IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 27 November 2023, accepted 7 December 2023, date of publication 22 December 2023,
date of current version 23 January 2024.

Digital Object Identifier 10.1109/ACCESS.2023.3344029

SURVEY

Exploring Deep Federated Learning for the Internet of Things: A GDPR-Compliant Architecture

ZAHRA ABBAS[1], SUNILA FATIMA AHMAD[1], MADIHA HAIDER SYED[1], ADEEL ANJUM[1], AND SEMEEN REHMAN[2], (Member, IEEE)
[1]Institute of Information Technology, Quaid-i-Azam University, Islamabad 15320, Pakistan
[2]Institute of Computer Technology, Technische Universität Wien (TU Wien), 1040 Vienna, Austria

Corresponding author: Semeen Rehman (semeen.rehman@tuwien.ac.at)

ABSTRACT With the emergence of intelligent services and applications powered by artificial intelligence (AI), the Internet of Things (IoT) affects many aspects of our daily lives. Traditional approaches to machine learning (ML) relied on centralized data collection and processing, where data was collected and analyzed in one place. However, with the development of Deep Federated Learning (DFL), models can now be trained on decentralized data, reducing the need for centralized data storage and processing. In this work, we provide a detailed analysis of DFL and its benefits, followed by an extensive survey of the use of DFL in various IoT services and applications. We have studied the impact of DFL and how to preserve security and privacy by ensuring compliance in machine learning-enabled IoT systems. In addition, we present a generic architecture for a GDPR-compliant DFL-based framework. Finally, we discuss the existing obstacles and possible future research directions for DFL in IoT.

INDEX TERMS Deep federated learning (DFL), Internet of Things (IoT), artificial intelligence (AI), compliance, general data protection regulation (GDPR).

I. INTRODUCTION

In recent years, we have seen the outburst of IoT, which offers connecting global sensing and computing capabilities to a wide variety of objects to the internet [1]. AI approaches like deep learning (DL) have been extensively used to train data models for enabling intelligent IoT applications like smart healthcare, and smart transportation to gain insights into the data generated from ubiquitous IoT devices.

The motivation for using DFL in IoT stems from the need to preserve privacy while training ML models on large amounts of decentralized data. IoT devices generate massive amounts of data, but often this data is sensitive and cannot be shared with a centralized server due to privacy concerns. DFL tackles this issue by enabling ML models to be trained on decentralized data without compromising privacy.

In DFL, each IoT device retains its data locally and trains a model on it, then aggregates model updates with those of other devices to update a global model. This makes sure that critical information stays on the device, lowering the possibility of data leaks, and enabling the creation of models that are trained on a more diverse and comprehensive dataset. By using DFL in IoT, organizations can unlock the full potential of their data while maintaining the privacy and security of their users. Therefore, creating novel AI approaches is crucial for achieving effective and privacy-enhancing smart IoT networks and applications.

The DFL concept has gained attention due to advancements in ML and privacy-preserving technologies. Recent proposals for DFL include using it to train personalized models for each user based on their local data, thus improving the accuracy of the model compared to those trained on centralized data alone. Another proposal is to use DFL for federated transfer learning (FTL), where knowledge from a centralized model is transferred to a decentralized model, reducing the amount of data required for training and enabling the creation of models that are more suited to edge devices. These proposals highlight the potential of

The associate editor coordinating the review of this manuscript and approving it for publication was Turgay Celik.

DFL to deal with the challenges of training ML models on decentralized, sensitive data while preserving privacy. DFL can provide several significant advantages for IoT applications, including the following:

- *Privacy protection*: By allowing models to be trained on decentralized data, DFL ensures that sensitive information remains on individual devices and is never transmitted to a centralized server. This protects users' privacy and reduces the risk of data breaches.
- *Improved model performance*: DFL enables the training of ML models on a more diverse and comprehensive dataset, as each IoT device contributes its local data. This results in improved model performance and accuracy as compared to models trained on centralized data alone.
- *Reduced latency and bandwidth requirements*: DFL reduces the amount of data transmitted between devices and a centralized server, as only model updates are transmitted. This reduces latency and bandwidth requirements, making it well-suited for low-power and resource-constrained IoT devices.
- *Scalability*: DFL enables ML models to be trained on a large number of IoT devices, allowing organizations to scale their systems as needed.
- *Offline training*: DFL allows for training to occur even when devices are offline, making it well-suited for IoT devices with limited or inconsistent connectivity.

With these various benefits, DFL has been suggested for use in several IoT applications, including DFL for healthcare [2], Smart Homes [3], [4], [5], IoT Networks [6] etc. Despite the many advantages, still privacy and security concerns hinder the broader adoption of the system; Specially regulations such as GDPR and HIPPA. Among others, they can put some restrictions on meeting their requirements regarding privacy. As we've described before, naturally the DFL does preserve the privacy of individual users or devices. But at the same time, additional measures might be necessary to make a system compliant with the above-mentioned regulation systems. Keeping this in mind, we presented a generic model for a GDPR-compliant DFL-based system later in the paper. After that, we'll also discuss the research gaps and the challenges for the adoption of this system. The latest existing surveys related to FL [7], FL and IoT [8], DL [9], DL and IoT [10], IoT [11],Compliance [12] are summarized in the table 1 below.

A. COMPARISON AND OUR CONTRIBUTIONS

To the best of our knowledge, there is no previous study to give a thorough and devoted evaluation of the usage of DFL in IoT, even though DFL has been widely examined in the literature. An overview of the organization and structure of this paper is illustrated in Figure 1. The following are the important contributions made by this study:

1) We bring the first comprehensive survey of deep federated learning.
2) A taxonomy for the different kinds of DFL is provided.
3) The IoT services of DFL are discussed in detail.
4) We present DFL for IoT-based applications.
5) Research challenges are identified and potential future research directions are discussed.
6) Finally, we present a GDPR-compliant DFL-based framework.

II. DFL AND IOT: STATE OF THE ART

In this section, we will examine the current state of DFL and IoT technology. Additionally, the visions of their unification are examined.

A. DEEP FEDERATED LEARNING

DFL is a sub-field of FL that deals with the training of Deep Neural Networks (DNNs) in a decentralized and privacy-preserving manner. In DFL, multiple participating devices such as smartphones or IoT devices, hold local models and collaborate to learn a shared global model without revealing their sensitive data. The central server coordinates the communication and aggregates the model updates from the devices, thereby allowing for the training of complex models on large and distributed datasets. This approach enables organizations to train models on sensitive or decentralized data without compromising privacy and security, making it an attractive solution for many real-world applications such as healthcare, finance, autonomous systems etc. The system architecture of DFL is shown in Figure 2. To minimize the quantity of data that has to be forwarded to the central server, each IoT device first processes the data on its local network. Over a trustworthy and secure network, IoT devices connect with a central server. To further limit the quantity of data required for training, the central server processes the supplied data further. To train an ML model utilizing FL approaches, the central server utilizes the processed data from the IoT devices. These methods involve teaching the model in a manner that is dispersed, where every connected device contributes to the server with their local model updates, which are then combined to enhance the overall model.

Each client trains a model using its local data without sharing it with other clients or the server. The clients then share the model parameters with the server. The server is responsible for processing all the shared parameters and builds a model based on them. Then the final model is shared with the clients [15]. The model may be returned to the IoT devices for local interpretation once it has been trained. As a result, the IoT devices may generate predictions close to where they are located without sending data to a centralized server. Using the most recent data from the IoT devices, the central server regularly updates the model. This may be accomplished by continuous learning, in which the model is modified as new data become available.

B. INTERNET OF THINGS

The IoT is expected to link a wide variety of items and things to the network using its pervasive sensing and computing capabilities. This makes it easier for businesses to provide services and applications to their customers.

TABLE 1. Comparison of our paper with domains relevant to DFL. Key indicators are denoted as follows: ●: "Comprehensive survey", ○: "Not included in the survey" and ◐: "Partially included in the survey."

Ref No	FL	DL	IoT	Compliance	DFL	Key Contribution
[7]	●	○	○	○	○	A comprehensive summary of the research in practical applications and future research directions of FL.
[9]	○	●	○	○	○	This paper mainly adopts the summary and the induction methods of deep learning.
[11]	○	○	●	○	○	The aim of this paper is to discuss the Internet of things prominence on protocols, technologies, and application along related issues.
[12]	○	○	○	●	○	In this survey, compliance challenges are identified, underscored by the absence of reference architectures and patterns, explore current industry trends, and offer guidelines for more effective solutions.
[8]	◐	○	◐	○	○	An extensive survey of the use of FL in various IoT applications and services.
[10]	○	◐	◐	○	○	A paper which explores IoT introduction, diverse DL approaches, summarizes key reporting efforts, and discusses features, applications, and challenges, aiming to inspire further developments in this promising field.
[13]	◐	○	○	◐	○	This article surveys privacy-preserving techniques in Federated Learning regarding GDPR requirements, exploring current challenges and proposing approaches for full GDPR compliance in FL-based systems.
[14]	○	○	◐	◐	○	This paper discusses IoT data disclosure compliance, finding half of manufacturers lack sufficient privacy policies, and two devices don't align with their stated privacy agreements.
Our paper	●	●	●	●	●	A comprehensive survey which analyzes DFL benefits in IoT, proposes a GDPR-compliant framework, and addresses security and privacy compliance , highlighting challenges and future research directions.

IoT devices play a significant role in DFL. DFL provides a solution for training ML models on data generated by IoT devices, which typically have limited computational resources and are distributed in nature. By collaborating and sharing their local models, these devices can contribute to the training of a global model without revealing their sensitive data. For example, in a healthcare scenario, IoT devices such as wearable devices and home monitoring systems can collect and process large amounts of health data. DFL can be used to train models on this data in a privacy-preserving manner, enabling healthcare organizations to gain insights into patient health without compromising their privacy.

Furthermore, the decentralized nature of DFL makes it a suitable solution for large-scale IoT systems, where data is generated and processed at the edge, and the centralized model is updated based on this data. This enables organizations to leverage the collective intelligence of IoT devices to train models that are robust, scalable, and effective in real-world applications.

C. VISIONS OF THE USE OF DFL IN IOT

Some of these challenges that led to the study of DFL include:

- *Privacy concerns*: In many IoT applications, sensitive data cannot be transferred to a centralized server due to privacy concerns. DFL solves this challenge by enabling ML processing to be performed locally on IoT devices, without the need for data to be transferred to a centralized location.
- *Network latency*: Slow communication results in long training times, which can be impractical or infeasible in many IoT applications. DFL allows IoT devices to train models locally, without the need for frequent communication with a centralized server.
- *Data ownership complexity*: Different parties may own different parts of the data generated by IoT devices, making it difficult to create centralized ML models. DFL provides collaborative learning across multiple devices, without the need for data to be transferred to a centralized location.
- *Computational limitations*: IoT devices often have limited computational resources, which can make it challenging to perform ML tasks. DFL overcomes this difficulty by facilitating group learning across various platforms, which can assist in spreading the computational effort.
- *Handling large-scale data*: IoT devices can generate vast amounts of data, which can be challenging to process using centralized ML approaches. DFL handles this issue by promoting collaborative learning across many platforms, which can aid in spreading the computational workload.
- *Scalability issues*: Centralized ML systems may not be well-suited to handle large numbers of IoT devices. To assist in spreading out the computational hustle, DFL overcomes this issue by enabling collaborative learning across numerous devices.
- *Limited data diversity*: Centralized ML systems may lack access to a diverse range of data, which can limit the accuracy and effectiveness of the models. DFL enables collaborative learning across multiple devices, which can provide access to a wider range of data.
- *Bandwidth constraints*: Transferring large amounts of data to a centralized server can strain network

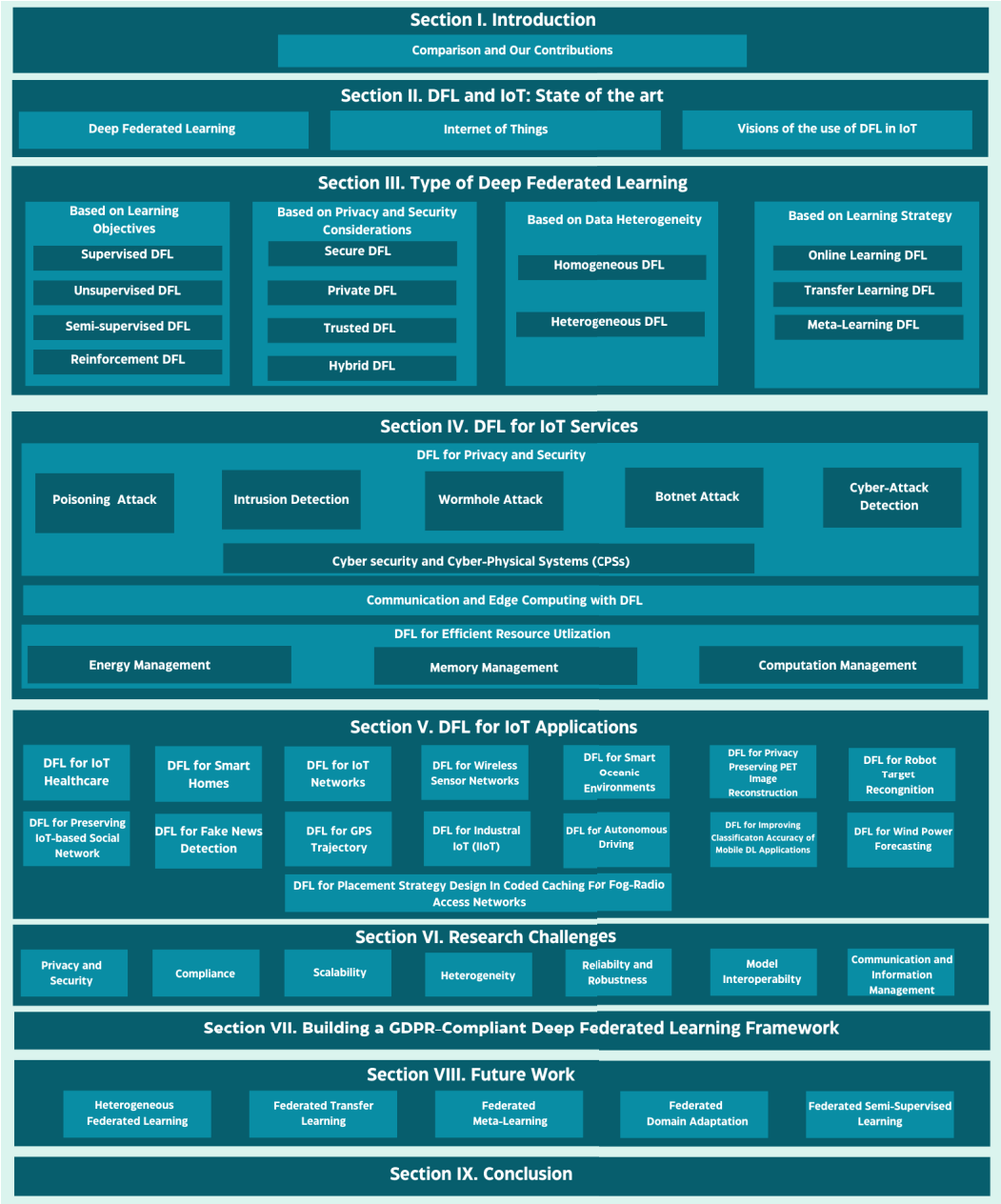

FIGURE 1. An overview of the survey paper's contents.

bandwidth, which can be impractical or infeasible in many IoT applications. DFL handles this challenge by enabling ML to be performed locally on IoT devices, without the need for frequent communication with a centralized server.

- *Maintenance costs*: Centralized ML systems require significant maintenance and management, which can be costly and time-consuming. DFL addresses this challenge by enabling collaborative learning across multiple devices, which can help to distribute the computational workload.
- *Power constraints*: IoT devices often have limited power resources, which can make it challenging to perform ML tasks. DFL fixes this challenge by enabling ML to be performed locally on IoT devices, without the need for frequent communication with a centralized server.
- *Lack of real-time processing*: Centralized ML systems may be unable to process data in real-time, which can be a critical requirement in many IoT applications. DFL copes with this challenge by enabling ML to be performed locally on IoT devices, without the need for frequent communication with a centralized server.

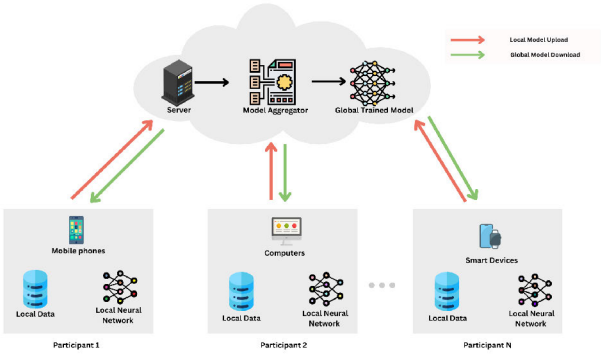

FIGURE 2. An architecture diagram of Deep federated learning.

- *Unreliable connectivity*: IoT devices may experience connectivity issues, which can make it challenging to use centralized ML systems. DFL addresses this challenge by enabling machine learning to be performed locally on IoT devices, without the need for frequent communication with a centralized server.
- *Data integrity*: Centralized ML systems may compromise data integrity, which can be a critical concern in many IoT applications. DFL answers this problem by enabling cross-device collaboration in learning without the requirement for data transfer to a centralized place.
- *Inefficient use of resources*: Centralized ML systems may not make efficient use of available resources, which can result in slow or ineffective models. DFL helps to distribute the computational workload and make more efficient use of available resources.
- *Lack of adaptability*: Centralized ML systems may not easily adapt to changing requirements, which can limit their usefulness in dynamic IoT environments. DFL allows ML to be performed locally on IoT devices, which can be more easily adapted to changing requirements.
- *Security vulnerabilities*: Centralized ML systems may be vulnerable to security threats, which can compromise the integrity of the data and the effectiveness of the models. DFL responds to this challenge by enabling collaborative learning across multiple devices, which can help reduce the risk of security breaches.
- *Inaccurate results*: Centralized ML systems may produce inaccurate results if they do not have access to sufficient data or if the data is not representative of the target population. DFL can provide access to a wider range of data and increase the accuracy of the models.
- *Insufficient data control*: Centralized ML systems may not provide adequate control over data, which can be a critical concern in many IoT applications. DFL can provide greater control over the data and reduce the risk of privacy violations.
- *Complexity*: Centralized ML systems can be complex to set up and manage, which can make them difficult to use in many IoT applications. DFL allows ML to be performed locally on IoT devices, which can simplify the setup and management of the system.
- *Inefficient data storage*: Centralized ML systems may not be efficient in storing and accessing data, which can result in slow or ineffective models. DFL helps to distribute the storage and access of the data and make more efficient use of available resources.

DFL is an exciting field of ML that allows distributed training of a shared model without requiring the raw data to be shared. In the next section, we will explore the different types of DFL that can be used depending on the nature of the data and the goals of the training. By understanding these different approaches, we can choose the most appropriate DFL technique for our specific needs and applications.

III. TYPES OF DEEP FEDERATED LEARNING

When it comes to protecting the confidentiality of sensitive information while training ML models on distributed data, DFL holds great promise [16]. The variety of data sources and the complexity of learning tasks necessitate specialized models and communication mechanisms, calling for various forms of DFL. Figure 3 shows the different types of deep federated learning. This division is considered the best due to its comprehensive coverage of the key factors that influenced DFL in IoT.

A. BASED ON LEARNING OBJECTIVES

Learning objectives are fundamental in any ML process, including DFL. By categorizing DFL based on learning objectives, it becomes easier to match the appropriate DFL technique with the specific goal of an IoT application. The four major categories of learning objectives are supervised, unsupervised, semi-supervised, and reinforcement learning which may be used to group the learning goals of DFL.

In general, the decision between these various learning goals is based on the particular specifications and features of the IoT software in question, alongside the visibility and caliber of the data produced by the dispersed devices.

1) SUPERVISED DFL

Federated learning is a distributed ML technique that enables several participants to collaborate and train a model without disclosing their data. This category deals with IoT applications where labeled data is available, and the primary objective is to make predictions or classifications.

The study [17] examined the difficulties and possible alternatives for boosting interpersonal efficiency in FL. The proposed method, compaction, induced conformational, and key recommendations are only a few of the methods discussed by J. Konecný et al. to lessen the burden of communication in FL. They also analyzed the efficacy of alternative communication-efficient strategies on different benchmarks and gave a detailed overview of the current research on FL.

The article [18] explained a distinctive solution to the challenge of developing powerful neural networks on distributed

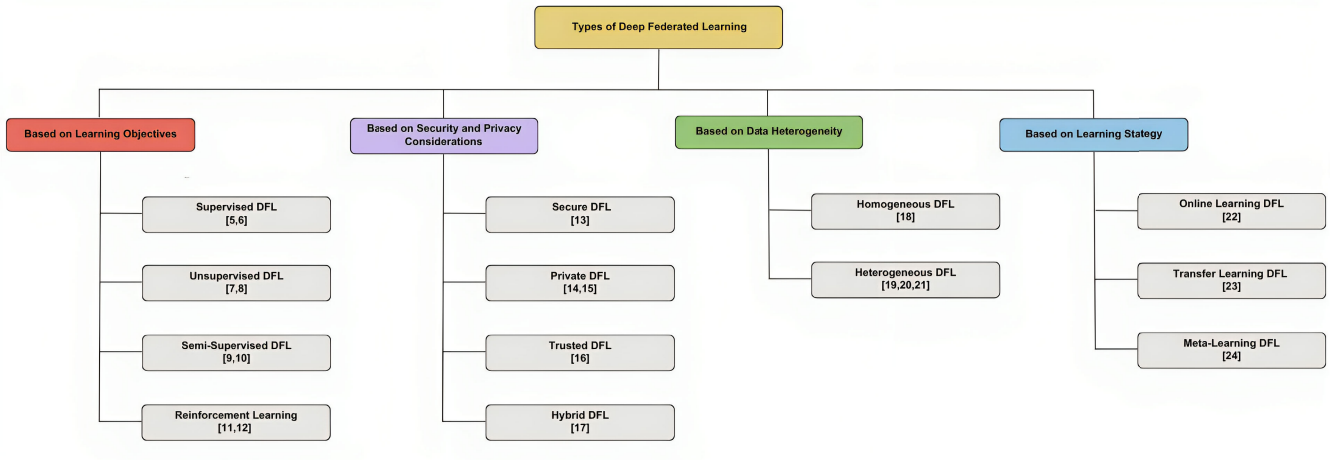

FIGURE 3. Taxonomy for the types of Deep federated learning.

data without sacrificing privacy or security. To effectively recruit a DNN on information that is dispersed across several devices, the authors offered a FL architecture that makes use of both local model modifications and global model aggregation. Using sparsification and quantization, the suggested approach minimizes the network bandwidth and computation cost of conventional FL methods. E Moore et al. also provided experimental findings showing that their method was successful in protecting the privacy and security of the distributed data while obtaining competitive performance on several benchmark datasets.

2) UNSUPERVISED DFL

When labeled data is scarce or unavailable, unsupervised DFL becomes essential. This is because IoT devices often generate vast amounts of unlabeled data, and uncovering hidden patterns or anomalies is crucial for various applications.

A peculiar technique for unsupervised learning was presented in the study [19] which makes use of privileged information to enhance the quality of the learned representations. Y Foucade et al. described a learning framework in which several agents work together to share and gain information from data that is normally kept secret. To recover the proprietary information of other agents, the suggested technique expands the conventional auto-encoder architecture with a privileged decoder. They showed that their method works by applying it to multiple benchmark datasets and demonstrating how the incorporation of privileged material greatly improves the performance of the trained representations.

To train ML models using imbalanced datasets that are spread over numerous devices, Servetnyk et al. described a unique unsupervised FL technique [20]. To train the local models, the authors provided a clustering-based approach that takes advantage of data commonalities across devices. The global model is derived by summing the results of all the local models. When dealing with sensitive data or data that is spread across several devices, the suggested solution is an excellent option since it does not need the exchange of labeled data. The authors demonstrated their method achieved competitive performance with standard supervised FL techniques while needing orders of magnitude less data exchange across devices by evaluating it on several benchmark datasets.

3) SEMI-SUPERVISED DFL

Semi-supervised DFL strikes a balance between supervised and unsupervised learning for IoT scenarios where labeled data is limited, but unlabeled data are abundant. It optimizes the use of available resources while achieving meaningful insights.

A new semi-supervised FL methodology is proposed [21], to identify intrusions in IoT systems. To train ML algorithms in a parallel environment across several IoT devices, Y Wang et al. provided a two-stage procedure that makes use of both unlabeled as well as labeled information. To boost the predictive power of the local models, the first step employs a self-training method to assign labels to the raw data. Step two involves refining the global model using the labeled data. The suggested strategy mitigated the risks associated with sharing private information by reducing the necessity for labeled data. Using a benchmark dataset, the authors demonstrated that their strategy outperforms both supervised and unsupervised approaches while protecting user anonymity.

The article [22] determined a thorough analysis of the several deep semi-supervised learning approaches that have been put out in recent years. X Yang et al. went through the benefits and drawbacks of semi-supervised learning, which trains DNNs using a small quantity of labeled data along with a massive proportion of unlabeled data. They discussed several semi-supervised learning strategies, including subconscious, co-training, and dynamic

modeling, and they highlighted current advancements in each discipline. The effectiveness of regularization approaches, such as entropy reduction, homogeneity generalized linear, and immersive confrontational training, in enhancing semi-supervised learning is also covered by the authors.

4) REINFORCEMENT LEARNING

IoT devices frequently interact with their environment and require continuous learning. Reinforcement DFL enables devices to learn and adapt their behavior in real-time, which is vital in dynamic IoT environments.

A thorough examination of the usage of deep reinforcement learning (DRL) in the atmosphere of the IoT is provided in [23]. W. Chen et al. began by outlining the fundamental ideas of DRL and IoT and the advantages of fusing the two technologies. Then they provided an overview of current research on DRL for IoT, classifying it into several application areas such as smart healthcare, traffic management, and energy management. The writers went through the prospects and difficulties, the most recent DRL methods, and the future directions for each application field. A taxonomy of the many DRL algorithms utilized in the IoT, notably Q-learning, policy gradient approaches, and actor-critic methods was also presented, along with a discussion of their respective advantages and disadvantages. The authors then discuss the difficulties and potential possibilities for DRL in the IoT, including how to solve the manageability, representatives, and computational modeling problems and create more effective and reliable algorithms.

A federated deep reinforcement learning (FDRL) technique [24] is suggested for monitoring systems in SDN-based IoT networks. TV Phan et al. provided a system for distributed learning where each IoT device uses its traffic data to train a local DRL model and communicates the hyperparameters with the primary station. The global model created by combining the local models is then utilized by the central controller to improve the routing of network traffic. The proposed approach lessened the need for disclosing private information while enabling effective resource use in the dispersed IoT network. The authors tested their method on a validation dataset and demonstrated that it outperformed conventional centralized learning techniques in terms of accuracy and efficiency while preserving data privacy.

B. BASED ON PRIVACY AND SECURITY CONSIDERATIONS

DFL is a workable ML strategy in the IoT, where data security and privacy are paramount concerns. To tackle these problems, several other DFL strategies have been proposed, each with its own set of privacy and security considerations. Privacy and security are paramount in IoT due to the sensitivity of data and potential risks. Categorizing DFL based on privacy and security considerations ensures that IoT systems can choose the right level of protection. Using Secure DFL ensures that patient data remains confidential, aligning with privacy requirements.

The decision between these several DFL methods ultimately comes down to the particular privacy and security needs of the IoT deployment, as well as the processing power of the endpoints and the host computer.

1) SECURE DFL

IoT devices often handle sensitive data, making secure communication and model updates crucial. Secure DFL is used to protect against data breaches and ensure the confidentiality of sensitive information.

A FL strategy for bearing problem detection in machinery systems is explained in [25]. J Chen et al. provided a system for distributed learning in which every machine gathered and developed a pre-trained model on its own orientation data and communicated the algorithms with the main controller. A dynamic weighted averaging approach, which gives larger weights to the models that perform better on the validation dataset, is used by the central server to aggregate the local models. The suggested approach lessened the need for disclosing private information while still enabling the decentralized machinery system to utilize its resources effectively. The authors tested their method on a gold standard and demonstrated that it outperforms conventional centralized learning techniques in terms of accuracy and efficiency while preserving data privacy. They further showed that by limiting overfitting and lessening the effect of subpar models, the dynamic weighted averaging method enhanced the reliability of the FL strategy.

2) PRIVATE DFL

Privacy is a paramount concern in IoT, especially in applications like healthcare or smart homes. Private DFL adds noise or distortion to data to preserve individual data privacy while allowing for collaborative learning.

A privacy-preserving method for collaborative DL was presented in [26]. The privacy of the participant's data is protected throughout the model training phase by the suggested method using homomorphic encryption (HE). X He et al. showed that their strategy achieved comparable accuracy while offering superior privacy protection by comparing its performance with that of a non-private participatory DL method. The suggested technique was experimentally evaluated in the research using two simulated data, proving its efficacy in maintaining privacy while producing precise findings for human activity identification. This research provided a strategy for private information collaboration DL that is useful and successful and may be used in a variety of areas other than human activity identification.

A privacy-preserving FL technique for biomedical monitoring using wearable IoT devices the difficulties involved in gathering sensitive personal information from many users while protecting their privacy [27]. The user's data is protected throughout the model-training process by the suggested approach's use of differential privacy (DP) approaches. YS Can et al. provided a safe aggregation

approach to combine model updates from several users without allowing any participant access to the data of other participants. Using only a trained classifier of electrocardiogram (ECG) signals, the research offered an experimental assessment of the suggested technique, proving its efficacy in protecting privacy while getting precise findings in biomedical monitoring. This research presented a useful and efficient method for private information federated deep learning (FDL) that may be used in wearable IoT-based biological monitoring and other fields involving the collection of sensitive personal data from several users.

3) TRUSTED DFL

Trust is critical in IoT ecosystems, especially in supply chain management or multi-organization collaborations. Trusted DFL establishes trust through techniques like blockchain and multi-party computation, ensuring transparency and accountability.

The study [28] presented a thorough analysis of the state of the art in the field of trustworthy FL. Y Zhang et al. explained the difficulties of FL, which included protecting privacy, maintaining security, and ensuring fairness when developing ML algorithms on distributed data. Topics discussed in the article included security, privacy, durability against various attacks and fairness in the context of trustworthy FL. They also talked about how FL may be used in other fields, including medicine, business, and even smart cities. The study wrapped up with an overview of the present issues and future research paths for trustworthy FL, emphasizing the need to develop more accurate and reliable FL computations, structures, and platforms that can fulfill the demanding needs of real-world applications.

4) HYBRID DFL

In complex IoT scenarios, a balance between speed, safety, and privacy is needed. Hybrid DFL combines various approaches to achieve this balance, making it suitable for diverse IoT applications.

The study [29] described a hybrid approach to FL that incorporated differential privacy (DP) and secure multiparty computation (SMC) methods to ensure that learner privacy is maintained. S Truex et al. discussed the difficulties of FL, which included protecting individual privacy while constructing models for ML on distributed data. The suggested method employed DP to safeguard participants' information during model training and SMC to conceal model parameters during aggregation. The authors also suggested a secure aggregation mechanism to combine the participants' model updates without letting anybody see the others' data or model parameters. The experimental assessment of the suggested method on a real-world dataset, presented in this research demonstrated its efficacy in protecting individual privacy while producing reliable FL findings. They also compared their method to others that aimed to preserve users' privacy when using FL and demonstrated that theirs is superior in both areas.

C. BASED ON DATA HETEROGENEITY

The devices may have various data distributions, feature sets, and data formats, which makes data heterogeneity a significant difficulty in DFL for IoT. Both homogeneous DFL and heterogeneous DFL have been suggested as solutions to this problem. Homogeneous DFL makes the assumption that the data distributions across devices are comparable [30], allowing the model to be trained across all devices using the same hyperparameters and techniques. This strategy makes device coordination easier and enables speedy convergence to a common model.

Contrarily, heterogeneous DFL makes the assumption that data distributions vary across devices and that each device will need a unique model [31], [32], [33]. This strategy demands additional coordination and communication between the devices, but it may improve model performance, particularly when the disparities between the devices are substantial. The decision between homogeneous and heterogeneous DFL relies on the particular objectives and features of the IoT application at hand.

1) HOMOGENEOUS DFL

Homogeneous DFL assumes data sources have similar distributions for IoT applications where devices generate consistent data. It simplifies model training and communication.

An innovative solution to the problem of data inconsistency in FL for industrial IoT is proposed in [30]. To facilitate FL, the suggested method involved picking a set of clients with comparable data distributions. Y Hu et al. demonstrated that this method may mitigate the detrimental effects of data heterogeneity on FL's overall performance. They tested the suggested method on a dataset obtained and showed that it outperforms other FL strategies in terms of modeling correctness and convergence time. Based on the findings, it seemed that the suggested method might be used in manufacturing IoT applications where the problem of data heterogeneity is prevalent.

2) HETEROGENEOUS DFL

IoT environments often have diverse data sources, such as different sensor types or locations. Heterogeneous DFL accommodates variations in data distributions, enabling effective collaboration.

The study [31] suggested a brand-new technique named ''Resilient Federated Learning with Compression'' (RFLC) for ML model training in a heterogeneous federated environment with constrained communication resources. To decrease the number of model updates exchanged between clients and servers, RFLC used model compression methods. It also included an adaptability mechanism to deal with connectivity issues and delayed updates. The proposed technique was tested on a variety of datasets, and it was shown that,

although using substantially fewer communication resources than current FL algorithms, it can attain accuracy that is competitive with them.

The study [32] described a model-neutral meta-learning method dubbed "MetaFedAvg," which was a customized FL methodology with theoretical guarantees. The proposed technique personalized the strategy for each user while protecting data privacy in order to overcome the difficulties of heterogeneous information as well as confidentiality issues in FL. Using a meta-learner, MetaFedAvg enables each user to train on their own local data while also customizing the hyperparameters for each user based on meta-knowledge from prior users.

The article [33] presented a thorough overview of heterogeneous FL, a subset of FL that responded to the difficulties of training neural network models using information from a wide variety of sources with varying degrees of consistency in these characteristics. Qiang et al. began with a brief introduction to the history and rationale behind heterogeneous FL before moving on to a comprehensive review of the literature on the topic's many subtopics, such as cooperation accumulation, prototype reconfigured, context adaptation, and privacy protection. The study also described resource limits and model selection as two of the practical issues of executing heterogeneous federated education in real-world systems and provides approaches to overcoming these obstacles.

D. BASED ON LEARNING STRATEGY

Different IoT scenarios require different learning strategies based on data dynamics and resource constraints. Categorizing DFL based on learning strategy enables IoT applications to choose the most suitable approach.

DFL approaches including online learning DFL, transfer learning DFL, and meta-learning DFL are all practical choices for this kind of learning in the IoT. Data from a range of IoT devices is continually streamed in to build a model utilizing online DFL [34]. Since it allows the model to account for changes in the data distribution over time, this strategy is well-suited to scenarios with a continuous and evolving data environment.

The predicted values on each device are initially established using pre-trained models in DFL with transfer learning [35]. This technique may lengthen the calculation time and improve the model's accuracy in situations when devices have little available data or computational power. In Meta-learning [36], each device's proportional gain in DFL is defined by a set of further learned meta-parameters.

The learning technique chosen depends on the specific requirements and constraints of the application scenario. In certain cases, such as those involving rapidly changing data or limited computing resources, online learning DFL may be the best option, while in others, transfer learning DFL may prove more useful. In situations when data is distributed unevenly among devices, meta-learning DFL may be effective.

1) ONLINE LEARNING DFL

Online Learning DFL focuses on continuous learning from new data as it arrives in real-time. It can adapt to changing patterns, helping the system optimize energy distribution and predict demand accurately.

A novel method for DL is introduced in the study [34] which enabled real-time learning and updating of neural networks. Online DL is a method developed to overcome the drawbacks of batch-based DL, which takes a long time to train and needs a lot of data and processing power. By putting neural networks through training on a continuously flowing stream of data, online DL allows the model to dynamically adapt to variations in the data distribution. To facilitate effective online training of DNNs, the authors suggested a new optimization technique they named "Online Learning with Stochastic Approximation" (OLSA). In this study, they compared OLSA to batch-based methods and demonstrated its superior performance on a variety of image classification and voice recognition datasets. The authors D Sahoo et al. also showed that online DL works well when the standard deviation changes over time, proving that the model can pick up new information fast and efficiently without requiring retraining. In sum, the research introduced a potential DL technique that may allow constant training and modification in actuality, making it suitable for a variety of purposes where the time series is dynamic and ever-changing.

2) TRANSFER LEARNING DFL

Transfer Learning DFL leverages pre-trained models on related tasks to accelerate learning on a new task with limited data. This is valuable in IoT scenarios where data is limited or expensive to collect, as pre-trained models provide a starting point for model development.

An in-depth analysis of the present status of deep transfer learning (DTL) for industrial defect identification is provided in [35]. It covered the philosophy behind DTL, its applications, and the challenges it encounters when used for industrial fault detection. While there is no doubt that DTL is a prospective strategy for enhancing fault detection in industrial situations, the author W Li et al. claimed that further research is needed to address the limitations and restrictions of DTL in actual applications.

3) META-LEARNING DFL

Meta-Learning DFL focuses on learning how to learn by optimizing the learning process itself. It can learn how to adapt to different manufacturing lines or products, optimizing quality control and minimizing defects by learning from past experiences.

The paper [36] presented an overview of meta-learning and how it is used in DNNs and provided a full introduction to meta-learning for people who are not acquainted with it or how it relates to DNNs. It began by defining meta-learning and describing some of its numerous forms, such as model-agnostic meta-learning (MAML) and quantifiable statistic

meta-learning. M Husiman et al. went into depth on how meta-learning can help DNNs by increasing their capacity to learn with less data. They emphasized the difficulties encountered during DNN training and provided possible solutions via meta-learning. Several meta-learning approaches were also included like gradient-based methods and Bayesian optimization. They also looked at how these strategies vary and are similar. Finally, the summary of the current state of the art in meta-learning for DNNs while highlighting some of the outstanding issues and potential future research directions are discussed.

In the upcoming section, we will explore the integration of DFL into various IoT services. DFL is a valuable tool for dealing with important IoT challenges such as privacy and security, efficient resource utilization and communication, and edge computing. We will examine the potential benefits of DFL in each of these areas and the challenges that must be overcome to realize its full potential in IoT.

IV. DFL FOR IOT SERVICES

DFL stands at the forefront of technological innovation, particularly in the realm of Internet of Things (IoT) services. This cutting-edge approach to machine learning is designed to address the challenges posed by decentralized and distributed IoT environments. In table 2, DFL for IoT services are summarized.

A. DFL FOR PRIVACY AND SECURITY

The architecture [37] accomplished collaborative fairness via local dependability, participation level, and transaction points, and the concept of different datasets is incorporated for privacy throughout the review process. The proposed technique, as per experimental data, proved resilient against poisoning attacks, leveraging networked devices for malware defense and threat classification [38].

Based on the findings of [39], the authors of the paper proposed a distributed DL architecture called Fair and Privacy-Preserving Federated Deep Models (FPPDL). By introducing the concept of geographical credibility and transaction points, and using blockchain technology for decentralization, this method seemed to improve impartiality in cooperative DL. The use of encryption in tandem with Partially Private GAN helped the system achieve its dual goals of confidentiality and precision. The MNIST accuracy achieved by the centralized framework using CNN architecture on P4 (four parties involved in the experiment) is 96.58%.

The susceptibility of DNNs to white-box inference attacks in both centralized and FL settings was proposed [40]. The paper proposed novel algorithms tailored to the white-box setting to exploit privacy vulnerabilities of the stochastic gradient descent algorithm used in DNN training. The paper evaluated the efficacy of white-box membership inference attacks against DL models and demonstrated the susceptibility of even well-generalized models to such attacks. It also showed how adversarial participants in FL can successfully run active membership inference attacks against other participants.

1) POISONING ATTACK

The study [37], proposed a FL system with concerns for fairness and robustness against poisoning assaults. By assigning the job to clients for cross-validation, a distinct local reliability mutual assessment technique is presented for identifying anomalous updates without having access to raw data.

2) INTRUSION DETECTION

The research [42] presented FDL method for wireless network heterogeneity intrusion detection. The strategy used exclusive datasets for local DNN model training and validation at several edge nodes. The characteristics of the model parameters were combined at a remote server utilizing Federated fusion methods to produce global DNN models. Comparing the local and global models' classification performance and generalization capacity revealed that the global models performed and generalized more effectively than the local models.

The paper [43] introduced "DeepFed," a Deep Federated Learning approach, for identifying and reducing cyber threats in industrial systems (CPSs). The authors created an FL model for several industrial CPSs to construct a thorough intrusion detection model while maintaining privacy. To maintain security and privacy during training, they also developed an intrusion detection model based on CNN-GRU and a secure communication protocol. An actual industrial CPS dataset was used in experiments to demonstrate the suggested DeepFed scheme's great efficacy and superiority to other state-of-the-art systems.

3) WORMHOLE ATTACK

In the paper [41], security and privacy issues have arisen as a result of the proliferation of IoT networks. Routing Protocol for Low-Power and Lossy Networks (RPL) assaults, such as wormhole attacks, are common examples of threat to a network's security because of the havoc they wreak on the navigation information of a system. Several studies have looked at the possibility of utilizing DL to identify wormhole assaults. By combining FL with DL models (CNN and LSTM), the suggested method ensured confidentiality, protected user privacy, and maximized performance. The cascading design reduced delays and saved resources without compromising the precision of wormhole identification.

4) BOTNET ATTACK

The creation of a novel technique dubbed FDL for identifying zero-day threats in IoT edge devices is discussed in [44]. The centralized DL (CDL), Localized DL (LDL) and distributed DL (DDL) models were compared to the FDL model, which was developed using the Malware data sets. Although the CDL model performed well at classification, it required security and confidentiality. While the FDL algorithm beat

TABLE 2. DFL for IoT services.

Ref No	Services	Techniques used	Contribution	Limitations	Accuracy
[41]	Wormhole attack Monitoring	Cascaded FDL	Data security and privacy aspects computation and processing issues are addressed	Lack of CNT	97%
[37]	Reputation-based Mechanism	Dynamic Asynchronous Anti-poisoning	Superior performance, Reputation Aware, Communication Reduction, Training time reduced by 30%	No real-world Evaluation, Single Dataset Evaluation, and Limited vulnerability coverage	Not provided
[42], [43]	Collaborative and Industrial Cyber-physical system Intrusion Detection	Federated Deep Learning	Improved detection accuracy, Preserved privacy and collaborative approach	Limited to homogeneous network and supervised learning tasks, Required a trusted aggregator and communication overhead	99.27 ± 0.79%, 99.20% (k=7)
[44]	Zero-day Botnet attack detection	Federated Deep Learning	Improved detection accuracy	Limited Model Capacity	99.79 ± 0.01%
[45]	Industrial Control System and FL	LSTM and CNN	Developed a novel DFL-Based ICS attack detection method, preserved privacy and security	Height computational cost and data privacy concerns	90.83%
[46]	Cyber-Physical System	Transformational Approach	Architectural Practices and System Integration	Interoperability issue, Scalability concerns	99.20%
[47]	Heating Load Demand Forecasting	Secure Federated Deep Learning-based Approach	Server has the lowest forecasting error, Global supermodel able to predict the heating load demand with correlation coefficient of 98.00%, 93.00%, and 70.00%.	Limited Dataset Availability	99.00%.
[48]	UAV-assisted RIS	LSTM and FL	Demonstrate the effectiveness with UAVs and RIS, Proposed a Novel Resource Allocation Strategy	Assumes a fix communication topology, Uses a simplified channel model	Not provided

the other methods but required a lengthy training period, the LDL and DDL methods exhibited poor classification results. The FL algorithm was to be improved by the authors to shorten the training time for the FDL framework, providing it with the most effective technique for detecting zero-day attacks in IoT edge devices.

5) CYBER-ATTACK DETECTION

A DL-based technique [45] for Industrial Control Systems (ICS) was presented that used FL to identify cyberattacks. Clients used their data to train stacked auto-encoders and then shared the features with a server. All clients utilized the global model developed by the server, which combined the parameters, to identify cyberattacks. The approach was far better than two non-FL-based methods when tested on a real-world ICS dataset. The suggested approach proved to be economical, and scalable and took security and privacy issues into account.

6) CYBER SECURITY AND CYBER-PHYSICAL SYSTEMS (CPSS)

The emergence of IoT and CPSs means that every object generates data, resulting in exponential growth. However, the inadequate processing mechanisms in place raised concerns about the quality of the output data in light of the increasing volume of data [46]. This led to the development of new technologies and approaches for data management and analysis, such as big data analytics and ML, to make sense of the vast amounts of information being generated.

The paper [49] provided a DFL approach to enable secure and private Point of Interest (POI) management in Cyber-Physical Systems (CPS). The recommended technique was tested using two real-world datasets, and the results showed promise in terms of achieving the design's goals.

The other way is to explore methods to reduce the computational complexity of DL algorithms while making them more understandable. The effectiveness of FDL techniques in enhancing individual privacy in the IoT is contrasted in [50]. FL systems were contrasted with blockchain, intrusion/malware tracking systems, and some other IoT application types. Additionally, the authors discussed the potential security and privacy issues with FL-based systems, in an experimental study of three DL models, three IoT connectivity datasets were employed. The results showed that FL algorithms provided superior confidentiality for data from IoT devices and achieved more accuracy in spotting risks than centralized ML approaches.

The smart grid, as a critical cyber-physical system (CPS), is highly susceptible to cyber-attacks. A method for detecting false data injection attacks (FDIA) in smart grids using secure FL with Transformer was proposed [51]. The approach involved building a Transformer-based FDIA detection model for the local training of each node and using an FL framework to enable all nodes to collaboratively

train a detection model while preserving the privacy of all the local training data. To improve the security of FL, the Paillier cryptosystem was combined with the framework to construct a secure FL, which protected the privacy of FL during training. Experimental results demonstrated that the proposed method outperforms conventional DL algorithms and centralized detection methods in terms of detection accuracy, privacy preservation, and communication overhead reduction.

B. DFL FOR EFFICIENT RESOURCE UTILIZATION

1) ENERGY MANAGEMENT

In [47], the authors proposed a new Cyber-Secure Federated Deep Learning (CSFDL) approach for predicting future energy consumption. The model used edge computing approaches to solve the problem of inconsistent data allocations between training and testing, while also protecting user privacy. As a solution to the problem of using resource-intensive algorithms like DNNs for FL in low-power IoT contexts for surveillance, [52] presented an approach dubbed Cost Effective Federated Deep Learning (REFDL). Using pruning and simulated micro-batching, REFDL improved upon the Federated Averaging (Fed-Avg) DNN-based approach to saving time and money. Virtual and test bed evaluations of the technique demonstrated an 81% reduction in memory consumption in the simulation environment and a 6% memory savings during execution time reduction of 15% without compromising accuracy.

2) MEMORY MANAGEMENT

A memory-efficient Multi-task Ensemble Deep Neural Network (MEDNN) approach based on a fully connected neural network (FCNN) for monitoring cyber assaults on IoT devices, investigating ways to reduce storage overhead during DNN development for information security in resource-constrained contexts. Using IoT benchmark datasets, the suggested technique was evaluated with both centralized and FL approaches, with encouraging results, particularly with FL, where it outperformed benchmark equivalents in both memory effectiveness and accuracy performance [52].

3) COMPUTATION MANAGEMENT

The paper [53] proposed a method called Resource Efficient Federated Deep Learning (REFDL) to deal with the problem of running FL with DNNs algorithms in resource-constrained IoT environments for security monitoring. The proposed method optimized Fed-Avg DNN using pruning and simulated micro-batching, which resulted in significant reductions in memory usage and execution time without sacrificing accuracy.

C. COMMUNICATION AND EDGE COMPUTING WITH DFL

The purpose of [54] was to enhance FL performance and lower communication costs. An asynchronous model update technique and a periodically weighted aggregation method were used in the strategy. The suggested technique outperformed conventional networked learning in terms of both effectiveness and communication cost, according to experiments on the Modified National Institute of Standards and Technology (MNIST) and natural action recognition datasets. New federated ML algorithms will be developed in future studies with the goal of enhancing performance and lowering communication costs.

The paper [48] described a two-step way to improve communication in RIS (Radio Frequency Intelligence Surface) systems that used unmanned aerial vehicles (UAVs). In the first step, LSTM (Long Short-Term Memory) and FL were used to train local models on each UAV to find phase shifts. In the second stage, the RIS controller made the best use of the resources so that the data analysis rate went up.

The paper [55] showed how important it was to protect DL and FL models from beginning to end. The frameworks, which were prepared with a lot of computing power, owner's intellectual capital need to be protected. Also, bad people could have used the models to do something illegal, so IP coverage should be thought about during the training and design phase before the frameworks were made public. Because DL models had a large number of parameters, they could automatically learn about hidden features.

In the paper [56], the authors proposed a Federated Transfer Learning (FTL) model for edge devices. The motivation for this model was that the computing resources and model designs of edge devices could vary widely, making it challenging to train ML models that can be deployed across all edge devices. A global model was created without compromising data privacy. The simulation showed that processing time for clients with adequate resources was less than that for clients with insufficient resources. Depending on the resources that customers had available, the recommended approach created several global models and ran a distinct training process for each of them. By sharing the inner structure of DNN models less often, the authors suggested a decentralized ML method that lowered communication costs.

The authors in [57], proposed a communication-efficient FL approach for distributed training of deep neural networks. The approach was based on quantization techniques, which compressed the model parameters and communication messages exchanged between the client devices and the central server. The authors conducted a numerical analysis to evaluate the performance of their proposed approach. The analysis showed that the proposed approach reduces the mean and variation of communication costs compared to traditional FL approaches, which could lead to quicker convergence and improved accuracy.

In the upcoming section, we will explore the integration of DFL into various IoT applications. We will delve into the practical applications of DFL in IoT, highlighting the opportunities and challenges that come with its integration.

V. DFL FOR IOT APPLICATIONS

DFL represents a pivotal paradigm shift in the realm of IoT applications, offering a sophisticated solution to the challenges posed by decentralized and sensitive data. The table 3 summarizes the different applications of DFL.

A. DFL FOR IOT HEALTHCARE

1) DFL FOR DIGITAL HEALTHCARE APPLICATIONS

The paper [58] proposed a decentralized DFL training scheme called Robust and Privacy-preserving Decentralized Federated Learning (RPDFL) for digital healthcare applications. RPDFL used a novel ring FL structure and a Ring-Allreduce-based data sharing scheme to improve communication efficiency and scalability while overcoming the problems of centralized FL. The proposed data-sharing plan updated the execution process of Chinese residual theorem (CRT) in the threshold secret-sharing method to support edge dropouts during training without data leakage and ensured the robustness of the RPDFL training. The proposed scheme also supported edge local gradient privacy. The security analysis showed that RPDFL is highly secure under the honest but curious (HbC) security model. The experiment results demonstrated the excellent performance of the RPDFL scheme.

2) SOCIAL MEDIA MENTAL HEALTH DETECTION

A model proposed in the paper [59] was used to monitor mental health using social media data by combining FL and DL. The model detected depression levels by collecting data from the user's keyboard and tested it daily with an RNN. The model was particularly relevant during the COVID-19 pandemic when depression rates were high.

3) MEDICAL IMAGING

A Guided-Weighted FDL framework was proposed for 3D brain Magnetic Resonance Imaging (MRI) images in the paper [60]. The framework enabled collaborative learning with multi-group data while preserving privacy. Results showed that the federated models outperformed local models with an average accuracy improvement of 1.54% - 1.89%.

Real clinical rectal image data were used to effectively illustrate the capability of FL across three academic institutions in [61]. The federated model showed enhanced performance on a test set from an outside source as well as expected to hold testing set from every school. In the context of medical image analysis, this concept might be usefully adapted to a broad range of DL applications.

The study [62], concentrated on developing a FL model using data from the public Kaggle repository to predict future hospitalizations for patients suffering from diabetic retinal illnesses. The experiment demonstrated that among the other models, FedSGD achieved the best global accuracy with the least global loss. During data encryption and decryption, computing time and cost provided was a challenge that researchers were functioning to solve mobility and simple access both for patients and professionals, medical records had to be stored in big data storage on the healthcare cloud.

The diagnosis of COVID-19 patients mostly relied on chest X-ray imaging. Healthcare systems have had a difficult time keeping up with the flood of patients suffering from COVID-19 symptoms as the pandemic has spread throughout the globe [63].

The authors proposed a methodology [64] to enhance ultrasound imaging using current information to aid in the recognition of COVID-19 patients. The authors proposed the use of computed tomography (CT) images to aid in ultrasound image recognition, as CT images could have provided more detailed information about the structure of the lung tissue. To deal with the diversity of data, the authors utilized data normalization techniques. Normalization helped to standardize the data to a common scale, enabling the use of various data sources in the model training. The authors also performed segmentation and classification based on capsule networks to identify COVID-19 patients. Overall, the proposed methodology aimed to improve the accuracy of COVID-19 diagnosis using a combination of ultrasound and CT images. By utilizing multiple sources of data and advanced DL techniques, the authors demonstrated a promising approach for enhancing the accuracy of COVID-19 diagnosis.

The challenges of using medical data for algorithm training and evaluation are due to privacy regulations and a lack of structured electronic medical records. To solve these issues, the authors [65] proposed incorporating technological solutions for secure and privacy-preserving AI, with a focus on medical imaging applications. They highlighted the importance of security and privacy concerns in other areas, such as large-scale automated contact detection and motion tracking during the COVID-19 pandemic. The authors suggested encryption and hardware-level privacy protections as potential solutions, including FL processes to preserve data and algorithm privacy. They also suggested that reliable performance conditions will become more predominant with the incorporation of edge hardware such as phones.

4) SKIN DISEASE DETECTION

In the study, [66], the DFL model for IoT-based, decentralized healthcare systems was suggested. It discussed how DFL was used for the identification of skin conditions. After several rounds, the results showed that the model's Area Under the Curve (AUC) percentage was greater.

5) EARLY PREDICTION OF THE RISK OF ICU MORTALITY WITH DFL

In paper [67], an FL methodology was described that enabled the early prediction of Intensive care unit (ICU) mortality. The findings demonstrated that FL outperforms both the Centralized Machine Learning (CML) method and the Local Machine Learning (LML) significantly, particularly as the client base grows. For 2, 4, and 8 users, performance in FL

TABLE 3. DFL for IoT applications.

Ref No	Application	Techniques used	Contribution	Limitations	Accuracy
[59]	Mental Health Monitor	LSTM-RNN	An alert system on users' devices, achieved the highest possible accuracy for depression levels	Only 60 days data monitored	93.46%
[60]	3D Brain, MRI Images	CNN Models, Weighted aggregation, Guaided propagation	Framework for Multi-Site Brain MRI Images, Enhances Learning via Data Privacy Protection	Shortage of training data, Global information aggregation limited	1.54-1.89%
[64], [65]	COVID-19 Detection using CT Imaging	Federated Blockchain, Capsule Network	New data normalization technique proposed, New dataset,	-	98. 68%
[66]	Decentralized Healthcare Systems	Transfer Learning (Resnet50)	Higher AUC percentage, implementation of skin disease detection	insufficient dataset, No minimum standard to run FL Models	Not provided
[67]	Prediction of the risk of ICU mortality	FL, Centralized ML, Local ML	Workflow for early ICU mortality prediction, Predictive performance analyzed	Limited to horizontal and stratified client	Not provided
[61]	DL for multi-institutional training	3D Anisotropic Hybrid Network	Real clinical prostate imaging data, Improved performance	No attempt to address the potential for an insider actor, the task used is simple	Not provided
[40]	Detection of Diabetic Retinopathy	federated stochastic gradient descent	Highest global accuracy , Least global loss	-	97.81%
[68], [69]	Diagnosis of Cerebellar Ataxia	Federated Learning, DL Model,Transfer Learning	Saved analysis and deployment time	DeseNet and other complex networks did not yield greater accuracies	86.69%
[70]	Relaying-Aided MEC-IoT System	Convergence Based DFL	Investigate Instantaneous and Statistical Convergence of Error	Convergence of Local and Global Training	Not provided
[71]	Smart Ocean DFL	MADDPG	80% and 41% of performance improvements, first work which considers FL procedures and systems for smart ocean application	Development of real-world scenarios	Not provided
[72]	Industrial IoT	Cyber Threat Hunting Model	Cyber-Threat Projection System proposed	Lack of SWAT	99.49%
[73]	IIoT and IWSN Network Services	SDN, NFV and Network Slicing	DFRL for future IIoT Networks	No integration of FPGA, SoC and Embraced Cloud Services	Not Provided
[6]	QoS Services in IIoT Networks	DFQL	Improved QoS Rewards	No advantages of exploration of DFQL	81.69%
[74]	PPSS for IIoT	Block-Chain Enabled FDL and (PoFDL)	Employed PPSS for Attack Identification	Future evaluating by Homomorphic encryption	Non-IID mode with 8 provers: 94.01% with K = 40 %

was unaffected, but with more clients, performance in LML significantly declined.

6) CEREBELLAR ATAXIA DETECTION

According to research [68], a lightweight convolutional architecture (MobileNetV2) with a recurrence plot transformer could successfully identify 86.69% of cases for Cerebellar Ataxia. The installation of DL-based FL algorithms resulted in a reduction in the amount of money that the service provider spent on operational expenses [69].

7) DFL FOR WEARABLE IOT-BASED BIOMEDICAL MONITORING

The study [27] presented an FDL algorithm for preserving privacy in heart activity data collected from wearable IoT devices. The study applied privacy-preserving FL on biomedical informatics data for the first time, with a focus on a use-case scenario of mental stress detection using photoplethysmography (PPG) based data. The study also investigated methods for aggregating separately collected event data to develop an improved shared model, which could be used by different health institutions without sharing their data. The results showed that FL is a promising method for IoT-based wearable biomedical monitoring research, achieving similar or better accuracies compared to traditional methods while protecting privacy.

8) DFL FOR LIVER TUMOR DIAGNOSIS

The article [75] discussed how computer-aided liver diagnosis using medical imaging techniques like MRI and CT could help doctors identify liver abnormalities and reduce the risk of unnecessary surgery. However, identifying and segmenting hepatic lesions in these images can be challenging due to low resolution and noise. The article reviewed various models for the automatic detection and diagnosis of hepatic lesions with CT and MRI and highlighted the need for a more accurate and automatic model that can track, detect, and diagnose hepatic lesions in 3D volumes of these images. The article also introduced the concept of FL and discussed the use

of multi-modality fused information and robust features to improve the accuracy of liver lesion detection and diagnosis.

B. DFL FOR SMART HOMES

To provide a smart capability, the suggested method [3] employed the use of layered compressed FL throughout the dwellings. This algorithm had the potential to be used in the future to automate a variety of various areas of the domain, including smart buildings and so on. When compared to the accuracy of other algorithms, this method had a decent level of accuracy.

In the proposed framework [4], FL is used to enable secure collaboration of multiparty data computation without transmitting data out of private data centers. The framework was empowered by public data centers, private data centers, and blockchain technology. The authors also compared the performance of FL with traditional centralized learning with the same neural network model.

DFL was also employed in study [5] as a key component to address the challenge of preserving consumer security and privacy while implementing Non-Intrusive Load Monitoring (NILM) with short Sequence-to-Point (Seq2Point) for energy consumption tracking in residential households.

In the article [76], DFL was employed to solve communication and computation challenges in edge networks, with a particular focus on data privacy within a smart home scenario. It presented an architecture that integrated federated edge learning to enhance data privacy. Simulation results based on real-world data demonstrated the effectiveness and efficiency of this approach, achieving a significant reduction of up to 80% in computation and 70% in communication compared to existing schemes while preserving data privacy.

Modern houses' security has benefited greatly from the use of smart doorbells. Existing methods for transferring video feeds to a centralized server (or Cloud) for video analytics have been confronted with several difficulties, including latency, high bandwidth costs, and most crucially, user privacy issues.

The article [77] demonstrated the capabilities of an intelligent smart doorbell built using FDL, that was able to install and manage video analytics solutions that included smart doorbells across Edge and Cloud resources. The research [78], described a FL-based intelligent smart doorbell that worked across local and cloud resources. Instead of sending photographs to a centralized server, smart doorbells upload parameters that were generated by a trained model. To cut down on the amount of time it takes for the doorbell to detect an item, the On Federated model is used and then pooled by the Federated Server.

C. DFL FOR IOT NETWORKS

IoT networks often consist of a large number of connected devices that generate vast amounts of data. By leveraging the power of DFL, IoT networks can take advantage of the distributed nature of their data sources, while still achieving high levels of accuracy in machine-learning models.

A DFL-based digital forensic method was proposed [6]. The method utilized FL to maintain data privacy and learned multi-stage attack events to identify cyber-attacks and analyze their attributes in IoT networks. The results of the evaluation demonstrated that the proposed method outperformed other machine-learning models in discovering attacks, achieving an 81.69% detection accuracy in less training time while guaranteeing data privacy.

D. DFL FOR WIRELESS SENSOR NETWORKS

The importance of investigating the signal-to-noise ratio (SNR) in a relaying-aided mobile edge computing (MEC)-IoT system was discussed [70], where DFL had gained interest among researchers in wireless communications. The paper analyzed the instantaneous and statistical convergence errors of the two-hop relaying channels to determine the system performance metrics such as capacity, outage probability, and bit-error rate. The results showed that the analysis of the convergence error is effective and can provide a theoretical foundation for DFL and computing networks in the context of MEC-IoT systems.

Indeed, in the book [73], a federated network slicing was proposed which was based on DRL approaches for channels and bandwidth management based on Long Range (LoRa) important technology that met Industrial Internet of Things (IIoT) and Industrial Wireless Sensor Networks (IWSN) network service requirement on the Software-Defined Networking (SDN), Network Functions Virtualization (NFV), network slicing, and DRL techniques. This was done in order to meet the requirements of both IWSN and IIoT networks.

E. DFL FOR SMART OCEANIC ENVIRONMENTS

An innovative strategy emerged in the field of smart oceans, where submerged networks struggled to establish trustworthy connections because of severe signal fading. In order to support FL computations that employed Internet-of-Underwater-Things (IoUT) devices in the oceanic environment, the research [71], offered a unique multi-agent DRL-based technique. FL-based decentralized DL appeared as a potential approach given the challenge of obtaining centralized training data. With the use of base station-like devices to allow the safe transfer of parameters to a centralized FL machine, the FL system gathered local model parameters from distinct IoUT devices in this IoUT network (IoUT-Net) context.

Another study [79] proposed a novel approach named adaptive privacy-preserving federated learning (AdaPFL), a DFL approach for fault diagnosis in the Internet of Ships (IoS). AdaPFL was designed to organize different shipping agents to collaboratively develop a model by sharing model parameters with no risk of data leakage. The paper demonstrated the effectiveness of DFL in improving shipping companies' maintenance performance and reducing operational costs in the maritime industry.

To develop a collision avoidance system for inland ships. The goal was to improve safety and reduce the likelihood of collisions while also respecting privacy concerns. In the approach, each ship had its own onboard sensor system that captured data about its surroundings, such as other nearby ships and environmental conditions.

The paper [80] proposed an FDL-based collision detection system for inland ships that aimed to improve safety and efficiency in the growing inland shipping industry. The system leveraged Multi-access Edge Computing (MEC) nodes to achieve ultra-low communication latency and guaranteed real-time reaction to avoid collisions. The proposed system provided a robust positioning prediction model while preserving the privacy of individual ships through collaborative learning. Extensive simulation results showed that the system was accurate, and efficient, and ensured timely and trusted communication to avoid collisions between ships.

Another system [81] aimed to provide a timely and accurate prediction of ships' positioning while ensuring data security and privacy. The proposed system was deployed at the MEC level for low-latency communication and relied on blockchain and smart contracts to ensure trust and valid communications. The results from a generated dataset representing ships' mobility in France showed the accuracy of the prediction model and the effectiveness of the proposed system in ensuring reliable communications and avoiding collisions between ships.

F. DFL FOR PRIVACY-PRESERVING PET IMAGE RECONSTRUCTION

A DL-based method was proposed [82] for positron emission tomography (PET) image reconstruction using data from multiple locations. The method utilized FL to train a DNN model using data from different locations without making the underlying datasets publicly available. The use of FL enabled the training of a robust and generalized model while preserving the privacy of sensitive personally identifiable information (PII) contained in the data. The authors demonstrated the effectiveness of their proposed approach in improving the generalizability and robustness of the model by evaluating it on unseen data from different locations.

The study [83] examined the problems and fixed FDL's security and privacy issues. By utilizing an adaptive noise injection technique and a layer-wise relevant propagation algorithm, the proposed Adaptive privacy-preserving federated learning (APFL) system seemed to balance security and accuracy. The proposed APFL framework achieved an accuracy of 88.46% after 200 epochs, outperforming Distributed Selective Stochastic Gradient Descent (DSSGD) and Deep learning with differential privacy (DLPP) models, while addressing security and privacy concerns in FDL.

G. DFL FOR ROBOT TARGET RECOGNITION

The paper [84] proposed InVision, a DFL approach for robot target recognition that used deep geometric learning to improve perception capabilities and resolution of representation maps. Federated metric learning was used to protect user data privacy across multiple devices and alleviated the problem of inadequately labeled training data. Additionally, a lightweight DNN was presented to improve the speed of the recognition system. The experimental results demonstrated that InVision outperformed existing approaches significantly.

H. DFL FOR PRESERVING IOT-BASED SOCIAL NETWORK

A novel DP-based DFL framework was proposed [85] that fulfilled DP's requirements under different privacy levels by adjusting scaled variances of Gaussian noise. The authors also developed a Differentially Private Data-Level Perturbation (DP-DLP) mechanism to conceal individual data points' impact on the training phase. Experiments on real-world datasets demonstrated that the proposed mechanism was able to offer high privacy, enhanced utility, and elevated efficiency, enabling the development of various DP-based FL models with different trade-off preferences on data utility and privacy levels.

I. DFL FOR FAKE NEWS DETECTION

The development of a decentralized DL model using FL for fake news detection in social media was discussed [86]. The authors highlighted the challenges of using a centralized training technique to build a generalized model and proposed the use of FL to overcome this problem. The proposed FL technique was evaluated using an Integrated Social Media and Open Web Fake News Dataset (ISOT) dataset and outperformed previous studies with an accuracy of 99.6% utilizing fewer communication rounds. The authors suggested that the FL technique could be more efficient than a centralized method for false news detection, and recommended the use of Blockchain-like technologies to improve the integrity and validity of news sources.

J. DFL FOR GPS TRAJECTORY

The authors [87] proposed an ensemble-based Federated Deep Neural Network (eFedDNN) architecture for travel mode inference. The model used privacy mechanisms to train a global model in a distributed manner, rather than allowing direct access to the user data. The performance of eFedDNN was evaluated and compared with the vanilla FL and non-federated learning methods on the dataset called MTL trajet open-access dataset. The results showed that the proposed ensemble technique outperformed the baseline models with better accuracy, with the LSTM model having the best accuracy among the three vanilla neural network-based FL models.

K. DFL FOR INDUSTRIAL IOT (IIOT)

The IIoT systems continued to grow in size and complexity, there was a need for efficient and effective methods to collect and analyze data from a large number of distributed devices. DFL emerged as a promising approach to enable

collaborative learning among geographically dispersed devices while preserving data privacy and security.

In the paper [72], an ensemble-based DFL cyber-threat hunting model was proposed to detect attack samples without data sharing. The model consisted of two parallel federated-based components and used an ensemble of classifiers to make the final decision. The proposed model outperformed previous works in the literature in the F1-score metric and was stable when facing different numbers of clients, with faster training time than centralized models of the same computational complexity.

The paper [88] suggested a novel approach for federated and dynamic network management and resource allocation for differentiated Quality of Service (QoS) services in future IIoT networks. By using federated reinforcement learning (FRL) to distribute data acquisition and computation tasks over distributed network agents and exploit local computation capacities and self-learning experiences.

A privacy-preserving secure framework (PPSS) framework [74], which used FL to detect intrusions in industrial systems. PPSS employed a blockchain-enabled FL approach to address challenges such as privacy protection, trusted validation, and consensus of the federation. The framework included two federated stages that used differentially private training and Proof-of-Federated Deep-Learning (PoFDL) protocol to ensure privacy, verifiability, and transparency. Evaluation of the PPSS framework on a new cyber security dataset demonstrated high performance in detecting industrial IIoT attacks under different distribution modes. Overall, PPSS proved to be an effective method for detecting cyber-attacks in industrial systems.

The proposed framework [89] aimed to ensure the trustworthy execution of FL-based DL models by addressing issues such as intermediate results and data structure leakage during model aggregation. The framework adopted an edge and cloud-powered service-oriented architecture and uses differential privacy to generate locally trained models. The service model decomposed the FDL process into services to ensure privacy preservation and trustworthy execution. Additionally, the paper also proposed a privacy-preserving local model aggregation mechanism.

L. DFL FOR AUTONOMOUS DRIVING

A new approach [90] to learn autonomous driving policy while preserving user privacy was proposed. The peer-to-peer DFL approach was fully decentralized and removed the need for central orchestration. The authors designed a Federated Autonomous Driving network (FADNet) that improved model stability, ensured convergence, and handled imbalanced data distribution problems while being trained with FL methods. The approach was tested on three datasets and achieved superior accuracy compared to other recent methods while maintaining privacy by not collecting user data on a central server.

In the article [91], Federated Learning for Connected Autonomous Vehicles (FLCAV) framework was utilized, to implement DFL to improve perception in open driving scenarios. To generate federated-DNNs from distributed data sources like autos and road sensors, FLCAV used vehicular networks. Compared to centralized learning, this strategy protected data privacy and lower communication costs. In this paper, networking, and training frameworks for FLCAV perception were introduced. These frameworks solved difficult issues including multi-modal datasets and sensor locations.

M. DFL FOR WIND POWER FORECASTING

A cyber-resilient approach based on FL and CNN for short-term wind power generation forecasting in different regions of Iran was proposed [92]. The approach ensured generalizability, and data independence, and preserved the security and privacy of data. The federated network was designed with an architecture of 9 clients to extract salient features from the data associated with each region via the CNN technique. The generalized global supermodel was produced based on the extracted features in each client to forecast the wind power in new and unknown regions. Various scenarios were developed to test the robustness of the suggested methodology, including a scaling attack and cyber-attack detection. The results demonstrated the high accuracy, generalizability, and cyber-resilience of the proposed approach in wind power forecasting in various regions of Iran.

To solve the issues regarding information privacy and data isolation in the context of ultra-short-term wind power forecasting in contemporary power networks with a substantial proportion of renewable energy sources, DFL is used in the article [93]. The suggested method was known as federated deep reinforcement learning (FedDRL), combined with DRL with FL to increase wind power forecast accuracy while protecting data privacy. In comparison to centralized forecasting systems, simulation findings showed that FedDRL performed more accurately than conventional prediction methods while also successfully protecting data privacy.

In another paper [94], FL-based wind energy forecasting was presented as a unique decentralized collaborative modeling technique capable of training a single model on data from several wind farms without endangering data security or privacy. To do this, local model parameters were securely exchanged rather than transferring private data across locations. The proposed FL-based wind power forecasting performed well, with 87.96% accuracy, when compared to non-private centralized, fully private localized, and non-private distributed models. Taking use of the smoothing effect, the suggested model had better generalizability with 83.63% accuracy was also supported, while the confidentiality of the underlying data was retained.

A privacy-preserving wind speed prediction framework based on FDL was proposed [95], which utilized multi-input inner-product functional encryption to offer extra data protection. A case study using the Wind Integration

National Dataset demonstrated how this strategy outperformed isolated training scenarios and came close to the ideal centralized one in terms of prediction performance without disclosing private information.

N. DFL FOR IMPROVING CLASSIFICATION ACCURACY OF MOBILE DL APPLICATIONS

The paper [96] presented Astraea, a self-balancing FL framework designed to alleviate imbalances in distributed training data, which could have caused accuracy degradation in FL applications. The proposed framework incorporated global data distribution-based data augmentation and mediator-based multi-client rescheduling to counter this problem. Astraea showed a significant improvement in top-1 accuracy of +5.59% and +5.89% on imbalanced EMNIST and imbalanced CINIC-10 datasets. Additionally, Astraea's communication traffic was found to be 92%.

O. DFL FOR PLACEMENT STRATEGY DESIGN IN CODED CACHING FOR FOG-RADIO ACCESS NETWORKS

With the growing demand for data-intensive applications, fog computing has emerged as a promising solution for enabling efficient and low-latency data processing at the edge of the network. Within the fog platform, the data present must comply with both cloud and device policies regarding security constraints, and these policies should be propagated throughout the system's various levels [97]. This is especially relevant in the fog-radio access networks (F-RANs). The delay in accessing content can be significantly impacted in fog-radio access networks (F-RANs) depending on the placement of the content within the network.

In fact, a recent paper [98] investigated the use of federated deep reinforcement learning to design placement strategies in F-RANs. The placement problem was modeled as a Markov decision process and solved using dueling double-deep Q-learning. Additionally, FL was applied to aggregate the global decision model. The results showed that the proposed scheme outperformed benchmarks in reducing content access delay, conserving bandwidth resources, and achieving a balance between local caching gain and global multicasting gain. The use of FL in this application demonstrated its potential for optimizing resource utilization and improving performance in decentralized networks.

DFL has emerged as a promising technique for collaborative learning across distributed devices while maintaining data privacy. However, there are a number of difficulties with the practical application of DFL that must be resolved before it can be used successfully in practical applications. In the next section, we will discuss the research challenges associated with DFL. We will highlight the key technical and theoretical challenges that must be addressed to ensure the effectiveness and efficiency of DFL in practical applications.

VI. RESEARCH CHALLENGES

DFL is a cutting-edge approach to machine learning that has garnered attention for its potential to address challenges in distributed learning while prioritizing data privacy. In a decentralized learning environment, preserving sensitive information and preventing privacy violations become paramount concerns. In the following sections, we delve into some of the key research challenges associated with DFL. The subsequent discussion highlights the complexity of these challenges and emphasizes the need for continuous research and development in these areas. By doing so, we can ensure that DFL remains a secure, compliant, and ethical approach to machine learning, paving the way for its continued adoption and application in diverse industries. Figure 4 illustrates the research challenges, providing a visual representation of the multifaceted landscape that researchers and practitioners must navigate to enhance the effectiveness and robustness of DFL.

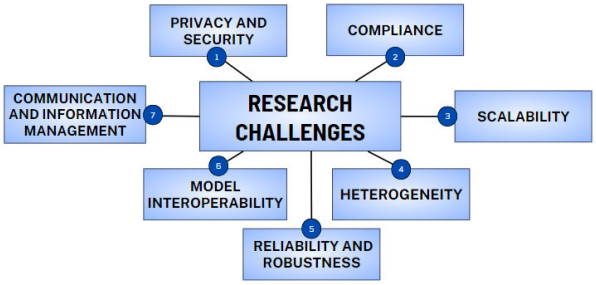

FIGURE 4. Research challenges in the field of Deep federated learning.

A. PRIVACY AND SECURITY

It might be difficult to preserve sensitive information and prevent privacy violations in a decentralized learning environment. A decentralized ML method called DFL allows several devices to work together and train from available information without sharing the original data with a centralized server. Protecting client data privacy is one of the main motivations for DFL [99], but it also poses a significant challenge. Research is needed to develop robust privacy-preserving methods that can withstand malicious attacks.

Through a data collection server, which gathers model upgrades from each device and merges them into something like a global model, DFL devices connect. The parameters and updates for the model as well as the data on the device might possibly be made public during this procedure. In addition, threats like data theft or manipulation might potentially target the aggregate server. Implementing privacy-preserving methods, such as different datasets, encrypted communications, and strong aggregation protocols, is crucial in order to confront these security threats and safeguard the shared data and models in an FL program. Additionally, it's crucial to safeguard the connection between the devices and the data collection server from hackers and other security risks.

B. COMPLIANCE

DFL is a cutting-edge approach to ML that involves training models on data distributed across multiple devices or edge

nodes. This approach has the potential to revolutionize the way, to train ML models, particularly in industries such as healthcare, finance, and environmental regulation. However, achieving compliance in DFL is a critical research challenge, given the complex nature of this approach.

One of the main compliance challenges in DFL is data privacy. With regulations such as the General Data Protection Regulation (GDPR), some people believe that the GDPR is the most significant shift to data privacy law in the past 20 years. Any organization that gathers and uses the personal data of EU citizens, whether inside or outside the EU, must comply with the GDPR privacy law as of May 2018 [100]. The Health Insurance Portability and Accountability Act (HIPPA) of 1996, includes strict guidelines for the security and privacy of patient data, and it has altered how businesses in the health services, insurance, life sciences, and other sectors of the economy think about and deal with security issues and privacy concerns [101]. Compliance with these regulations requires implementing robust security measures to ensure that sensitive data is securely aggregated and analyzed without exposing private information to unauthorized parties. Techniques such as DP and HE can be used to ensure data privacy in FL.

Another important research challenge in DFL is the difference between privacy and security, particularly with respect to the protection of personal information. While privacy refers to the individual's right to control their personal information and how it is used, security refers to the measures taken to protect that information from unauthorized access, theft, or damage. DFL compliance entails resolving both security and privacy issues as well as understanding the differences between them. For example, techniques such as FL with secure aggregation and secure multi-party computation (SMC) can be used to ensure data security in FL.

Overall, compliance is an essential research challenge in DFL, requiring ongoing development and refinement of techniques and frameworks that enable organizations to achieve compliance while leveraging the benefits of FL. Addressing compliance challenges such as data privacy, regulatory compliance, and the difference between privacy and security will be crucial for the continued success of DFL and its adoption in a wide range of industries. It is essential to continue research and development in this area to ensure that DFL remains secure, compliant, and ethical.

C. SCALABILITY

Scalability is one of the major difficulties in DFL in IoT. To train a DL model, each device must have adequate processing power, and the data collection server must have the capacity to handle model upgrades from all devices. This may result in longer training periods and expensive prices, and it demands a substantial amount of computer resources.

Researchers have suggested several methods to improve the effectiveness of DFL in the IoT and overcome the scalability issue. One strategy is to arrange devices into groups using a hierarchical structure, with just a portion of the devices directly communicating with the data collection server. As a result, less communication is required between the equipment and the data collection server, which may decrease training time and increase computational efficiency.

Utilizing a hybrid strategy, where devices execute certain calculations locally and some on a central server, is an additional strategy. This may reduce communication overhead and balance the computing strain.

The capacity to adapt to modifications in the number of devices and the distribution of data is another component of adaptability in DFL in the IoT. The DL models must be capable of handling new devices entering or departing the network as well as changes in data distribution. To overcome these difficulties, researchers have suggested FTL and dynamic aggregation. In FTL, the models may learn from other equipment even when the data distribution changes, but in dynamic aggregation, the aggregation server modifies the aggregation technique depending on the number of machines and their model updates. These methods may aid in preserving the DFL system and the IoT's scalability and effectiveness.

D. HETEROGENEITY

FL has difficulties managing the variety of devices and their various data distributions, network configurations, and hardware requirements. In the IoT, heterogeneity is a significant concern because of the range of products and their capabilities. The hardware requirements, processing power, and storage capacity of devices connected to an IoT network might vary, which can affect how well they can train and maintain DL models. In addition to affecting model completion and accuracy, this heterogeneity may raise communication costs between the equipment and the data collection server.

Researchers have put forward several strategies to make sure that devices with various capabilities may participate in and contribute to the learning process to overcome the heterogeneity problem in DFL in the IoT. Utilizing adaptive federated averaging is one method in which the load updates for each device are modified in accordance with their processing power and data volume. This improves the integration of the model structure and balances the participation of each device. Another strategy is to employ a learning algorithm, where the DL is first tweaked on local data at each device after being pre-trained on a centralized dataset. Using the information acquired from other devices enables devices with constrained computing capabilities to take part in the learning process.

The variety in data distribution across devices is another facet of variability in DFL in IoT. Each device may gather data with a distinct distribution, which might cause problems with model correctness and convergence. Researchers have suggested approaches like federated domain adaptation where the DL models are adjusted to the local data

distribution—and federated multi-task learning where the models are trained on a variety of related activities performed on many devices to overcome this problem. The variability in data distribution may be dealt with the help of these strategies and enhance the resilience and accuracy of the DFL system in the IoT. DFL is often applied to large-scale and heterogeneous datasets [102], which poses challenges in terms of data alignment and model convergence. For a solution to these difficulties, research is required so DFL can effectively handle heterogeneous data.

E. RELIABILITY AND ROBUSTNESS

Ensuring the resilience of a federated classification algorithm in the presence of damaged or unreliable hardware and communication networks, DFL in the IoT must be reliable and resilient since mistakes during the learning process might lead to inaccurate predictions and judgments. The decentralized aspect of FL, where several devices take part in the learning process, raises the possibility of data inaccuracies and communication breakdowns, which may have a detrimental effect on the system's resilience and dependability. Additional difficulties may be brought about by inaccurate model upgrades or data manipulation when there are fraudulent or untrustworthy devices present in the network.

Researchers have developed several strategies to make sure the process of learning is robust and dependable to meet the difficulties of dependability and robustness in DFL in the IoT. To lessen the influence of isolated incidents or harmful devices in the model updates, one strategy is to employ robust aggregation techniques, such as a reduced mean or median. An alternative strategy is to utilize privacy-preserving methods, including DP, to prevent hostile devices from altering the models and data. Researchers have also suggested strategies like federated anomaly detection to recognize and exclude faulty connections from the learning process.

The capacity to manage mistakes and failures throughout the learning process is another facet of resilience and dependability in DFL in the IoT. In an IoT network, devices may face hardware or connectivity issues that result in inaccurate model updates or data inaccuracies. To overcome these difficulties, academics have suggested strategies like federated resilience and federated retraining to guarantee that the learning process is strong and dependable even in the face of failures and mistakes. These methods may assist in strengthening the DFL system's resilience and reliability and guarantee the accuracy and dependability of the system's predictions and judgments.

F. MODEL INTEROPERABILITY

It is difficult to comprehend how global models created by FL make decisions and explain their outcomes. Model interoperability is a crucial problem in DFL in the IoT, since the models learned by many devices may get complicated and difficult to comprehend. This might make it difficult to comprehend the reasoning behind a model's choice of prediction or action, which is crucial for establishing confidence and making sure the algorithms are applied responsibly and legally. Furthermore, since FL is decentralized, it might be challenging to comprehend how each device contributes to the overall model and how limited information and context affect the models.

Researchers have suggested numerous methods to make the models visible and intelligible to meet the interoperability difficulty in DFL in the IoT. One method is to depict the key attributes and choices made by the model using explainable AI tools, such as salience maps. A different strategy is to utilize federated distillation, in which the models are taught to imitate the behavior of a more straightforward and understandable model. This may guarantee that the models, even in complicated and decentralized contexts, remain clear and intelligible.

Understanding connections between equipment and the data collection server is another part of the applicability of DFL in the IoT. It may be challenging to comprehend how interactions between machines and the clustering server affect the overall model throughout the learning process of FL, which includes the interchange of model upgrades and data.

Researchers have suggested approaches to this problem, such as federated model visualization and federated debugging, to comprehend how devices interact with the aggregate server. These methods may assist in increasing the DFL's interoperability and transparency and guarantee that the models are utilized morally and responsibly.

G. COMMUNICATION AND INFORMATION MANAGEMENT

In a FL system, an effective model updates communication and coordinates data transfers across various devices. DFL in the IoT is crucial since communication and information management are what make the learning process efficient and successful. Multiple devices communicate model modifications and information with the clustering server as part of FL, which calls for efficient and safe communication protocols. FL requires a large amount of communication between client devices and the server, leading to slow convergence and high latency. Improving the communication efficiency of DFL is a crucial area of research [17].

Researchers have developed several ways to make sure that the information is transferred and stored effectively and securely to handle the data and communication management difficulties in DFL in the IoT. To decrease connection overhead and guard against data interception or manipulation, one strategy is to deploy compression and encryption methods, such as federated reduction and federated encryption. Another strategy is to control the data produced by the devices and make sure that it is correctly stored and processed by using federated data management methods, such as federated data segmentation and federated data selection.

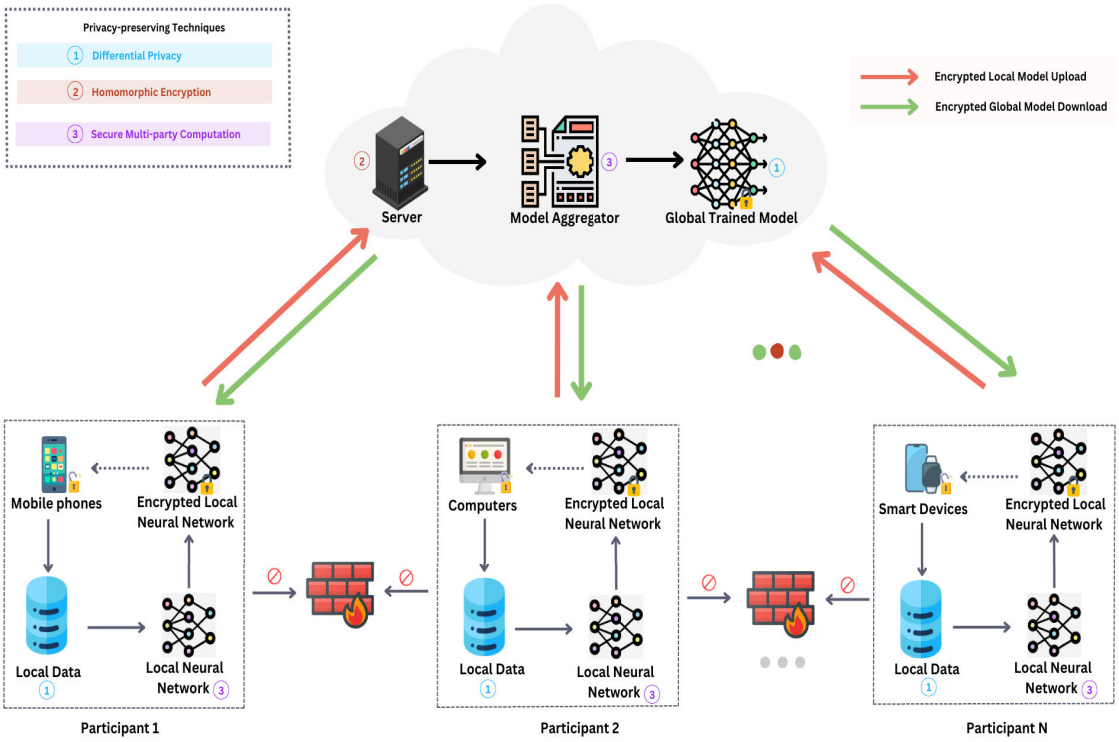

FIGURE 5. An architecture diagram of GDPR-Compliant DFL-based framework.

Another aspect of communications and data management in DFL in the IoT is the ability to handle transmission latency and communication failures. FL requires connections between several pieces of equipment and the data-gathering server since it is decentralized, which might be hampered by propagation delays and communication mistakes. As a solution to these problems, researchers have proposed solutions like federated interactive transmission and federated edge computing to improve the efficiency and dependability of communication. These techniques could help to improve DFL in the IoT and information management, making the learning process efficient and speedy.

DFL has garnered notable interest in addressing key issues in distributed learning while maintaining data privacy. Its potential lies in overcoming critical challenges associated with collaborative learning. The upcoming section will explore the creation of a deep federated learning framework that adheres to GDPR regulations, ensuring compliance with data protection standards. This approach reflects the growing importance of privacy considerations in the development of advanced machine learning techniques.

VII. BUILDING A GDPR-COMPLIANT DEEP FEDERATED LEARNING FRAMEWORK

The privacy of a user is very important when we talk about IoT-based systems. DFL does support user privacy preservation, but there are several rules and regulations that govern the system. In the previous section, we discussed the available regulatory systems like GDPR and HIPPA, etc.

As an example, we have selected GDPR [103] to build an abstract GDPR-Compliant DFL framework and architecture. A collection of Internet of Things gadgets that gather and interpret data locally using various local neural network designs. The devices' data may be diverse and come from several organizations or areas. Other learning goals for the devices may include anomaly detection, regression, or classification. A central server that manages the FL process by gathering the local model parameters across the devices and communicating the updated global model parameters back to the devices.

To safeguard the data and model against malicious assaults or breaches, the server could additionally include various Privacy Preserving Techniques (PPTs), such as Differential Privacy [104], Secure Multi-Party Computation [105], and Homomorphic Encryption [106]. A FL approach enables the gadgets to work together to develop a common prediction model while protecting data privacy and cutting down on communication overhead. The devices may learn from the instance-level representations acquired from peer devices and enhance their local models using automatic attention mechanisms like authentication and authorization. According to the method shown in the above picture, IoT devices analyze the local data they produce before transferring it, encrypted on both ends, through an encrypted communication channel to a centralized server.

TABLE 4. Privacy preserving techniques (PPTs) for Secure Data processing and collaboration.

Component	Privacy Preserving Techniques	Explanation	Importance (Yes/No)
Local Data	Differential Privacy	The local data is subjected to Differential Privacy by introducing noise. While keeping the general statistical features of the data, this approach aids in protecting individual privacy. Privacy protection for local datasets is seen as crucial	Yes
Local Neural Network	Secure Multi-Party Computation	Multiple parties may calculate operations over their local models using the optional Secure Multi-Party Computation approach without disclosing any information. It offers a safe method for maintaining anonymity while working together on calculations	Optional
Server	Homomorphic Encryption	To allow computation on encrypted data, homomorphic encryption is an optional approach. It preserves the data's confidentiality by enabling an analysis on it by the server without having to decode it	Optional
Model Aggregator	Secure Multi-Party Computation	Joint calculation of local models is made possible while maintaining privacy with Secure Multi-Party calculation. Without disclosing any specifics about individual models, it guarantees that the process of model aggregation is carried out safely	Yes
Global Training Model	Differential Privacy	The aggregated models are subjected to Differential Privacy by introducing noise. This method contributes to the global training process' accuracy while protecting privacy	Yes

After receiving the input, the central server processes it further and uses FL techniques to build an ML model. The resultant model is then distributed to the connected IoT devices for local interpretation using a model deployment layer. Additionally, the server uses a model updating layer to regularly update the model with the most current information gathered from IoT devices. Figure 5 shows the GDPR-compliant DFL-based Architecture.

As we continued along the path shown in Figure 5, it became clear that relying simply on Deep Federated Learning (DFL) did not offer a complete answer for data security. This understanding led to the inclusion of GDPR principles into our framework, detailing certain actions and procedures to comply with GDPR rules. The Figure 5 explanation, which focuses on the following important factors, provides more clarification of these improvements.

To strengthen data security, we first created Privilege-Protected Tokens (PPTs) as a key security mechanism. The decision was based on their demonstrated efficacy in preserving the security and privacy of personal data, which was perfectly in line with the stringent GDPR regulations. We carefully included a firewall in our system design in addition to this. This safeguard guarantees secure data transmission between devices, to the main server, and for international model upgrades. It ensures the secrecy and integrity of the data throughout its transfer over the network.

Additionally, we carried out a thorough evaluation of the system's benefits and drawbacks, taking important factors like scalability and a precise breakdown of the processes shown in the diagram into account. This assessment offers a fair knowledge of the framework's advantages and disadvantages.

Diverse PPTs are used in various stages of the process to accomplish this, including differential privacy to protect confidentiality in local data and aggregated models, secure multi-party computation to enable joint computation of local models while protecting privacy, and homomorphic encryption to enable computation on encrypted data. These methods allow for accurate and fast model training in an interconnected environment while simultaneously guaranteeing privacy and secrecy. Thus, DFL is a formidable tool for realizing the promise of group machine learning while protecting the security and privacy of data.

The particular use case and specifications of the program determine which PEM is best for each component. Although it's not a full list, the table below in Table 3 gives a broad overview of several frequently used strategies for each component. Depending on the particulars of the use case, other techniques could be more appropriate. Additionally, based on the different needs of the application, the significance of each approach for every element may change. We acknowledge that this work serves as a starting point, and we are working on extending it to develop a formally verified, comprehensive GDPR-compliant DFL architecture, evaluated with established metrics to ensure effectiveness and reliability.

In the next section, we will explore the future research directions of DFL, focusing on areas such as privacy-preserving algorithms, communication-efficient techniques, and scalability issues. By highlighting the emerging trends and opportunities in DFL research, this section aims to provide insights into the future development and deployment of this exciting technology.

VIII. FUTURE WORK

As DFL advances, we aim to contribute to ongoing improvements and innovations in this dynamic field by exploring future research directions. This proactive approach plays a pivotal role in shaping the trajectory of DFL and maximizing its impact on the broader landscape of machine learning. Figure 6 represents potential directions, guiding our exploration of upcoming research avenues to enhance and advance this technology in the future. In this section, we explore the upcoming research avenues, offering insights

TABLE 5. Techniques, description, challenges, and benefits of DFL future directions.

Reference No.	Technique	Description	Challenges	Benefits
[107]	Heterogeneous Federated Learning (HFL)	Training a single model across devices with different hardware and software configurations	Ensuring that the model can perform effectively across all devices	Makes FL applicable to a wider range of real-world scenarios
[108]	Federated Transfer Learning (FTL)	Fine-tuning a pre-trained model on a new task using a small amount of data in a decentralized manner	Sharing the pre-trained model across devices while maintaining data privacy	Enables faster and more accurate convergence, especially for tasks with limited labeled data
[109]	Federated Meta-Learning (FedMeta)	Shares a parameterized algorithm or meta-learner instead of a global model	Maintaining data privacy and reducing communication overhead	More efficient and effective meta-learning across multiple devices
[110]	Federated Domain Adaptation (FDA)	Adapts the model to the different data distributions on each device in an FL system	Training a single model that will perform well across all devices in an FL system with different data distributions	Improves the overall performance of the model in the FL system
[111]	Federated Semi-Supervised Learning (FSSL)	Extends FL to a semi-supervised setting, where each device has both labeled and unlabeled data	Tackling specific challenges in decentralized machine learning and allowing for more advanced and practical applications of FL	Improves the performance of FL models by leveraging unlabeled data

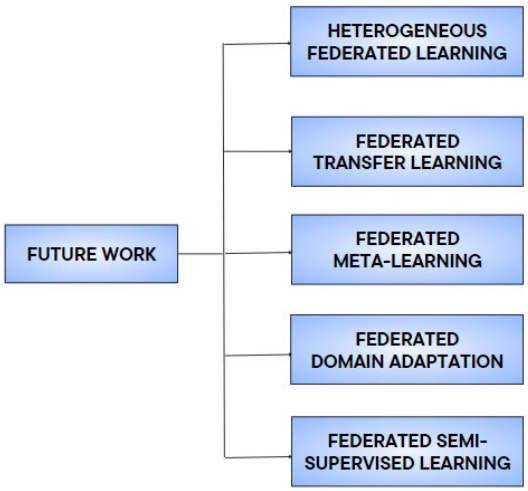

FIGURE 6. Future research directions of Deep federated learning.

into the evolving world of DFL. These efforts aim to provide valuable ideas for further enhancing and advancing this technology in the future. The future directions of DFL along with their techniques,description, challenges, and benefits are summarized in table 5.

A. HETEROGENEOUS FEDERATED LEARNING

Heterogeneous Federated Learning refers to a scenario where devices participating in the training process have different hardware and software configurations. This poses a significant challenge to training a single model that can perform effectively across all devices. To resolve this issue, researchers developed frameworks such as [107] that effectively increased the applicability of FL to a wide range of heterogeneous environments. These frameworks offered several advantages over traditional FL techniques, including superior convergence rate, accuracy, and computation/communication economy. By tailoring the training process to the specific hardware and software configurations of each device, these frameworks enable more effective and efficient FL in diverse real-world scenarios.

B. FEDERATED TRANSFER LEARNING

Transfer learning is a popular technique in ML where a pre-trained model is fine-tuned on a new task using a small amount of data. However, when it comes to FL, training a model in a decentralized manner using transfer learning poses significant challenges. To overcome this challenge, a new technique and framework [108] called Federated Transfer Learning (FTL) was been introduced. FTL enabled efficient model sharing across devices while maintaining data privacy, which is crucial in FL scenarios. This approach allowed for a pre-trained model to be transferred to different devices for fine-tuning on a specific task, resulting in faster and more accurate convergence. By integrating the benefits of transfer learning with FL, FTL provides a promising solution for training models on distributed datasets in a privacy-preserving manner.

C. FEDERATED META-LEARNING

The results of the a novel federated meta-learning framework called FedMeta [109] demonstrated that it outperformed previous approaches in terms of convergence speed, model accuracy, and communication efficiency, making it a promising framework for future research in federated meta-learning.

The FedMeta differed from previous approaches by sharing a parameterized algorithm or meta-learner instead of a global model. This framework allowed for more efficient and effective meta-learning across multiple devices while maintaining data privacy. In traditional FL, a global model is shared across all devices, which can lead to privacy concerns and communication overhead. In contrast, the FedMeta framework shared a parameterized algorithm, which is updated based on the local data of each device, leading to more accurate and efficient meta-learning.

D. FEDERATED DOMAIN ADAPTATION

Federated Domain Adaptation (FDA) is a technique that is utilized when the data distribution on each device in an FL system is different. This creates a challenge when attempting to train a single model that will perform well across all devices. In such scenarios, the FDA is used to adapt the model to the different data distributions on each device, allowing the model to perform well across all devices. The process of FDA involves training a classifier of the target model in a self-supervised manner using information maximization and pseudo-labeling techniques [110]. These techniques are employed to maximize the amount of information captured from the data and to assign labels to unlabeled data samples in a way that is consistent with the true labels. The self-supervised classifier is then used to adapt the model to the different data distributions on each device, improving the overall performance of the model in the FL system.

E. FEDERATED SEMI-SUPERVISED LEARNING

Federated Semi-Supervised Learning (FSSL) extends FL to a semi-supervised setting, where each device has both labeled and unlabeled data. In the work [111], two essential scenarios of FSSL were studied, based on the location of the labeled data.

These expansions of DFL were designed with the explicit goal of addressing distinct challenges inherent in decentralized machine learning. These enhancements provided tailored solutions to overcome specific obstacles, thereby enabling the technology to be applied in more sophisticated and practical ways. By refining the capabilities of DFL through these extensions, the framework became better equipped to handle intricacies associated with decentralized learning environments, facilitating its application in a broader range of real-world scenarios.

IX. CONCLUSION

DFL has emerged as a promising distributed AI technique that can enable private and scalable IoT services and applications. The article provides a comprehensive overview of DFL and various DFL services and applications. The challenges to the privacy of individual users and devices are also identified which can have legal as well as ethical implications.

DFL-based systems need to prioritize enhancing security and privacy protections to safeguard sensitive data during collaborative learning. Keeping this in mind, we presented the initial idea of GDPR-Compliant DFL architecture in this paper. This architecture combined various privacy preservation techniques employed by existing DFL-based systems studied in the literature. We intend to further extend this idea into a comprehensive framework which will be formally verified and evaluated in our future work. The aim of our work is to enable wide scale adoption of DFL by addressing security and privacy concerns of the stakeholders. Furthermore, exploring federated learning techniques for other machine learning algorithms and data types could broaden DFL's applicability to various domains. In conclusion, we believe that this article will generate increased interest in DFL, encouraging further research endeavors aimed at fully realizing the potential of DFL.

ACKNOWLEDGMENT

The authors acknowledge TU Wien Bibliothek for financial support through its Open Access Funding Program.

REFERENCES

[1] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A survey on Internet of Things: Architecture, enabling technologies, security and privacy, and applications," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1125–1142, Oct. 2017.

[2] H. Lin, K. Kaur, X. Wang, G. Kaddoum, J. Hu, and M. M. Hassan, "Privacy-aware access control in IoT-enabled healthcare: A federated deep learning approach," *IEEE Internet Things J.*, vol. 10, no. 4, pp. 2893–2902, Feb. 2023.

[3] P. Ravichandran, C. Saravanakumar, J. D. Rose, M. Vijayakumar, and V. M. Lakshmi, "Efficient multilevel federated compressed reinforcement learning of smart homes using deep learning methods," in *Proc. Int. Conf. Innov. Comput., Intell. Commun. Smart Electr. Syst. (ICSES)*, Sep. 2021, pp. 1–11.

[4] B. Yin, H. Yin, Y. Wu, and Z. Jiang, "FDC: A secure federated deep learning mechanism for data collaborations in the Internet of Things," *IEEE Internet Things J.*, vol. 7, no. 7, pp. 6348–6359, Jul. 2020.

[5] S. Kaspour and A. Yassine, "A federated learning model with short sequence to point mechanism for smart home energy disaggregation," in *Proc. IEEE Symp. Comput. Commun. (ISCC)*, Jun. 2022, pp. 1–6.

[6] H. Mohamed, N. Koroniotis, and N. Moustafa, "Digital forensics based on federated learning in IoT environment," in *Proc. Australas. Comput. Sci. Week*, Jan. 2023, pp. 92–101.

[7] J. Wen, Z. Zhang, Y. Lan, Z. Cui, J. Cai, and W. Zhang, "A survey on federated learning: Challenges and applications," *Int. J. Mach. Learn. Cybern.*, vol. 14, no. 2, pp. 513–535, Feb. 2023.

[8] 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. Surveys Tuts.*, vol. 23, no. 3, pp. 1622–1658, 3rd Quart., 2021.

[9] S. Dong, P. Wang, and K. Abbas, "A survey on deep learning and its applications," *Comput. Sci. Rev.*, vol. 40, May 2021, Art. no. 100379.

[10] K. Lakshmanna, R. Kaluri, N. Gundluru, Z. S. Alzamil, D. S. Rajput, A. A. Khan, M. A. Haq, and A. Alhussen, "A review on deep learning techniques for IoT data," *Electronics*, vol. 11, no. 10, p. 1604, May 2022.

[11] S. H. Shah and I. Yaqoob, "A survey: Internet of Things (IoT) technologies, applications and challenges," in *Proc. IEEE Smart Energy Grid Eng. (SEGE)*, Aug. 2016, pp. 381–385.

[12] D. Yimam and E. B. Fernandez, "A survey of compliance issues in cloud computing," *J. Internet Services Appl.*, vol. 7, no. 1, pp. 1–12, Dec. 2016.

[13] N. Truong, K. Sun, S. Wang, F. Guitton, and Y. Guo, "Privacy preservation in federated learning: An insightful survey from the GDPR perspective," *Comput. Secur.*, vol. 110, Nov. 2021, Art. no. 102402.

[14] A. Subahi and G. Theodorakopoulos, "Ensuring compliance of IoT devices with their privacy policy agreement," in *Proc. IEEE 6th Int. Conf. Future Internet Things Cloud (FiCloud)*, Aug. 2018, pp. 100–107.

[15] Q. Yang, Y. Liu, T. Chen, and Y. Tong, "Federated machine learning: Concept and applications," *ACM Trans. Intell. Syst. Technol.*, vol. 10, no. 2, pp. 1–19, 2019.

[16] P. Kairouz et al., *Advances and Open Problems in Federated Learning*. Boston, MA, USA: Now, 2021.

[17] J. Konečnỳ, H. B. McMahan, F. X. Yu, P. Richtárik, A. T. Suresh, and D. Bacon, "Federated learning: Strategies for improving communication efficiency," 2016, *arXiv:1610.05492*.

[18] B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. Y. Arcas, "Communication-efficient learning of deep networks from decentralized data," in *Proc. Artif. Intell. Statist.*, 2017, pp. 1273–1282.

[19] Y. Foucade and Y. Bennani, "Unsupervised collaborative learning using privileged information," 2021, *arXiv:2103.13145*.

[20] M. Servetnyk, C. C. Fung, and Z. Han, "Unsupervised federated learning for unbalanced data," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2020, pp. 1–6.

[21] R. Zhao, Y. Wang, Z. Xue, T. Ohtsuki, B. Adebisi, and G. Gui, "Semisupervised federated-learning-based intrusion detection method for Internet of Things," *IEEE Internet Things J.*, vol. 10, no. 10, pp. 8645–8657, May 2023.

[22] X. Yang, Z. Song, I. King, and Z. Xu, "A survey on deep semi-supervised learning," *IEEE Trans. Knowl. Data Eng.*, vol. 35, no. 9, pp. 8934–8954, Nov. 2023.

[23] W. Chen, X. Qiu, T. Cai, H.-N. Dai, Z. Zheng, and Y. Zhang, "Deep reinforcement learning for Internet of Things: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 3, pp. 1659–1692, 3rd Quart., 2021.

[24] T. G. Nguyen, T. V. Phan, D. T. Hoang, T. N. Nguyen, and C. So-In, "Federated deep reinforcement learning for traffic monitoring in SDN-based IoT networks," *IEEE Trans. Cognit. Commun. Netw.*, vol. 7, no. 4, pp. 1048–1065, Dec. 2021.

[25] J. Chen, J. Li, R. Huang, K. Yue, Z. Chen, and W. Li, "Federated learning for bearing fault diagnosis with dynamic weighted averaging," in *Proc. Int. Conf. Sens., Meas. Data Anal. era Artif. Intell. (ICSMD)*, Oct. 2021, pp. 1–6.

[26] L. Lyu, X. He, Y. W. Law, and M. Palaniswami, "Privacy-preserving collaborative deep learning with application to human activity recognition," in *Proc. ACM Conf. Inf. Knowl. Manage.*, Nov. 2017, pp. 1219–1228.

[27] Y. S. Can and C. Ersoy, "Privacy-preserving federated deep learning for wearable IoT-based biomedical monitoring," *ACM Trans. Internet Technol.*, vol. 21, no. 1, pp. 1–17, Feb. 2021.

[28] Y. Zhang, D. Zeng, J. Luo, Z. Xu, and I. King, "A survey of trustworthy federated learning with perspectives on security, robustness, and privacy," 2023, *arXiv:2302.10637*.

[29] S. Truex, N. Baracaldo, A. Anwar, T. Steinke, H. Ludwig, R. Zhang, and Y. Zhou, "A hybrid approach to privacy-preserving federated learning," in *Proc. 12th ACM Workshop Artif. Intell. Secur.*, Nov. 2019, pp. 1–11.

[30] Z. Li, Y. He, H. Yu, J. Kang, X. Li, Z. Xu, and D. Niyato, "Data heterogeneity-robust federated learning via group client selection in industrial IoT," *IEEE Internet Things J.*, vol. 9, no. 18, pp. 17844–17857, Sep. 2022.

[31] Z. Zhu, J. Hong, S. Drew, and J. Zhou, "Resilient and communication efficient learning for heterogeneous federated systems," in *Proc. Mach. Learn. Res. (PMLR)*, vol. 162. Cambridge, MA, USA, Jul. 2022, pp. 27504-27526.

[32] A. Fallah, A. Mokhtari, and A. Ozdaglar, "Personalized federated learning with theoretical guarantees: A model-agnostic meta-learning approach," in *Proc. Adv. Neural Inf. Process. Syst.*, vol. 33, 2020, pp. 3557–3568.

[33] D. Gao, X. Yao, and Q. Yang, "A survey on heterogeneous federated learning," 2022, *arXiv:2210.04505*.

[34] D. Sahoo, Q. Pham, J. Lu, and S. C. Hoi, "Online deep learning: Learning deep neural networks on the fly," 2017, *arXiv:1711.03705*.

[35] W. Li, R. Huang, J. Li, Y. Liao, Z. Chen, G. He, R. Yan, and K. Gryllias, "A perspective survey on deep transfer learning for fault diagnosis in industrial scenarios: Theories, applications and challenges," *Mech. Syst. Signal Process.*, vol. 167, Mar. 2022, Art. no. 108487.

[36] M. Huisman, J. N. van Rijn, and A. Plaat, "Metalearning for deep neural networks," in *Metalearning: Applications to Automated Machine Learning and Data Mining*. Cham, Switzerland: Springer, 2022, pp. 237–267.

[37] Z. Chen, H. Cui, E. Wu, and X. Yu, "Dynamic asynchronous anti poisoning federated deep learning with blockchain-based reputation-aware solutions," *Sensors*, vol. 22, no. 2, p. 684, Jan. 2022.

[38] A. Hussain, S. F. Ahmad, M. Tanveer, and A. S. Iqbal, "Computer malware classification, factors, and detection techniques: A systematic literature review (SLR)," *Int. J. Innov. Sci. Technol.*, vol. 4, no. 3, pp. 899–918, 2022.

[39] L. Lyu, J. Yu, K. Nandakumar, Y. Li, X. Ma, J. Jin, H. Yu, and K. S. Ng, "Towards fair and privacy-preserving federated deep models," *IEEE Trans. Parallel Distrib. Syst.*, vol. 31, no. 11, pp. 2524–2541, Nov. 2020.

[40] M. Nasr, R. Shokri, and A. Houmansadr, "Comprehensive privacy analysis of deep learning: Passive and active white-box inference attacks against centralized and federated learning," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2019, pp. 739–753.

[41] R. Alghamdi and M. Bellaiche, "A cascaded federated deep learning based framework for detecting wormhole attacks in IoT networks," *Comput. Secur.*, vol. 125, Feb. 2023, Art. no. 103014.

[42] S. I. Popoola, G. Gui, B. Adebisi, M. Hammoudeh, and H. Gacanin, "Federated deep learning for collaborative intrusion detection in heterogeneous networks," in *Proc. IEEE 94th Veh. Technol. Conf. (VTC-Fall)*, Sep. 2021, pp. 1–6.

[43] B. Li, Y. Wu, J. Song, R. Lu, T. Li, and L. Zhao, "DeepFed: Federated deep learning for intrusion detection in industrial cyber–physical systems," *IEEE Trans. Ind. Informat.*, vol. 17, no. 8, pp. 5615–5624, Aug. 2021.

[44] S. I. Popoola, R. Ande, B. Adebisi, G. Gui, M. Hammoudeh, and O. Jogunola, "Federated deep learning for zero-day botnet attack detection in IoT-edge devices," *IEEE Internet Things J.*, vol. 9, no. 5, pp. 3930–3944, Mar. 2022.

[45] A. N. Jahromi, H. Karimipour, and A. Dehghantanha, "Deep federated learning-based cyber-attack detection in industrial control systems," in *Proc. 18th Int. Conf. Privacy, Secur. Trust (PST)*, Dec. 2021, pp. 1–6.

[46] I. Fatima, S. U. R. Malik, A. Anjum, and N. Ahmad, "Cyber physical systems and IoT: Architectural practices, interoperability, and transformation," *IT Prof.*, vol. 22, no. 3, pp. 46–54, May 2020.

[47] A. Moradzadeh, H. Moayyed, B. Mohammadi-Ivatloo, A. P. Aguiar, and A. Anvari-Moghaddam, "A secure federated deep learning-based approach for heating load demand forecasting in building environment," *IEEE Access*, vol. 10, pp. 5037–5050, 2022.

[48] H. Park, T.-H. Nguyen, and L. Park, "Federated deep learning for RIS-assisted UAV-enabled wireless communications," in *Proc. 13th Int. Conf. Inf. Commun. Technol. Converg. (ICTC)*, Oct. 2022, pp. 831–833.

[49] Z. Guo, K. Yu, Z. Lv, K. R. Choo, P. Shi, and J. J. P. C. Rodrigues, "Deep federated learning enhanced secure POI microservices for cyber-physical systems," *IEEE Wireless Commun.*, vol. 29, no. 2, pp. 22–29, Apr. 2022.

[50] M. A. Ferrag, O. Friha, L. Maglaras, H. Janicke, and L. Shu, "Federated deep learning for cyber security in the Internet of Things: Concepts, applications, and experimental analysis," *IEEE Access*, vol. 9, pp. 138509–138542, 2021.

[51] Y. Li, X. Wei, Y. Li, Z. Dong, and M. Shahidehpour, "Detection of false data injection attacks in smart grid: A secure federated deep learning approach," *IEEE Trans. Smart Grid*, vol. 13, no. 6, pp. 4862–4872, Nov. 2022.

[52] I. Zakariyya, H. Kalutarage, and M. O. Al-Kadri, "Memory efficient federated deep learning for intrusion detection in IoT networks," in *Proc. Workshop AI Cybersecur. (AI-Cybersec)*, in CEUR Workshop Proceedings, vol. 3125. Cambridge, U.K., Dec. 2021, pp. 85–99.

[53] I. Zakariyya, H. Kalutarage, and M. O. Al-Kadri, "Resource efficient federated deep learning for IoT security monitoring," in *Attacks and Defenses for the Internet-of-Things*, W. Li, S. Furnell, and W. Meng, Eds. Cham, Switzerland: Springer, 2022, pp. 122–142.

[54] Y. Chen, X. Sun, and Y. Jin, "Communication-efficient federated deep learning with layerwise asynchronous model update and temporally weighted aggregation," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 31, no. 10, pp. 4229–4238, Oct. 2020.

[55] F. Koushanfar, "Intellectual property (IP) protection for deep learning and federated learning models," in *Proc. ACM Workshop Inf. Hiding Multimedia Secur.*, Jun. 2022, p. 5.

[56] K. M. Ahmed, A. Imteaj, and M. H. Amini, "Federated deep learning for heterogeneous edge computing," in *Proc. 20th IEEE Int. Conf. Mach. Learn. Appl. (ICMLA)*, Dec. 2021, pp. 1146–1152.

[57] A. Elgabli, J. Park, S. Ahmed, and M. Bennis, "L-FGADMM: Layer-wise federated group ADMM for communication efficient decentralized deep learning," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, May 2020, pp. 1–6.

[58] Y. Tian, S. Wang, J. Xiong, R. Bi, Z. Zhou, and M. Z. A. Bhuiyan, "Robust and privacy-preserving decentralized deep federated learning training: Focusing on digital healthcare applications," *IEEE/ACM Trans. Comput. Biol. Bioinf.*, pp. 1–12, Mar. 2023, doi: 10.1109/TCBB.2023.3243932.

[59] Md. A. M. Pranto and N. Al Asad, "A comprehensive model to monitor mental health based on federated learning and deep learning," in *Proc. IEEE Int. Conf. Signal Process., Inf., Commun. Syst. (SPICSCON)*, Dec. 2021, pp. 18–21.

[60] Z. Fan, J. Su, K. Gao, D. Hu, and L.-L. Zeng, "A federated deep learning framework for 3D brain MRI images," in *Proc. Int. Joint Conf. Neural Netw. (IJCNN)*, Jul. 2021, pp. 1–6.

[61] K. V. Sarma, S. Harmon, T. Sanford, H. R. Roth, Z. Xu, J. Tetreault, D. Xu, M. G. Flores, A. G. Raman, R. Kulkarni, B. J. Wood, P. L. Choyke, A. M. Priester, L. S. Marks, S. S. Raman, D. Enzmann, B. Turkbey, W. Speier, and C. W. Arnold, "Federated learning improves site performance in multicenter deep learning without data sharing," *J. Amer. Med. Inform. Assoc.*, vol. 28, no. 6, pp. 1259–1264, Jun. 2021.

[62] N. Z. Abidin and A. Ritahani Ismail, "Federated deep learning for automated detection of diabetic retinopathy," in *Proc. IEEE 8th Int. Conf. Comput., Eng. Design (ICCED)*, Jul. 2022, pp. 1–5.

[63] Z. Abbas, M. Fiorino, S. M. Naqi, and M. Abbas, "COVID-19 prediction infrastructure using deep learning," in *Proc. 19th Int. Conf. Intell. Environ. (IE)*, 2023, pp. 125–134.

[64] R. Kumar, A. A. Khan, J. Kumar, Zakria, N. A. Golilarz, S. Zhang, Y. Ting, C. Zheng, and W. Wang, "Blockchain-federated-learning and deep learning models for COVID-19 detection using CT imaging," *IEEE Sensors J.*, vol. 21, no. 14, pp. 16301–16314, Jul. 2021.

[65] U. Shah, I. Dave, J. Malde, J. Mehta, and S. Kodeboyina, "Maintaining privacy in medical imaging with federated learning, deep learning, differential privacy, and encrypted computation," in *Proc. 6th Int. Conf. Converg. Technol. (I2CT)*, Apr. 2021, pp. 1–6.

[66] H. Elayan, M. Aloqaily, and M. Guizani, "Deep federated learning for IoT-based decentralized healthcare systems," in *Proc. Int. Wireless Commun. Mobile Comput. (IWCMC)*, Jun. 2021, pp. 105–109.

[67] K. Rand, N. L. Armengol, L. Mondrejevski, and I. Miliou, "Early prediction of the risk of ICU mortality with deep federated learning," 2022, *arXiv:2212.00554*.

[68] T. Ngo, D. C. Nguyen, P. N. Pathirana, L. A. Corben, M. B. Delatycki, M. Horne, D. J. Szmulewicz, and M. Roberts, "Federated deep learning for the diagnosis of cerebellar ataxia: Privacy preservation and auto-crafted feature extractor," *IEEE Trans. Neural Syst. Rehabil. Eng.*, vol. 30, pp. 803–811, 2022.

[69] K. Kaur, S. Verma, and A. Bansal, "IoT big data analytics in healthcare: Benefits and challenges," in *Proc. 6th Int. Conf. Signal Process., Comput. Control (ISPCC)*, Oct. 2021, pp. 176–181.

[70] J. Liu et al., "Deep federated learning based convergence analysis in relaying-aided MEC-IoT networks," *J. Eng.*, vol. 2022, pp. 1–6, Sep. 2022.

[71] D. Kwon, J. Jeon, S. Park, J. Kim, and S. Cho, "Multiagent DDPG-based deep learning for smart ocean federated learning IoT networks," *IEEE Internet Things J.*, vol. 7, no. 10, pp. 9895–9903, Oct. 2020.

[72] A. N. Jahromi, H. Karimipour, and A. Dehghantanha, "An ensemble deep federated learning cyber-threat hunting model for industrial Internet of Things," *Comput. Commun.*, vol. 198, pp. 108–116, Jan. 2023.

[73] S. Messaoud, S. Bouaafia, A. Bradai, M. A. Hajjaji, A. Mtibaa, and M. Atri, "Network slicing for industrial IoT and industrial wireless sensor network: Deep federated learning approach and its implementation challenges," in *Emerging Trends in Wireless Sensor Networks*. London, U.K.: IntechOpen, Oct. 2022, doi: 10.5772/intechopen.102472.

[74] D. Hamouda, M. A. Ferrag, N. Benhamida, and H. Seridi, "PPSS: A privacy-preserving secure framework using blockchain-enabled federated deep learning for industrial IoTs," *Pervas. Mobile Comput.*, vol. 88, Jan. 2023, Art. no. 101738.

[75] A. M. Anter and L. Abualigah, "Deep federated machine learning-based optimization methods for liver tumor diagnosis: A review," *Arch. Comput. Methods Eng.*, vol. 30, no. 5, pp. 3359–3378, Jun. 2023.

[76] B. Nour, S. Cherkaoui, and Z. Mlika, "Federated learning and proactive computation reuse at the edge of smart homes," *IEEE Trans. Netw. Sci. Eng.*, vol. 9, no. 5, pp. 3045–3056, Sep. 2022.

[77] V. Patel, S. Kanani, T. Pathak, P. Patel, M. I. Ali, and J. Breslin, "A demonstration of smart doorbell design using federated deep learning," 2020, *arXiv:2010.09687*.

[78] V. Patel, S. Kanani, T. Pathak, P. Patel, M. I. Ali, and J. Breslin, "An intelligent doorbell design using federated deep learning," in *Proc. 3rd ACM India Joint Int. Conf. Data Sci. Manage. Data, 8th ACM IKDD CODS 26th COMAD)*, Jan. 2021, pp. 380–384.

[79] Z. Zhang, C. Guan, H. Chen, X. Yang, W. Gong, and A. Yang, "Adaptive privacy-preserving federated learning for fault diagnosis in Internet of ships," *IEEE Internet Things J.*, vol. 9, no. 9, pp. 6844–6854, May 2022.

[80] W. Hammedi, B. Brik, and S. M. Senouci, "Federated deep learning-based framework to avoid collisions between inland ships," in *Proc. Int. Wireless Commun. Mobile Comput. (IWCMC)*, May 2022, pp. 967–972.

[81] W. Hammedi, B. Brik, and S. M. Senouci, "Toward optimal MEC-based collision avoidance system for cooperative inland vessels: A federated deep learning approach," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 2, pp. 2525–2537, Feb. 2023, doi: 10.1109/TITS.2022.3154158.

[82] I. Shiri, A. V. Sadr, A. Sanaat, S. Ferdowsi, H. Arabi, and H. Zaidi, "Federated learning-based deep learning model for PET attenuation and scatter correction: A multi-center study," in *Proc. IEEE Nucl. Sci. Symp. Med. Imag. Conf. (NSS/MIC)*, Oct. 2021, pp. 1–3.

[83] X. Liu, H. Li, G. Xu, R. Lu, and M. He, "Adaptive privacy-preserving federated learning," *Peer-Peer Netw. Appl.*, vol. 13, pp. 2356–2366, Nov. 2020.

[84] B. Xue, Y. He, F. Jing, Y. Ren, L. Jiao, and Y. Huang, "Robot target recognition using deep federated learning," *Int. J. Intell. Syst.*, vol. 36, no. 12, pp. 7754–7769, Dec. 2021.

[85] S. Salim, N. Moustafa, B. Turnbull, and I. Razzak, "Perturbation-enabled deep federated learning for preserving Internet of Things-based social networks," *ACM Trans. Multimedia Comput., Commun., Appl.*, vol. 18, no. 2s, pp. 1–19, Jun. 2022.

[86] N. Jayakody, A. Mohammad, and M. N. Halgamuge, "Fake news detection using a decentralized deep learning model and federated learning," in *Proc. 48th Annu. Conf. IEEE Ind. Electron. Soc. (IECON)*, Oct. 2022, pp. 1–6.

[87] D. O. Mensah, G. Badu-Marfo, R. Al Mallah, and B. Farooq, "EFedDNN: Ensemble based federated deep neural networks for trajectory mode inference," in *Proc. IEEE Int. Smart Cities Conf. (ISC)*, Sep. 2022, pp. 1–7.

[88] S. Messaoud, A. Bradai, O. B. Ahmed, P. T. A. Quang, M. Atri, and M. S. Hossain, "Deep federated Q-learning-based network slicing for industrial IoT," *IEEE Trans. Ind. Informat.*, vol. 17, no. 8, pp. 5572–5582, Aug. 2021.

[89] N. Bugshan, I. Khalil, M. S. Rahman, M. Atiquzzaman, X. Yi, and S. Badsha, "Toward trustworthy and privacy-preserving federated deep learning service framework for industrial Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 19, no. 2, pp. 1535–1547, Feb. 2023.

[90] A. Nguyen, T. Do, M. Tran, B. X. Nguyen, C. Duong, T. Phan, E. Tjiputra, and Q. D. Tran, "Deep federated learning for autonomous driving," in *Proc. IEEE Intell. Vehicles Symp. (IV)*, Jun. 2022, pp. 1824–1830.

[91] S. Wang, C. Li, D. W. K. Ng, Y. C. Eldar, H. V. Poor, Q. Hao, and C. Xu, "Federated deep learning meets autonomous vehicle perception: Design and verification," *IEEE Netw.*, vol. 37, no. 3, pp. 16–25, Dec. 2023.

[92] H. Moayyed, A. Moradzadeh, B. Mohammadi-Ivatloo, A. P. Aguiar, and R. Ghorbani, "A cyber-secure generalized supermodel for wind power forecasting based on deep federated learning and image processing," *Energy Convers. Manage.*, vol. 267, Sep. 2022, Art. no. 115852.

[93] Y. Li, R. Wang, Y. Li, M. Zhang, and C. Long, "Wind power forecasting considering data privacy protection: A federated deep reinforcement learning approach," *Appl. Energy*, vol. 329, Jan. 2023, Art. no. 120291.

[94] A. Ahmadi, M. Talaei, M. Sadipour, A. M. Amani, and M. Jalili, "Deep federated learning-based privacy-preserving wind power forecasting," *IEEE Access*, vol. 11, pp. 39521–39530, 2023.

[95] Y. Wang, W. Zhang, Q. Guo, and Y. Wu, "A privacy-preserving wind speed prediction method based on federated deep learning," in *Proc. 4th Int. Conf. Power Energy Technol. (ICPET)*, Jul. 2022, pp. 638–643.

[96] M. Duan, D. Liu, X. Chen, Y. Tan, J. Ren, L. Qiao, and L. Liang, "Astraea: self-balancing federated learning for improving classification accuracy of mobile deep learning applications," in *Proc. IEEE 37th Int. Conf. Comput. Design (ICCD)*, Nov. 2019, pp. 246–254.

[97] E. Fernandez, N. Yoshioka, H. Washizaki, and M. Syed, "Modeling and security in cloud ecosystems," *Future Internet*, vol. 8, no. 4, p. 13, Apr. 2016.
[98] Y. Chen, Y. Jiang, F.-C. Zheng, M. Bennis, and X. You, "Coded caching via federated deep reinforcement learning in fog radio access networks," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC Workshops)*, May 2022, pp. 403–408.
[99] K. Bonawitz, V. Ivanov, B. Kreuter, A. Marcedone, H. B. Mcmahan, S. Patel, D. Ramage, A. Segal, and K. Seth, "Practical secure aggregation for privacy-preserving machine learning," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Oct. 2017, pp. 1175–1191.
[100] R. N. Zaeem and K. S. Barber, "The effect of the GDPR on privacy policies: Recent progress and future promise," *ACM Trans. Manage. Inf. Syst.*, vol. 12, no. 1, pp. 1–20, Mar. 2021.
[101] S. Mbonihankuye, A. Nkunzimana, and A. Ndagijimana, "Healthcare data security technology: HIPAA compliance," *Wireless Commun. Mobile Comput.*, vol. 2019, pp. 1–7, Oct. 2019.
[102] Y. Chen, X. Qin, J. Wang, C. Yu, and W. Gao, "FedHealth: A federated transfer learning framework for wearable healthcare," *IEEE Intell. Syst.*, vol. 35, no. 4, pp. 83–93, Jul. 2020.
[103] A. Brauneck, L. Schmalhorst, M. M. K. Majdabadi, M. Bakhtiari, U. Völker, C. C. Saak, J. Baumbach, L. Baumbach, and G. Buchholtz, "Federated machine learning in data-protection-compliant research," *Nature Mach. Intell.*, vol. 5, no. 1, pp. 2–4, Jan. 2023.
[104] T. Liu, B. Di, B. Wang, and L. Song, "Loss-privacy tradeoff in federated edge learning," *IEEE J. Sel. Topics Signal Process.*, vol. 16, no. 3, pp. 546–558, Apr. 2022.
[105] R. Ma, Y. Li, C. Li, F. Wan, H. Hu, W. Xu, and J. Zeng, "Secure multiparty computation for privacy-preserving drug discovery," *Bioinformatics*, vol. 36, no. 9, pp. 2872–2880, May 2020.
[106] D. H. Utku, F. O. Catak, M. Kuzlu, S. Sarp, V. Jovanovic, U. Cali, and N. Zohrabi, "Digital twin applications for smart and connected cities," in *Digital Twin Driven Intelligent Systems and Emerging Metaverse*. Singapore: Springer, 2023, pp. 141–154.
[107] F. Yu, W. Zhang, Z. Qin, Z. Xu, D. Wang, C. Liu, Z. Tian, and X. Chen, "Heterogeneous federated learning," 2020, *arXiv:2008.06767*.
[108] Y. Liu, Y. Kang, C. Xing, T. Chen, and Q. Yang, "A secure federated transfer learning framework," *IEEE Intell. Syst.*, vol. 35, no. 4, pp. 70–82, Jul. 2020.
[109] F. Chen, M. Luo, Z. Dong, Z. Li, and X. He, "Federated meta-learning with fast convergence and efficient communication," 2018, *arXiv:1802.07876*.
[110] B. Wang, G. Li, C. Wu, W. Zhang, J. Zhou, and Y. Wei, "A framework for self-supervised federated domain adaptation," *EURASIP J. Wireless Commun. Netw.*, vol. 2022, no. 1, p. 37, Dec. 2022.
[111] W. Jeong, J. Yoon, E. Yang, and S. J. Hwang, "Federated semi-supervised learning with inter-client consistency & disjoint learning," 2020, *arXiv:2006.12097*.

ZAHRA ABBAS received the Bachelor of Science degree in computer science from Quaid-i-Azam University, Islamabad, where she is currently pursuing the Master of Science degree from the Institute of Information Technology. She has participating in the International Conference of Digital Transitions: Research and Development, Italy, in 2022, and the 19th International Conference on Intelligent Environments, Mauritius, in 2023. Her research interests include artificial intelligence, deep federated learning, and the IoT security.

SUNILA FATIMA AHMAD was born in Bhakkar, Pakistan. She received the Bachelor of Science degree from the University of Sargodha, Bhakkar Campus. She is currently pursuing the Master of Science degree with the Institute of Information Technology, Quaid-i-Azam University, Islamabad. Her research interests include deeply rooted in the fields of artificial intelligence (AI) and machine learning (ML), with a specialized focus on security and privacy in the Internet of Things (IoT) and the emerging area of deep federated learning.

MADIHA HAIDER SYED received the Ph.D. degree in computer science from Florida Atlantic University, USA, in 2019. She is currently an Assistant Professor with the Institute of Information Technology, Quaid-i-Azam University, Pakistan. Her research interests include cloud computing, security, privacy, software architecture, the IoT, machine learning, and deep learning. She was a recipient of the Prestigious Fulbright Scholarship, in 2014, for the Ph.D. degree.

ADEEL ANJUM received the Ph.D. degree in computer science from Polytech Nantes, Nantes, France, in 2013. He is currently an Associate Professor with the Institute of Information Technology, Quaid-i-Azam University, Islamabad. He has several publications and authored a book on data privacy. His research interest includes AI-based data privacy. He was on the technical program committees of various international conferences.

SEMEEN REHMAN (Member, IEEE) received the Habilitation degree in embedded systems from the Faculty of Electrical Engineering and Information Technology, Technische Universität Wien (TU Wien), in October 2020, and the Ph.D. degree from KIT, Germany. She is a University Dozentin and an Assistant Professor at TU Wien. She has coauthored one book, multiple book chapters, and more than 70 publications in premier journals and conferences. Her research interests include dependable and energy-efficient embedded systems, approximate computing, security, and CPS/the IoT. She received the CODES+ISSS 2011, the 2015 Best Paper Award, the DATE 2017 Best Paper Award Nomination, the HiPEAC Paper Award, the DAC Richard Newton Young Student Fellow Award, and the Research Student Award from KIT. She served as the topic track chair/co-chair and served as a technical program committee member, conference organizing committee member for multiple premier conferences on design automation and embedded systems.