Computers, Materials & Continua

Tech Science Press

DOI: 10.32604/cmc.2024.058926

REVIEW

The Internet of Things under Federated Learning: A Review of the Latest Advances and Applications

Jinlong Wang[1,2,*], Zhenyu Liu[1], Xingtao Yang[1], Min Li[1] and Zhihan Lyu[3]

[1]School of Information and Control Engineering, Qingdao University of Technology, Qingdao, 260043, China

[2]Anhui Province Key Laboratory of Intelligent Building & Building Energy Saving, Anhui Jianzhu University, Hefei, 230000, China

[3]Department of Game Design, Uppsala University, Uppsala, 75310, Sweden

*Corresponding Author: Jinlong Wang. Email: qdwangjinlong@163.com

Received: 24 September 2024 Accepted: 03 December 2024 Published: 03 January 2025

ABSTRACT

With the rapid development of artificial intelligence, the Internet of Things (IoT) can deploy various machine learning algorithms for network and application management. In the IoT environment, many sensors and devices generate massive data, but data security and privacy protection have become a serious challenge. Federated learning (FL) can achieve many intelligent IoT applications by training models on local devices and allowing AI training on distributed IoT devices without data sharing. This review aims to deeply explore the combination of FL and the IoT, and analyze the application of federated learning in the IoT from the aspects of security and privacy protection. In this paper, we first describe the potential advantages of FL and the challenges faced by current IoT systems in the fields of network burden and privacy security. Next, we focus on exploring and analyzing the advantages of the combination of FL on the Internet, including privacy security, attack detection, efficient communication of the IoT, and enhanced learning quality. We also list various application scenarios of FL on the IoT. Finally, we propose several open research challenges and possible solutions.

KEYWORDS

Federated learning; Internet of Things; sensors; machine learning; privacy security

1 Introduction

IoT refers to a network technology that connects various smart devices, sensors, and terminals through the Internet to realize the exchange and sharing of information [1]. The development of the IoT has attracted global attention, and it is considered to be the third information technology revolution after the computer and the Internet. The application fields of the IoT are vast, covering many aspects such as smart medical treatment, smart homes, intelligent transportation, and smart cities. The development of the IoT has not only brought convenience and efficiency to people's lives and work but also provided impetus and support for social progress and economic growth. However, the development of the IoT also faces some challenges and problems [2], the most prominent of which are data security and privacy protection. Since the IoT involves a large amount of personal and sensitive data, such as health data, location data, behavioral data, etc., if this data is maliciously attacked or

leaked, it will bring serious loss and harm to users. In addition, the amount of data in the IoT is also very large, resulting in the cost and pressure of data transmission and storage. According to statistics, by 2030, the number of IoT devices will reach 125 billion [3]. These IoT devices will generate huge amounts of data. A recent report [4] suggests that by 2025, the data generated by IoT devices will reach 794.4 zettabytes. In addition, the difficulty and complexity of data analysis and processing has become an important challenge. Therefore, how to realize the safe sharing and efficient use of data in the IoT is an urgent problem to be solved.

To overcome these challenges, an emerging distributed machine learning framework, FL, has attracted a lot of attention. FL is a machine learning technique that can use multiple distributed clients (such as smartphones, tablets, IoT devices, etc.) to collaborate on training a global machine learning model without centralizing data to a central server [5]. As shown in Fig. 1, The advantage of FL is that it can protect the privacy and security of the data, as the data is only processed locally and does not need to be uploaded to the cloud or elsewhere. At the same time, FL can also reduce the overhead of data transmission and storage, and improve the utilization and value of data. FL has been applied in many fields, such as intelligent keyboards, speech recognition, image classification, etc. [6].

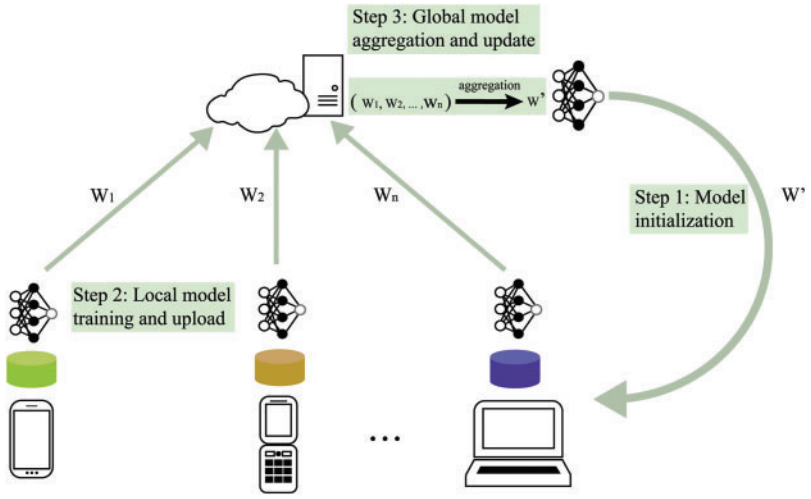

Figure 1: A schematic diagram of federated learning [7]

FL, when combined with IoT, can bring many advantages to IoT systems. First, FL can effectively protect sensitive data generated and stored in IoT devices from data breaches or misuse. Second, FL can reduce communication overhead in IoT systems, as only model parameters need to be transmitted instead of raw data. In addition, FL can adapt to the heterogeneity in IoT systems, as it can handle different devices, different data sources, different data distribution, and so on. At present, FL already has some application scenarios in IoT systems, such as smart homes, intelligent transportation, and intelligent medical care. For example, in the smart home scenario, multiple families can build a shared voice recognition or image recognition model through FL, thereby improving the service quality and user experience of smart devices; In the intelligent traffic scenario, multiple vehicles can realize information exchange and collaboration among vehicles through FL, so that road data can be used to judge congestion [8]. In the intelligent medical scenario, multiple medical institutions can share medical knowledge and experience through federal learning, thereby improving the diagnostic accuracy and treatment effect [9].

In order to compare our work with various existing reviews on federated learning, it is essential to point out that reference [10] primarily focuses on the applications of federated learning in the field of computer vision, emphasizing specific use cases and the challenges faced, particularly in the technological advancements related to object detection and video surveillance. In contrast, our manuscript encompasses the fundamentals, advantages, application scenarios of federated learning, and its integration within the Internet of Things (IoT), thereby providing a broader perspective. In terms of content depth, we explore the classification of federated learning and its adaptability to different application scenarios, particularly how its combination with IoT can enhance data security, communication efficiency, and the quality of learning. Furthermore, when discussing open challenges, we outline in detail the specific issues that may arise in the application of federated learning within the IoT context and propose corresponding solutions. This comparison not only highlights the differences in research directions and perspectives between the two papers but also underscores the unique contributions of our study within the context of the Internet of Things.

After determining the research objectives, topic-based keywords were selected, and a research retrieval was conducted through the Web of Science platform to find relevant research papers on the application of FL in the IOT. The complete search string used is as follows:

"(TS=(Federated learning) OR TS=(Federated) OR TS=(Machine Learning) OR TS=(Neural Network) OR TS=(Security) OR TS=(Privacy security) OR TS=(Attack detection)) AND (TS=(Internet of Things) OR TS=(Industrial Internet of Things) OR TS=(Sensors) OR TS=(Smart Healthcare) OR TS=(Smart City) OR TS=(Networking of vehicles))"

The Web of Science search yielded 60,035 records up to October 2024. A total of 231 papers were selected through initial screening. The number of papers was reduced to 84 after an in-depth analysis of the abstracts and full papers.

The main content and structure of this paper are shown in Fig. 2. Chapter 2 introduces the concept, advantages, and applications of FL, and analyzes the limitations of centralized FL, as well as the characteristics and applicable scenarios of different types of FL. Chapter 3 summarizes the definition, development, characteristics, and problems of the IoT, pointing out the shortcomings and challenges of the IoT in data privacy security, communication efficiency, attack detection, and other aspects. Chapter 4 expounds on the vision of the combination of FL and the IoT, analyzes the advantages of the application of federal learning in the IoT, such as privacy security, communication efficiency, attack detection, learning quality, etc., as well as the application fields of FL in the IoT, such as smart medicine, sensors, car networking, etc. Chapter 5 summarizes the challenges faced by the IoT under FL, such as high communication load, security and privacy issues, heterogeneous type, hardware constraints, standard specifications, etc., and puts forward possible solutions to these challenges. I hope this paper can provide some reference and inspiration for the development of FL in the IoT.

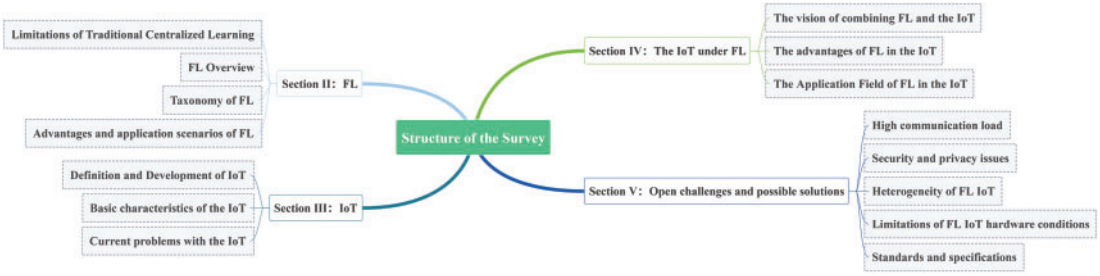

Figure 2: Architecture of this article

2 Overview and Current Status of Federated Learning

In this section, we will provide a comprehensive and detailed introduction to FL, starting from the limitations of traditional Centralized Learning (CL). This will mainly include the basis of FL, the classification of FL, the advantages of FL, and the application fields of FL.

2.1 Limitations of Traditional Centralized Learning

Machine learning (ML) is a data-based method that builds a model with the ability to generalize by learning rules and knowledge from extensive data [11]. It has a wide range of applications in various fields, such as image recognition, natural language processing, and recommendation systems. However, with the increasing amount of data and the diversification of data distribution, traditional CL in ML is facing more and more challenges and limitations [12]. This approach typically requires all data to be centralized to a central node (Fig. 3), where model training and inference are then performed. There are several main problems with this CL approach [13]:

1. Data privacy risks in CL: CL necessitates the transfer of raw data from multiple data owners to a central server for model training. This centralized data storage introduces significant privacy risks, as data is vulnerable to leakage, unauthorized access, or malicious exploitation during transmission or at the server. For instance, in healthcare, patient data can be highly sensitive, and any breach of privacy could lead to a loss of trust and legal repercussions for institutions. In contrast, FL mitigates these risks by keeping data localized. Instead of sharing raw data, only encrypted model updates are transmitted between the client devices and the central server. This approach significantly enhances privacy protection, ensuring that sensitive information remains secure at its source. Moreover, FL can be combined with techniques such as differential privacy and secure multi-party computation to further enhance data privacy.
2. Communication overhead in CL: CL typically requires the transfer of vast amounts of raw data to the central server for model training, which results in high network bandwidth consumption. In data-intensive scenarios such as the Internet of Things (IoT), where numerous devices generate large amounts of data, this can lead to network congestion and significant delays. Moreover, many IoT devices have limited computational and storage capabilities, making such data transmission inefficient and resource-intensive. In contrast, FL significantly reduces communication overhead by only transmitting model parameters or updates, which are often orders of magnitude smaller than the raw data. This not only conserves bandwidth but also minimizes the delay, making it particularly suitable for low-bandwidth environments or scenarios with limited connectivity.
3. Computational inefficiency in CL: CL centralizes all computation at a single server, which can create a bottleneck, especially when dealing with large-scale datasets and complex models. The central server may become overwhelmed by the volume of data and the complexity of the computations, leading to slower processing times and lower overall efficiency. FL, on the other hand, leverages the distributed computational power of client devices. Model training is performed locally on each device, and the results are aggregated at the central server. This distributed approach allows for parallel processing, significantly improving computational efficiency. Additionally, FL can dynamically adjust training strategies based on the capabilities of individual devices, further enhancing performance in heterogeneous environments like IoT.

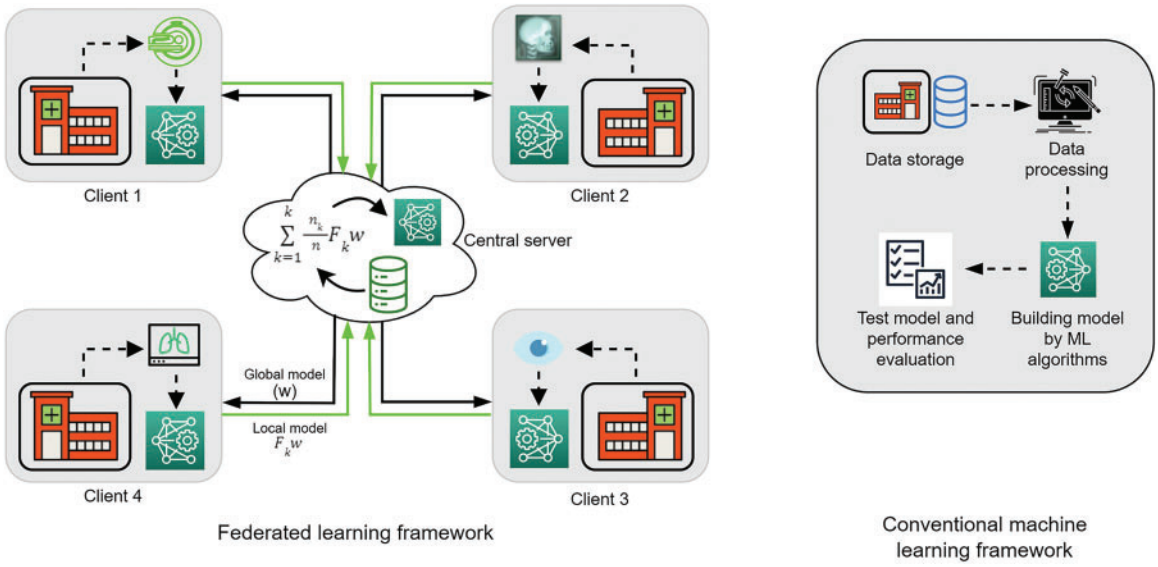

Figure 3: Comparison of FL and CL [14]

2.2 Foundations of Federated Learning

FL is an emerging ML paradigm that allows multiple distributed data owners to collaboratively train a shared model while preserving data privacy. Instead of transmitting data from data owners to the central node, FL distributes the model from the central node to each data owner, updates the model locally, and returns the updated model parameters to the central node for aggregation [15]. In this way, data owners can use their data for model training and inference, and can also enjoy the advantages brought by the global model. FL was first proposed by Google and implemented on its smart keyboard [13]. The basic algorithm of FL is Federated Averaging (FedAvg) [16]. The algorithm consists of the following steps [17], as shown in Fig. 4:

1. Initialization: The server initializes a global model and randomly selects a subset of data owners as participants;
2. Distribution: The central node sends the global model to the participants and specifies a local number of training rounds;
3. Update: Participants perform model updates on their local data and send the updated model parameters encrypted to the server.
4. Aggregation: The server aggregates the model parameters of the received participants to obtain a new global model;
5. Repeat: The server repeats the above steps until a preset termination condition is reached.

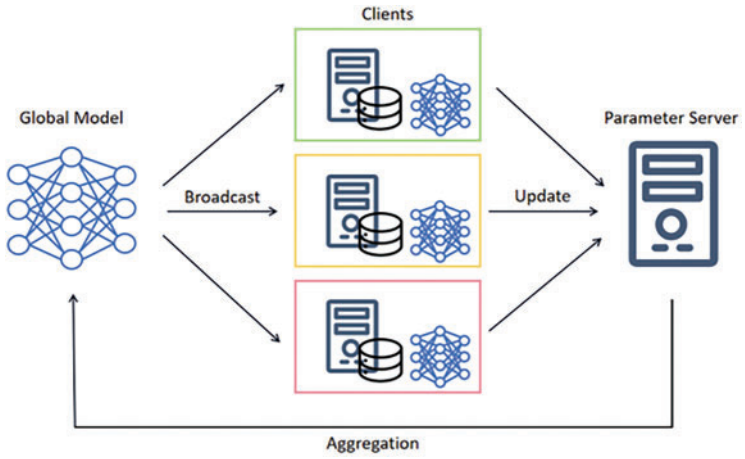

Figure 4: Process of FL

The basic assumptions of FL:

1. The data of data owners is non-independent and identically distributed (Non-IID), that is, each data owner's data comes from the same population distribution and is independent of each other. Studies have shown that traditional FL may converge slowly when the distribution of training data between clients is very different [18]. For example, a convolutional neural network trained with the FedAvg algorithm on a Non-IID dataset will suffer a significant reduction in accuracy, up to 55% for a highly skewed Non-IID dataset, the Keyword Detection (KWS) dataset [19].
2. The communication between the data owner and the central server is reliable, that is, the model parameters transmitted each time arrive at the destination intact and correctly, and will not be tampered with or corrupted.

2.3 Classification of Federated Learning

We divide FL into two categories based on data distribution and network structure, as shown in the Fig. 5.

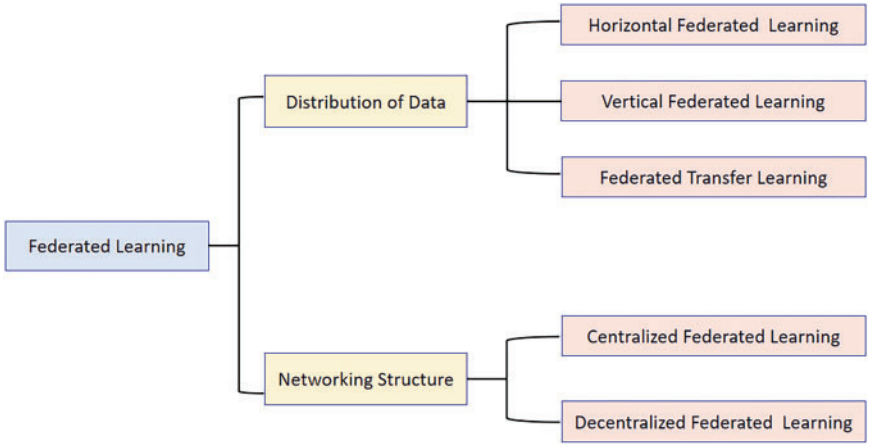

Figure 5: Classification of federated learning

2.3.1 Classification by Data Distribution

FL can be classified into horizontal FL, vertical FL and federated transfer learning according to the different distribution of training data, that is, the different distribution of training data in the sample space and feature space.

Horizontal FL (HFL) (Fig. 6): It is suitable for situations where the data features are similar between data owners but the data samples are different [20]. For example, banks in different regions can share credit scoring models of customers through HFL without revealing customers' personal information. In 2017, Google designed a HFL scheme for Android phone model updates. The core idea of this scheme is to let each Android phone user update the model parameters locally on his/her terminal device, and then transmit the updated parameters to the Android cloud, to build a centralized model with other users [17]. This approach has a notable advantage in its ability to manage data sources that share the same feature space, such as user data across multiple devices. The training process is relatively straightforward and easy to implement, allowing HFL to significantly enhance model performance while safeguarding user privacy through the use of diverse datasets. However, challenges may arise when HFL encounters Non-IID datasets, which can affect performance [21]. Additionally, as the volume of data increases, both communication overhead and computational costs may rise correspondingly;

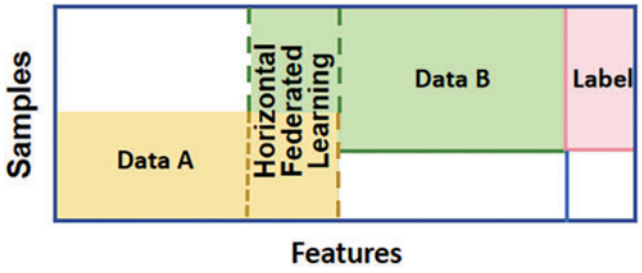

Figure 6: Horizontal federated learning (HFL)

Vertical FL (VFL) (Fig. 7): It is suitable for similar data samples between data owners but with different data characteristics. For example, a bank and an e-commerce company in the same region can share a customer's consumption behavior model through VFL without revealing the customer's transaction history or shopping preferences. Hardy et al. [22] proposed a VFL scheme to train a logistic regression model that can achieve privacy protection. Serpanos et al. [23] proposed a malware detection solution based on VFL, in which FL is used to develop detection models in environments with cross-island configurations. Experiments show that VFL can bring high malware detection accuracy for all clients. An advantage of VFL is its ability to manage data from different feature sets, such as patient records across multiple healthcare institutions, while protecting user privacy. VFL can improve model performance by leveraging complementary features and helps address challenges like label distribution skew and attribute skew [24]. However, VFL implementations are more complex compared to other methods, as they require entity alignment and data modeling. Additionally, when there are significant differences in the feature sets, model performance may be affected;

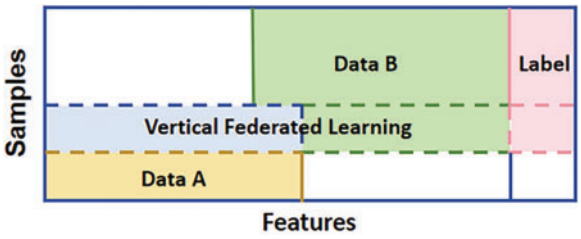

Figure 7: Vertical federated learning (VFL)

Federated Transfer Learning (FTL) (Fig. 8): It is suitable for the situation where data characteristics and data samples are different between data owners, which helps to reuse existing experience from the source domain to another related target domain to quickly adapt to the task of the target domain. For example, enterprises in different domains can use FTL to share related but different task models without revealing their own business data or domain knowledge. Majeed et al. [25] proposed and designed an FTL scheme for traffic classification. Tan et al. [26] used transfer learning to pre-train the dataset for breast cancer classification. One significant advantage of FTL is its ability to reduce training time and computational resource consumption by reusing pre-trained models on new tasks, making it particularly beneficial in scenarios where data is scarce or labels are limited. Additionally, FTL can enhance the generalization capabilities of models when applied to new tasks. However, the effectiveness of FTL can be influenced by the choice of pre-trained models and tuning strategies. Furthermore, when there is a considerable discrepancy in data distributions between the source and target tasks, the performance of the transfer learning process may be compromised [27].

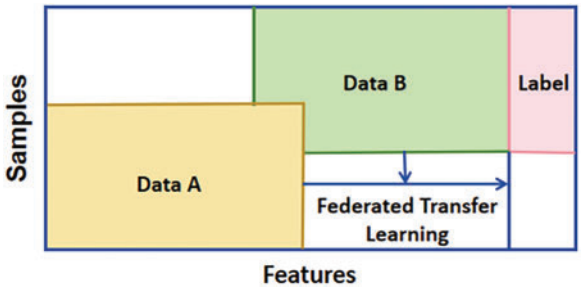

Figure 8: Federated transfer learning (FTL)

2.3.2 Classification by Network structure

According to different network structures, that is, different communication patterns between clients and servers, FL can be divided into centralized FL and decentralized FL [28]. The basic principles of centralized FL and decentralized FL are shown in Fig. 9.

Centralized FL (CFL): CFL adopts a client-server architecture, where all clients communicate with a central server, which coordinates and aggregates model training and updates for clients. CFL can effectively utilize the computing power and storage space of the central server to achieve fast and efficient model training and model updates. CFL is suitable for situations of stable network environment, low communication cost and small security risk. The reliance of CFL on a central server greatly enhances the speed and efficiency of model training, particularly when handling large datasets. This centralized framework facilitates model updates, thereby accelerating optimization processes.

However, such dependence may introduce potential bottlenecks, as network issues or bandwidth constraints can negatively impact performance [29]. Furthermore, the central server serves as a single point of failure, presenting security vulnerabilities if targeted by malicious attacks [30]. Additionally, privacy protection remains a significant concern, as centralized data processing heightens the risk of sensitive information leakage [31];

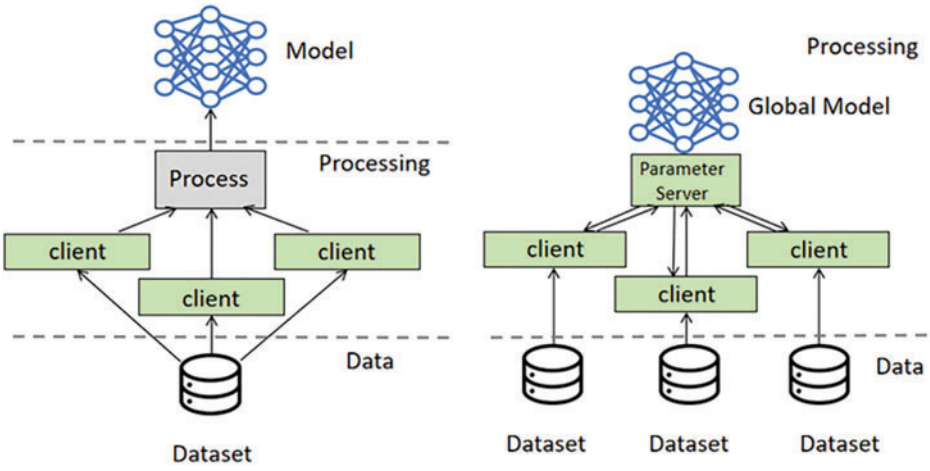

Figure 9: Comparison of centralized FL and distributed FL

Decentralized FL (DFL): DFL refers to the FL that does not set up a central server, and the clients communicate directly with each other. In a peer-to-peer manner, model information is directly exchanged between data owners for model training and updating. DFL can effectively protect the data privacy and model security of data owners, and realize flexible and reliable model training and model updating. It can be seen that DFL is suitable for situations of unstable network environments, high communication costs, and large security risks. Du et al. [32] proposed a DFL strategy and conducted experiments on the CIFAR-10 dataset. The results show that the ResNet50 model trained with this strategy is as good as the model trained with the CFL strategy. A key advantage of Decentralized Federated Learning (DFL) is its decentralized structure, which eliminates the need for centralized data storage and thus reduces the risk of data breaches. Additionally, by enabling direct communication between clients, DFL preserves flexibility in model training, even in unstable network environments. However, this approach has its drawbacks. The absence of central coordination can complicate network communication, potentially leading to longer model update times. Furthermore, the decentralized architecture may slow model convergence, adversely affecting overall training efficiency.

2.4 Advantages of Federated Learning and Its Application Scenarios

2.4.1 Potential Advantages of Federated Learning

The advantages of FL are as follows:

1. Effective data privacy protection: FL does not need to transfer data from the data owner to the central node, but only the model parameters, which can effectively protect data privacy. In addition, FL can also be combined with other privacy-preserving techniques, such as differential privacy, homomorphic encryption, and secure multiparty computation, to further enhance data privacy protection.

2. Small communication overhead: FL only needs to transmit the model parameters over the network instead of directly transmitting the raw data, which can greatly reduce the communication overhead. In addition, FL can also adopt some communication optimization techniques, such as compression, coding, layering, etc., to further reduce communication overhead.
3. High computational efficiency: FL can leverage the local computing power of the data owner to perform model updates in parallel and aggregate at a central node, which can significantly improve computational efficiency. In addition, FL can al-so perform adaptive model selection and update strategies according to the characteristics and needs of the data owner, thus further improving the computational efficiency.

2.4.2 Application Scenarios of Federated Learning

There are many potential application scenarios for FL in different domains (Fig. 10), such as:

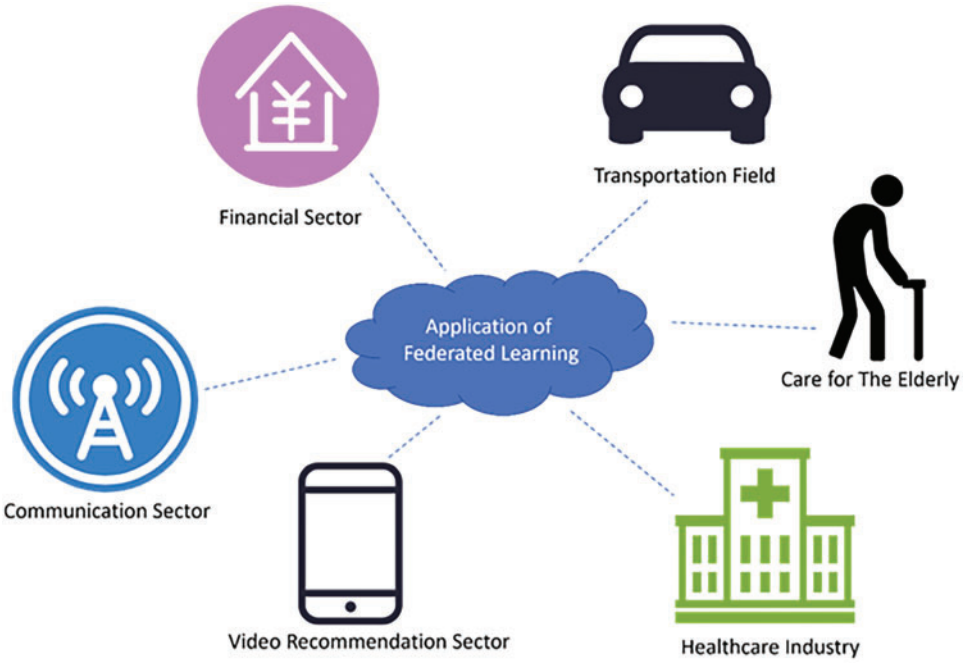

Figure 10: Applications of FL in different domains

Financial domain: Financial institutions can leverage data from different sources through FL to build more accurate and comprehensive risk assessment models, thereby reducing the risk of credit default, fraud, money laundering, etc. At the same time, financial institutions can also use FL to provide more convenient and reasonable financial services to users who lack credit information, such as rural areas and the self-employed. In addition, financial institutions can also use FL to combine user behavior data on different platforms to make more refined user pro-files and recommendations.

Medical field: Medical institutions can realize the sharing and analysis of medical data across institutions, regions and countries through FL, to improve the quality and efficiency of medical care. For example, medical institutions can use distributed medical image data to train more accurate diagnostic models through FL. Alternatively, healthcare organizations can leverage distributed genetic data through FL for more effective drug discovery and personalized treatment.

Communication field: Communication operators can optimize the allocation and management of network resources through FL to improve network performance and user experience. For example, communication operators can use FL to utilize network quality data on user devices for more intelligent network planning and scheduling. Alternatively, communication operators can use FL to leverage ap-plication usage data on user devices for more accurate traffic control and service recommendations.

Transportation: Traffic management departments and transportation service providers can achieve more efficient and safe traffic management and services through FL. For example, traffic management departments can use distributed traffic monitoring data and vehicle sensor data through FL to perform more re-al-time and accurate traffic state prediction and congestion control. Alternatively, transportation service providers can use distributed vehicle driving data and user travel data through FL for more intelligent and personalized driver assistance and trip recommendations.

Video recommendation: Video platforms can achieve video recommendation that is more in line with users' needs and preferences through FL. For example, video platforms can use video viewing data and feedback data on users' devices to train more accurate video recommendation models through FL.

Elderly care: Community service agencies can use the health data and behavior data on the elderly's devices through FL to provide more timely and intimate care services for the elderly.

3 Internet of Things Overview

This section comprehensively explores multiple aspects of the IoT, from its development history and core concepts to its characteristics and problems. For a comprehensive understanding of IoT, we subdivide the research content into three sub-chapters. Each of these sub-chapters provides an in-depth analysis of the historical background, key features, and key challenges of IoT. We review the literature in related fields to gain a deeper understanding of it through the perspectives and findings of different researchers. Table 1 is a summary of the papers on it.

Table 1: Summary of papers in the application fields of FL

Ref.	Domains	Key contributions	Advantages of FL	Limitations	Year
[13]	Healthcare Industry	Discussed the implementation of FL in medical imaging	Protect data privacy, improve model performance	High Communication Cost, Data Heterogeneity	2020
[33]	Healthcare Industry	Proposed a sensor-based PFL model for OCD detection	Protect data privacy	Data Heterogeneity, Personalization Complexity	2021
[34]	Healthcare Industry	Proposed an intelligent healthcare system based on FL	Protect data privacy Improve computational efficiency	High Communication Cost, Model Convergence and Accuracy	2021

(Continued)

Table 1 (continued)

Ref.	Domains	Key contributions	Advantages of FL	Limitations	Year
[35]	Healthcare Industry	Proposed a FL based model for masked psoriasis severity classification	Protect data privacy	Data Quality and Integrity, High Communication Cost	2022
[36]	Communication Sector	Proposed an SDN-based FL approach for satellite-IoT framework	Protect data privacy	High Communication Cost, Complex Network Topology	2023
[37]	Communication Sector	Proposed a UAV-Assisted edge intelligent system based on FL	Improve model performance	High Communication Cost, Resource Allocation Complexity	2023
[38]	Transportation Field	Proposed a FL based cooperative positioning scheme for social Internet of vehicles	Protect data privacy	High Communication Cost, Data Heterogeneity	2021
[39]	Video Recommendation Sector	Proposed an improved video recommendation system for IoT devices using FL	Reduce communication overhead	Data Heterogeneity, Device Selection and Coordination	2023
[40]	Care for the Elderly	Proposed a fall detection algorithm based on FL and extreme learning machine (Fed-ELM)	Protect data privacy	Manual Labeling Requirement, Data Heterogeneity	2022

3.1 Definition and Development History of IoT

The IoT, defined as a wirelessly connected network of things that enables various objects to interact with each other without human intervention, is expected to form an important part of the future Internet, consisting of billions of intelligent communication devices. With the development of technology, the IoT has begun to penetrate many fields such as healthcare, cities, and automobiles. It is combined with federal learning, thus giving birth to several emerging fields including smart healthcare, smart cities, and intelligent transportation [41]. For example, the Industrial IoT leverages RFID, wireless, mobile, and sensor devices to build powerful industrial systems and applications [42], while the medical IoT represents a deep integration of IoT with the medical industry. The Internet of Vehicles (IoV), as an emerging in-vehicle network infrastructure, demonstrates agility and interoperability,

enabling the building of vehicle networks using components from multiple vendors, and facilitating market competition and customization options [43].

It is a revolutionary technology paradigm that seamlessly connects the physical world with the digital world, allowing a variety of physical objects to communicate and collaborate via the Internet. Physical objects can be the vision of the IoT lies in the seamless connection between people and things, and between things, to enable real-time perception of the physical world, precise management, and scientific decision-making. The IoT is a network of sensors and devices that continuously generate data and exchange messages through a complex network, supporting machine-to-machine communication and monitoring and controlling critical smart world infrastructure [44]. The general definition of the IoT refers to various information sensing devices such as sensors, RFID technology, global positioning systems, infrared sensors, laser scanners, gas sensors, and other devices and technologies, objects, or processes that capture any monitoring, connection, interaction in real time to collect their sound, light, heat, electrical, mechanical, chemical, biological, location and other necessary information, Forming a huge network combined with the Internet [45].

3.2 Deficiencies of IoT

At present, the development of the IoT has penetrated into various industries, such as automotive, medical, urban architecture, personal homes, etc., which also means that a large amount of data may be generated that may contain users' private information, and the traditional centralized learning and processing methods on the cloud are faced with challenges due to high communication and storage costs and privacy issues [46]. However, due to the extensive application of the IoT and large-scale connectivity, various challenges and obstacles have been brought, including heterogeneity, scalability, security, big data, energy demand, etc. [47,48]. We describe three of these major deficiencies, as shown in Fig. 11. As shown in Table 2, we have also summarized the existing work of the IOT to demonstrate the existing problems in the IOT.

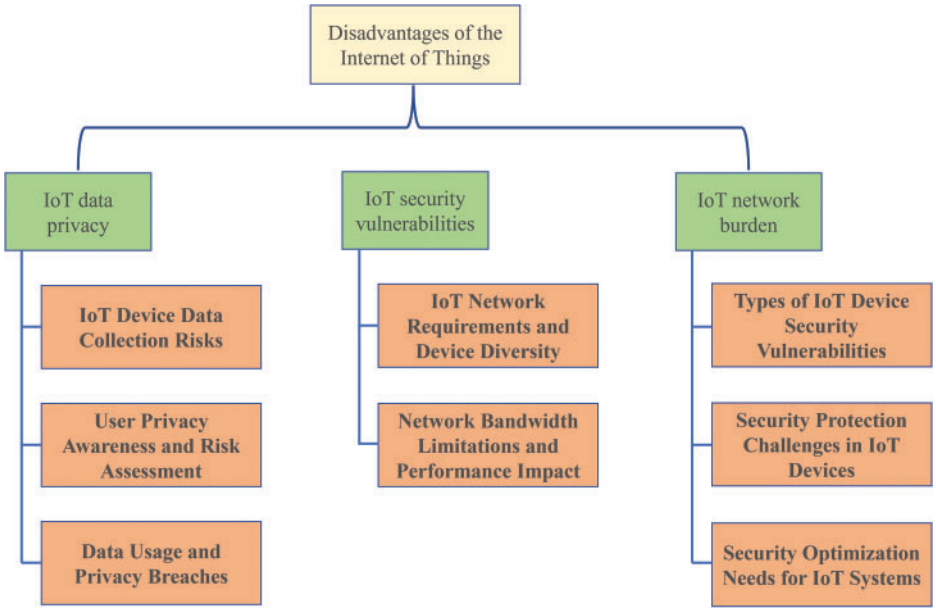

Figure 11: Three main shortcomings of the Internet of Things

a. Internet of Things data privacy: As an important area of current technological development, the IoT is playing an increasingly critical role in improving the convenience of daily life and the efficiency of industrial automation. However, the IoT extreme reliance on data also raises a series of profound questions about privacy and security. First, the proliferation of IoT devices means sensors and devices everywhere, from home environments to public Spaces, are constantly collecting data about individuals and the environment. This data can range from sensitive information such as an individual's activity habits to precise location information. The problem is that there is often a lack of transparency in the collection, storage, and processing of such personal data, which brings hidden risks to users' privacy and security. For example, smart home devices may collect detailed information about residents' daily activities, and this collection of personal data, combined with the increasing deployment of Internet-connected devices in homes, exposes residents to new privacy and security risks [49], which could be accessed by unauthorized third parties if not properly handled. Secondly, in the process of large-scale deployment and use of IoT devices, since most users are not Internet or security experts and do not have the ability to assess risks or security and privacy measures [50], they often lack a full understanding of the data collection and processing mechanisms of these devices. Even many users may use these devices without fully understanding the relevant privacy policies, which undoubtedly increases the risk of personal privacy being inadvertently disclosed or abused [51]. With the further development of artificial intelligence and machine learning technology, the data collected in large quantities is used to train complex algorithm models, which may further aggravate the privacy problem. For example, centralized learning is a traditional machine learning method, but it may leak user privacy because it uploads local data sets to the server [52].

b. Internet of Things network burden: The essence of the IoT lies in connecting devices and objects in the physical world through network technology to form a large and complex network system. This system not only connects physical objects but also covers multiple aspects such as data collection, transmission, and processing. As a network-based system, it puts a series of special requirements on the network. Different devices (such as mobile phones, wristbands, smart watches, laptops, etc.) may use different wireless communication technologies (such as Wi-Fi, Bluetooth, 5G, NFC, etc.), and may need to exchange data seamlessly between these different network technologies. Not only does the large number of devices communicating with each other make the already limited bandwidth of IoT gateways even more difficult. But also makes maximizing throughput while efficiently allocating bandwidth to connected devices a challenging problem [53]. If the network bandwidth is not satisfied, it will inevitably cause network congestion. Congestion will have a huge impact on the network, which will affect the network performance and lead to network failures [54]. When large amounts of data are trying to be transmitted over limited bandwidth, packets in the network begin to queue for transmission, causing latency to increase significantly. For applications that require real-time or fast response (such as emergency services, and real-time monitoring systems), this delay can seriously affect their functionality and efficiency.

c. IoT security vulnerabilities: IoT security vulnerabilities essentially stem from flaws or vulnerabilities in the system and can lead to serious security threats if not addressed promptly. These vulnerabilities include physical security risks against IoT nodes, exploitation of open debug ports, and leaving devices vulnerable to resource depletion attacks due to a lack of effective energy harvesting capabilities, as shown in detail in Fig. 12 of the classification of IoT vulnerabilities [55]. IoT devices are particularly vulnerable to adversary attacks due to their often limited computing power and energy. They are more exposed to cyberattacks than traditional computers. And, unfortunately, it is more difficult for these devices to obtain effective protection against cyberattacks [56]. Security vulnerabilities in IoT systems include inadequate physical security, open debug ports, lack of energy

harvesting capabilities, and weak authentication mechanisms. As a result, these vulnerabilities make IoT devices vulnerable to threats from direct physical access, such as node cloning and side-channel attacks, etc. [55]. Of particular concern is that since IoT deployments often consist of a group of devices with similar or nearly identical characteristics, this similarity amplifies the severity of security vulnerabilities [57]. The simplicity and regularity of IoT devices make them vulnerable targets. At the same time, because these devices often have access to users' sensitive data, it further increases the likelihood that they will be targeted. Therefore, when optimizing IoT systems, we must focus on addressing these vulnerabilities to ensure the security and stability of the system [56].

Table 2: Existing work in the Internet of Things

Ref.	Topic	Key contribution	Key problem
[44]	Internet of Things Edge Computing	Enhance the computing power of the Internet of Things and reduce communication overhead by using edge computing.	Network burden
[45]	Internet of Things Review	Introduced the concept of the Internet of Things, what technologies are used, what aspects it can be used for, and explained the importance of data privacy.	Data privacy
[58]	Internet of Things Challenges	Challenges of the IoT and related technologies of Thread networks are discussed.	Network burden
[59]	Internet of Things Privacy Protection	To study privacy protection technology, the Privacy Information Security Classification (PISC) model is proposed, which divides privacy into four security classifications, and studies the security objectives of each classification.	Data privacy
[60]	Internet of Things Reliable	This article provides an overview of future IoT applications and their main communication needs, and briefly reviews recent work in four main areas: resource allocation, latency management, security and reliability metrics.	Network burden
[47]	Internet of Things Review	It concisely explains the concepts and applications of the Internet of Things, as well as challenges and opportunities.	Network burden
[49]	Smart Home	Study smart home technology adoption and related factors such as privacy concerns, performance expectations, trust in outcomes and social impact.	Data privacy
[50]	Internet of Things Privacy	Through quantitative survey and analysis, we provide an in-depth exploration of users' perceptions of IoT security and privacy issues, and how these issues affect the adoption of IoT technology in the home field.	Data privacy

(Continued)

Table 2 (continued)

Ref.	Topic	Key contribution	Key problem
[53]	Internet of Things Data Processing	A method called BACOFF is proposed, which takes into account the characteristics of IoT devices and gateways as well as the needs of specific services.	Network burden, Data privacy, and Security vulnerability
[55]	Internet of Things Challenge	The paper delves into security vulnerabilities and energy efficiency issues of IoT devices and provides practical solutions and recommendations for IoT sustainability.	Security Vulnerability
[56]	Internet of Things Security	This paper effectively solves the problem of lack of label information in IoT networks by proposing a new deep transfer learning model, while achieving significant improvements in the accuracy of IoT attack detection.	Security Vulnerability
[57]	Internet of Things Challenge and Security	This paper provides an effective solution to protect user privacy and security information by proposing a new IoT hierarchical model and implementing a cloud/edge supported IoT system.	Security Vulnerability

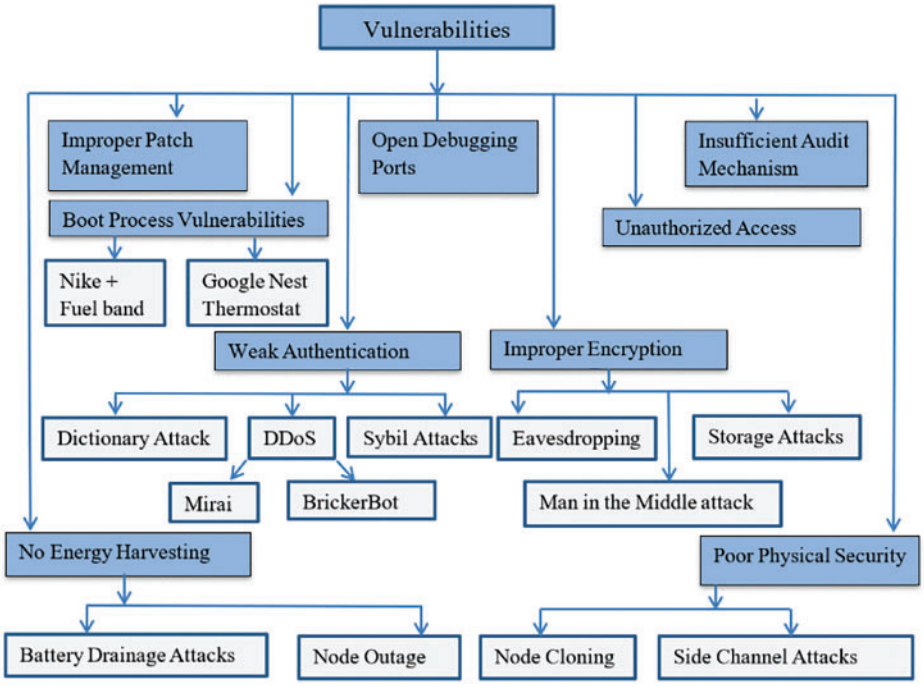

Figure 12: Classification of IoT vulnerabilities [55]

4 Internet of Things under Federated Learning

4.1 Vision of Federated Learning Combined with the Internet of Things

With the rapid development of the IoT, there has been an explosion in the number of devices and the amount of data. However, in the traditional IoT system, the model training is often on the data center or cloud server, due to the limited computing power and storage capacity of IoT devices, as well as the existence of data privacy and security issues, so the data of IoT devices cannot be fully utilized, which poses a huge challenge to the development of data-driven intelligent applications. FL, as a new machine learning framework, can make full use of the data of distributed devices while protecting data privacy, to achieve more efficient model training and prediction. Therefore, the combination of FL and the IoT will provide new possibilities for intelligent, personalized, and secure IoT.

First of all, the combination of federal learning and the IoT can realize the intelligence of IoT devices. IoT devices usually require a lot of data processing and analysis to enable various intelligent applications, such as smart cities, smart healthcare, etc. However, due to the limited computing power and storage capacity of IoT devices, as well as the existence of data privacy and security issues, the data of IoT devices cannot be fully utilized, which poses a huge challenge for the development of data-driven intelligent applications. FL, through model training on the device side, can make full use of the data of IoT devices, thus achieving more efficient model training and prediction. In addition, FL can realize knowledge sharing among devices through model aggregation, thus improving the generalization ability and prediction accuracy of the model. Secondly, the combination of FL and the IoT can realize the personalization of IoT devices. IoT devices usually need to provide customized services according to the individual needs of users. However, traditional machine learning methods usually need to centralize the data of all devices into one place for training, which not only leads to data privacy and security issues but also fails to meet the personalized needs of users. FL can protect the user's data privacy through model training on the device side and also can customize the model training according to the user's personalized needs, to realize the personalized IoT devices.

The data of the IoT device usually contains a large amount of sensitive information, such as the user's location information, health information, etc. The disclosure of this information may pose a threat to the user's privacy and security. By conducting model training on the device side, Federal Learning can protect the data privacy of users, and at the same time, it can realize knowledge sharing among devices through model aggregation, without the need to share data directly, to realize the security of IoT devices.

In the following, we will introduce through extensive work what services are provided for the IoT by introducing FL and the applications of FL in the IoT.

4.2 Services Provided by Federated Learning in the Internet of Things

In the context of the Internet of Things (IoT), the application of Federated Learning (FL) primarily focuses on several key areas, including privacy security, attack detection, communication efficiency enhancement, and learning quality improvement. FL effectively safeguards user privacy by allowing devices to process data locally and share model parameters, while also enhancing the accuracy and efficiency of attack detection. Furthermore, FL optimizes data transmission, reducing communication overhead, and improves model performance and adaptability through distributed learning. To systematically present these research findings, Table 3 summarizes the key information from the relevant studies, including the datasets used and evaluation metrics, providing readers with a clearer understanding of the practical applications of FL in the IoT domain.

4.2.1 Privacy Security

In the IoT environment, the data generated by the device usually contains a large amount of sensitive information, such as the user's personal information, location information, health status, etc. If this information is used improperly, it may cause serious infringement on the user's privacy. Therefore, how to protect users' privacy and security while ensuring data utilization has become an important issue in the development of the IoT. Common problems to solve are data encryption algorithms, such as AES (Advanced Encryption Standard), ECC (Elliptic curve cryptography) and SHA (secure hash algorithm), and access control algorithms (access control algorithms are mainly used to control user's access to data), such as RBAC (role-based access control), ABAC (attribute-based access control) and so on. However, although these traditional privacy protection methods improve the security of IoT data to a large extent, they may affect the performance of IoT devices with limited resources, and there is a risk of exposing users' privacy in the process of data collection. FL, as a distributed machine learning method, provides a new way to solve this problem. In FL, each device no longer needs to send the original data to the central server, but trains the model on the local device. Each device only needs to send the parameters of the model to the central server, and the central server does the aggregation of the model. In this way, the user's original data will not leave the local device, thus effectively protecting the user's privacy. For example, FL has been applied in the medical field to protect the privacy of patient information. Sun et al. explored the classification of massive medical sensor data by developing a scalable and transferable FL Classification System (SCALT) [61]. In this process, FL only shares computational results by keeping patient data at the source While concealing the patient's personal information, thus realizing data privacy protection. Also in the field of smart medicine, Wang et al. proposed a privacy-enhancing disease diagnosis mechanism using federal learning for medical IoT [62]. The mechanism first reconstructs medical data via variational autoencoders (VAE) and adds differential privacy noise to enhance privacy protection. This data is then used to train a local disease diagnosis model, thereby protecting patient privacy. The work designs incentives to encourage participants to participate in federal learning and rewards participants accordingly. In addition, to ensure the security and privacy of sensor IoT architecture, a blockchain-based FL approach for sensor networks is proposed [63]. The challenges of low latency, availability, real-time data traceability, and security in IoT-based systems are addressed by introducing a permission-enabled blockchain architecture that supports FL. The architecture supports end-device privacy, prioritizes data and user privacy, and provides anonymity and transparency upon user request.

Table 3: Summary of federated learning services in IoT

Ref.	Datasets used	Key contribution	Best performance	Year
[61]	MIT-BIH-AR, MIT-BIH-SUP, INCART, Sleep-EDF, Wrist PPG During Exercise	Proposed a scalable and transferable federated learning system (SCALT) for classifying healthcare sensor data, which addresses the challenges of dynamic data distributions and the appearance of initially unknown classes	Accuracy: 98.65%	2023

(Continued)

Table 3 (continued)

Ref.	Datasets used	Key contribution	Best performance	Year
[62]	MIT-BIH	Proposed a privacy-enhanced disease diagnosis mechanism using federated learning (FL) that incorporates variational autoencoder (VAE) and differential privacy to protect patient data from inference attacks	N/A	2023
[63]	Sampled Electrochemical Sensors (ECS)	Proposed PPFchain, a privacy-preserving blockchain-based federated learning framework for sensor networks, which ensures data security and traceability	N/A	2023
[64]	MNIST, CIFAR-10, Shakespeare	Provided the first theoretical and experimental analysis of free-rider attacks in federated learning, demonstrating how attackers can obtain the final aggregated model without contributing data	N/A	2021
[65]	Various datasets depending on specific experiments	Conducted a comprehensive survey on privacy and robustness in federated learning, covering threat models, privacy attacks and defenses, and poisoning attacks and defenses	N/A	2023
[66]	Car Hacking: Attack & Defense Challenge 2020 Dataset	Proposed a federated learning-based attack detection framework for vehicular sensor networks using a combination of Gated Recurrent Units (GRU) and Random Forest (RF)	Accuracy: 99.52%, Precision: 99.77%, Recall: 99.54%, F1-score: 99.65%	2022
[67]	IoT-Botnet 2020	Proposed a federated deep learning framework using a deep neural network (DNN) and mutual information (MI) for effective anomaly detection in IoT networks	Accuracy: 99.52%	2023

(Continued)

Table 3 (continued)

Ref.	Datasets used	Key contribution	Best performance	Year
[69]	MNIST, Fashion-MNIST, CIFAR-10	Introduced FedQNN, a framework that combines low-bitwidth quantization with federated learning to reduce computational and communication overheads for IoT devices	Computational energy savings: Up to 90%, Model size reduction: Reduced by 30+ times, Maintained reasonable accuracy across datasets	2023
[70]	MNIST, EMNIST	Proposed HCFL, a high compression approach for federated learning in large-scale IoT networks, which reduces communication costs and makes intensive learning processes more adaptable on low-computing resource IoT devices	Compression Ratio: Up to 32 times, Test Accuracy on MNIST (LeNet-5): 99% with a compression ratio of 1:16	2023

4.2.2 Attack Detection

In the IoT environment, due to the large number and wide distribution of devices, this makes IoT devices an important target for attackers. Traditional centralized attack detection methods need to centralize the data of all devices into one place for analysis, which may not only lead to data privacy disclosure but also bring huge computing and storage pressure in the case of a large amount of data. To deal with the attacks in the IoT, methods such as adversarial training [64] have been proposed, but most of these methods are applied to specific types of attacks and cannot be well extended to the current environment of distributed IoT. For this reason, federation learning has become an effective means for IoT attack detection. In IoT attack detection, FL can be used to identify various types of malicious activities, such as DDoS attacks, intrusion attempts, and abnormal traffic patterns [65].

With the rapid development of vehicle technology, modern vehicles have introduced several smart sensors that help drivers effectively identify traffic and road signs, monitor roads, reduce the risk of collisions, and provide an accurate estimate of the distance between the vehicle and surrounding objects. However, the complexity of the architecture of vehicle-mounted sensor networks, the diversity of communications, and the high mobility of vehicles make these networks vulnerable to multiple cyber attacks. Recently, MDriss et al. have proposed a federal learning framework for vehicle sensor network attack detection [66] in which a gated cycle unit (GRU) of a set of random forest (RF) integrated units is employed for the efficiency of processing sequential data, which is critical for detecting patterns that indicate a network attack. RF is used to improve the accuracy and robustness of GRU model predictions. Moreover, the federal learning method proposed in this paper shows high accuracy in detecting cyber attacks in vehicle sensor networks, with accuracy, recall, and F1 scores of 99.77%, 99.54%, and 99.65%, respectively. By combining FL and deep learning, it can be applied to anomaly

detection in the IoT. A recent method combines deep neural networks and FL [67] and uses mutual information as an effective detection method to detect anomalies in the IoT. In addition, this method uses dispersed device-side data for model training, saves the information on localized IoT devices, and shares the modified weight only in the centralized FL server, which greatly protects the privacy of the data. By deploying the FL model on each IoT device, network traffic, and device behavior can be monitored in real-time. When an abnormal state is detected, the system can take quick measures, such as isolating the affected device, to prevent further data leakage or system damage.

4.2.3 Achieving Efficient Communication for the Internet of Things

In an IoT environment, thousands of devices need to communicate with each other to collect, share, and process data. However, due to the limited computing power and storage capacity of IoT devices, as well as the constraints of network bandwidth, the traditional cloud-centered learning approach faces significant challenges [68]. FL, as a distributed machine learning paradigm, can realize learning tasks through the aggregation of local computation and model updates without directly sharing data, thus providing a solution for efficient communication for IoT. FL allows IoT devices to do data processing and model training locally, which means that only model parameters or gradient information need to be transmitted in the network, not the raw data [7]. This greatly reduces the communication load, as the model parameters are typically much smaller than the original data set. FL supports asynchronous communication, which is important for devices in IoT environments that may not be constantly online due to energy constraints, shaky network connections, or other environmental factors. In FL, devices can perform calculations locally and upload updates when conditions permit, without the need for all devices to be online at once. In addition, FL can optimize communication efficiency through intelligent scheduling and resource allocation strategies. For example, a recently proposed FL framework for computing and communication efficiency in IoT scenarios [69]. It introduces ultra-low bit-width quantization technology into the FL environment for the first time, enabling end devices to perform fixed-point computation with low power consumption and low memory footprint. At the same time, it adopts a combination strategy of quantization and sparsity to compress data transmission down and down lines, which greatly reduces the communication bandwidth and data volume. In addition, it also considers the case of unbalanced data distribution, ensuring the convergence and accuracy of the model. For large-scale IoT networks, MD Nguyen et al. also proposed a new compression scheme [70], called High Compression FL (HCFL), for large-scale IoT networks. HCFL utilizes an incomplete autoencoder structure to achieve improved communication efficiency in the FL process while maintaining the quality of the model. Moreover, the relationship between the number of IoT devices and the convergence level of the FL model is also studied in this paper to better evaluate the quality of FL. As the number of IoT devices continues to increase, these advantages of FL will become more and more significant, which is of great significance for promoting the development and application of IoT technology.

4.2.4 Enhance the Quality of Learning

In the context of IoT, FL offers a unique way to enhance the quality of learning by training models across multiple devices in a distributed manner without the need to centralize data into a single location. By drawing large amounts of computing resources and different datasets from a network of IoT devices, leveraging local data on individual devices can improve the generalization and accuracy of the model, something that cannot be done with centralized learning that uses insufficient data and limited computing power. Here are a few aspects of how FL can enhance the quality of learning in IoT:

1. Data diversity: IoT devices are distributed in different geographical locations and environments, and the data of each node is usually Non-IID [71]. For example, air quality monitors in cities may have significantly different characteristics of the data collected compared with those in rural areas, and frequently uploaded models on certain specific nodes may attract divergence from the global model. These devices are distributed in different geographical locations, and the data collected is highly diverse. FL allows these devices to train the model together without sharing the original data, which allows the model to learn a wider and more diverse set of data features, thereby improving the model's generalization performance.
2. Real-time learning and adaptation: IoT devices can continuously collect large amounts of data that reflect changing environments and user behavior. With FL, these devices can not only collect data in real-time but also update and optimize their models locally. This means that the models can adapt to new data distributions and environmental changes in real time, without having to send data to a central server for processing. Such a learning mechanism greatly enhances the flexibility and timeliness of the learning process, while also improving the efficiency of data processing and privacy protection. In addition, FL enables devices to achieve collaborative learning by sharing learning outcomes while maintaining their independence, further enhancing the overall learning effect and application value.
3. Improve model robustness: In FL, the model needs to perform well on a variety of devices, which forces the model to have better robustness. The improvement of model robustness is conducive to resisting various adversarial attacks, protecting the training process and the effectiveness of the model; It is beneficial to promote the performance fairness of the system and ensure the balanced performance of different clients. In the face of diverse devices and data environments, strengthening model robustness becomes a key strategy to improve the overall system performance and security in FL.
4. Personalized services: FL supports personalized model training while protecting user privacy [72]. This means that IoT devices can provide more customized services to better meet the personalized needs of users. This personalized service can be used for home health monitoring, with trained cloud models based on common data sets from dispersed homes, which may not capture the specific characteristics of a single target user well. For personalized home health monitoring, each user can train a personalized model by integrating the trained global model with his health data. Of course, this kind of personalized service can also benefit the development of other industries, such as connected vehicles, smart homes, precision agriculture, personalized digital immersion, and wireless systems.
5. Cross-domain collaboration: FL allows IoT devices of different domains and ownership to collaborate to train and improve models together, without directly ex-changing data. This cross-domain collaboration dramatically enhances the quality of learning, especially in complex application scenarios that require the fusion of knowledge from multiple domains. Under this concept, the federal imitation learning framework realizes the imitation of the cross-domain model state through the knowledge-sharing module, to optimize traffic scheduling in the IoT environment, reflecting the practical application and benefits of cross-domain collaboration.

4.2.5 Limitations of the Study

In this study, although FL demonstrates numerous advantages in its application within IoT, such as enhanced privacy protection, improved attack detection capabilities, optimized communication

efficiency, and elevated learning quality, it still faces several challenges and limitations during implementation.

Firstly, high communication costs present a significant issue. Research across various fields indicates that the implementation of FL may incur substantial communication overhead. For instance, studies in the healthcare, telecommunications, and video recommendation sectors highlight that the frequent demand for data transmission increases network burdens, particularly in large-scale distributed environments, where such costs become even more pronounced. Additionally, data heterogeneity poses another major obstacle for FL applications. The differences in data generated by various devices and users not only affect the training effectiveness of the models but may also lead to a decline in model performance. Relevant studies have shown that this issue is especially prominent in the healthcare and transportation sectors, where data diversity and inconsistency are particularly evident.

Furthermore, the effective allocation of computational resources to support the efficient operation of FL remains a challenge. This is particularly crucial in scenarios involving drone-assisted edge intelligence systems or sensor networks within vehicular networks, where the proper allocation of resources is vital to ensuring overall system performance. At the same time, the quality and integrity of data directly impact the training outcomes of the models. In healthcare studies, inaccurate or missing data can lead to erroneous decisions, subsequently affecting the quality and reliability of services. Moreover, in the field of elder care, training effective fall detection algorithms necessitates a substantial amount of manually annotated data, which is not only time-consuming but also costly.

Lastly, the complexity of personalization is another critical concern. In the healthcare sector, designing and implementing FL models to meet specific user needs entails considerable complexity, particularly in highly personalized application scenarios such as mental health detection. In summary, while FL offers many potential advantages for IoT, overcoming the aforementioned challenges is essential to ensure the effectiveness and practicality of the technology in real-world applications. Future research could focus on reducing communication costs, improving data quality, and optimizing resource allocation, thereby further promoting the widespread adoption of FL in the IoT domain.

4.3 Application Fields of Federated Learning in the Internet of Things

4.3.1 Sensors

Sensors are the fundamental components of the IoT, responsible for collecting environmental data such as temperature, humidity, light, and movement. The application of Federated Learning (FL) in this context must address the critical needs for data privacy and efficient real-time processing, as centralized data storage and processing can lead to significant risks of data breaches and bandwidth constraints. This data often requires processing and analysis to provide valuable insights and intelligent decision support. However, due to privacy protection and bandwidth constraints, centralizing all sensor data into one central location for processing may not always be feasible [73]. In such cases, FL offers an effective solution. Under the Federation learning framework, sensor devices can train shared machine learning models locally as participants (otherwise known as clients). Each sensor updates the model parameters based on the data it collects and then sends these updates to a central server. The server is responsible for aggregating these updates from multiple sensors to improve the global model. This approach not only reduces data transfer and reduces communication costs, but also enhances data privacy protection.

Recently, there has been extensive research on applying FL to sensors to address various challenges. For instance, acoustic sensor networks enable the use of data from widely distributed acoustic sensors for location services, voice enhancement, and activity monitoring [74–76]. To enhance the privacy protection of acoustic sensor networks, the introduction of FL becomes an effective means [77]. This privacy-protecting unsupervised clustering FL method groups microphones by evaluating the similarity of model weight updates introduces a lightweight variational autoencoder and provides supplementary control criteria for the algorithm to speed up convergence. Similarly, aiming at the detection of abnormal states in sensor systems, DH Tran et al. proposed an improved sensor anomaly detection method in IoT systems using FL [78]. This method tackles the challenge of detecting anomalies in manufacturing systems caused by abnormal behavior of smart sensors, which may indicate failures or potential risks during operation. Such approaches demonstrate the significant potential of FL in processing sensor data effectively while maintaining privacy and responsiveness.

As federated learning technologies continue to evolve, more innovative applications are expected to emerge, maximizing the potential of sensors in IoT. The ability of FL to adapt to the unique requirements of sensor networks positions it as a promising approach for enhancing data privacy, enabling efficient real-time processing, and facilitating collaborative learning among devices.

4.3.2 Smart Healthcare

In smart medicine, AI-based approaches have been widely used to learn health data to facilitate medical services, such as medical imaging [79] and drug prediction [80]. Medical data often contains sensitive personal health information, has extremely high requirements for privacy protection, and has different patient populations and data sets for different healthcare institutions. In complex healthcare environments, deleting data such as patient information is not enough to protect patient privacy, and multiple parties such as hospitals and insurance companies have access to medical databases, including data analysis and processing. Clearly, using traditional AI methods and relying on a central server for analysis is not an effective solution. Federal learning allows for joint training and improvement of predictive models across healthcare institutions without sharing raw patient data, thereby facilitating the development of medical research and services without violating privacy regulations [81]. Recent work has demonstrated the advanced capabilities of federal learning in the field of smart health care. FL is a viable way to connect healthcare institutions' electronic medical record data, allowing them to share their experience instead of their data and guaranteeing privacy. Specifically, Lee et al. [82] proposed a privacy protection platform in an FL environment for patient similarity learning across institutions. Their model can find similar patients from one hospital to another without sharing patient information. In the field of medical images, Lai et al. [83] proposed a lightweight federal learning method to detect COVID-19 in chest CT images, addressing the need for effective and rapid diagnostic methods in the face of the global spread of the novel coronavirus. This method standardizes the local training process through the global average feature vector, reducing the communication burden of joint learning while maintaining the accuracy of detecting COVID-19 on chest CT images. Many customers choose different local models according to their computing power and do not need to transmit the parameters of the model, only need to transmit the average feature vector, which can protect the privacy of the data. To sum up, the application of federal learning in the field of smart medicine provides new possibilities for improving the quality and efficiency of medical services as well as the treatment experience of patients.

4.3.3 Smart City

A smart city refers to the use of modern information technologies, including the IoT, cloud computing, big data, and artificial intelligence, to optimize a city's infrastructure, services, and management, and enhance a city's sustainability, economic development and residents' quality of life [84,85]. The core objectives of a smart city are to achieve optimal allocation of resources, improve the efficiency of public services, enhance urban safety, and promote environmental protection through efficient data management and analysis. In addition, the aim is to. Although the concept and practice of smart cities have made remarkable progress, there are still a number of challenges in practical operation:

1. Data privacy and security: Smart cities rely on a large amount of data collection and processing, which involves the personal privacy and data security of residents. How to protect personal privacy while collecting and utilizing data is an important issue in the development of smart cities.
2. Data silos: Different city administrations and service providers may form data silos, that is, data is stored in isolation and difficult to share and integrate across departments, which limits the value of data and the overall effectiveness of smart cities.
3. Data processing power: With the increase of IoT devices, the amount of data is exploding, which puts higher demands on data processing power. How to effectively process and analyze massive amounts of data is one of the technical challenges facing smart cities
4. System integration and interoperability: Smart cities involve the integration of multiple systems and applications, and poor interoperability between different systems can lead to inefficiencies and increase management costs.

In view of the above problems, federal learning provides new ideas and technical support for the development of smart cities. Through FL, decentralized data resources can be used more effectively, and the intelligent level of urban management and services can be improved. FL has the advantages of distributed processing and effective privacy protection. Some scholars apply FL to road defect detection called the 3Pod system [86], in which computer vision technology is used to automatically detect road defects to ensure road safety and efficiency. FL then trains the model on data distributed across multiple devices or locations without centralizing the data, and it enables the system to utilize data from a variety of sources without compromising privacy. By using FL, the 3Pod system can continuously learn and improve its detection capabilities by aggregating knowledge from different locations and devices, thus ensuring that the model stays up to date with the latest road conditions. Predicting urban traffic flow is an important application for smart cities, however, data privacy has become a real concern. Recently, Djenouri et al. [87] proposed a new federal deep learning method for predicting urban traffic flow forecasts by pre-processing road networks to eliminate noise from traffic data. Next, anomaly feature detection is performed to trim uncorrelated edges and patterns. The generated graph is then used to learn the graph convolutional neural network to calculate the traffic flow of the future city. In this process, massive data is effectively processed based on the FL framework, and the data privacy is well protected by the characteristics of the FL place.

4.3.4 Networking of Vehicles

Vehicle networking technology is in a stage of rapid development. With the commercialization of 5G communication technology and the progress of intelligent vehicle technology, the application scenarios of vehicle networking are constantly expanding, including intelligent traffic management, vehicle remote monitoring, automatic driving assistance systems, vehicle maintenance prediction, and

so on. At present, many countries and regions have begun to deploy vehicle-connected infrastructure, such as intelligent street lights, traffic signal systems, roadside units (Rsus), etc., and more and more vehicles are equipped with vehicle-based communication systems (V2X). At the same time, major automakers are actively developing and promoting vehicle-connected technologies to improve vehicle safety and driving experience. However, the rapid development of connected vehicles has also brought a series of problems, and privacy and security issues have always been the focus of attention, as connected vehicle systems need to process and store a large amount of personal location data and behavioral information. In addition, due to the huge amount of data generated by the Internet of Vehicles, high requirements are put forward for data processing capabilities, and traditional data processing methods of centralized learning may not be able to meet the needs of real-time and efficiency. In addition, network latency and bandwidth limitations are also technical challenges facing the Internet of Vehicles, which may affect the quality of the Internet of Vehicles service and user experience.

FL offers an innovative solution to these challenges. As a distributed machine learning method, FL allows vehicles to train data models locally and share only model parameters or updates, rather than raw data, which can effectively reduce the amount of data transfer and reduce dependence on central servers while protecting user privacy. In addition, when computing locally in the vehicle or roadside unit, FL can improve data processing efficiency, reduce network latency, and improve the real-time performance of vehicle-connected systems. Recently, researchers have applied the improved FL method to the Internet of Vehicles. For example, Pervej et al. [88] applied FedProx [89] as the core to the Internet of Vehicles, which can solve the problem of unbalanced data distribution in the Internet of Vehicles. By introducing a near-end entry to control data heterogeneity. The FedProx is also improved to adapt to the online learning requirements of vehicles. In terms of communication optimization, the authors consider the high-speed movement and delay limits of vehicles, and propose an optimized communication and computing resource allocation scheme, which enables each vehicle to complete the local model training and upload within the specified time, while ensuring the accuracy and robustness of the global model. With the rapid development of new energy, the battery technology of electric vehicles continues to advance, the battery energy density increases and the cost decreases, making the endurance capacity of electric vehicles significantly improved. At the same time, charging technology is also constantly developing, with fast charging stations becoming more and more popular and charging speeds improving. However, electric vehicles need an effective charging network, and intelligent charging network management has become a challenge for the development of electric vehicles. Federal learning can help optimize the distribution and charging scheduling of charging stations to reduce charging wait times and balance grid loads, and by running learning algorithms on local EVs and charging stations, model updates rather than detailed charging data can be shared, thus protecting user privacy. Recently, Li et al. proposed [90] an FL framework that enables mobile slave stations to train model parameters locally and upload them to edge servers periodically for global parameter aggregation. This paper uses a stacked long Short-term memory (LSTM) model to predict future charging locations and a scoring mechanism to preprocess local datasets. After a lot of simulation experiments and comparisons, this federal learning framework significantly shortens the waiting time of electric vehicles, improves the charging ratio, reduces the charging cost, and speeds up the training convergence speed.

5 Open Challenges and Possible Solutions

As mentioned above, the combination of FL and IoT has great development potential and broad application prospects, which can provide ML solutions with low data leakage risk, low data

transmission overhead, low latency, and high generalization ability for intelligent applications in various fields [91]. However, despite FL offering new ideas and innovative solutions for processing the large amount of data generated by smart devices in IoT, numerous studies have shown that applying FL to IoT still faces several challenges. In this paper, we analyze and summarize the typical challenges faced by the current combination of FL and IoT starting from the limitations of FL and IoT as well as the difficulties encountered when applying FL in the field of IoT.

5.1 High Communication Load

In FL, participants do not need to exchange raw data but still need to exchange model parameters or gradient information frequently, which leads to the consumption of a large number of communication resources. Especially when FL is applied to IoT, the explosive growth of data generated by massive devices in IoT makes the challenge of the high communication load faced by FL more severe. However, excessive communication load will lead to communication delay, seriously reducing communication efficiency and model convergence speed. Frequent communication will also increase energy consumption and computational overhead, which will affect the performance and lifetime of the device. Several possible solutions to the problem of high communication load in FL have been proposed. They can be mainly divided into the following categories.

Communication compression. Communication compression refers to the use of compression algorithms to quantize or sparsify the model parameters or gradient information to be transmitted to reduce the size of model updates. The quantization algorithm maps the model updates to a set of discrete values [5], and the sparsification algorithm selects only a small number of important model updates for transmission. Cui et al. [92] systematically studied the relationship between compression ratio and model accuracy in FL in the network environment and proposed a framework suitable for different compression algorithms. The framework maximizes the model accuracy by adjusting the compression rate and is tested on popular datasets such as MNIST and CIFAR-10. The test results show that the framework can effectively reduce network traffic while maintaining high model accuracy.

Communication Optimization. Communication optimization refers to designing more efficient FL algorithms to reduce the number of communication rounds or reduce the frequency of communication. For example, the FedDM method aims to reduce the number of communication rounds in FL by using iterative distribution matching, which constructs local surrogate functions by learning a synthetic dataset to approximate the local training objective. These surrogate functions are transmitted to the server to construct and update a global surrogate function. By sending synthetic data instead of local model updates, FedDM reduces the amount of information required by the server and significantly improves communication efficiency [93].

Communication scheduling. Communication scheduling refers to dynamically adjusting the policy or parameters of communication to adapt to different network environments or device states by selecting appropriate participants. Yang et al. [94] proposed that FL at the edge of the network can be optimized through radio resource allocation and scheduling, including user selection, bandwidth allocation, and batch allocation. They define a new performance metric: training efficiency, which accelerates convergence, reduces the number of communication rounds, and improves the accuracy of the training process, and propose an effective algorithm that adjusts the user's wireless channel, computing power, and local data set to achieve a significant improvement in system performance.

5.2 Security and Privacy Issues

With the gradual popularization of IoT technology and the rapid development of FL, there have been significant changes in users' lifestyles and work practices. An increasing number of individual and enterprise users are utilizing IoT devices to process personal data, financial data, and business data [95]. This data often involves users' privacy and sensitive information, which, if not adequately protected, could lead to data breaches and privacy violations. Although FL does not directly share raw data, there remains a potential risk of privacy leakage. Therefore, it is particularly important to propose effective strategies and implement robust measures to enhance privacy protection.

In terms of security challenges related to the application of FL in the IoT environment, the types of attacks can primarily be categorized into adversarial attacks and privacy attacks. Adversarial attacks include model poisoning attacks and backdoor attacks. In a model poisoning attack, an attacker submits malicious model updates to contaminate the global model, leading to a degradation in model performance or incorrect outputs [96]. Backdoor attacks involve embedding specific triggers within the model, causing it to exhibit the attacker's desired erroneous behavior when certain input conditions are met [30]. On the other hand, privacy attacks aim to leak participants' personal information or data characteristics during the model training process, encompassing attribute inference attacks and membership inference attacks. Attribute inference attacks leverage the model's outputs to infer sensitive attributes of specific users, while membership inference attacks attempt to determine whether a particular data record belongs to the training dataset [97].

To address these security challenges, several defensive strategies can be employed. Differential privacy is an effective privacy protection technique that adds noise to data, ensuring that attackers find it difficult to infer sensitive information from observing individual model updates. For example, the differential noise addition-based FL method (DDPFL) proposed by Han et al. [98] and the FLBDP method by Zhu et al. [99] both incorporate noise during the local update phase to mitigate the risk posed by attackers. Additionally, secure multi-party computation (SMPC) allows for the joint computation of functions without disclosing individual data, thereby ensuring the security of the FL system during parameter updates and aggregation processes [100]. Another noteworthy defensive measure is the blockchain-based security mechanism, which leverages blockchain technology to ensure the security and integrity of data transmission [101]. Each parameter update can be recorded on the blockchain, thereby enhancing the system's transparency and trustworthiness.

Moreover, in the applications of FL-IoT, privacy protection issues cannot be overlooked. While FL avoids the direct transmission of data, local model parameters may still inadvertently disclose certain information. Thus, combining differential privacy and encryption techniques can effectively prevent malicious third parties or central servers from inferring user privacy through parameter updates [102]. Additionally, user consent mechanisms are critical, ensuring that users are informed about how their data will be used and have the right to choose whether to participate in data sharing or model training [103]. During the data sharing process, it is essential to balance the level of sharing with privacy protection, establishing reasonable sharing standards and regulations to ensure the secure and reliable transfer and utilization of data across different devices.

In conclusion, while FL holds immense potential for application in the IoT landscape, it also faces numerous security and privacy challenges. By conducting an in-depth analysis of various attack types and defensive strategies, and integrating technologies such as differential privacy and multi-party computation, FL can promote the widespread adoption and development of IoT while safeguarding privacy.

5.3 Heterogeneity of FL-IoT

IoT refers to the massive heterogeneous smart devices connected by heterogeneous communication technologies such as Ethernet, WiFi, Bluetooth, and ZigBee [104]. The data heterogeneity of IoT refers to the differences in data distribution, data quality, data volume, and data dimension of data collected by massive IoT devices, which lead to statistical heterogeneity and structural heterogeneity of data. IoT devices are widely distributed across the globe, from home automation systems to industrial monitoring devices, and they continuously generate large amounts of data. The heterogeneity of these data is mainly reflected in statistical heterogeneity and model heterogeneity.

Statistical heterogeneity: Statistical heterogeneity means that the data distribution of each customer in FL is inconsistent and does not obey the same sampling, that is, Non-IID [105]. In real-world applications, this situation is very common because different clients may originate from different regions, backgrounds, or user groups, and therefore the data they collect and generate have different characteristics and patterns. Secondly, some devices often generate and collect data on the web in highly different distributed ways, e.g., mobile phone users use different languages in the context of the next word prediction task [106]. These problems can lead to unstable model performance and poor generalization ability, which leads to lower learning efficiency and complications of the update aggregation process.

Model heterogeneity: In the context of FL refers to the use of machine learning models with different architectures or configurations by different clients. When unevenly distributed data is collected from multiple devices to train a federated model, it will seriously affect the final efficiency of the model [7]. In real IoT applications, different devices want to build their models to adapt to their application environment and resource constraints (i.e., computing power). And, they may not be willing to share the model details due to privacy concerns. As a result, the model architectures of different local models take on different shapes, causing the simple aggregation methods in traditional FL to become inapplicable [107]. Therefore, to accommodate this model heterogeneity, FL needs to adopt more flexible strategies and techniques to ensure effective collaborative learning even in diverse and privacy-sensitive environments.

The widespread adoption of IoT devices and the heterogeneity of their data pose significant challenges and opportunities for FL to overcome statistical heterogeneity and model heterogeneity, researchers and engineers need to develop more advanced algorithms and techniques. These include improved data preprocessing methods, more sophisticated model aggregation strategies, and a high degree of adaptability to device heterogeneity. At the same time, privacy protection and data security become important considerations when designing these systems. Ultimately, through these efforts, FL will be able to more effectively address the challenges in the IoT environment, enabling smarter and more secure global data collaboration and knowledge sharing.

5.4 FL Limitations of IoT Hardware Conditions

Federated Learning-Internet of Things (FL-IoT) systems face a series of hardware limitations in their implementation and operation, which have a significant impact on the performance and efficiency of the system. IoT devices often have limited computing power, battery life, and network constraints, and these characteristics determine the challenges of deploying efficient and sustainable learning algorithms in FL-IoT systems.

Computational Power Constraints: IoT devices are usually equipped with low-power and low-performance processors. These devices need to perform complex machine learning model training, but the training process may become slow or unable to handle more complex models due to computational

resource constraints. In response to the growing demand for services in areas such as smart cities, factories, and medical systems, IoT devices deployed at large scale mainly perform monitoring, data collection, preprocessing, and real-time decision-making tasks. Due to the relatively weak and heterogeneous computing power of these devices [108], they are usually not suitable for complex machine learning training.

Energy constraints: Many IoT devices rely on battery power, so energy efficiency becomes an important consideration. Most of the devices in IoT have fairly small sizes and are not fixed. Due to their size and often changing location attributes, devices cannot get power all the time. So low power consumption is a universal constraint for IoT. They either use battery technology or they use some technology that uses other devices to get power from the environment. Therefore, it is necessary to design such power consumption techniques or low power schemes that enable devices to have a long lifetime [54]. Performing complex computing tasks and communication operations can significantly consume battery energy, which is particularly critical for devices that find it difficult to replace their batteries frequently.

Network limitations: Although IoT devices are connected through multiple communication technologies, such as Wi-Fi, Bluetooth, ZigBee, etc., when simultaneous messages from multiple devices eventually lead to extreme overload situations, congestion problems occur, which can have a huge impact on the network, thereby affecting network performance and leading to network failures [54]. The network connection may be unstable or bandwidth limited, which also affects the uploading of data and the synchronization of model parameters, thus affecting the efficiency of FL.

To overcome these hardware limitations, FL-IoT systems need to adopt lightweight machine-learning models, efficient data compression techniques, and energy-efficient computing methods. In addition, it is necessary to intelligently manage the energy and storage resources of devices, as well as optimize the communication process between devices. These measures help to maximize the performance and reliability of FL-IoT systems under limited hardware conditions.

5.5 Standards and Specifications

After a period of development, FL and IoT have formed some preliminary protocols [109]. However, the application of FL in the field of IoT is still in its initial stage, and there is still a lack of unified standards and mature norms to guide and lead its development. It is urgent to establish corresponding legal norms, policy standards, and ethical frameworks to ensure its efficient and sustainable development on the road of legality, reasonability, and compliance. The main challenges faced by the combination of FL and IoT in terms of standards and norms are as follows.

Data quality and security: The data generated by IoT devices may have problems such as low quality, incomplete, inconsistent, and unreliable. Effective data cleaning, verification, and encryption operations are required to ensure the availability and security of the data. At present, there is still a lack of unified data quality and security standards. Different IoT devices and FL platforms may adopt different data processing methods, which will lead to data incompatibility and non-interoperability.

Model Evaluation and Validation: The goal of FL is to train models with high performance and generalization ability while preserving data privacy. However, there is still a lack of unified model evaluation and verification standards for the application of FL in the Internet field. Different IoT devices and FL platforms may adopt different model metrics, evaluation methods, and verification processes, which will lead to incomparability and unreliability of the model.

Communication protocols and interfaces: The communication process of FL involves data exchange and coordination between multiple IoT devices and the FL platform, which needs to follow certain communication protocols and interfaces to ensure the efficiency and stability of communication. However, there is still a lack of unified communication protocols and interface standards. Shome et al. [110] explored the high dependence of FL on wireless communication technologies, particularly in optimizing network resources and managing real-time decision-making. Due to the dynamic nature of wireless communication channels, the FL model update process requires efficient communication protocols to address issues like channel variability and interference. Current solutions, such as the Federated Averaging (FedAvg) method, ensure model synchronization but still necessitate more advanced communication-efficient protocols—such as gradient compression and asynchronous update mechanisms—to handle bandwidth limitations and reduce network congestion during the transmission of large-scale model parameters.

Data Format: Standardizing data formats is essential for the efficient processing and analysis of data in IoT and FL applications. IoT devices generate data in diverse formats, including text, images, audio, and video, all of which must be standardized to ensure compatibility and interoperability across different devices and platforms. For instance, Seljeseth et al. [111] introduced a data fusion framework for smart city applications that integrates data from various sources, such as sensors, cameras, and social media, underscoring the critical role of data format standardization in enabling efficient data fusion and analysis. Despite this, there remains a significant lack of unified data format standards. The heterogeneity of data produced by IoT device creates substantial challenges in processing and sharing data across platforms [112]. Different IoT devices and FL platforms may employ varying data encoding methods, compression techniques, and data structures, resulting in incompatibility and poor interoperability. Therefore, the establishment of unified data format standards is crucial to facilitate seamless data exchange and collaboration between devices, ultimately enhancing the efficiency and performance of FL model training in IoT applications.

6 Future Directions

The integration of Federated Learning (FL) with the Internet of Things (IoT) presents significant potential; however, challenges remain in terms of model interpretability, scalability, and large language model (LLM) integration. Future research could focus on the following three key areas:

Enhancing Model Interpretability in Federated Learning: As FL becomes widely adopted in critical IoT applications, such as healthcare and cybersecurity, model interpretability has become essential. Kalakoti et al. [113] propose a SHAP-based framework that aggregates local explanations from devices to derive global feature importance, providing high-quality interpretability for server-side models, thus greatly enhancing FL transparency and credibility in multi-device environments. Additionally, Salim et al. [114] integrated blockchain and differential privacy techniques to further strengthen FL' s trustworthiness and privacy protection, enabling the identification of features with significant predictive contributions and thereby improving model interpretability. Future research should further explore FL-based interpretability mechanisms that enhance model transparency while safeguarding privacy, allowing FL to support a broader range of IoT applications.

Improving the Scalability of Federated Learning in Large-Scale IoT Networks: As the number of IoT devices surges, enhancing FL scalability becomes a key challenge, especially in resource-constrained environments. Huba et al. [115] proposed a strategy that combines edge computing with communication optimization to effectively reduce data transmission latency between devices, while ensuring efficient allocation of computing resources, thereby significantly improving FL efficiency

and scalability. Building on these findings, future research could further optimize FL performance in environments with limited device resources and dynamic network conditions to meet the increasing number and complexity of IoT devices and data processing demands.

Integrating Large Language Models (LLMs) within FL and IoT: Incorporating large language models (LLMs) like GPT and BERT into the FL framework can provide IoT with advanced language processing capabilities, supporting high-level applications such as virtual assistants and sentiment analysis. However, fine-tuning LLMs in FL environments poses challenges in terms of communication and computational costs. Kuang et al. [116] introduced the FederatedScope-LLM (FS-LLM) toolkit, which integrates parameter-efficient tuning (PEFT) methods, such as LoRA and prefix-tuning, to reduce resource overhead and enhances privacy through the offsite-tuning algorithm. Additionally, Fan et al. [117] proposed the FATE-LLM framework, which employs a multi-center architecture to optimize communication efficiency and privacy management, balancing the communication costs and performance of LLM fine-tuning. These studies lay the groundwork for applying LLMs in FL and IoT settings.

7 Conclusion

This paper describes the application of FL in the field of IoT, and explores its current status, challenges, and possible solutions. We first introduce the basic concepts of FL, including its limitations compared with centralized learning, different classifications, and the advantages of its application in multiple domains. Then, we expounded the definition, development process, basic characteristics and current problems of IoT. We look forward to the vision of the combination of FL and IoT, and discuss in detail the multiple advantages of the application of FL in IoT, such as privacy security, efficient communication, attack detection, and enhancement of learning quality. In addition, we explore the practical use cases and potential value of FL in specific IoT application areas such as smart healthcare, sensor networks, Internet of vehicles, and smart cities. Despite the many improvements brought by FL for IoT, there are still challenges in the actual deployment and application process. In short, as a cutting-edge distributed machine learning method, FL provides new impetus and possibilities for the development of the IoT.

Acknowledgement: The authors are grateful to all the editors and anonymous reviewers for their comments and suggestions.

Funding Statement: This research was supported by the Shandong Province Science and Technology Project (2023TSGC0509, 2022TSGC2234), Qingdao Science and Technology Plan Project (23-1-5-yqpy-2-qy) and Open Topic Grants of Anhui Province Key Laboratory of Intelligent Building & Building Energy Saving, Anhui Jianzhu University (IBES2024KF08).

Author Contributions: The authors confirm contribution to the paper as follows: study conception and design: Zhenyu Liu; draft manuscript preparation: Zhenyu Liu, Xingtao Yang, Min Li; Funding acquisition and supervision: Jinglong Wang; Review: Zhihan Lyu. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: Not applicable.

Ethics Approval: Not applicable.

Conflicts of Interest: The authors declare no conflicts of interest to report regarding the present study.

References

[1] S. Li, L. D. Xu, and S. Zhao, "The internet of things: A survey," *Inf. Syst. Front.*, vol. 17, no. 2, pp. 243–259, Apr. 2015. doi: 10.1007/s10796-014-9492-7.

[2] S. C. Mukhopadhyay and N. K. Suryadevara, "Internet of Things: Challenges and opportunities," in *Smart Sensors, Measurement and Instrumentation*, S. C. Mukhopadhyay, Ed. Cham: Springer International Publishing, 2014, pp. 1–17. doi: 10.1007/978-3-319-04223-7_1.

[3] Lionel Sujay Vailshery, "Number of connected IoT devices will surge to 125 billion by 2030 | Semiconductor Digest," Accessed: Dec. 02, 2023. [Online]. Available: https://sst.semiconductor-digest.com/2017/10/number-of-connected-iot-devices-will-surge-to-125-billion-by-2030/

[4] R. Najat, E. Haitam, and A. Jaafar, "Comparative study of the Security Analysis of IoT systems using attack trees algorithm," *E3S Web Conf.*, vol. 412, no. 8, 2023, Art. no. 01087. doi: 10.1051/e3sconf/202341201087.

[5] J. Konečný, H. B. McMahan, F. X. Yu, P. Richtárik, A. T. Suresh and D. Bacon, "Federated learning: Strategies for improving communication efficiency," Oct. 30, 2017. doi: 10.48550/arXiv.1610.05492.

[6] P. M. Mammen, "Federated learning: Opportunities and challenges," Jan. 13, 2021. doi: 10.48550/arXiv.2101.05428.

[7] C. Zhang, Y. Xie, H. Bai, B. Yu, W. Li and Y. Gao, "A survey on federated learning," *Knowl.-Based Syst.*, vol. 216, no. 1, Mar. 2021, Art. no. 106775. doi: 10.1016/j.knosys.2021.106775.

[8] C. Xu and Y. Mao, "An improved traffic congestion monitoring system based on federated learning," *Information*, vol. 11, no. 7, Jul. 2020. doi: 10.3390/info11070365.

[9] M. J. Sheller, G. A. Reina, B. Edwards, J. Martin, and S. Bakas, "Multi-institutional deep learning modeling without sharing patient data: A feasibility study on brain tumor segmentation," *Brainlesion*, vol. 11383, pp. 92–104, 2019. doi: 10.1007/978-3-030-11723-8.

[10] Y. Himeur *et al.*, "Federated learning for computer vision," Aug. 24, 2023, *arXiv:2308.13558*.

[11] Q. Li *et al.*, "A survey on federated learning systems: Vision, hype and reality for data privacy and protection," *IEEE Trans. Knowl. Data Eng.*, vol. 35, no. 4, pp. 3347–3366, Apr. 2023. doi: 10.1109/TKDE.2021.3124599.

[12] F. Meng, Z. Xiao, Y. Zhang, and J. Wang, "RI-PCGrad: Optimizing multi-task learning with rescaling and impartial projecting conflict gradients," *Appl. Intell.*, vol. 54, no. 22, pp. 12009–12019, Nov. 2024. doi: 10.1007/s10489-024-05805-3.

[13] S. Abdulrahman, H. Tout, H. Ould-Slimane, A. Mourad, C. Talhi and M. Guizani, "A survey on federated learning: The journey from centralized to distributed on-site learning and beyond," *IEEE Internet Things J.*, vol. 8, no. 7, pp. 5476–5497, Apr. 2021. doi: 10.1109/JIOT.2020.3030072.

[14] M. F. Sohan and A. Basalamah, "A systematic review on federated learning in medical image analysis," *IEEE Access*, vol. 11, no. 23, pp. 28628–28644, 2023. doi: 10.1109/ACCESS.2023.3260027.

[15] Y. Mei, B. Guo, D. Xiao, and W. Wu, "FedVF: Personalized federated learning based on layer-wise parameter updates with variable frequency," in *2021 IEEE Int. Perform., Comput., Commun. Conf. (IPCCC)*, Austin, TX, USA, IEEE, Oct. 2021, pp. 1–9. doi: 10.1109/IPCCC51483.2021.9679416.

[16] L. Witt, M. Heyer, K. Toyoda, W. Samek, and D. Li, "Decentral and incentivized federated learning frameworks: A systematic literature review," *IEEE Internet Things J.*, vol. 10, no. 4, Feb. 2023, Art. no. 4. doi: 10.1109/JIOT.2022.3231363.

[17] H. B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. Y. Arcas, "Communication-efficient learning of deep networks from decentralized data," Jan. 26, 2023, *arXiv:1602.05629*.

[18] Y. Deng, M. M. Kamani, and M. Mahdavi, "Adaptive personalized federated learning," Nov. 05, 2020, *arXiv:2003.13461*.

[19] S. -A. Naas and S. Sigg, "Fast converging federated learning with Non-IID data," in *2023 IEEE 97th Veh. Technol. Conf. (VTC2023-Spring)*, Florence, Italy, IEEE, Jun. 2023, pp. 1–6. doi: 10.1109/VTC2023-Spring57618.2023.10200108.

[20] Q. Yang, Y. Liu, T. Chen, and Y. Tong, "Federated machine learning: Concept and applications," Feb. 13, 2019, *arXiv:1902.04885*.

[21] X. Zhang, A. Mavromatis, A. Vafeas, R. Nejabati, and D. Simeonidou, "Federated feature selection for horizontal federated learning in IoT networks," *IEEE Internet Things J.*, vol. 10, no. 11, pp. 10095–10112, Jun. 2023. doi: 10.1109/JIOT.2023.3237032.

[22] S. Hardy *et al.*, "Private federated learning on vertically partitioned data via entity resolution and additively homomorphic encryption," Nov. 28, 2017, *arXiv:1711.10677*.

[23] D. Serpanos and G. Xenos, "Vertical federated learning in malware detection for smart cities," in *2023 IEEE Int. Smart Cities Conf. (ISC2)*, Bucharest, Romania, IEEE, Sep. 2023, pp. 1–5. doi: 10.1109/ISC257844.2023.10293429.

[24] "Vertical federated learning: Concepts, advances, and challenges | IEEE Journals & Magazine | IEEE Xplore," Accessed: Nov. 02, 2024. [Online]. Available: https://ieeexplore.ieee.org/document/10415268

[25] U. Majeed, S. S. Hassan, and C. S. Hong, "Cross-silo model-based secure federated transfer learning for flow-based traffic classification," in *2021 Int. Conf. Inf. Netw. (ICOIN)*, Jeju Island, Republic of Korea, IEEE, Jan. 2021, pp. 588–593. doi: 10.1109/ICOIN50884.2021.9333905.

[26] Y. N. Tan, V. P. Tinh, P. D. Lam, N. H. Nam, and T. A. Khoa, "A transfer learning approach to breast cancer classification in a federated learning framework," *IEEE Access*, vol. 11, pp. 27462–27476, 2023. doi: 10.1109/ACCESS.2023.3257562.

[27] W. Guo, F. Zhuang, X. Zhang, Y. Tong, and J. Dong, "A comprehensive survey of federated transfer learning: Challenges, methods and applications," *Front Comput. Sci.*, vol. 18, no. 6, Jul. 2024, Art. no. 186356. doi: 10.1007/s11704-024-40065-x.

[28] D. C. Nguyen, M. Ding, P. N. Pathirana, A. Seneviratne, J. Li and H. V. Poor, "Federated learning for Internet of Things: A comprehensive survey," *IEEE Commun. Surv. Tutorials.*, vol. 23, no. 3, pp. 1622–1658, 2021. doi: 10.1109/COMST.2021.3075439.

[29] S. Li and C. Zhu, "Towards client driven federated learning," May 24, 2024. doi: 10.48550/arXiv.2405.15407.

[30] "Backdoor attacks and defenses in federated learning: Survey, challenges and future research directions-ScienceDirect," 2024. Accessed: Nov. 02, 2024. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0952197623013507

[31] W. Liu, Y. He, X. Wang, Z. Duan, W. Liang and Y. Liu, "BFG: Privacy protection framework for internet of medical things based on blockchain and federated learning," *Connect. Sci.*, Dec. 2023. doi: 10.1080/09540091.2023.2199951.

[32] H. Du *et al.*, "Decentralized federated learning strategy with image classification using ResNet architecture," in *2023 IEEE 20th Consum. Commun. Netw. Conf. (CCNC)*, Las Vegas, NV, USA, IEEE, Jan. 2023, pp. 706–707. doi: 10.1109/CCNC51644.2023.10060275.

[33] K. Kirsten, B. Pfitzner, L. Loper, and B. Arnrich, "Sensor-based obsessive-compulsive disorder detection with personalised federated learning," in *2021 20th IEEE Int. Conf. Mach. Learn. Appl. (ICMLA)*, Pasadena, CA, USA, IEEE, Dec. 2021, pp. 333–339. doi: 10.1109/ICMLA52953.2021.00058.

[34] K. S. Arikumar *et al.*, "FL-PMI: Federated learning-based person movement identification through wearable devices in smart healthcare systems," *Sensors*, vol. 22, no. 4, Feb. 2022, Art. no. 1377. doi: 10.3390/s22041377.

[35] C. -I. Moon, J. Lee, S. Kye, Y. S. Baek, and O. Lee, "Federated learning for masked psoriasis severity classification," in *2022 IEEE Sensors*, Dallas, TX, USA, IEEE, Oct. 2022, pp. 1–4. doi: 10.1109/SENSORS52175.2022.9967333.

[36] R. Uddin and S. A. P. Kumar, "SDN-based federated learning approach for satellite-IoT framework to enhance data security and privacy in space communication," *IEEE J. Radio Freq. Identif.*, vol. 7, pp. 424–440, 2023. doi: 10.1109/JRFID.2023.3279329.

[37] B. Hu, M. Isaac, O. M. Akinola, H. Hafizh, and W. Zhang, "Federated learning empowered resource allocation in UAV-assisted edge intelligent systems," in *2023 IEEE 3rd Int. Conf. Comput. Commun. Artif. Intell. (CCAI)*, Taiyuan, China, IEEE, May 2023, pp. 336–341. doi: 10.1109/CCAI57533.2023.10201325.

[38] X. Kong, H. Gao, G. Shen, G. Duan, and S. K. Das, "FedVCP: A federated-learning-based cooperative positioning scheme for social internet of vehicles," *IEEE Trans. Comput. Soc. Syst.*, vol. 9, no. 1, pp. 197–206, Feb. 2022. doi: 10.1109/TCSS.2021.3062053.

[39] M. Kabir, R. Tasfia, and M. G. Mostafa, "An improved video recommendation system for IoT devices using federated learning," in *2023 Int. Conf. Device Intell., Comput. Commun. Technol. (DICCT)*, Dehradun, India, IEEE, Mar. 2023, pp. 608–613. doi: 10.1109/DICCT56244.2023.10110183.

[40] Z. Yu, J. Liu, M. Yang, Y. Cheng, J. Hu and X. Li, "An elderly fall detection method based on federated learning and extreme learning machine (Fed-ELM)," *IEEE Access*, vol. 10, pp. 130816–130824, 2022. doi: 10.1109/ACCESS.2022.3229044.

[41] J. A. Stankovic, "Research directions for the internet of things," *IEEE Internet Things J.*, vol. 1, no. 1, pp. 3–9, 2014. doi: 10.1109/JIOT.2014.2312291.

[42] L. Da Xu, W. He, and S. Li, "Internet of things in industries: A survey," *IEEE Trans. Ind. Inform.*, vol. 10, no. 4, pp. 2233–2243, 2014. doi: 10.1109/TII.2014.2300753.

[43] Z. Lian, Q. Zeng, W. Wang, D. Xu, W. Meng and C. Su, "Traffic sign recognition using optimized federated learning in internet of vehicles," *IEEE Internet Things J.*, 2023. Accessed: Nov. 30, 2023. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/10242044/

[44] W. Yu *et al.*, "A survey on the edge computing for the Internet of Things," *IEEE Access*, vol. 6, pp. 6900–6919, 2017. doi: 10.1109/ACCESS.2017.2778504.

[45] X. Xingmei, Z. Jing, and W. He, "Research on the basic characteristics, the key technologies, the network architecture and security problems of the internet of things," in *Proc. 2013 3rd Int. Conf. Comput. Sci. Netw. Technol.*, IEEE, 2013, pp. 825–828. doi: 10.1109/ICCSNT.2013.6967233.

[46] M. Younan, E. H. Houssein, M. Elhoseny, and A. A. Ali, "Challenges and recommended technologies for the industrial internet of things: A comprehensive review," *Measurement*, vol. 151, 2020, Art. no. 107198. doi: 10.1016/j.measurement.2019.107198.

[47] L. Farhan, R. Kharel, O. Kaiwartya, M. Quiroz-Castellanos, A. Alissa and M. Abdulsalam, "A concise review on Internet of Things (IoT)-problems, challenges and opportunities," in *2018 11th Int. Symp. Communicat. Syst., Netw. Dig. Signal Process. (CSNDSP)*, Budapest, Hungary, IEEE, Jul. 2018, pp. 1–6. doi: 10.1109/CSNDSP.2018.8471762.

[48] X. Zhao, H. Qu, J. Yi, J. Wang, M. Tian and F. Zhao, "A fuzzer for detecting use-after-free vulnerabilities," *Mathematics*, vol. 12, no. 21, Jan. 2024, Art. no. 21. doi: 10.3390/math12213431.

[49] N. Guhr, O. Werth, P. P. H. Blacha, and M. H. Breitner, "Privacy concerns in the smart home context," *SN Appl. Sci.*, vol. 2, no. 2, Feb. 2020, Art. no. 247. doi: 10.1007/s42452-020-2025-8.

[50] F. Schuster and A. Habibipour, "Users' privacy and security concerns that affect IoT adoption in the home domain," *Int. J. Hum. Comput. Interact.*, vol. 40, no. 7, pp. 1–12, Nov. 2022. doi: 10.1080/10447318.2022.2147302.

[51] E. H. Houssein, M. A. Othman, W. M. Mohamed, and M. Younan, "Internet of Things in smart cities: Comprehensive review, open issues, and challenges," *IEEE Internet Things J.*, vol. 11, no. 21, pp. 34941–34952. doi: 10.1109/JIOT.2024.3449753.

[52] A. M. Elbir, S. Coleri, and K. V. Mishra, "Hybrid federated and centralized learning," in *2021 29th Eur. Signal Process. Conf. (EUSIPCO)*, IEEE, 2021, pp. 1541–1545. 2023. doi: 10.23919/EUSIPCO54536.2021.9616120.

[53] M. Al-Zihad, S. A. Akash, T. Adhikary, and M. A. Razzaque, "Bandwidth allocation and computation offloading for service specific IoT edge devices," in *2017 IEEE Region 10 Humanit. Technol. Conf. (R10-HTC)*, Dhaka, Bangladesh, IEEE, Dec. 2017, pp. 516–519. doi: 10.1109/R10-HTC.2017.8289012.

[54] A. Haroon, M. A. Shah, Y. Asim, W. Naeem, M. Kamran and Q. Javaid, "Constraints in the IoT: The world in 2020 and beyond," *Int. J. Adv. Comput. Sci. Appl.*, vol. 7, no. 11, 2016. doi: 10.14569/issn.2156-5570.

[55] P. Anand, Y. Singh, A. Selwal, M. Alazab, S. Tanwar and N. Kumar, "IoT vulnerability assessment for sustainable computing: Threats, current solutions, and open challenges," *IEEE Access*, vol. 8, pp. 168825–168853, 2020. doi: 10.1109/ACCESS.2020.3022842.

[56] L. Vu, Q. U. Nguyen, D. N. Nguyen, D. T. Hoang, and E. Dutkiewicz, "Deep transfer learning for IoT attack detection," *IEEE Access*, vol. 8, pp. 107335–107344, 2020. doi: 10.1109/ACCESS.2020.3000476.

[57] L. Tawalbeh, F. Muheidat, M. Tawalbeh, and M. Quwaider, "IoT privacy and security: Challenges and solutions," *Appl. Sci.*, vol. 10, no. 12, 2020, Art. no. 4102. doi: 10.3390/app10124102.

[58] H. Zhang and L. Zhu, "Internet of Things: Key technology, architecture and challenging problems," in *2011 IEEE Int. Conf. Comput. Sci. Automat. Eng.*, IEEE, 2011, pp. 507–512. doi: 10.1109/CSAE.2011.5952899.

[59] X. Lu, Z. Qu, Q. Li, and P. Hui, "Privacy information security classification for Internet of Things based on internet data," *Int. J. Distrib. Sens. Netw.*, vol. 11, no. 8, Aug. 2015, Art. no. 932941. doi: 10.1155/2015/932941.

[60] M. Z. Khan, O. H. Alhazmi, M. A. Javed, H. Ghandorh, and K. S. Aloufi, "Reliable Internet of Things: Challenges and future trends," *Electronics*, vol. 10, no. 19, 2021, Art. no. 2377. doi: 10.3390/electronics10192377.

[61] "A scalable and transferable federated learning system for classifying healthcare sensor data | IEEE Journals & Magazine | IEEE Xplore," Accessed: Dec. 06, 2023. [Online]. Available: https://ieeexplore.ieee.org/document/9765749

[62] X. Wang, J. Hu, H. Lin, W. Liu, H. Moon and M. J. Piran, "Federated learning-empowered disease diagnosis mechanism in the internet of medical things: From the privacy-preservation perspective," *IEEE Trans. Ind. Inform.*, vol. 19, no. 7, pp. 7905–7913, Jul. 2023. doi: 10.1109/TII.2022.3210597.

[63] B. B. Sezer, H. Turkmen, and U. Nuriyev, "PPFchain: A novel framework privacy-preserving blockchain-based federated learning method for sensor networks," *Internet Things*, vol. 22, no. 1, Jul. 2023, Art. no. 100781. doi: 10.1016/j.iot.2023.100781.

[64] Y. Fraboni, R. Vidal, and M. Lorenzi, "Free-rider attacks on model aggregation in federated learning," Feb. 22, 2021. doi: 10.48550/arXiv.2006.11901.

[65] L. Lyu *et al.*, "Privacy and robustness in federated learning: Attacks and defenses," 2023, *arXiv:2012.06337v3*.

[66] M. Driss, I. Almomani, Z. e Huma, and J. Ahmad, "A federated learning framework for cyberattack detection in vehicular sensor networks | Complex & Intelligent Systems," Accessed: Dec. 07, 2023. [Online]. Available: https://link.springer.com/article/10.1007/s40747-022-00705-w

[67] X. Wang, Y. Wang, Z. Javaheri, L. Almutairi, N. Moghadamnejad and O. S. Younes, "Federated deep learning for anomaly detection in the internet of things," *Comput. Electr. Eng.*, vol. 108, no. 7, May 2023, Art. no. 108651. doi: 10.1016/j.compeleceng.2023.108651.

[68] O. Bello and S. Zeadally, "Internet of underwater things communication: Architecture, technologies, research challenges and future opportunities," *Ad Hoc Netw.*, vol. 135, no. 6, Oct. 2022, Art. no. 102933. doi: 10.1016/j.adhoc.2022.102933.

[69] Y. Ji and L. Chen, "FedQNN: A computation-communication-efficient federated learning framework for IoT with low-bitwidth neural network quantization," *IEEE Internet Things J.*, vol. 10, no. 3, pp. 2494–2507, Feb. 2023. doi: 10.1109/JIOT.2022.3213650.

[70] M. -D. Nguyen, S. -M. Lee, Q. -V. Pham, D. T. Hoang, D. N. Nguyen and W. -J. Hwang, "HCFL: A high compression approach for communication-efficient federated learning in very large scale IoT networks," Jun. 21, 2022. doi: 10.48550/arXiv.2204.06760.

[71] H. Ge, X. Yang, J. Wang, and Z. Lyu, "A decentralised federated learning scheme for heterogeneous devices in cognitive IoT," *Int. J. Cognit. Comput. Eng.*, vol. 5, no. 2, pp. 357–366, Jan. 2024. doi: 10.1016/j.ijcce.2024.08.001.

[72] H. Ge, S. R. Pokhrel, Z. Liu, J. Wang, and G. Li, "PFL-DKD: Modeling decoupled knowledge fusion with distillation for improving personalized federated learning," *Comput. Netw.*, vol. 254, no. 3, Dec. 2024, Art. no. 110758. doi: 10.1016/j.comnet.2024.110758.

[73] B. Saylam and Ö.D. İncel, "Federated learning on edge sensing devices: A review," Nov. 02, 2023. doi: 10.48550/arXiv.2311.01201.

[74] "A regression approach to speech enhancement based on deep neural networks | IEEE Journals & Magazine | IEEE Xplore," Accessed: Dec. 08, 2023. [Online]. Available: https://ieeexplore.ieee.org/document/6932438

[75] A. Brendel and W. Kellermann, "Distributed source localization in acoustic sensor networks using the coherent-to-diffuse power ratio," *IEEE J. Sel. Top. Signal Process.*, vol. 13, no. 1, pp. 61–75, Mar. 2019. doi: 10.1109/JSTSP.2019.2900911.

[76] J. Ebbers, M. C. Keyser, and R. Haeb-Umbach, "Adapting sound recognition to a new environment via self-training," in *29th Eur. Signal Process. Conf. (EUSIPCO)*, Aug. 2021, pp. 1135–1139. doi: 10.23919/EUSIPCO54536.2021.9616009.

[77] L. Becker, A. Nelus, R. Glitza, and R. Martin, "Accelerated unsupervised clustering in acoustic sensor networks using federated learning and a variational autoencoder," in *2022 Int. Workshop Acoust. Signal Enhan. (IWAENC)*, Sep. 2022, pp. 1–5. doi: 10.1109/IWAENC53105.2022.9914753.

[78] D. H. Tran, V. L. Nguyen, I. B. K. Y. Utama, and Y. M. Jang, "An improved sensor anomaly detection method in IoT system using federated learning," in *2022 Thirteenth Int. Conf. Ubiquit. Future Netw. (ICUFN)*, Jul. 2022, pp. 466–469. doi: 10.1109/ICUFN55119.2022.9829561.

[79] "Deep EHR: A survey of recent advances in deep learning techniques for electronic health record (EHR) analysis | IEEE Journals & Magazine | IEEE Xplore," Accessed: Dec. 08, 2023. [Online]. Available: https://ieeexplore.ieee.org/document/8086133

[80] T. N. K. Hung *et al.*, "An AI-based prediction model for drug-drug interactions in osteoporosis and paget's diseases from SMILES," *Mol. Inform.*, vol. 41, no. 6, Jun. 2022, Art. no. e2100264. doi: 10.1002/minf.202100264.

[81] "The future of digital health with federated learning | npj Digital Medicine," Accessed: Dec. 08, 2023. [Online]. Available: https://www.nature.com/articles/s41746-020-00323-1

[82] J. Lee, J. Sun, F. Wang, S. Wang, C. -H. Jun and X. Jiang, "Privacy-preserving patient similarity learning in a federated environment: Development and analysis," *JMIR Med. Inform.*, vol. 6, no. 2, Apr. 2018, Art. no. e20. doi: 10.2196/medinform.7744.

[83] W. Lai and Q. Yan, "Federated learning for detecting COVID-19 in chest CT images: A lightweight federated learning approach," in *2022 4th Int. Conf. Front. Technol. Inform. Comput. (ICFTIC)*, Dec. 2022, pp. 146–149. doi: 10.1109/ICFTIC57696.2022.10075165.

[84] "Privacy-preserving and efficient aggregation based on blockchain for power grid communications in smart communities | IEEE Journals & Magazine | IEEE Xplore," Accessed: Dec. 08, 2023. [Online]. Available: https://ieeexplore.ieee.org/document/8419184

[85] "Nei-TTE: Intelligent traffic time estimation based on fine-grained time derivation of road segments for smart city | IEEE Journals & Magazine | IEEE Xplore," Accessed: Dec. 08, 2023. [Online]. Available: https://ieeexplore.ieee.org/document/8850027

[86] S. Alshammari and S. Song, "3Pod: Federated learning-based 3 dimensional pothole detection for smart transportation," in *2022 IEEE Int. Smart Cities Conf. (ISC2)*, Sep. 2022, pp. 1–7. doi: 10.1109/ISC255366.2022.9922195.

[87] Y. Djenouri, T. P. Michalak, and J. C. -W. Lin, "Federated deep learning for smart city edge-based applications," *Future Gener. Comput. Syst.*, vol. 147, no. 2, pp. 350–359, Oct. 2023. doi: 10.1016/j.future.2023.04.034.

[88] M. F. Pervej *et al.*, "Mobility, communication and computation aware federated learning for internet of vehicles," in *2022 IEEE Intell. Veh. Symp. (IV)*, Jun. 2022, pp. 750–757. doi: 10.1109/IV51971.2022.9827190.

[89] T. Li, A. K. Sahu, M. Zaheer, M. Sanjabi, A. Talwalkar, and V. Smith, "Federated optimization in heterogeneous networks," Apr. 21, 2020. doi: 10.48550/arXiv.1812.06127.

[90] "Mobile charging station placements in internet of electric vehicles: A federated learning approach | IEEE Journals & Magazine | IEEE Xplore," Accessed: Dec. 08, 2023. [Online]. Available: https://ieeexplore.ieee.org/document/9899383

[91] H. Bodagala and H. Priyanka, "Security for IoT using federated learning," in *2022 Int. Conf. Recent Trends Microelectron., Automat., Comput. Commun. Syst. (ICMACC)*, Hyderabad, India, IEEE, Dec. 2022, pp. 131–136. doi: 10.1109/ICMACC54824.2022.10093557.

[92] L. Cui, X. Su, Y. Zhou, and J. Liu, "Optimal rate adaption in federated learning with compressed communications," in *IEEE INFOCOM 2022-IEEE Conf. Comput. Commun.*, London, UK, IEEE, May 2022, pp. 1459–1468. doi: 10.1109/INFOCOM48880.2022.9796982.

[93] Y. Xiong, R. Wang, M. Cheng, F. Yu, and C. -J. Hsieh, "FedDM: Iterative distribution matching for communication-efficient federated learning," in *2023 IEEE/CVF Conf. Comput. Vis. Pattern Recognit. (CVPR)*, Vancouver, BC, Canada, IEEE, Jun. 2023, pp. 16323–16332. doi: 10.1109/CVPR52729.2023.01566.

[94] S. Yang and Y. Liu, "Training efficiency of federated learning: A wireless communication perspective," in *2020 Int. Conf. Wirel. Commun. Sig. Process. (WCSP)*, Nanjing, China, IEEE, Oct. 2020, pp. 922–926. doi: 10.1109/WCSP49889.2020.9299704.

[95] J. Pang, Y. Huang, Z. Xie, Q. Han, and Z. Cai, "Realizing the heterogeneity: A self-organized federated learning framework for IoT," *IEEE Internet Things J.*, vol. 8, no. 5, pp. 3088–3098, Mar. 2021. doi: 10.1109/JIOT.2020.3007662.

[96] S. Kianpisheh, C. Benzaid, and T. Taleb, "Multi-model based federated learning against model poisoning attack: A deep learning based model selection for MEC systems," Sep. 12, 2024. doi: 10.48550/arXiv.2409.08237.

[97] G. D. Németh, M.Á. Lozano, N. Quadrianto, and N. Oliver, "Addressing membership inference attack in federated learning with model compression," Jul. 04, 2024, *arXiv:2311.17750*.

[98] L. Han, D. Fan, J. Liu, and W. Du, "Federated learning differential privacy preservation method based on differentiated noise addition," in *2023 8th Int. Conf. Cloud Comput. Big Data Anal. (ICCCBDA)*, Chengdu, China, IEEE, Apr. 2023, pp. 285–289. doi: 10.1109/ICCCBDA56900.2023.10154864.

[99] G. Zhu, J. Zhang, S. Zhang, and Y. Yin, "Federated learning privacy-preserving method based on bregman optimization," in *2023 IEEE 10th Int. Conf. Cyber Secur. Cloud Comput. (CSCloud)/2023 IEEE 9th Int. Conf. Edge Comput. Scal. Cloud (EdgeCom)*, Xiangtan, China, IEEE, Jul. 2023, pp. 85–90. doi: 10.1109/CSCloud-EdgeCom58631.2023.00023.

[100] H. Wang *et al.*, "XFL: A high performace, lightweighted federated learning framework," Feb. 10, 2023, *arXiv:2302.05076*.

[101] E. Moore, A. Imteaj, S. Rezapour, and M. H. Amini, "A survey on secure and private federated learning using blockchain: Theory and application in resource-constrained computing," *IEEE Internet Things J.*, vol. 10, no. 24, pp. 21942–21958, Dec. 2023. doi: 10.1109/JIOT.2023.3313055.

[102] "Client-based differential privacy federated learning | IEEE Conference Publication | IEEE Xplore," Accessed: Nov. 03, 2024. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/10401762

[103] "A secure and fair federated learning framework based on consensus incentive mechanism," Accessed: Nov. 02, 2024. [Online]. Available: https://www.mdpi.com/2227-7390/12/19/3068

[104] I. Bedhief, M. Kassar, and T. Aguili, "SDN-based architecture challenging the IoT heterogeneity," in *2016 3rd Smart Cloud Netw. Syst. (SCNS)*, Dubai, United Arab Emirates, IEEE, Dec. 2016, pp. 1–3. doi: 10.1109/SCNS.2016.7870558.

[105] M. Ye, X. Fang, B. Du, P. C. Yuen, and D. Tao, "Heterogeneous federated learning: State-of-the-art and research challenges," *ACM Comput. Surv.*, vol. 56, no. 3, pp. 1–44, Mar. 2024. doi: 10.1145/3625558.

[106] T. Li, A. K. Sahu, A. Talwalkar, and V. Smith, "Federated learning: Challenges, methods, and future directions," *IEEE Signal Process. Mag.*, vol. 37, no. 3, pp. 50–60, 2020. doi: 10.1109/MSP.2020.2975749.

[107] Q. Wu, K. He, and X. Chen, "Personalized federated learning for intelligent IoT applications: A cloud-edge based framework," *IEEE Open J. Comput. Soc.*, vol. 1, pp. 35–44, 2020. doi: 10.1109/OJCS.2020.2993259.

[108] Y. Han, D. Li, H. Qi, J. Ren, and X. Wang, "Federated learning-based computation offloading optimization in edge computing-supported internet of things," in *Proc. ACM Turing Celebrat. Conf.-China*, Chengdu, China, ACM, May 2019, pp. 1–5. doi: 10.1145/3321408.3321586.

[109] "IEEE draft guide for architectural framework and application of federated machine learning," in *IEEE P3652.1/D6*, Apr. 2020, pp. 1–70.
[110] D. Shome, O. Waqar, and W. U. Khan, "Federated learning and next generation wireless communications: A survey on bidirectional relationship," Jan. 10, 2022, *arXiv:2110.07649*.
[111] M. Seljeseth, M. M. Yamin, and B. Katt, "UIOT-FMT: A universal format for collection and aggregation of data from smart devices," *Sensors*, vol. 20, no. 22, 2020, Art. no. 6662. doi: 10.3390/s20226662.
[112] H. Zhang and J. Kim, "Towards a federated learning framework for heterogeneous devices of Internet of Things," May 31, 2021. doi: 10.48550/arXiv.2105.14675.
[113] R. Kalakoti, H. Bahsi, and S. Nõmm, "Explainable federated learning for botnet detection in IoT networks," in *IEEE Int. Conf. Cyber Secur. Resil. (CSR)*, Sep. 2024, pp. 01–08. doi: 10.1109/CSR61664.2024.10679348.
[114] S. Salim, B. Turnbull, and N. Moustafa, "A blockchain-enabled explainable federated learning for securing Internet-of-Things-based social media 3.0 networks," *IEEE Trans. Comput. Soc. Syst.*, vol. 11, no. 4, pp. 4681–4697, Aug. 2024. doi: 10.1109/TCSS.2021.3134463.
[115] D. Huba *et al.*, "PAPAYA: Practical, private, and scalable federated learning," 2022. doi: 10.48550/arXiv.2111.04877.
[116] W. Kuang *et al.*, "FederatedScope-LLM: A comprehensive package for fine-tuning large language models in federated learning," Sep. 01, 2023, *arXiv:2309.00363*.
[117] T. Fan *et al.*, "FATE-LLM: A industrial grade federated learning framework for large language models," Oct. 16, 2023. doi: 10.48550/arXiv.2310.10049.