that require targeted and innovative solutions. One of the foremost research directions involves the development of highly efficient communication protocols tailored specifically for the constraints of IoT networks. Given that communication overhead remains a significant bottleneck, there is an urgent need for protocols that minimize bandwidth usage while maintaining the integrity and accuracy of model updates. Techniques such as gradient compression, sparsification, and adaptive communication schedules need to be refined and rigorously tested in real-world IoT scenarios to ensure their efficacy [171–174].

Another pivotal area of research is the enhancement of FL algorithms to effectively handle non-IID data in IoT environments. Current FL models often struggle with data heterogeneity, leading to biased or suboptimal global models. Future work should focus on developing more sophisticated aggregation strategies and personalized models that can better accommodate the diversity of data across different devices. This could involve the use of meta-learning or multi-task learning frameworks, which allow models to adapt more flexibly to the varying data distributions found in IoT networks. Meta-learning addresses non-IID data challenges in FL for IoT by enabling models to adapt quickly across tasks while preserving privacy. Federated Meta-Learning (FedMeta) extends this to solve multi-task problems, improving learning performance without extensive retraining. Techniques like Model-Agnostic Meta-Learning (MAML) and its variants (e.g., Bayesian MAML and Reptile) enhance adaptability and model convergence in dynamic IoT environments. By leveraging shared patterns while allowing personalized adjustments for device-specific data, FedMeta tackles the diversity of IoT networks effectively. While computational overhead and scalability challenges persist, FedMeta holds great promise for enhancing FL's efficiency in real-world applications such as healthcare, smart cities, and predictive maintenance [175–178].

Security remains a paramount concern in the deployment of FL for IoT, particularly in light of evolving attack vectors. While DP and secure aggregation are current areas of focus, the landscape of threats is rapidly changing, necessitating continuous innovation in security mechanisms. Research into HE and federated adversarial training is crucial, as these methods offer promising avenues to enhance the robustness of FL against model inversion attacks and other sophisticated threats. Additionally, the integration of blockchain technology with FL could provide a decentralized and immutable ledger for tracking and verifying the integrity of model updates, further bolstering security in IoT applications [179–182].

The scalability of FL in IoT is another pressing issue, particularly as the number of connected devices is expected to grow exponentially. Research should prioritize the development of decentralized and hierarchical FL architectures that can efficiently manage large-scale deployments. Hierarchical FL, where model updates are aggregated at multiple levels (e.g., edge, fog, and cloud), could reduce the burden on central servers and improve the scalability of FL systems. Moreover, exploring federated optimization algorithms that can operate under the constraints of large, dynamic IoT networks is essential to ensure that FL remains viable as IoT ecosystems expand [183–186].

Energy efficiency is a crucial consideration in the design of FL for IoT due to the resource-constrained nature of many IoT devices. Future research should explore energy-

aware FL algorithms that optimize computational and communication costs. Techniques such as energy-adaptive learning rates and model pruning, which reduce the computational load on devices, are promising but require further development to be applicable across a wide range of IoT devices with varying capabilities. Additionally, hierarchical FL architectures, where intermediate aggregations occur at edge nodes, can significantly reduce communication overhead and energy consumption. Adaptive device selection and scheduling strategies based on energy availability and task priority offer another promising direction to balance energy efficiency and fairness. Moreover, integrating energy-harvesting technologies, such as solar or kinetic energy, with FL systems could help sustain energy-limited IoT devices, though challenges remain in ensuring stable and consistent contributions across heterogeneous environments [187–190].

Lastly, the lack of standardized benchmarks and datasets specific to FL in IoT presents a significant barrier to progress. To accelerate research and facilitate comparative studies, it is necessary to create benchmark datasets that accurately reflect the conditions of IoT environments, including data heterogeneity, network constraints, and device diversity. Collaborative efforts between academia and industry could lead to the development of open, standardized testing frameworks that would allow researchers to evaluate the performance, scalability, and security of their FL algorithms in more realistic IoT scenarios [191–194]. Table 6 summarizes the works surveyed for identifying key future and open issues in FL.

The future of FL in IoT is contingent on overcoming these critical challenges through targeted, innovative research. Addressing these issues will enhance the performance and security of FL systems and pave the way for their widespread adoption in diverse IoT applications. As research in this area continues to evolve, the integration of FL into IoT environments holds the potential to revolutionize how we harness the power of distributed data, enabling smarter, more secure, and more efficient IoT systems [17,195–201].

**Table 6.** Summary of future directions and open issues in FL for IoT.

| Topic  | References   | Description  |
|--|--------------|--|
| Efficient Communication Protocols            | [171–174]    | Discusses the need for communication protocols tailored to IoT constraints, including gradient compression, sparsification, and adaptive communication schedules.          |
| Handling Non-IID Data                        | [175–178]    | Explores strategies to improve FL models' ability to handle non-IID data in IoT environments, focusing on aggregation strategies, personalized models, and meta-learning.  |
| Enhancing Security Mechanisms                | [179–182]    | Focuses on evolving security mechanisms in FL, such as homomorphic encryption, federated adversarial training, and the integration of blockchain for secure model updates. |
| Scalability in Large-Scale IoT Deployments   | [183–186]    | Addresses scalability issues in FL for IoT, emphasizing decentralized and hierarchical FL architectures to manage large-scale deployments efficiently.                     |
| Energy Optimization Strategies for FL in IoT | [187–190]    | Exploring strategies to enhance energy efficiency in FL for IoT through adaptive algorithms, hierarchical architectures, and energy-harvesting integration.                |
| Standardized Benchmarks and Datasets         | [191–194]    | Highlight the need for standardized benchmarks and datasets that reflect IoT environments, aiding in the evaluation of FL algorithms.                                      |
| Additional Future Research Directions        | [17,195–201] | Concludes with a discussion on critical challenges and the future research directions necessary to enhance the adoption of FL in diverse IoT applications.                 |

The identification of open issues, such as the need for standardized benchmarks and better handling of non-IID data, reveals that FL for IoT is still in its developmental phase. This highlights an opportunity for interdisciplinary collaboration to address these gaps effectively. It underscores the importance of energy-efficient designs and hierarchical FL structures to pave the way for large-scale, real-world implementations.

## 6. Conclusions

FL offers a promising solution to the challenges posed by traditional centralized ML in IoT environments, particularly with respect to privacy, data security, and the constraints of distributed resource-limited devices. By enabling decentralized model training while keeping data local, FL aligns well with the privacy needs and scalability demands of IoT systems. This survey has highlighted the key techniques that enable FL in IoT, the specific challenges it faces, and the wide range of applications that stand to benefit from this technology.

However, the integration of FL into IoT is not without its obstacles. Communication overhead, device heterogeneity, and the need for enhanced security and privacy measures are critical areas that require continued research and innovation. Addressing these challenges will be essential for FL to realize its full potential in IoT environments, especially as these networks grow more complex and the data they generate becomes more sensitive.

Looking forward, the successful deployment of FL in IoT will depend on overcoming these challenges while maintaining robust performance and scalability. The ongoing evolution of FL algorithms and architectures, combined with real-world implementations, will shape the future of IoT, enabling more secure, efficient, and intelligent applications across various domains. The progress in this field will not only enhance IoT systems but also drive broader advancements in distributed ML and data-driven technologies.

**Author Contributions:** E.D. and M.T. conceived the idea, designed and performed the experiments, analyzed the results, drafted the initial manuscript, and revised the final manuscript. All authors have read and agreed to the published version of the manuscript

**Funding:** This research received no external funding

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

## References

1. Tawalbeh, L.; Muheidat, F.; Tawalbeh, M.; Quwaider, M. IoT Privacy and security: Challenges and solutions. *Appl. Sci.* **2020**, *10*, 4102. [\[CrossRef\]](#)
2. Rahman, S.A.; Tout, H.; Talhi, C.; Mourad, A. Internet of things intrusion detection: Centralized, on-device, or federated learning? *IEEE Netw.* **2020**, *34*, 310–317. [\[CrossRef\]](#)
3. Zikria, Y.B.; Ali, R.; Afzal, M.K.; Kim, S.W. Next-generation Internet of Things (IoT): Opportunities, challenges, and solutions. *Sensors* **2021**, *21*, 1174. [\[CrossRef\]](#) [\[PubMed\]](#)
4. Dritsas, E.; Trigka, M.; Mylonas, P. A Survey on Privacy-Enhancing Techniques in the Era of Artificial Intelligence. In Proceedings of the Novel & Intelligent Digital Systems, Athens, Greece, 25–27 September 2024; pp. 385–392.
5. Zhou, P.; Lin, Q.; Loghin, D.; Ooi, B.C.; Wu, Y.; Yu, H. Communication-efficient decentralized machine learning over heterogeneous networks. In Proceedings of the IEEE 37th International Conference on Data Engineering (ICDE), Chania, Greece, 19–22 April 2021; pp. 384–395.
6. Froelicher, D.; Troncoso-Pastoriza, J.R.; Pyrgelis, A.; Sav, S.; Sousa, J.S.; Bossuat, J.P.; Hubaux, J.P. Scalable privacy-preserving distributed learning. *arXiv* **2020**, arXiv:2005.09532. [\[CrossRef\]](#)
7. Dritsas, E.; Trigka, M. Machine Learning in Information and Communications Technology: A Survey. *Information* **2024**, *16*, 8. [\[CrossRef\]](#)
8. Chen, Z.; Liao, W.; Hua, K.; Lu, C.; Yu, W. Towards asynchronous federated learning for heterogeneous edge-powered internet of things. *Digit. Commun. Netw.* **2021**, *7*, 317–326. [\[CrossRef\]](#)
9. Alsagheer, D.; Xu, L.; Shi, W. Decentralized machine learning governance: Overview, opportunities, and challenges. *IEEE Access* **2023**, *11*, 96718–96732. [\[CrossRef\]](#)

10. Gosselin, R.; Vieu, L.; Loukil, F.; Benoit, A. Privacy and security in federated learning: A survey. *Appl. Sci.* **2022**, *12*, 9901. [\[CrossRef\]](#)
11. Wang, H.; Kaplan, Z.; Niu, D.; Li, B. Optimizing federated learning on non-iid data with reinforcement learning. In Proceedings of the IEEE Conference on Computer Communications (INFOCOM), Toronto, ON, Canada, 6–9 July 2020; pp. 1698–1707.
12. Li, Z.; He, Y.; Yu, H.; Kang, J.; Li, X.; Xu, Z.; Niyato, D. Data heterogeneity-robust federated learning via group client selection in industrial IoT. *IEEE Internet Things J.* **2022**, *9*, 17844–17857. [\[CrossRef\]](#)
13. Lu, Z.; Pan, H.; Dai, Y.; Si, X.; Zhang, Y. Federated learning with non-iid data: A survey. *IEEE Internet Things J.* **2024**, *11*, 19188–19209. [\[CrossRef\]](#)
14. Yuan, B.; Ge, S.; Xing, W. A federated learning framework for healthcare iot devices. *arXiv* **2020**, arXiv:2005.05083.
15. Zheng, Z.; Zhou, Y.; Sun, Y.; Wang, Z.; Liu, B.; Li, K. Applications of federated learning in smart cities: Recent advances, taxonomy, and open challenges. *Connect. Sci.* **2022**, *34*, 1–28. [\[CrossRef\]](#)
16. Qolomany, B.; Ahmad, K.; Al-Fuqaha, A.; Qadir, J. Particle swarm optimized federated learning for industrial IoT and smart city services. In Proceedings of the IEEE Global Communications Conference (GLOBECOM), Taipei, Taiwan, 7–11 December 2020; pp. 1–6.
17. Khan, L.U.; Saad, W.; Han, Z.; Hossain, E.; Hong, C.S. Federated learning for internet of things: Recent advances, taxonomy, and open challenges. *IEEE Commun. Surv. Tutor.* **2021**, *23*, 1759–1799. [\[CrossRef\]](#)
18. Imteaj, A.; Thakker, U.; Wang, S.; Li, J.; Amini, M.H. A survey on federated learning for resource-constrained IoT devices. *IEEE Internet Things J.* **2021**, *9*, 1–24. [\[CrossRef\]](#)
19. 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. Tutor.* **2021**, *23*, 1622–1658. [\[CrossRef\]](#)
20. Zhang, T.; Gao, L.; He, C.; Zhang, M.; Krishnamachari, B.; Avestimehr, A.S. Federated learning for the internet of things: Applications, challenges, and opportunities. *IEEE Internet Things Mag.* **2022**, *5*, 24–29. [\[CrossRef\]](#)
21. 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. [\[CrossRef\]](#)
22. 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. [\[CrossRef\]](#)
23. Zhang, Y.; Zeng, D.; Luo, J.; Xu, Z.; King, I. A survey of trustworthy federated learning with perspectives on security, robustness and privacy. In Proceedings of the Companion Proceedings of the ACM Web Conference 2023, Austin, TX, USA, 30 April 2023–4 May 2023; pp. 1167–1176.
24. Tariq, A.; Serhani, M.A.; Sallabi, F.; Qayyum, T.; Barka, E.S.; Shuaib, K.A. Trustworthy federated learning: A survey. *arXiv* **2023**, arXiv:2305.11537.
25. Yaacoub, J.P.A.; Noura, H.N.; Salman, O. Security of federated learning with IoT systems: Issues, limitations, challenges, and solutions. *Internet Things Cyber-Phys. Syst.* **2023**, *3*, 155–179. [\[CrossRef\]](#)
26. Manzoor, H.U.; Shabbir, A.; Chen, A.; Flynn, D.; Zoha, A. A survey of security strategies in federated learning: Defending models, data, and privacy. *Future Internet* **2024**, *16*, 374. [\[CrossRef\]](#)
27. Jiang, Y.; Ma, B.; Wang, X.; Yu, G.; Yu, P.; Wang, Z.; Ni, W.; Liu, R.P. Blockchain federated learning for internet of things: A comprehensive survey. *ACM Comput. Surv.* **2024**, *56*, 1–37. [\[CrossRef\]](#)
28. Wu, Q.; He, K.; Chen, X. Personalized federated learning for intelligent IoT applications: A cloud-edge based framework. *IEEE Open J. Comput. Soc.* **2020**, *1*, 35–44. [\[CrossRef\]](#)
29. Aminizadeh, S.; Heidari, A.; Toumaj, S.; Darbandi, M.; Navimipour, N.J.; Rezaei, M.; Talebi, S.; Azad, P.; Unal, M. The applications of machine learning techniques in medical data processing based on distributed computing and the Internet of Things. *Comput. Methods Prog. Biomed.* **2023**, *241*, 107745. [\[CrossRef\]](#)
30. Meng, Z.; Xu, H.; Chen, M.; Xu, Y.; Zhao, Y.; Qiao, C. Learning-driven decentralized machine learning in resource-constrained wireless edge computing. In Proceedings of the IEEE Conference on Computer Communications (INFOCOM), Vancouver, BC, Canada, 10–13 May 2021; pp. 1–10.
31. Sun, H.; Li, S.; Yu, F.R.; Qi, Q.; Wang, J.; Liao, J. Toward communication-efficient federated learning in the Internet of Things with edge computing. *IEEE Internet Things J.* **2020**, *7*, 11053–11067. [\[CrossRef\]](#)
32. Ranathunga, T.; McGibney, A.; Rea, S. The convergence of blockchain and machine learning for decentralized trust management in IoT ecosystems. In Proceedings of the 19th ACM Conference on Embedded Networked Sensor Systems, Coimbra, Portugal, 15–17 November 2021; pp. 499–504.
33. Chen, S.; Zhu, X.; Zhang, H.; Zhao, C.; Yang, G.; Wang, K. Efficient privacy preserving data collection and computation offloading for fog-assisted IoT. *IEEE Trans. Sustain. Comput.* **2020**, *5*, 526–540. [\[CrossRef\]](#)
34. Deng, Y.; Lyu, F.; Ren, J.; Chen, Y.C.; Yang, P.; Zhou, Y.; Zhang, Y. Fair: Quality-aware federated learning with precise user incentive and model aggregation. In Proceedings of the IEEE Conference on Computer Communications (INFOCOM), Vancouver, BC, Canada, 10–13 May 2021; pp. 1–10.

35. Ficco, M.; Guerriero, A.; Milite, E.; Palmieri, F.; Pietrantuono, R.; Russo, S. Federated learning for IoT devices: Enhancing TinyML with on-board training. *Inf. Fusion* **2024**, *104*, 102189. [\[CrossRef\]](#)
36. Savazzi, S.; Nicoli, M.; Rampa, V. Federated learning with cooperating devices: A consensus approach for massive IoT networks. *IEEE Internet Things J.* **2020**, *7*, 4641–4654. [\[CrossRef\]](#)
37. Brecko, A.; Kajati, E.; Koziorek, J.; Zolotova, I. Federated learning for edge computing: A survey. *Appl. Sci.* **2022**, *12*, 9124. [\[CrossRef\]](#)
38. Zhang, H.; Bosch, J.; Olsson, H.H. Real-time end-to-end federated learning: An automotive case study. In Proceedings of the 45th IEEE Annual Computers, Software, and Applications Conference (COMPSAC), Madrid, Spain, 12–16 July 2021; pp. 459–468.
39. Campolo, C.; Genovese, G.; Singh, G.; Molinaro, A. Scalable and interoperable edge-based federated learning in IoT contexts. *Comput. Netw.* **2023**, *223*, 109576. [\[CrossRef\]](#)
40. Nguyen, M.D.; Lee, S.M.; Pham, Q.V.; Hoang, D.T.; Nguyen, D.N.; Hwang, W.J. HCFL: A high compression approach for communication-efficient federated learning in very large scale IoT networks. *IEEE Trans. Mob. Comput.* **2022**, *22*, 6495–6507. [\[CrossRef\]](#)
41. Yang, H.; Liu, J.; Bentley, E.S. CFedAvg: Achieving efficient communication and fast convergence in non-iid federated learning. In Proceedings of the 19th IEEE International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks (WiOpt), Philadelphia, PA, USA, 18–21 October 2021; pp. 1–8.
42. Bibikar, S.; Vikalo, H.; Wang, Z.; Chen, X. Federated dynamic sparse training: Computing less, communicating less, yet learning better. *AAAI Conf. Artif. Intell.* **2022**, *36*, 6080–6088. [\[CrossRef\]](#)
43. Li, Y.; Zhou, Y.; Jolfaei, A.; Yu, D.; Xu, G.; Zheng, X. Privacy-preserving federated learning framework based on chained secure multiparty computing. *IEEE Internet Things J.* **2020**, *8*, 6178–6186. [\[CrossRef\]](#)
44. Park, J.; Lim, H. Privacy-preserving federated learning using homomorphic encryption. *Appl. Sci.* **2022**, *12*, 734. [\[CrossRef\]](#)
45. Ghimire, B.; Rawat, D.B. Recent advances on federated learning for cybersecurity and cybersecurity for federated learning for internet of things. *IEEE Internet Things J.* **2022**, *9*, 8229–8249. [\[CrossRef\]](#)
46. Yu, X.; Cherkasova, L.; Vardhan, H.; Zhao, Q.; Ekaireb, E.; Zhang, X.; Mazumdar, A.; Rosing, T. Async-HFL: Efficient and robust asynchronous federated learning in hierarchical IoT networks. In Proceedings of the 8th ACM/IEEE Conference on Internet of Things Design and Implementation, San Antonio, TX, USA, 9–12 May 2023; pp. 236–248.
47. Saputra, Y.M.; Hoang, D.T.; Nguyen, D.N.; Tran, L.N.; Gong, S.; Dutkiewicz, E. Dynamic federated learning-based economic framework for internet-of-vehicles. *IEEE Trans. Mob. Comput.* **2021**, *22*, 2100–2115. [\[CrossRef\]](#)
48. Kang, J.; Xiong, Z.; Niyato, D.; Zou, Y.; Zhang, Y.; Guizani, M. Reliable federated learning for mobile networks. *IEEE Wirel. Commun.* **2020**, *27*, 72–80. [\[CrossRef\]](#)
49. Chen, H.; Huang, S.; Zhang, D.; Xiao, M.; Skoglund, M.; Poor, H.V. Federated learning over wireless IoT networks with optimized communication and resources. *IEEE Internet Things J.* **2022**, *9*, 16592–16605. [\[CrossRef\]](#)
50. Ji, X.; Tian, J.; Zhang, H.; Wu, D.; Li, T. Joint device selection and bandwidth allocation for cost-efficient federated learning in industrial internet of things. *IEEE Internet Things J.* **2023**, *10*, 9148–9160. [\[CrossRef\]](#)
51. 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.
52. Shah, S.M.; Lau, V.K. Model compression for communication efficient federated learning. *IEEE Trans. Neural Netw. Learn. Syst.* **2021**, *34*, 5937–5951. [\[CrossRef\]](#) [\[PubMed\]](#)
53. Wen, D.; Jeon, K.J.; Huang, K. Federated dropout—A simple approach for enabling federated learning on resource constrained devices. *IEEE Wirel. Commun. Lett.* **2022**, *11*, 923–927. [\[CrossRef\]](#)
54. Wang, H.; Liu, W.; Xiong, N.N.; Zhang, S.; Wang, T. LIAA: A listen interval adaptive adjustment scheme for green communication in event-sparse IoT systems. *Inf. Sci.* **2022**, *584*, 235–268. [\[CrossRef\]](#)
55. Javani, A.; Wang, Z. Load Balancing in Federated Learning. *arXiv* **2024**, arXiv:2408.00217.
56. Yan, X.; Miao, Y.; Li, X.; Choo, K.K.R.; Meng, X.; Deng, R.H. Privacy-preserving asynchronous federated learning framework in distributed iot. *IEEE Internet Things J.* **2023**, *10*, 13281–13291. [\[CrossRef\]](#)
57. Liu, S.; Chen, Q.; You, L. Fed2a: Federated learning mechanism in asynchronous and adaptive modes. *Electronics* **2022**, *11*, 1393. [\[CrossRef\]](#)
58. Li, S.; Ngai, E.C.H.; Voigt, T. An experimental study of byzantine-robust aggregation schemes in federated learning. *IEEE Trans. Big Data* **2023**, *10*, 978–988. [\[CrossRef\]](#)
59. Su, N.; Li, B. How asynchronous can federated learning be? In Proceedings of the 2022 IEEE/ACM 30th International Symposium on Quality of Service (IWQoS), Oslo, Norway, 10–12 June 2022; pp. 1–11.
60. Xia, J.; Liu, T.; Ling, Z.; Wang, T.; Fu, X.; Chen, M. PervasiveFL: Pervasive federated learning for heterogeneous IoT systems. *IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst.* **2022**, *41*, 4100–4111. [\[CrossRef\]](#)
61. Khan, L.U.; Alsenwi, M.; Yaqoob, I.; Imran, M.; Han, Z.; Hong, C.S. Resource optimized federated learning-enabled cognitive internet of things for smart industries. *IEEE Access* **2020**, *8*, 168854–168864. [\[CrossRef\]](#)



62. Abdellatif, A.A.; Mhaisen, N.; Mohamed, A.; Erbad, A.; Guizani, M.; Dawy, Z.; Nasreddine, W. Communication-efficient hierarchical federated learning for IoT heterogeneous systems with imbalanced data. *Future Gener. Comput. Syst.* **2022**, *128*, 406–419. [\[CrossRef\]](#)
63. Wang, H.; Qu, Z.; Zhou, Q.; Zhang, H.; Luo, B.; Xu, W.; Guo, S.; Li, R. A comprehensive survey on training acceleration for large machine learning models in IoT. *IEEE Internet Things J.* **2021**, *9*, 939–963. [\[CrossRef\]](#)
64. Zhao, Z.; Feng, C.; Hong, W.; Jiang, J.; Jia, C.; Quek, T.Q.; Peng, M. Federated learning with non-IID data in wireless networks. *IEEE Trans. Wirel. Commun.* **2021**, *21*, 1927–1942. [\[CrossRef\]](#)
65. Huang, W.; Ye, M.; Du, B. Learn from others and be yourself in heterogeneous federated learning. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, New Orleans, LA, USA, 18–21 June 2022; pp. 10143–10153.
66. Byabazaire, J.; O'Hare, G.; Delaney, D. Data quality and trust: Review of challenges and opportunities for data sharing in iot. *Electronics* **2020**, *9*, 2083. [\[CrossRef\]](#)
67. Wang, H.; Muñoz-González, L.; Eklund, D.; Raza, S. Non-IID data re-balancing at IoT edge with peer-to-peer federated learning for anomaly detection. In Proceedings of the 14th ACM Conference on Security and Privacy in Wireless and Mobile Networks, Abu Dhabi, United Arab Emirates, 28 June–2 July 2021; pp. 153–163.
68. Kishor, K. Personalized federated learning. In *Federated Learning for IoT Applications*; Springer: Berlin/Heidelberg, Germany, 2022; pp. 31–52. [\[CrossRef\]](#)
69. Yang, C.; Wang, Q.; Xu, M.; Chen, Z.; Bian, K.; Liu, Y.; Liu, X. Characterizing impacts of heterogeneity in federated learning upon large-scale smartphone data. In Proceedings of the Web Conference 2021, Ljubljana, Slovenia, 19–23 April 2021; pp. 935–946.
70. Wu, X.; Huang, F.; Hu, Z.; Huang, H. Faster adaptive federated learning. *AAAI Conf. Artif. Intell.* **2023**, *37*, 10379–10387. [\[CrossRef\]](#)
71. Chen, S.; Shen, C.; Zhang, L.; Tang, Y. Dynamic aggregation for heterogeneous quantization in federated learning. *IEEE Trans. Wirel. Commun.* **2021**, *20*, 6804–6819. [\[CrossRef\]](#)
72. Li, Q.; Diao, Y.; Chen, Q.; He, B. Federated learning on non-iid data silos: An experimental study. In Proceedings of the 2022 IEEE 38th International Conference on Data Engineering (ICDE), Kuala Lumpur, Malaysia, 9–12 May 2022; pp. 965–978.
73. 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; Volume 965, pp. 21–50. [\[CrossRef\]](#)
74. Li, J.; Rakin, A.S.; Chen, X.; He, Z.; Fan, D.; Chakrabarti, C. Ressfl: A resistance transfer framework for defending model inversion attack in split federated learning. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, New Orleans, LA, USA, 18–21 June 2022; pp. 10194–10202.
75. 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. [\[CrossRef\]](#)
76. Wei, W.; Liu, L.; Wu, Y.; Su, G.; Iyengar, A. Gradient-leakage resilient federated learning. In Proceedings of the 2021 IEEE 41st International Conference on Distributed Computing Systems (ICDCS), Washington DC, USA, 7–10 July 2021; pp. 797–807.
77. 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. [\[CrossRef\]](#)
78. Alghamdi, W.; Salama, R.; Sirija, M.; Abbas, A.R.; Dilnoza, K. Secure multi-party computation for collaborative data analysis. *E3S Web Conf.* **2023**, *399*, 04034. [\[CrossRef\]](#)
79. Fang, H.; Qian, Q. Privacy preserving machine learning with homomorphic encryption and federated learning. *Future Internet* **2021**, *13*, 94. [\[CrossRef\]](#)
80. Mendoza-Cardenas, F.; Aparcana-Tasayco, A.J.; Leon-Aguilar, R.S.; Quiroz-Arroyo, J.L. Cryptography for privacy in a resource-constrained IoT: A systematic literature review. *IEIE Trans. Smart Process. Comput.* **2022**, *11*, 351–360. [\[CrossRef\]](#)
81. Yang, X.; Shu, L.; Liu, Y.; Hancke, G.P.; Ferrag, M.A.; Huang, K. Physical security and safety of IoT equipment: A survey of recent advances and opportunities. *IEEE Trans. Ind. Inform.* **2022**, *18*, 4319–4330. [\[CrossRef\]](#)
82. Tao, Y.; Cui, S.; Xu, W.; Yin, H.; Yu, D.; Liang, W.; Cheng, X. Byzantine-resilient federated learning at edge. *IEEE Trans. Comput.* **2023**, *72*, 2600–2614. [\[CrossRef\]](#)
83. Abbasian Dehkordi, S.; Farajzadeh, K.; Rezazadeh, J.; Farahbakhsh, R.; Sandrasegaran, K.; Abbasian Dehkordi, M. A survey on data aggregation techniques in IoT sensor networks. *Wirel. Netw.* **2020**, *26*, 1243–1263. [\[CrossRef\]](#)
84. Sánchez, P.M.S.; Celdrán, A.H.; Schenk, T.; Iten, A.L.B.; Bovet, G.; Pérez, G.M.; Stiller, B. Studying the robustness of anti-adversarial federated learning models detecting cyberattacks in iot spectrum sensors. *IEEE Trans. Dependable Secur. Comput.* **2022**, *21*, 573–584. [\[CrossRef\]](#)
85. 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. [\[CrossRef\]](#)
86. Zhai, S.; Jin, X.; Wei, L.; Luo, H.; Cao, M. Dynamic federated learning for GMEC with time-varying wireless link. *IEEE Access* **2021**, *9*, 10400–10412. [\[CrossRef\]](#)



87. Lai, F.; Dai, Y.; Singapuram, S.; Liu, J.; Zhu, X.; Madhyastha, H.; Chowdhury, M. FedScale: Benchmarking model and system performance of federated learning at scale. In Proceedings of the International Conference on Machine Learning, Baltimore, MD, USA, 17–23 July 2022; pp. 11814–11827.
88. Gedawy, H.K.; Harras, K.A.; Bui, T.; Tanveer, T. RealFL: A realistic platform for federated learning. In Proceedings of the Int'l ACM Conference on Modeling Analysis and Simulation of Wireless and Mobile Systems, Montreal, QC, Canada, 29 October–2 November 2023; pp. 313–317.
89. De Rango, F.; Guerrieri, A.; Raimondo, P.; Spezzano, G. HED-FL: A hierarchical, energy efficient, and dynamic approach for edge Federated Learning. *Pervasive Mob. Comput.* **2023**, *92*, 101804. [\[CrossRef\]](#)
90. Wang, T.; Liu, Y.; Zheng, X.; Dai, H.N.; Jia, W.; Xie, M. Edge-based communication optimization for distributed federated learning. *IEEE Trans. Netw. Sci. Eng.* **2021**, *9*, 2015–2024. [\[CrossRef\]](#)
91. Kim, J.; Park, G.; Kim, M.; Park, S. Cluster-based secure aggregation for federated learning. *Electronics* **2023**, *12*, 870. [\[CrossRef\]](#)
92. Hosseinalipour, S.; Azam, S.S.; Brinton, C.G.; Michelusi, N.; Aggarwal, V.; Love, D.J.; Dai, H. Multi-stage hybrid federated learning over large-scale D2D-enabled fog networks. *IEEE/ACM Trans. Netw.* **2022**, *30*, 1569–1584. [\[CrossRef\]](#)
93. Sun, W.; Lei, S.; Wang, L.; Liu, Z.; Zhang, Y. Adaptive federated learning and digital twin for industrial internet of things. *IEEE Trans. Ind. Inform.* **2020**, *17*, 5605–5614. [\[CrossRef\]](#)
94. Durmus, A.E.; Yue, Z.; Ramon, M.; Matthew, M.; Paul, W.; Venkatesh, S. Federated learning based on dynamic regularization. In Proceedings of the International Conference on Learning Representations, Online, 3–7 May 2021.
95. Xu, J.; Wang, S.; Wang, L.; Yao, A.C.C. Fedcm: Federated learning with client-level momentum. *arXiv* **2021**, arXiv:2106.10874.
96. Tahir, M.; Ali, M.I. On the performance of federated learning algorithms for IoT. *IoT* **2022**, *3*, 273–284. [\[CrossRef\]](#)
97. Nguyen, V.D.; Sharma, S.K.; Vu, T.X.; Chatzinotas, S.; Ottersten, B. Efficient federated learning algorithm for resource allocation in wireless IoT networks. *IEEE Internet Things J.* **2020**, *8*, 3394–3409. [\[CrossRef\]](#)
98. Tekin, N.; Acar, A.; Aris, A.; Uluagac, A.S.; Gungor, V.C. Energy consumption of on-device machine learning models for IoT intrusion detection. *Internet Things* **2023**, *21*, 100670. [\[CrossRef\]](#)
99. Li, Y.; Liang, W.; Li, J.; Cheng, X.; Yu, D.; Zomaya, A.Y.; Guo, S. Energy-aware, device-to-device assisted federated learning in edge computing. *IEEE Trans. Parallel Distrib. Syst.* **2023**, *34*, 2138–2154. [\[CrossRef\]](#)
100. Arouj, A.; Abdelmoniem, A.M. Towards energy-aware federated learning on battery-powered clients. In Proceedings of the 1st ACM Workshop on Data Privacy and Federated Learning Technologies for Mobile Edge Network, Sydney, Australia, 17 October 2022; pp. 7–12.
101. Yang, Z.; Chen, M.; Saad, W.; Hong, C.S.; Shikh-Bahaei, M. Energy efficient federated learning over wireless communication networks. *IEEE Trans. Wirel. Commun.* **2020**, *20*, 1935–1949. [\[CrossRef\]](#)
102. Qi, P.; Chiaro, D.; Piccialli, F. Small models, big impact: A review on the power of lightweight Federated Learning. *Future Gener. Comput. Syst.* **2024**, *162*, 107484. [\[CrossRef\]](#)
103. Aghli, N.; Ribeiro, E. Combining weight pruning and knowledge distillation for cnn compression. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, Nashville, TN, USA, 18–25 June 2021; pp. 3191–3198.
104. Wu, D.; Ullah, R.; Harvey, P.; Kilpatrick, P.; Spence, I.; Varghese, B. Fedadapt: Adaptive offloading for iot devices in federated learning. *IEEE Internet Things J.* **2022**, *9*, 20889–20901. [\[CrossRef\]](#)
105. Vu, T.T.; Ngo, H.Q.; Dao, M.N.; Ngo, D.T.; Larsson, E.G.; Le-Ngoc, T. Energy-efficient massive MIMO for federated learning: Transmission designs and resource allocations. *IEEE Open J. Commun. Soc.* **2022**, *3*, 2329–2346. [\[CrossRef\]](#)
106. Russo, E.; Palesi, M.; Monteleone, S.; Patti, D.; Mineo, A.; Ascia, G.; Catania, V. DNN model compression for IoT domain-specific hardware accelerators. *IEEE Internet Things J.* **2021**, *9*, 6650–6662. [\[CrossRef\]](#)
107. Lee, S.; Julien, C.; Zheng, X. Facilitating Decentralized and Opportunistic Learning in Pervasive Computing. In Proceedings of the 2022 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops), Pisa, Italy, 21–25 March 2022; pp. 144–145.
108. Çakir, Z.; Arslan, E.T.C. Federated Learning with Channel and Energy Aware Scheduling. In Proceedings of the 2022 IEEE 30th Signal Processing and Communications Applications Conference (SIU), Safranbolu, Turkey, 15–18 May 2022; pp. 1–4.
109. Dao, N.N.; Na, W.; Tran, A.T.; Nguyen, D.N.; Cho, S. Energy-efficient spectrum sensing for IoT devices. *IEEE Syst. J.* **2020**, *15*, 1077–1085. [\[CrossRef\]](#)
110. Thakur, D.; Guzzo, A.; Fortino, G. Hardware-algorithm co-design of Energy Efficient Federated Learning in Quantized Neural Network. *Internet Things* **2024**, *26*, 101223. [\[CrossRef\]](#)
111. Khowaja, S.A.; Dev, K.; Khowaja, P.; Bellavista, P. Toward energy-efficient distributed federated learning for 6G networks. *IEEE Wirel. Commun.* **2021**, *28*, 34–40. [\[CrossRef\]](#)
112. Hamdi, R.; Said, A.B.; Baccour, E.; Erbad, A.; Mohamed, A.; Hamdi, M.; Guizani, M. Optimal resource management for hierarchical federated learning over HetNets with wireless energy transfer. *IEEE Internet Things J.* **2023**, *10*, 16945–16958. [\[CrossRef\]](#)
113. Wang, H.; Muñoz-González, L.; Hameed, M.Z.; Eklund, D.; Raza, S. SparSFA: Towards robust and communication-efficient peer-to-peer federated learning. *Comput. Secur.* **2023**, *129*, 103182. [\[CrossRef\]](#)

114. Hu, F.; Zhou, W.; Liao, K.; Li, H.; Tong, D. Toward federated learning models resistant to adversarial attacks. *IEEE Internet Things J.* **2023**, *10*, 16917–16930. [\[CrossRef\]](#)
115. Sun, G.; Cong, Y.; Dong, J.; Wang, Q.; Lyu, L.; Liu, J. Data poisoning attacks on federated machine learning. *IEEE Internet Things J.* **2021**, *9*, 11365–11375. [\[CrossRef\]](#)
116. Ma, Z.; Ma, J.; Miao, Y.; Li, Y.; Deng, R.H. ShieldFL: Mitigating model poisoning attacks in privacy-preserving federated learning. *IEEE Trans. Inf. Forensics Secur.* **2022**, *17*, 1639–1654. [\[CrossRef\]](#)
117. Queyrut, S.; Schiavoni, V.; Felber, P. Mitigating adversarial attacks in federated learning with trusted execution environments. In Proceedings of the 2023 IEEE 43rd International Conference on Distributed Computing Systems (ICDCS), Hong Kong, China, 18–21 July 2023; pp. 626–637.
118. Gao, J.; Zhang, B.; Guo, X.; Baker, T.; Li, M.; Liu, Z. Secure partial aggregation: Making federated learning more robust for industry 4.0 applications. *IEEE Trans. Ind. Inform.* **2022**, *18*, 6340–6348. [\[CrossRef\]](#)
119. Kumar, K.N.; Mohan, C.K.; Cenkeramaddi, L.R. The Impact of Adversarial Attacks on Federated Learning: A Survey. *IEEE Trans. Pattern Anal. Mach. Intell.* **2023**, *46*, 2672–2691. [\[CrossRef\]](#) [\[PubMed\]](#)
120. Colosimo, F.; De Rango, F. Median-krum: A joint distance-statistical based byzantine-robust algorithm in federated learning. In Proceedings of the Int'l ACM Symposium on Mobility Management and Wireless Access, Montreal, QC, Canada, 30 October–3 November 2023; pp. 61–68.
121. Almanifi, O.R.A.; Chow, C.O.; Tham, M.L.; Chuah, J.H.; Kanesan, J. Communication and computation efficiency in federated learning: A survey. *Internet Things* **2023**, *22*, 100742. [\[CrossRef\]](#)
122. Li, S.; Ngai, E.; Voigt, T. Byzantine-robust aggregation in federated learning empowered industrial iot. *IEEE Trans. Ind. Inform.* **2021**, *19*, 1165–1175. [\[CrossRef\]](#)
123. Mahor, V.; Bijrothiya, S.; Mishra, R.; Rawat, R. ML Techniques for Attack and Anomaly Detection in Internet of Things Networks. In *Autonomous Vehicles Volume 1: Using Machine Intelligence*; Scrivener Publishing LLC: Austin, TX, USA, 2022; pp. 235–252.
124. Zizzo, G.; Rawat, A.; Sinn, M.; Maffei, S.; Hankin, C. Certified federated adversarial training. *arXiv* **2021**, arXiv:2112.10525.
125. Alsulaimawi, Z. Securing Federated Learning with Control-Flow Attestation: A Novel Framework for Enhanced Integrity and Resilience against Adversarial Attacks. *arXiv* **2024**, arXiv:2403.10005.
126. Nguyen, D.C.; Pham, Q.V.; Pathirana, P.N.; Ding, M.; Seneviratne, A.; Lin, Z.; Dobre, O.; Hwang, W.J. Federated learning for smart healthcare: A survey. *ACM Comput. Surv. (Csur.)* **2022**, *55*, 1–37. [\[CrossRef\]](#)
127. Javed, A.R.; Sarwar, M.U.; Beg, M.O.; Asim, M.; Baker, T.; Tawfik, H. A collaborative healthcare framework for shared healthcare plan with ambient intelligence. *Hum.-Centric Comput. Inf. Sci.* **2020**, *10*, 40. [\[CrossRef\]](#)
128. Dimitropoulos, N.; Togias, T.; Zacharaki, N.; Michalos, G.; Makris, S. Seamless human–robot collaborative assembly using artificial intelligence and wearable devices. *Appl. Sci.* **2021**, *11*, 5699. [\[CrossRef\]](#)
129. Naresh, V.S.; Thamarai, M. Privacy-preserving data mining and machine learning in healthcare: Applications, challenges, and solutions. *Wiley Interdiscip. Rev. Data Min. Knowl. Discov.* **2023**, *13*, e1490. [\[CrossRef\]](#)
130. Xu, J.; Glicksberg, B.S.; Su, C.; Walker, P.; Bian, J.; Wang, F. Federated learning for healthcare informatics. *J. Healthc. Inform. Res.* **2021**, *5*, 1–19. [\[CrossRef\]](#)
131. Liu, L.; Tian, Y.; Chakraborty, C.; Feng, J.; Pei, Q.; Zhen, L.; Yu, K. Multilevel federated learning-based intelligent traffic flow forecasting for transportation network management. *IEEE Trans. Netw. Serv. Manag.* **2023**, *20*, 1446–1458. [\[CrossRef\]](#)
132. Liu, Y.; James, J.; Kang, J.; Niyato, D.; Zhang, S. Privacy-preserving traffic flow prediction: A federated learning approach. *IEEE Internet Things J.* **2020**, *7*, 7751–7763. [\[CrossRef\]](#)
133. Fakhar, A.; Haidar, A.M.; Abdullah, M.; Das, N. Smart grid mechanism for green energy management: A comprehensive review. *Int. J. Green Energy* **2023**, *20*, 284–308. [\[CrossRef\]](#)
134. Ramírez-Moreno, M.A.; Keshtkar, S.; Padilla-Reyes, D.A.; Ramos-López, E.; García-Martínez, M.; Hernández-Luna, M.C.; Mogro, A.E.; Mahlkecht, J.; Huertas, J.I.; Peimbert-García, R.E.; et al. Sensors for sustainable smart cities: A review. *Appl. Sci.* **2021**, *11*, 8198. [\[CrossRef\]](#)
135. Wang, T.; Liang, T.; Li, J.; Zhang, W.; Zhang, Y.; Lin, Y. Adaptive traffic signal control using distributed marl and federated learning. In Proceedings of the 2020 IEEE 20th International Conference on Communication Technology (ICCT), Nanning, China, 28–31 October 2020; pp. 1242–1248.
136. 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. [\[CrossRef\]](#)
137. Li, L.; Fan, Y.; Tse, M.; Lin, K.Y. A review of applications in federated learning. *Comput. Ind. Eng.* **2020**, *149*, 106854. [\[CrossRef\]](#)
138. Brik, B.; Ksentini, A. On predicting service-oriented network slices performances in 5G: A federated learning approach. In Proceedings of the 2020 IEEE 45th Conference on Local Computer Networks (LCN), Sydney, Australia, 16–19 November 2020; pp. 164–171.
139. Zhou, J.; Zhang, S.; Lu, Q.; Dai, W.; Chen, M.; Liu, X.; Pirttikangas, S.; Shi, Y.; Zhang, W.; Herrera-Viedma, E. A survey on federated learning and its applications for accelerating industrial internet of things. *arXiv* **2021**, arXiv:2104.10501.

140. Pham, Q.V.; Dev, K.; Maddikunta, P.K.R.; Gadekallu, T.R.; Huynh-The, T. Fusion of federated learning and industrial internet of things: A survey. *arXiv* **2021**, arXiv:2101.00798.
141. Vyas, J.; Das, D.; Das, S.K. Vehicular edge computing based driver recommendation system using federated learning. In Proceedings of the 2020 IEEE 17th International Conference on Mobile Ad Hoc and Sensor Systems (MASS), Online, 10–13 December 2020; pp. 675–683.
142. Zhang, R.; Mao, J.; Wang, H.; Li, B.; Cheng, X.; Yang, L. A Survey on Federated Learning in Intelligent Transportation Systems. *IEEE Trans. Intell. Veh.* **2024**, Early Access.
143. Malik, S.; Khan, M.A.; El-Sayed, H. Collaborative autonomous driving—A survey of solution approaches and future challenges. *Sensors* **2021**, *21*, 3783. [\[CrossRef\]](#) [\[PubMed\]](#)
144. Yoshikawa, A. Privacy-Preserving Machine Learning Models for Autonomous Vehicle Data Analysis. *J. AI-Assist. Sci. Discov.* **2023**, *3*, 90–110.
145. Chellapandi, V.P.; Yuan, L.; Brinton, C.G.; Žak, S.H.; Wang, Z. Federated learning for connected and automated vehicles: A survey of existing approaches and challenges. *IEEE Trans. Intell. Veh.* **2023**, *9*, 119–137. [\[CrossRef\]](#)
146. Mehta, S.; Kukreja, V.; Gupta, R. Empowering Precision Agriculture: Detecting Apple Leaf Diseases and Severity Levels with Federated Learning CNN. In Proceedings of the 2023 3rd International Conference on Intelligent Technologies (CONIT), Hubli, India, 23–25 June 2023; pp. 1–6.
147. Mehta, S.; Kukreja, V.; Gupta, A. Transforming Agriculture: Federated Learning CNNs for Wheat Disease Severity Assessment. In Proceedings of the 2023 8th International Conference on Communication and Electronics Systems (ICCES), Coimbatore, India, 1–3 June 2023; pp. 792–797.
148. Gaikwad, S.V.; Vibhute, A.D.; Kale, K.V.; Mehrotra, S.C. An innovative IoT based system for precision farming. *Comput. Electron. Agric.* **2021**, *187*, 106291. [\[CrossRef\]](#)
149. Kumar, P.; Gupta, G.P.; Tripathi, R. PEFL: Deep privacy-encoding-based federated learning framework for smart agriculture. *IEEE Micro* **2021**, *42*, 33–40. [\[CrossRef\]](#)
150. Manoj, T.; Makkithaya, K.; Narendra, V. A federated learning-based crop yield prediction for agricultural production risk management. In Proceedings of the 2022 IEEE Delhi Section Conference (DELCON), New Delhi, India, 11–13 February 2022; pp. 1–7.
151. Liu, Y.; Yuan, X.; Xiong, Z.; Kang, J.; Wang, X.; Niyato, D. Federated learning for 6G communications: Challenges, methods, and future directions. *China Commun.* **2020**, *17*, 105–118. [\[CrossRef\]](#)
152. Niknam, S.; Dhillon, H.S.; Reed, J.H. Federated learning for wireless communications: Motivation, opportunities, and challenges. *IEEE Commun. Mag.* **2020**, *58*, 46–51. [\[CrossRef\]](#)
153. Chen, M.; Poor, H.V.; Saad, W.; Cui, S. Convergence time optimization for federated learning over wireless networks. *IEEE Trans. Wirel. Commun.* **2020**, *20*, 2457–2471. [\[CrossRef\]](#)
154. Xu, J.; Wang, H.; Chen, L. Bandwidth allocation for multiple federated learning services in wireless edge networks. *IEEE Trans. Wirel. Commun.* **2021**, *21*, 2534–2546. [\[CrossRef\]](#)
155. Lim, W.Y.B.; Luong, N.C.; Hoang, D.T.; Jiao, Y.; Liang, Y.C.; Yang, Q.; Niyato, D.; Miao, C. Federated learning in mobile edge networks: A comprehensive survey. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 2031–2063. [\[CrossRef\]](#)
156. Long, G.; Tan, Y.; Jiang, J.; Zhang, C. Federated learning for open banking. In *Federated Learning: Privacy and Incentive*; Springer: Cham, Switzerland, 2020; Volume 12500, pp. 240–254. [\[CrossRef\]](#)
157. Nevraiki, T.; Iliadou, A.; Ntolkeras, G.; Sfakianakis, I.; Lazaridis, L.; Maraslidis, G.; Asimopoulos, N.; Fragulis, G.F. A survey on federated learning applications in healthcare, finance, and data privacy/data security. In *AIP Conference Proceedings*; AIP Publishing: Melville, NY, USA, 2023; Volume 2909.
158. Zetzsche, D.A.; Arner, D.W.; Buckley, R.P. Decentralized finance. *J. Financ. Regul.* **2020**, *6*, 172–203. [\[CrossRef\]](#)
159. Ozili, P.K. Decentralized finance research and developments around the world. *J. Bank. Financ. Technol.* **2022**, *6*, 117–133. [\[CrossRef\]](#)
160. Shayan, M.; Fung, C.; Yoon, C.J.; Beschastnikh, I. Biscotti: A blockchain system for private and secure federated learning. *IEEE Trans. Parallel Distrib. Syst.* **2020**, *32*, 1513–1525. [\[CrossRef\]](#)
161. Nour, B.; Cherkaoui, S.; Mlika, Z. Federated learning and proactive computation reuse at the edge of smart homes. *IEEE Trans. Netw. Sci. Eng.* **2021**, *9*, 3045–3056. [\[CrossRef\]](#)
162. Kabir, S.; Gope, P.; Mohanty, S.P. A security-enabled safety assurance framework for IoT-based smart homes. *IEEE Trans. Ind. Appl.* **2022**, *59*, 6–14. [\[CrossRef\]](#)
163. Malik, I.; Bhardwaj, A.; Bhardwaj, H.; Sakalle, A. IoT-enabled smart homes: Architecture, challenges, and issues. In *Revolutionizing Industrial Automation Through the Convergence of Artificial Intelligence and the Internet of Things*; IGI Global Scientific Publishing: Hershey, PA, USA, 2023; pp. 160–176.
164. Perry, D.; Wang, N.; Ho, S.S. Energy demand prediction with optimized clustering-based federated learning. In Proceedings of the 2021 IEEE Global Communications Conference (GLOBECOM), Madrid, Spain, 7–11 December 2021; pp. 1–6.

165. Qashlan, A.; Nanda, P.; He, X.; Mohanty, M. Privacy-preserving mechanism in smart home using blockchain. *IEEE Access* **2021**, *9*, 103651–103669. [\[CrossRef\]](#)
166. Yadav, S.P.; Bhati, B.S.; Mahato, D.P.; Kumar, S. *Federated Learning for IOT Applications*; Springer: Berlin/Heidelberg, Germany, 2022. [\[CrossRef\]](#)
167. Amiri-Zarandi, M.; Dara, R.A.; Fraser, E. A survey of machine learning-based solutions to protect privacy in the Internet of Things. *Comput. Secur.* **2020**, *96*, 101921. [\[CrossRef\]](#)
168. Aledhari, M.; Razzak, R.; Parizi, R.M.; Saeed, F. Federated learning: A survey on enabling technologies, protocols, and applications. *IEEE Access* **2020**, *8*, 140699–140725. [\[CrossRef\]](#) [\[PubMed\]](#)
169. Shen, S.; Zhu, T.; Wu, D.; Wang, W.; Zhou, W. From distributed machine learning to federated learning: In the view of data privacy and security. *Concurr. Comput. Pract. Exp.* **2022**, *34*, e6002. [\[CrossRef\]](#)
170. Shahid, O.; Pouriyeh, S.; Parizi, R.M.; Sheng, Q.Z.; Srivastava, G.; Zhao, L. Communication efficiency in federated learning: Achievements and challenges. *arXiv* **2021**, arXiv:2107.10996.
171. Guo, X.; Liu, Z.; Li, J.; Gao, J.; Hou, B.; Dong, C.; Baker, T. Verifi: Communication-efficient and fast verifiable aggregation for federated learning. *IEEE Trans. Inf. Forensics Secur.* **2020**, *16*, 1736–1751. [\[CrossRef\]](#)
172. Albasyoni, A.; Safaryan, M.; Condat, L.; Richtárik, P. Optimal gradient compression for distributed and federated learning. *arXiv* **2020**, arXiv:2010.03246.
173. Ren, D.; Gui, X.; Zhang, K. Adaptive request scheduling and service caching for MEC-assisted IoT networks: An online learning approach. *IEEE Internet Things J.* **2022**, *9*, 17372–17386. [\[CrossRef\]](#)
174. Zhang, W.; Yang, D.; Wu, W.; Peng, H.; Zhang, N.; Zhang, H.; Shen, X. Optimizing federated learning in distributed industrial IoT: A multi-agent approach. *IEEE J. Sel. Areas Commun.* **2021**, *39*, 3688–3703. [\[CrossRef\]](#)
175. Zhu, H.; Xu, J.; Liu, S.; Jin, Y. Federated learning on non-IID data: A survey. *Neurocomputing* **2021**, *465*, 371–390. [\[CrossRef\]](#)
176. Liu, X.; Deng, Y.; Nallanathan, A.; Bennis, M. Federated Learning and Meta Learning: Approaches, Applications, and Directions. *IEEE Commun. Surv. Tutor.* **2023**, *26*, 571–618. [\[CrossRef\]](#)
177. Ye, M.; Fang, X.; Du, B.; Yuen, P.C.; Tao, D. Heterogeneous federated learning: State-of-the-art and research challenges. *ACM Comput. Surv.* **2023**, *56*, 1–44. [\[CrossRef\]](#)
178. Tan, A.Z.; Yu, H.; Cui, L.; Yang, Q. Towards personalized federated learning. *IEEE Trans. Neural Netw. Learn. Syst.* **2022**, *34*, 9587–9603. [\[CrossRef\]](#)
179. Cui, L.; Qu, Y.; Xie, G.; Zeng, D.; Li, R.; Shen, S.; Yu, S. Security and privacy-enhanced federated learning for anomaly detection in IoT infrastructures. *IEEE Trans. Ind. Inform.* **2021**, *18*, 3492–3500. [\[CrossRef\]](#)
180. Madi, A.; Stan, O.; Mayoue, A.; Grivet-Sébert, A.; Gouy-Pailler, C.; Sirdey, R. A secure federated learning framework using homomorphic encryption and verifiable computing. In Proceedings of the 2021 Reconciling Data Analytics, Automation, Privacy, and Security: A Big Data Challenge (RDAAPS), Hamilton, ON, Canada, 18–19 May 2021; pp. 1–8.
181. Zhang, H.; Liu, M.; Chen, Y.; Zhao, N. Attacking Modulation Recognition with Adversarial Federated Learning in Cognitive Radio-Enabled IoT. *IEEE Internet Things J.* **2023**, *11*, 10911–10923. [\[CrossRef\]](#)
182. Rückel, T.; Sedlmeir, J.; Hofmann, P. Fairness, integrity, and privacy in a scalable blockchain-based federated learning system. *Comput. Netw.* **2022**, *202*, 108621. [\[CrossRef\]](#)
183. Huang, X.; Wu, Y.; Liang, C.; Chen, Q.; Zhang, J. Distance-aware hierarchical federated learning in blockchain-enabled edge computing network. *IEEE Internet Things J.* **2023**, *10*, 19163–19176. [\[CrossRef\]](#)
184. Grafberger, A.; Chadha, M.; Jindal, A.; Gu, J.; Gerndt, M. Fedless: Secure and scalable federated learning using serverless computing. In Proceedings of the IEEE International Conference on Big Data (Big Data), Orlando, FL, USA, 15–18 December 2021; pp. 164–173.
185. Pathak, R.; Wainwright, M.J. FedSplit: An algorithmic framework for fast federated optimization. *Adv. Neural Inf. Process. Syst.* **2020**, *33*, 7057–7066.
186. Chen, S.; Wang, Y.; Yu, D.; Ren, J.; Xu, C.; Zheng, Y. Privacy-enhanced decentralized federated learning at dynamic edge. *IEEE Trans. Comput.* **2023**, *72*, 2165–2180. [\[CrossRef\]](#)
187. Salh, A.; Ngah, R.; Audah, L.; Kim, K.S.; Abdullah, Q.; Al-Moliki, Y.M.; Aljaloud, K.A.; Talib, H.N. Energy-efficient federated learning with resource allocation for green IoT edge intelligence in B5G. *IEEE Access* **2023**, *11*, 16353–16367. [\[CrossRef\]](#)
188. Mukherjee, A.; Buyya, R. EnFed: An Energy-aware Opportunistic Federated Learning in Resource Constrained Environments for Human Activity Recognition. *arXiv* **2024**, arXiv:2412.00768.
189. Sarhan, M.; Lo, W.W.; Layeghy, S.; Portmann, M. HBFL: A hierarchical blockchain-based federated learning framework for collaborative IoT intrusion detection. *Comput. Electr. Eng.* **2022**, *103*, 108379. [\[CrossRef\]](#)
190. Hamdi, R.; Chen, M.; Said, A.B.; Qaraqe, M.; Poor, H.V. Federated learning over energy harvesting wireless networks. *IEEE Internet Things J.* **2021**, *9*, 92–103. [\[CrossRef\]](#)



191. Liang, Y.; Guo, Y.; Gong, Y.; Luo, C.; Zhan, J.; Huang, Y. Flbench: A benchmark suite for federated learning. In Proceedings of the Intelligent Computing and Block Chain: First BenchCouncil International Federated Conference (FICC), Qingdao, China, 30 October–3 November 2020; Springer: Singapore, 2021; pp. 166–176. [\[CrossRef\]](#)
192. Booiij, T.M.; Chiscop, I.; Meeuwissen, E.; Moustafa, N.; Den Hartog, F.T. ToN\_IoT: The role of heterogeneity and the need for standardization of features and attack types in IoT network intrusion data sets. *IEEE Internet Things J.* **2021**, *9*, 485–496. [\[CrossRef\]](#)
193. Wu, J.M.T.; Teng, Q.; Huda, S.; Chen, Y.C.; Chen, C.M. A privacy frequent itemsets mining framework for collaboration in iot using federated learning. *ACM Trans. Sens. Netw.* **2023**, *19*, 1–15. [\[CrossRef\]](#)
194. Kholod, I.; Yanaki, E.; Fomichev, D.; Shalugin, E.; Novikova, E.; Filippov, E.; Nordlund, M. Open-source federated learning frameworks for IoT: A comparative review and analysis. *Sensors* **2020**, *21*, 167. [\[CrossRef\]](#)
195. Gómez, Á.L.P.; Maimó, L.F.; Clemente, F.J.G.; Morales, J.A.M.; Celdrán, A.H.; Bovet, G. A methodology for evaluating the robustness of anomaly detectors to adversarial attacks in industrial scenarios. *IEEE Access* **2022**, *10*, 124582–124594. [\[CrossRef\]](#)
196. Kponyo, J.J.; Agyemang, J.O.; Klogo, G.S.; Boateng, J.O. Lightweight and host-based denial of service (DoS) detection and defense mechanism for resource-constrained IoT devices. *Internet Things* **2020**, *12*, 100319. [\[CrossRef\]](#)
197. Mousavi, S.K.; Ghaffari, A.; Besharat, S.; Afshari, H. Security of internet of things based on cryptographic algorithms: A survey. *Wirel. Netw.* **2021**, *27*, 1515–1555. [\[CrossRef\]](#)
198. Xing, L. Cascading failures in internet of things: Review and perspectives on reliability and resilience. *IEEE Internet Things J.* **2020**, *8*, 44–64. [\[CrossRef\]](#)
199. Campos, E.M.; Saura, P.F.; González-Vidal, A.; Hernández-Ramos, J.L.; Bernabe, J.B.; Baldini, G.; Skarmeta, A. Evaluating Federated Learning for intrusion detection in Internet of Things: Review and challenges. *Comput. Netw.* **2022**, *203*, 108661. [\[CrossRef\]](#)
200. 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. Assess.* **2023**, *55*, 102987. [\[CrossRef\]](#)
201. Singh, P.; Singh, M.K.; Singh, R.; Singh, N. Federated learning: Challenges, methods, and future directions. In *Federated Learning for IoT Applications*; Springer: Cham, Switzerland, 2022; pp. 199–214. [\[CrossRef\]](#)

**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.