Computers, Materials & Continua

Tech Science Press

DOI: 10.32604/cmc.2024.049846

REVIEW

Federated Learning on Internet of Things: Extensive and Systematic Review

Meenakshi Aggarwal[1], Vikas Khullar[1], Sunita Rani[2], Thomas André Prola[3,4,5], Shyama Barna Bhattacharjee[6], Sarowar Morshed Shawon[7] and Nitin Goyal[8,*]

[1]Chitkara University Institute of Engineering and Technology, Chitkara University, Rajpura, Punjab, 140401, India

[2]Department of CSE & IT, BPS Mahila Vishwavidyalaya, Khanpur Kalan, Sonipat, Haryana, 131305, India

[3]Engineering Research & Innovation Group, Universidad Europea del Atlántico, C/Isabel Torres 21, Santander, 39011, Spain

[4]Department of Project Management, Universidad Internacional Iberoamericana, Arecibo, PR, 00613, USA

[5]Department of Project Management, Universidade Internacional do Cuanza, Estrada Nacional 250, Bairro Kaluapanda, Cuito-Bié, Angola

[6]Department of Computer Science and Engineering, University of Science and Technology Chittagong (USTC), Chattogram, 4202, Bangladesh

[7]Deptartment of EEE, University of Science and Technology Chittagong (USTC), Chattogram, 4202, Bangladesh

[8]Department of Computer Science and Engineering, School of Engineering and Technology, Central University of Haryana, Mahendragarh, Haryana, 123031, India

*Corresponding Author: Nitin Goyal. Email: dr.nitin@cuh.ac.in

Received: 19 January 2024 Accepted: 03 April 2024 Published: 15 May 2024

ABSTRACT

The proliferation of IoT devices requires innovative approaches to gaining insights while preserving privacy and resources amid unprecedented data generation. However, FL development for IoT is still in its infancy and needs to be explored in various areas to understand the key challenges for deployment in real-world scenarios. The paper systematically reviewed the available literature using the PRISMA guiding principle. The study aims to provide a detailed overview of the increasing use of FL in IoT networks, including the architecture and challenges. A systematic review approach is used to collect, categorize and analyze FL-IoT-based articles. A search was performed in the IEEE, Elsevier, Arxiv, ACM, and WOS databases and 92 articles were finally examined. Inclusion measures were published in English and with the keywords "FL" and "IoT". The methodology begins with an overview of recent advances in FL and the IoT, followed by a discussion of how these two technologies can be integrated. To be more specific, we examine and evaluate the capabilities of FL by talking about communication protocols, frameworks and architecture. We then present a comprehensive analysis of the use of FL in a number of key IoT applications, including smart healthcare, smart transportation, smart cities, smart industry, smart finance, and smart agriculture. The key findings from this analysis of FL IoT services and applications are also presented. Finally, we performed a comparative analysis with FL IID (independent and identical data) and non-ID, traditional centralized deep learning (DL) approaches. We concluded that FL has better performance, especially in terms of privacy protection and resource utilization. FL is excellent for preserving privacy because model training takes place on individual devices or edge nodes, eliminating the need for centralized data aggregation, which poses significant privacy risks. To facilitate development in this rapidly evolving field, the insights presented are intended to help practitioners and researchers navigate the complex terrain of FL and IoT.

KEYWORDS
Internet of Things; federated learning; PRISMA; framework of FL; applications of FL; data privacy; communication

1 Introduction

The rapid proliferation of data has changed the landscape of data generation, necessitating advanced artificial intelligence (AI) techniques such as DL for insightful analytics. Traditional AI approaches use centralized cloud servers for learning and modeling data, but this model is reaching its limits, especially with the explosion of IoT data. The sheer volume of data, estimated at 850 zetabytes (ZB), and the expected increase in connected IoT devices (more than 75 billion) pose significant challenges for data management, availability and resilience [1]. The need for IoT applications where timeliness and quality are critical, such as in smart healthcare, smart transportation, and smart cities, underscores the need for a robust infrastructure with high availability and flexibility. However, efficiently managing data and delivering services with cloud infrastructure is becoming increasingly difficult in the face of massive, distributed, and heterogeneous IoT data [2].

AI is used to make decisions quickly and automatically in IoT systems, which rely on a wide variety of data sources, ranging from sensor telemetry to movies. Despite this, security and privacy are key problems in the adoption of the IoT because of the heterogeneity and resource restrictions of devices, which make it difficult to upgrade and patch programs. In addition, the majority of IoT systems have a centralized design, which places them at risk of security breaches because they are easy targets for malicious actors. Traditional techniques that include central servers for data processing have several obstacles, including communication overhead, privacy concerns, and vulnerability to specialized attacks. Despite their benefits, these approaches confront several challenges [3].

Recently, the concept of using FL has emerged as a possible option for the development of smart and privacy-friendly IoT systems. It has been suggested that FL could be used for a variety of applications within the IoT, including smart transportation and smart healthcare facilities. For example, the use of FL enables machine learning (ML) models to be run in smart healthcare without the need for medical institutions to share patient data directly with each other. Instead, institutions that store healthcare data, such as hospitals, can train AI models locally and then share only the learned parameters with the aggregator for global calculations. Implementing this collaborative strategy improves healthcare services across a variety of institutions, speeding up the process of patient diagnosis and treatment while maintaining user confidentiality. Similarly, FL has prove1n its effectiveness in providing intelligent vehicle services in transportation networks [4].

Although holding potential, the implementation of FL raises intriguing research inquiries related to efficiency, resilience, and security, particularly in real-world IoT deployments on a large scale. This review examines FL advancements within IoT contexts, focusing on FL communication protocol, and implementation framework with FL architecture [1]. The survey provides an overview of applications and ongoing challenges in coordinating intelligent decisions across decentralized IoT devices and users through FL's distributed model training approach.

1.1 Motivation and Contribution

The designs of several fundamental challenges, including privacy, security, communication costs, heterogeneity, architecture and, differ depending on the domain and the use cases considered. Although several studies have focused on FL and IoT and discussed these methods in depth in terms of FL-IoT architecture, data services and applications, there are still more studies that have been conducted. The aim of this study is to provide an overview of the current state of research and summarize the most advanced methods that have been developed recently to solve these difficulties. As part of our research, we examine articles in related fields and conduct a thorough review of the latest survey studies in these areas. We use several categories to categorize the topics covered in FL survey articles. These categories include communication costs, heterogeneity, privacy/security as a primary challenge, FL architectures, implementation frameworks, communication protocols, and FL applications in different domains. The main Contributions of the manuscript are as follows:

1) The main focus of this manuscript is to thoroughly investigate and analyze existing FL-IoT reviews.

2) The manuscript classifies FL research into broad categories of communication protocol, implementation framework, FL architectures, challenges, and application areas.

3) It will address the various challenges of IoT applications and explore how FL can address these challenges.

4) Finally, the advantages of FL over traditional ML models will be discussed and a comparative analysis between FL (IID and Non-IID) and centralized ML algorithms will be conducted.

The following research questions (RQs) were formulated to accomplish the aim and objective of the review.

RQ1: What is the relationship between FL and IoT?

RQ2: What is the implementation framework for FL-IoT?

RQ3: What are various application areas of FL-IoT?

RQ4: What are various Challenges and limitations of FL-IoT?

RQ5: What is the need of FL over ML?

Therefore, the notable contribution of this research is as follows:

1. Federated learning uses the network of IoT devices to train machine learning models locally, which enables collaborative learning while protecting privacy and avoiding data aggregation at a central location. Further relationship between FL-IoT discussed in Section 4.3.
2. Several libraries and framework such as Tensor flow federated, Pysft, FederatedAI, IBM FL in detail discussed in Section 5.2 have been utilized to implement the FL-IoT approach.
3. FL with IoT can be used in variety of application areas such as healthcare, smart city, smart agriculture, smart finance as discussed in the Section 6.
4. FL demands effective communication that addresses challenges like limited resources, data privacy, and hardware specifications on IoT devices. Discussed the challenges and limitations of FL-IoT in Section 7.
5. Many researchers have demonstrated the FL approach's effectiveness over traditional ML algorithms. Comparative analysis discussed in Section 8.1 was done between FL and ML approaches.

The paper's structure is structured as follows: In Section 3, we provide an overview of the fundamentals of FL with IoT. Section 4 delves into the discussion of the FL-IoT framework, protocols, and various architectures of FL. Popular applications of FL, particularly utilizing IoT network data in domains such as smart healthcare, smart cities, smart industry, agriculture, transportation, and finance, are detailed in Section 5. In Section 6, we address the challenges that arise due to the decentralized nature of FL.

2 Literature Survey

FL has attracted a lot of attention due to its advantages, such as increased data protection and lower communication costs. In the IoT domain, FL integration has been extensively explored to address privacy concerns by enabling decentralized model training and storing sensitive information locally. This approach fits well with the resource constraints of IoT devices and makes FL an attractive solution for efficient, privacy-friendly ML. Sirohi et al. [5] examines the vulnerabilities of FL in air, ground, space and underwater communications and provides an overview of the threats and the latest defence strategies. Furthermore, Chen et al. [6] explored the initial advances of FL for the Metaverse (FL4M) and examined key technologies such as big data, IoT, edge computing (EC), blockchain and augmented reality. While FL offers promising solutions, the challenges and promising directions outlined by the authors underscore the complexity in this evolving field. Rahman et al. [7] presents a comprehensive overview of the latest trends in FL, IoT and Information-Centric Networking (ICN), highlighting their characteristics, integration potential and sharing for robust security. It also examines application areas, outlines open questions and proposes future research directions for the integration of these technologies.

Qammar et al. [8] conducted a systematic literature review on the integration of blockchain in FL, addressing security and privacy concerns with traditional FL. It examines blockchain-based FL approaches with a focus on security, privacy, record-keeping, rewards, verification, and accountability, and discusses open questions while suggesting future research directions for robust development. However, Aledhari et al. [9] offer a systematic examination of associated protocols and platforms, delineating challenges, and illustrating real-world applications to offer a comprehensive understanding of FL technology. Meanwhile, Yang et al. [10] proposed a safe FL approach, covering horizontal FL, vertical FL, and federated transfer learning (FTL), aiming to enable information exchange between organizations through the utilization of FL techniques. In addition, Liu et al. [11] examine the strengths and limitations of conventional ML within the 6G context. Further authors of reference [12] explored the differences between FL and traditional Distributed ML, examining the unique characteristics and challenges of FL. The study encompassed various techniques and prospects, addressing four fundamental challenges, particularly those related to privacy and security, without restricting its scope to a specific field. Nguyen et al. [13] assess FL's potential in diverse IoT services, incorporating data sharing, offloading, attack detection, localization, crowd sensing, and data privacy. The survey broadly covers FL applications in IoT sectors, including healthcare, transportation, unmanned aerial vehicles (UAVs), cities, and industry, highlighting crucial insights and concluding with an overview of current challenges and future research directions in this burgeoning field. Further authors of reference [14] discuss the application of blockchain to FL for enhancing IoT data security, addressing current issues, and proposing emerging approaches. It includes a comprehensive survey on blockchain-based FL for IoT applications. Abreha et al. [15] systematically review the execution of FL in EC, providing insights into protocols, applications, challenges, and case studies, along with identifying open issues for future research. It aims to enhance understanding of the connection between FL and EC technologies. In comparative analysis, Kholod et al. [16] conducted a comparative analysis of open-source FL

frameworks. Evaluating features like ease of use, development, analysis capabilities, accuracy, and performance using signal and image datasets on low-power IoT devices, the study identifies FL frameworks suitable for current IoT applications with certain usage restrictions. Zeng et al. [17] proposed a lightweight truth-discovery-based multidimensional bidding framework to test industrial edge device parameters by using the Asynchronous Advantage Actor–Critic (A3C) algorithm. The authors conclude that the proposed approach provides an efficient offloading technique in terms of model accuracy and system revenue. Liu et al. [18] suggest an Internet of UAVs trajectory planning algorithm that uses local search approaches to emphasize safety and energy economy. It incorporates TinyML to make decisions in real time and modifies the placements of virtual nodes to handle any situation. Comprehensive simulation studies highlight the potential of the suggested algorithm for secure and effective data collecting from IoT networks by showcasing its effectiveness when compared to baseline methods.

The summary of existing surveys related to FL-IoT is discussed in Table 1 with their contributions. These diverse studies collectively contribute to the evolving landscape of FL, emphasizing its potential, challenges, and avenues for future research.

Table 1: Summary of existing survey papers related to FL-IoT

Reference	Year	Summary	Advantages	Limitations/ Suggestions
[19]	2021	Explores security and privacy aspects of FL, addressing current challenges and emphasizing the need for future research directions to facilitate its mass adoption.	Security and privacy aspects of FL were discussed with addressing challenges and future direction.	Case studies are not present and need more detailed insights into emerging threats.
[16]	2021	Comparative analysis of open-source FL frameworks for IoT systems, evaluating features and identifying applicable frameworks	They discussed all frameworks related to FL-IoT with various features.	The study focuses on all frameworks of FL-IoT except PySyft, which is limited to the OpenMined ecosystem.
[4]	2021	Provides a thorough survey of FL applications in IoT networks, covering diverse services and key sectors, and addresses current challenges while suggesting future research directions.	Explored FL-IoT services such as IoT data sharing, offloading, catching, privacy, security and attack detection, and localization in detail.	–
[20]	2023	Defines FL systems, categorizes them across six aspects, and provides insights into, case studies, and research opportunities.	The study discussed in detail two important design factors heterogeneity and autonomy of FL systems.	The discussion of challenges related to FL-IoT could be discussed.

(Continued)

Table 1 (continued)

Reference	Year	Summary	Advantages	Limitations/ Suggestions
[21]	2022	The work discusses and surveys existing Multi-Access EC (MEC) initiatives, comparing strategies, and assessing limitations and tools, to provide insights for researchers and developers to design and improve MEC systems.	All tools, strategies, and issues related to MEC implementation are discussed.	There is more discussion required to address the challenges posed by MEC implementations.
[22]	2022	The survey underscores the impact of EC on IoT, analyzes the necessity of investigating Edge-Computing-Driven IoT (ECDriven-IoT), categorizes recent advances, and concludes with lessons learned and proposed challenges.	This study helps review and summarize existing research work and promotes cross-collaboration in related areas.	Data privacy and communication cost aspects could be discussed.
[23]	2022	Discuss the data privacy and security in Internet of Underwater Things (IoUT) frameworks, with FL.	An overview of the IoUT technology with AI/ML applications in information sensing and data transmission is discussed.	The implementation framework for FL-IoUT could be provided.
[24]	2021	Discuss the recent advances in FL-IoT over IoT networks, and identifies open research challenges along with potential solutions.	Recently developed metrics for FL-IoT, including sparsification, robustness, quantization, scalability, security, and privacy, are discussed.	Encryption methods could be discussed.
[25]	2022	Privacy and security issues with FL are discussed.	Recognizing significant security threats like poisoning, backdoors, and GAN-based attacks, as well as significant privacy concerns in FL.	The paper focuses only on privacy and security issues.
[2]	2023	Explores the integration of FL with IoT to address the increasing threat of malware.	The manuscript explains FL is a good fit for IoT malware analysis and contrasts it with centralized learning techniques.	Case studies or empirical evaluations of FL integration with IoT malware analysis could be discussed.

(Continued)

Table 1 (continued)

Reference	Year	Summary	Advantages	Limitations/ Suggestions
[5]	2023	Extensively analyzes vulnerabilities in FL across diverse applications, reviews defensive strategies, and compares methodologies.	Discuss the most recent FL deployments in various applications in different domains and propose privacy and security measures.	There is a need to discuss the Challenges associated with securing robust aggregators.
[6]	2023	Explores the integration of FL4M), emphasizing its potential to address data privacy concerns and reduce computational requirements, while highlighting the challenges and future directions.	The key objectives, challenges, and possible directions of metaverse technology with FL are discussed.	Practical implementations demonstrating the application of FL in the metaverse could be discussed.
[14]	2023	Explores the potential of blockchain-based FL methods for enhancing security and privacy in IoT ecosystems.	This study examines blockchain-based FL methods for comprehensively preserving IoT systems.	Concrete solutions or practical implementations to address the challenges could be discussed
[26]	2023	Comprehensively explores FL applications in IoT, emphasizing challenges and solutions for distributed decision-making.	Federated optimization techniques, communication-efficient algorithms, and privacy-preserving mechanisms are the focus.	Need to discuss detailed examination of specific implementation case studies.
[27]	2022	Explores the integration of FL with the Industrial Internet of Things (IIoT), focusing on privacy preservation, resource management, and applications.	Summarize how to preserve data privacy and learn on-device within the FL-IIoT framework.	Requiring more empirical evidence to validate their effectiveness in real-world IIoT environments.

3 Research Methodology

3.1 Selected and Data Gathering Procedures

The literature search used the IEEE, ACM, arXiv, Elsevier, and Web of Science libraries. The general search terms used are: 'federated learning', 'federated learning Internet of Things', 'Internet of Things applications', or 'federated learning architecture'. Following the initial literature investigation, each article's title, keywords, and abstract were examined, and possibly relevant articles were obtained and tested for suitability using full-text articles. The PRISMA flow diagram provides a comprehensive overview of the research selection process. Fig. 1 depicts the entire procedure of searching and selecting literature. This procedure consisted of four stages: Identification, screening, eligibility, and inclusion. In the identification stage, 160 papers were gathered and 22 duplicate papers were removed.

Furthermore, papers were screened with titles and keywords and 44 papers were excluded after screening. 104 papers were selected for full-text eligibility criteria, and out of them 12 were excluded because of no relevance and did not focus on quantitative evaluation. Therefore, 92 papers were chosen for full-text access.

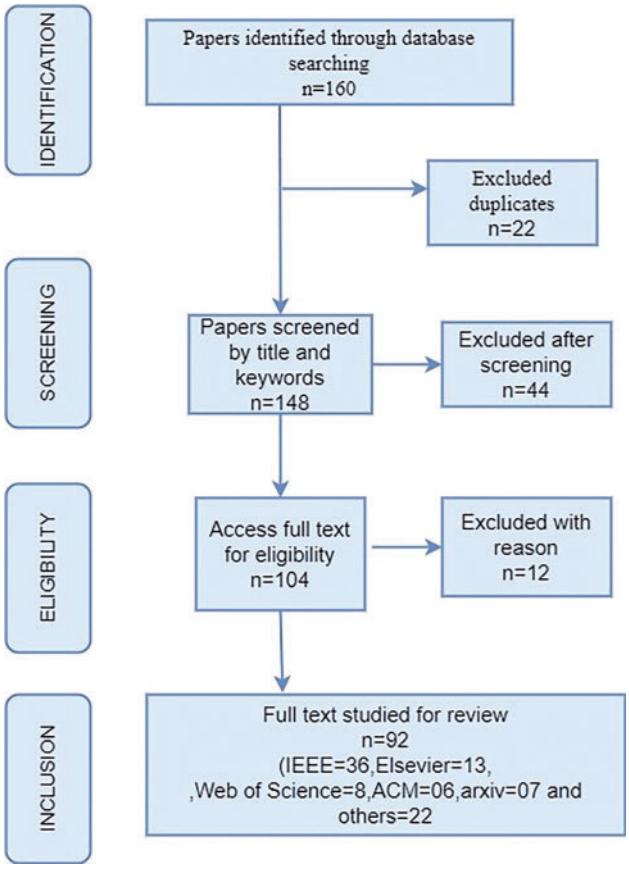

Figure 1: PRISMA flow diagram

3.2 Search Criteria

The authors utilized five databases to conduct their electronic search, including IEEE, Elsevier, Arxiv, ACM, and WoS. The search was restricted to the English language. The AND function was utilized as a logical operator. A targeted search supplemented the computerized search. This consisted of a Google Scholar online search and a manual examination of the cited references of relevant publications using the search approach.

3.3 Selection Execution

The search aimed to create a preliminary list of research that will be evaluated in more detail. The papers were then examined to determine whether they were appropriate and could be utilized to answer the research questions formulated, further we summarize some of the studies chosen based on the formulated research questions.

4 Vision of FL and IoT

The shared vision of FL and IoT is to enable decentralized collaborative ML across a variety of devices, promoting privacy, efficiency and smart IoT applications. This partnership aims to transform data analytics and decision making securely and at scale by creating a connected ecosystem where devices independently acquire knowledge about their local data and contribute to globally enhanced and adaptive intelligence while protecting user privacy.

4.1 Federated Learning

FL is an ML approach introduced by Google scientists that makes it possible to train models on decentralized devices with raw data without exchanging it. In an FL system, the model is trained jointly on the local data of each device, and only the model updates are shared with an aggregation server or between devices [28,29]. This privacy-friendly technique enables the development of ML models for distributed datasets while mitigating the privacy concerns associated with sharing sensitive information. It is particularly beneficial in scenarios where data is sensitive, located in different locations or cannot be centralized due to limitations such as network bandwidth. This approach is consistent with the principles of data privacy and security and is therefore suitable for applications in healthcare, finance and other areas where the protection of sensitive data is of paramount importance [30].

FL functions by conducting model training directly on individual devices, enabling the learning process to occur at the data sources themselves for both training and prediction [19]. Following the training phase, the models or model updates are transmitted back to a central server for aggregation. Later, the consolidated model is sent back to the devices utilizing principles derived from distributed computing, allowing efficient tracking and redistribution of models across diverse devices [31]. The process starts with the training of the local model on your client side. After training the model, each client sends its local model to the aggregation server, leaving the raw data on the client side. The aggregation server receives all local models from each client and starts training. After training the global model, the aggregation server sends this global model to all clients. This collaborative method maximizes training quality while minimizing the potential for data breaches. The local sneakers then retrieve the global update from the aggregator and continue this iterative process of computing subsequent local updates until the global training is complete [32].

4.2 Internet of Things

Internet-based applications are in high demand today. Therefore, the IoT is the most important technology for the development of Internet-based applications. An IoT is a network in which different physical devices are connected to the Internet via different routers or network devices and exchange data. It is an intelligent technology that reduces human effort and makes physical devices easily accessible [33]. It enables remote control of devices and also has an autonomous control function that can be used to control any device without human interaction. It enables communication from person to person, person to thing and thing to thing. The IoT can be a thing in a world where everything can be connected and communicate with each other. There are numerous technologies such as big data, data analytics, AI, ML, wireless sensor networks (WSNs) and various sensor technologies, etc. In WSNs, multiple sensor nodes are deployed in different areas to monitor and control the relevant environmental conditions and collect the data [34,35]. IoT became popular after the invention of Radio Frequency Identification (RFID) chips.

The diverse types of communication in IoT systems are mentioned as follows [35]:

i) ***People to People (P2P)*:** Communication/data transmission occurs between people to people through video calls, social calls, or social communication. It is also called "collaborative communication."
ii) ***Machine to People (M2P):*** Communication/data transmission occurs between machines like sensors, computers, and processors and people/users to analyze the data. For example, in agriculture, the smart greenhouse system uses smart devices to collect data and send it to control centers so it can be analyzed.
iii) ***Machine to Machine (M2M):*** Communication/data transmission is done between machine to machine without human intervention, e.g., Vehicle to Vehicle (V2V) communication, in which vehicles communicate with other vehicles or any smart device.

IoT has a different vision to benefit various areas, such as the environment, industry, medicine, transportation, etc. Many researchers have explained the IoT in different ways in specific aspects and areas of interest [36]. The working model of IoT is structured in Fig. 2.

An IoT system consists of smart devices with embedded capabilities. These devices gather data through sensors and transmit it to an IoT gateway. The data is then either sent to the cloud/server for analysis or analyzed locally. These devices typically operate autonomously, with minimal human intervention. Users interact directly with the devices, configuring them, providing instructions, or accessing the data independently. IoT technologies have enhanced agricultural capabilities [37]. It can support farmers at any phase of their farming operations by offering the latest crop and weather data, enabling remote monitoring of their farms. Additionally, early detection of agricultural issues is possible, preventing the spread of diseases and safeguarding production. Agricultural IoT applications play a crucial role in boosting agricultural output and minimizing crop losses due to diseases [24].

Figure 2: Working model of IoT

4.3 Federated Learning with IoT

The FL concept within IoT networks consists of two primary components: Firstly, the data clients, which are exemplified by IoT nodes, and secondly, an aggregation server as shown in Fig. 3. In this framework, IoT devices act as data clients, contributing their local data for model training. Meanwhile, an aggregation server strategically plays a crucial role in consolidating and processing the decentralized insights gathered from the various IoT devices.

This collaborative learning paradigm allows IoT devices to enhance their models collectively without the necessity of transmitting raw data to a centralized server. The aggregation server facilitates the synchronization of model updates, thereby promoting a more privacy-preserving and efficient approach to ML in the context of IoT networks. By decentralizing the learning process, FL concerns related to data privacy, network bandwidth, and latency while fostering continual improvement of models in a distributed and cooperative manner [38].

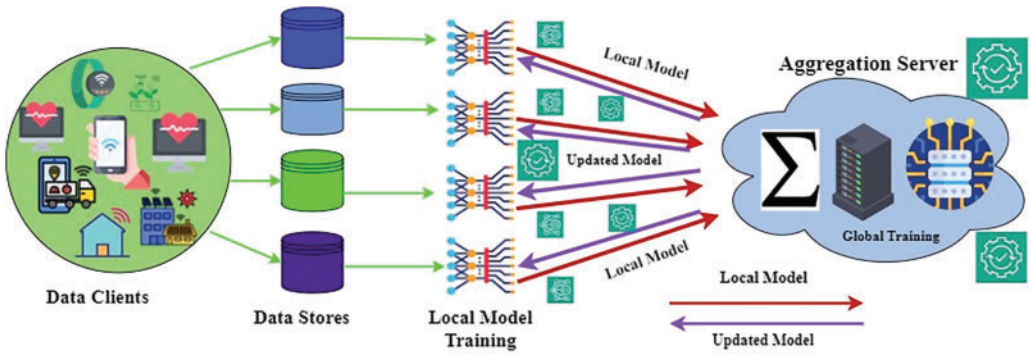

Figure 3: Working of FL-IoT

The FL-IoT process typically encompasses three main steps [28]:

***1. Initialization of global model*:** The central server outlines the training task, including defining the intended application, generating an initial global model, setting hyperparameters, and determining the objective function $j\ (\theta,\ Dn)$ for each client n. The initialized global model is disseminated to local participants involved in the training.

The mathematical expression of the objective function is given by:

$$j\left(\theta, Dn\right) = \Sigma nL(f\ (\theta, x)\ , y) \tag{1}$$

θ represents global model parameters, and Dn denotes the local dataset for the client. $F\ (\theta,\ x)$ predicts the output of the model for input x using θ, and y represents the true label. L denotes the loss function.

2. Local training of model: Each client participating in the FL network has its unique dataset. In every training round, a subset of clients or devices, denoted as Cn, is chosen, where n takes values from 1 to K, and K represents the number of selected clients. Each selected client Cn performs local model training using its local dataset Dn, optimizing local parameters θn to minimize the objective function $J\ (\theta n,\ Dn)$.

$$\theta n\left(m1 + 1\right) = \theta n\left(m1\right) - \eta.\nabla j(\theta n\left(m1\right), Dn) \tag{2}$$

η is the learning rate, $m_{l,}$ is for the iteration, and ∇J signifies the gradient function.

3. Local model aggregation: After the local model has been trained, the subsequent step is to collect updates from selected clients and then combine them to create an updated global model. The following are some of the aggregation methods that are utilized: Weighted averaging, simple averaging, and several others:

$$\theta\_g(m1 + 1) = N/1\Sigma\theta n(m1 + 1) \tag{3}$$

θ_g signifies the updated global model parameters post-aggregation.

This method has substantial potential by achieving impressive learning accuracy, putting an emphasis on the preservation of privacy, and decreasing communication overhead, as proven in a comparative evaluation *vs*. traditional methodologies.

5 FL-IoT: Protocol, Framework, and Architecture

In this section, we will explore the FL protocol, framework, diverse architectures of FL, and the mechanism through which parameters are exchanged between clients and the FL coordinator.

5.1 Communication Protocol in FL-IoT

The communication protocol oversees the complete training process of FL, dealing with issues like security, unreliable device connections, and availability [39]. In the FL system, a cloud-based distributed service serves as the FL server, while end devices, such as phones, participate in FL operations. The protocol involves devices signaling readiness for FL operations, initiated by the server for specific FL populations identified by a global name. During each round, a subset of devices is selected to process a specific FL task, and devices remain connected to the server throughout the round. The server sends an FL checkpoint with global model parameters to participants, collects checkpoints from participants, and updates the global state for subsequent rounds. This iterative process ensures collaborative learning across distributed devices in the FL system. The FL communication protocol is structured into three phases during each training round:

i. ***Selection:*** Devices that fulfill certain suitability criteria regularly establish communication with the server via bidirectional streams. The server monitors the availability of clients by checking the vitality of these streams to ensure effective communication scheduling. In addition, an FL parameter server uses a client selection algorithm, such as FedCS [40], to choose active clients for training round participation. These selected clients then carry out a specified FL task.
ii. ***Configuration:*** The server configuration adapts depending on the update method selected, whether it is a simple or secure method. Each selected device receives an FL plan, an FL checkpoint and the updated model. The server is set up by the selected aggregation mechanism, be it simple or secure aggregation [41]. Subsequently, the server transmits the updated model to each client.
iii. ***Reporting:*** The FL server patiently awaits updates from participating clients. Upon receiving updates, the server employs predefined algorithms like FedAvg to aggregate them [42]. If important clients remain connected, the federated training orchestrated by the server is completed, resulting in an update of the server's global model. If this condition is not met, the round is cancelled. The model updates are consistently sent to the server via encrypted communication to ensure security.

In addition to the efficiency of communication, ensuring the security of communication during the transmission of local updates is another challenge that needs to be considered.

iv. ***Secure aggregation:*** It refers to the use of cryptographic methods such as encryption, homomorphic encryption, secure multiparty computation (SMPC) and threshold cryptography. These methods are used to ensure the confidentiality of model updates transmitted from the participating devices to the central server. Encryption and homomorphic encryption are used to make individual updates unreadable during transmission so that the central server can summarize them without accessing the raw data [38].
v. ***Differential privacy:*** Collaborative model training is a method that protects individual privacy and attempts to preserve the sensitive information associated with each participant, specifically by ensuring that the statistical impact of each participant's data is indistinguishable from the influence of the other participants by introducing controlled noise or randomness into the aggregate model [38,39].

5.2 Implementation Framework in FL-IoT

To make the implementation of FLs easier, several frameworks and libraries have been developed. The building of FL models may be simplified with the help of these libraries, which include tools, application programming interfaces (APIs), and pre-built functionality.

Tensor Flow Federated (TFF): TFF is an open source framework for ML designed to perform computations on data distributed across multiple locations. It serves as the foundation for TensorFlow-based FL. Google is responsible for developing this framework for Python 3 for FL. In the real world, this paradigm has been put into practice for the first time. By using TFF, researchers can test new algorithms on their models and data. The interfaces of TFF consist of two basic levels. These layers are the FL API and the Federated Core API. When using TensorFlow, the FL application programming interface is an interface that simplifies the execution of actions associated with FL, model training and model evaluation. The three components that make up the interfaces provided by this layer are: Datasets, Federated Computing Builders and Models [43].

PySyft: PySyft makes it easy to identify and isolate private data from training models by using FL principles protected by a variety of privacy-enhancing methods. The only mode of operation PySyft is capable of is simulation mode. It must be combined with PyGrid and other projects of the OpenMined ecosystem to enable federated mode. Nevertheless, several projects, such as PySyft, are currently still under active development. The goal of PySyft is to make privacy-friendly ML techniques widely usable by providing Python connections and an interface reminiscent of traditional techniques. This enables the development and integration of new methods. One of PySyft's main goals is to provide the highest possible level of protection to customers participating in the training. PySyft can provide robust privacy guarantees to data consumers by developing and deploying automated differential privacy protection. These guarantees are independent of the ML architecture used and the data itself. In this particular scenario, PySyft is primarily concerned with encryption and improving privacy security for clients through the use of homophobic encryption or encrypted computation. TensorFlow and Pytorch are the two types of libraries supported by PySyft [44].

Flower (FL over the World Wide Web): The impressive open source architecture called Flower, an acronym for "FL over the World Wide Web", was developed to simplify FL operations across remote devices. The development of Flower was part of a research study conducted at Oxford University. Extending or rewriting a large number of components enables the creation of new, contemporary systems that can be stored for later use. Flower takes advantage of ML frameworks, even though the different frameworks for ML each have their own competencies. PyTorch, TensorFlow, Sci-kit-learn, TFLite and raw NumPy are some examples of well-known frameworks for ML. Flower not only has a large user base, but also a large community. With this in mind, this framework includes. This framework is characterised by its excellent documentation and tutorials that make implementation quick and easy [45].

IBM FL: Solutions for customer privacy protection, regulatory compliance in data integration and big data are the main focus of IBM's FL, which is deployed in various locations. There is a wide range of deployment scenarios that can be configured with IBM FL. It is common for data centers and cloud instances from different vendors to participate in FL. IBM's contributions to FL demonstrate IBM's commitment to advancing innovative technologies with a strong focus on data protection. IBM's FL integrates seamlessly with multiple ML libraries such as Keras, TensorFlow, PyTorch, SK Learn and RLLib, ensuring compatibility with its architecture. Providing APIs to create new FL algorithms increases its versatility and enables customization to different ML libraries and paradigms. In addition, fairness strategies within FL are emphasized to mitigate biases and reinforce

the commitment to ethical and inclusive ML practices. Please note that the paraphrased content combines information from the indicated paragraphs for coherence and clarity [46]. Table 2 shows the comparison of supported features of some existing frameworks. The cell is left empty if the system does not support the corresponding feature.

Table 2: Comparison between existing FL frameworks

Features		TFF	FLOWER	Pysft	FATE	IBM FL
Operating system	Linux	√	√	√	√	√
	Windows	√				√
	iOS			√		
	Mac	√	√	√	√	√
	Android			√		
Data partitioning	Horizontal	√		√	√	√
	Vertical	√		√	√	√
Communication	Simulated	√	√	√		
	Distributed	√	√	√	√	√
Hardware	CPUs	√	√	√	√	√
	GPUs	√	√	√	√	√

Federated AI(Federated AI Technology Enabler): It is an open source initiative with the aim of creating a safe and collaborative AI system. FATE-Flow is the name of the platform that hosts the FL pipeline. Inference processing, modeling, training, review and publishing are all applications of this technology. FATEBoard is a platform that allows users to view, explore and better understand specific ML models. It offers a variety of visualization options and displays the results in the form of tables or charts in different formats. The FATE network not only facilitates communication between devices, but also offers developers and scientists the opportunity to construct algorithms by using the Federation's APIs with the help of various tools. The FATE framework is integrated into the KubeFATE element, which is the final component. By using cloud-based technologies such as Docker and Kubernetes, this aspect is used to deploy FATE. FATE not only offers comprehensive documentation, but is also easy to implement in practice [47].

In the next section we discussed the performance parameters utilized to evaluate FL-IoT framework along with implementation steps of FL and various vulnerabilities that were examined during FL-IoT implementation process.

5.2.1 Performance Metrics

When assessing the efficacy, efficiency, and resilience of FL implementations customized for IoT contexts, performance measures in FL for the youth are essential. Table 3 discusses the various performance metrics with various parameters.

Table 3: Performance metrics with definition

Metrics	Evaluation parameters	Definition
Accuracy	Accuracy, Precision, Recall, F1-score, AuC (area under curve)	Evaluates the FL model accuracy with different data samples received for IoT devices.
Resource utilization	CPU and GPU utilization, Virtual memory, GPU memory	Evaluates how much power and computing resources are used on IoT devices while training models.
Privacy preservation	Information leakage, privacy loss	Evaluate how well privacy-preserving methods work in FL-IoT implementations.
Convergence speed	Convergence time and rate, number of iterations	Determines how quickly the FL model converges to an acceptable performance level.
Fairness and bias	Disparate impact and demographic parity, Equal opportunity, Disparate impact	Assesses how biased and equitable the FL model is in diverse IoT contexts.
Robustness	Evasion and inference attacks, model poisoning	Assesses how resistant FL models are two efforts at information poisoning and hostile assaults.
Communication cost	Network traffic, latency, and message size	Measures how much information is sent between edge nodes/IoT devices and the central server.

5.2.2 FL-IoT Implementation Process [7,48]

- Identify a specific problem or use case in the context of FL-IoT.
- Modify the customer application, if necessary, by integrating FL libraries, updating data collection mechanisms or implementing privacy-preserving approaches.
- To test and validate the proposed solution before deployment, FL prototypes are simulated using samples.
- Training of federated models on globally distributed IoT devices. Federated averaging, differential privacy or secure aggregation are used to train the model
- Evaluate the performance of the federated model using validation metrics such as accuracy, loss and convergence rate
- Deploy the trained, updated FL model to cloud servers and IoT devices.

At the same time, to implement FL, the following challenges must be solved:

- Develop techniques to deal with non-IID data distributions commonly encountered in IoT environments.
- Develop FL algorithms that can adapt to devices with different computational and memory capacities as well as different levels of scaling and stability.
- Support for different communication methods, including centralized and decentralized approaches, depending on network topology and device capabilities.
- Include security mechanisms such as encryption, authentication and access control to protect the transmitted data and analysis results from different types of attacks.
- Develop algorithms for aggregating results coming from distributed IoT devices to calculate global metrics or insights. Implement secure aggregation procedures to prevent the loss of information during the aggregation of results.

5.2.3 Vulnerabilities in FL-IoT

FL is a concept that has emerged as collaborative learning by utilizing data from various organizations to train ML and DL models without disclosing their private data. It is important to analyze the FL environment thoroughly before applying it extensively to uncover any potential shortcomings and vulnerabilities in the system. Table 4 discuss the major vulnerabilities in context of implementation of FL with IoT devices [5,49,50].

Table 4: Major vulnerabilities in FL-IoT environment

Vulnerabilities	Definition	Description
Limited model capacity	There is a lack of model complexity for certain tasks	Resource-constrained IoT devices often require lightweight model architectures that FL can deploy.
Communication overhead	Increased the network traffic and latency	Large-scale FL deployments with numerous devices can experience increased network traffic, latency, and energy consumption due to communication overhead.
Heterogeneous data distribution	Devices have data distribution that is not consistent	Heterogeneous data distributions are common in IoT devices due to differences in device types, deployment environments or user behavior. Non-identically distributed (non-IID) data across devices can be caused by heterogeneous data distributions, making it difficult to assume identical data distribution in traditional FL settings.

(Continued)

Table 4 (continued)

Vulnerabilities	Definition	Description
Privacy and security concerns	Data privacy and security are at risk during the FL process	The exchange of model updates and aggregated information across IoT devices is part of FL, leading to concerns about data privacy and security. Privacy and security risks can arise when sensitive data is potentially exposed during model training or inference, vulnerable to adversarial attacks, and unauthorized access to transmitted information.
FL overhead	More computational and algorithmic complexity	FL and algorithmic complexity than centralized learning implementation in IoT environments entails more computational approaches.
Model convergence challenges	Convergence across devices is a challenge	FL is able to achieve convergence towards a global optimal solution by relying on collaborative model training across distributed devices. FL-IoT deployments can be an obstacle to convergence due to factors such as device heterogeneity, communication delays and byzantine behavior.

5.3 Architecture of FL-IoT

Some papers, such as [4,9,15,51] explain FL architectures.

5.3.1 Horizontal FL (HFL)

With HFL, the data is distributed horizontally among the clients, with each client having access to a subset of the data that contains the same characteristics, as shown in Fig. 4. This solution is suitable for situations where clients are concerned about their privacy and want to work together on an ML challenge without exposing their entire datasets [39]. HFL includes collaborative global model training without exchanging raw data. Instead, only model updates reflecting local data insights are exchanged and aggregated. It is used in scenarios such as mobile devices and healthcare, where it ensures collaborative model training while maintaining data privacy. In the IoT context, HFL is exemplary for tasks such as recognizing wake words as they occur in voice assistants in smart

homes [52]. Users speaking a consistent sentence with different voice characteristics on smartphones contribute to local updates, which are then averaged by a parameter server to formulate a global speech recognition model. This ensures collaborative learning while maintaining privacy in IoT applications.

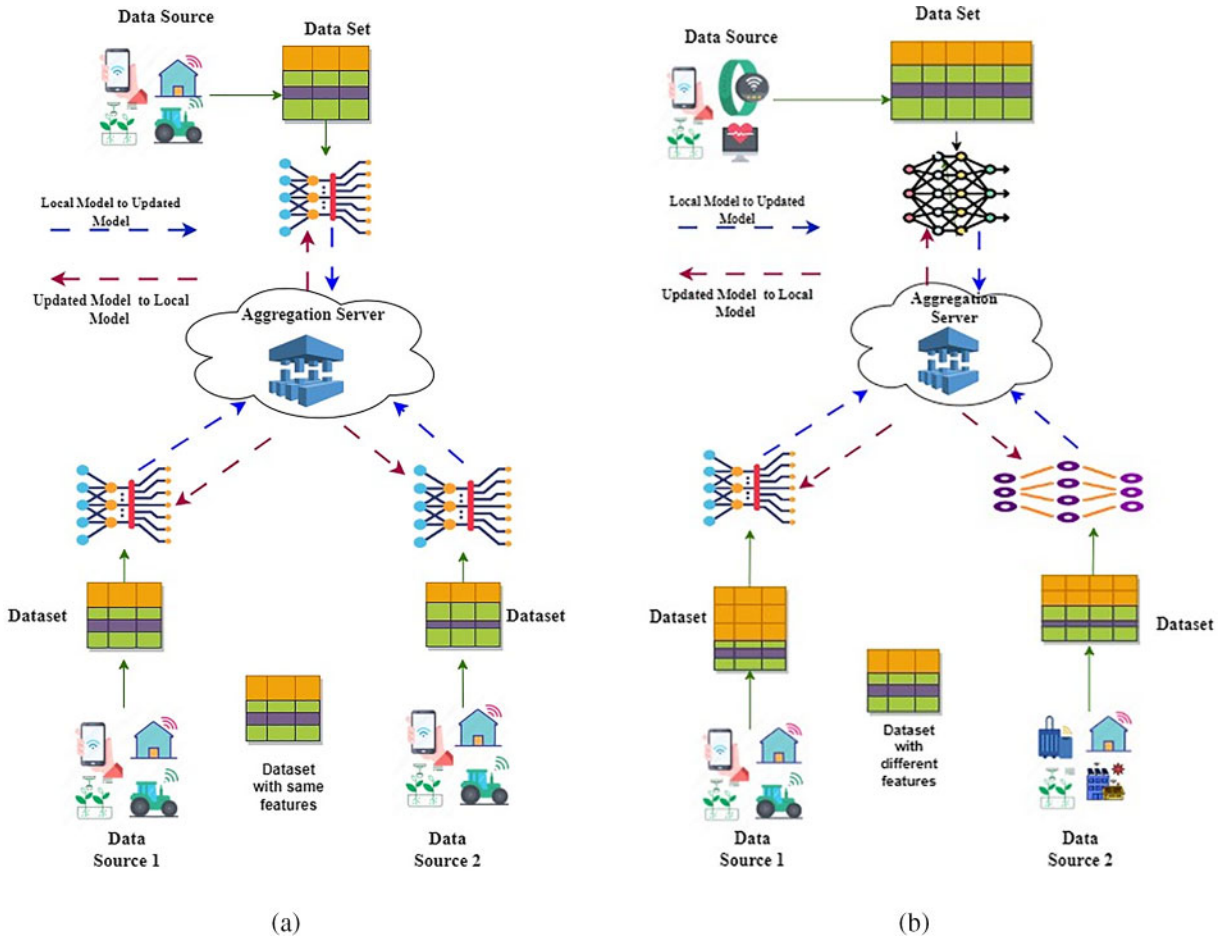

Figure 4: (a) Horizontal FL. (b) Vertical FL

5.3.2 Vertical FL (VFL)

It is a variant of FL in which the participating nodes have different data types and focus on different features of the same instances, as shown in Fig. 4. In VFL, each device has examples from its own feature space, and the common goal is to train a global model that captures the insights from all these different feature spaces. This approach is advantageous when comprehensive model training requires data that is distributed across different units, each of which contributes certain aspects of the overall dataset [30]. It is particularly useful in scenarios where different entities contribute data with different features, necessitating collaborative efforts for comprehensive model training. VFL effectively addresses privacy concerns and enables collaborative learning across different data sets. In an IoT use case, companies within a smart city, such as e-commerce companies and a banking institution, jointly participate in a learning model [53].

5.3.3 Federated Transfer Learning (FTL)

Transfer Learning and FL are combined in one model. When clients work together, they share an already trained model and then match it with the data they have in the field. The features from multiple feature spaces are transferred into a single representation, which is then used for the training data collected from multiple clients. This is done to protect the confidentiality of the data and ensure the security of the learning process [54]. This strategy is advantageous when clients have data sets that are related but distinct and can leverage an existing pre-trained model. There are various applications for FTL in IoT networks, including federated healthcare. It can be used to assist in the diagnosis of diseases by working with numerous hospitals in different locations. These hospitals have a variety of patients who require a variety of pharmaceutical tests. In this way, FTL can improve the performance of the shared AI model, increasing the accuracy of diagnosis.

5.3.4 Centralized FL-CFL

The centralized FL method incorporates the fundamentals of both the centralized and FL methods in a transparent manner. To run an FL model, the CFL system consists of a centralized server and a collection of clients. All clients participate simultaneously in the creation of a network model during a single training round. Afterwards, all clients send the trained parameters to the aggregation server, which then aggregates them and applies weighted average methods. Afterwards, the calculated updated model is sent to all clients to prepare for the next training session. After the training process, each client completes the process with a global model that is identical to their personalized model [55]. It is generally agreed that the server is the most important part of the network in CFL, as it is responsible for organizing the arbitration and sending the model updates to the client to complete an FL job while ensuring the confidentiality and security of the training data [56]. The safety and confidentiality of the training data that is stored on individual customers is given the highest priority in this tedious procedure.

5.3.5 Decentralized FL-DFL

With DFL, there is no need for a central server. The clients establish direct connections with each other in order to train the models, which ultimately leads to an improvement in data protection and scalability. The training process is distributed across different devices within a decentralized network, deviating from traditional technology that focuses on a central server. This new paradigm is a departure from the usual approach. It is a network architecture that, unlike CFL, does not include an aggregation server responsible for coordinating the training process [55]. Peer-to-peer allows DFL clients to connect via blockchain ledgers, which enables the offloading of model changes to the blockchain to ensure the secure exchange and aggregation of models [57]. The applications of DFL are quite diverse, including a wide range of fields such as EC, networks for the IoT, and industries that require increased privacy precautions, such as the healthcare industry [13].

5.4 Optimization and Convergence Techniques in FL-IoT

FL-IoT networks need optimization and convergence techniques to train models while addressing the challenges posed by decentralized, heterogeneous, and resource-constrained IoT devices [58,59]. Some key techniques are discussed as follows:

FL-IoT optimization algorithms: Various optimization algorithms such as Federated Averaging (FedAvg), Federated stochastic gradient descent (FedSGD) and FL with Adaptive Gradient Clipping

(FLAG) are popular, which deal with decentralization and non-IID data distributions while incorporating FL with IoT devices. The local model updates from all IoT devices are collected by FedAvg and sent to the aggregation server. FedSGD is used to improve the convergence speed and efficiency of communication.

Model compression: IoT devices have limited computational resources and bandwidth. Model quantization and compression techniques such as knowledge distillation, weight pruning, and quantization are used. These approaches reduce the model size and minimize the communication cost during updates.

Data privacy-preserving techniques: Data privacy of individual clients is the main aim of FL. Secure aggregation, differential privacy, and homomorphic encryption approaches are used to ensure data privacy on the client side.

Learning rate: The AdaGrad, RMSpoprop, and Adam tools serve to offset the effects of non-stationary data distributions and accelerate convergence by dynamically adjusting the learning rate.

6 Application Areas of FL-IoT

FL is applicable in a variety of circumstances that occur in the real world. In the next section, we will discuss some applications of different scenarios where FL could be used in the future, as shown in Fig. 5. The use of FL is particularly beneficial in situations where data confidentiality and security are major concerns. Early adopters recognized the enormous potential of FL and initiated several research projects and efforts to use FL in practice. This was despite the limitations and significant challenges that FL brought with it, especially in the area of security.

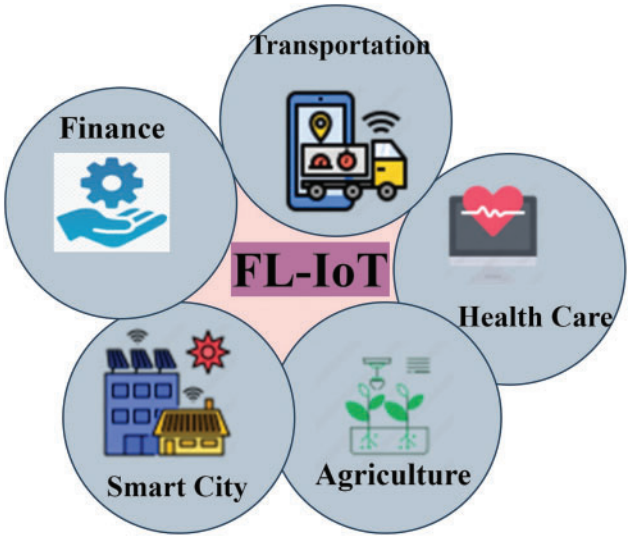

Figure 5: Application of FL-IoT

6.1 FL-IoT for Smart Healthcare

AI-based technologies are already widely used in the field of intelligent healthcare. One example of this is the use of intelligent imaging to identify diseases. When it comes to classic AI models, one of the most important issues is the question of data privacy, which arises from the transfer of

data to the cloud for computer training. This is because, compared to other areas, the data stored in healthcare systems is extremely sensitive and subject to health regulations such as the United States Health Insurance Portability and Accountability Act (HIPPA) [60]. Traditional methods of AI are not sufficient to meet the privacy requirements of modern healthcare, emphasizing the need for IoT to protect privacy in healthcare ecosystems. FL operates in a decentralized manner, unlike traditional AI systems that depend on a central server for data analysis and involve the sharing of data. The use of this decentralized technology eliminates the need for data sharing, providing a solution that prioritizes privacy for healthcare applications [61].

6.1.1 Remote Patient Monitoring

FL-IoT facilitates the development of personalized predictive health models by involving local devices in the analysis of patient data, ensuring confidentiality and prioritizing data privacy. Collaborative use of diverse health data helps refine disease monitoring models for early intervention and improves the overall efficiency of healthcare solutions.

The referenced research paper presents collaborative health frameworks that utilize FL in medical IoT devices and show reduced communication overhead and marginal accuracy loss in arrhythmia detection compared to FedAvg. Differential private learning in FL for electronic health records is investigated, achieving performance comparable to centralized approaches [62]. The FedHealth framework for transfer learning aggregates data from various wearable IoT devices and improves AI models for medical applications while preserving privacy through homomorphic encryption. Cluster-specific ML models tailored to hospital communities improve efficiency in predicting mortality and length of hospital stay from electronic health records [63]. By using smartphones, FL solves the "cold start" problem in collaborative mobile healthcare. The integration of blockchain with FL of healthcare systems improves network connectivity, accelerates training and ensures reliable authentication through fine-grained data access policies, as has been investigated in various studies [64,65]. This decentralized P2P approach among data centers mitigates the risk of data leakage and communication delays.

6.1.2 Disease Surveillance

Disease monitoring in FL-IoT is about bringing together insights from decentralized devices to develop predictive models for disease detection, monitoring and intervention. This approach ensures privacy and security by training models locally without centralizing sensitive health data. FL-IoT improves accuracy with real-time IoT data, contributing to effective public health management and personalized healthcare. In reference [66], FL predicts heart disease hospitalizations, using a distributed approach in medical cyber systems. Some authors proposed an FL-based approach for predicting brain tumors without sharing patient data [67–69].

6.2 FL-IoT for Smart Cities

The integration of smart devices and advanced infrastructures as well as integrated monitoring systems together with communication frameworks form a smart city. The goal of these ecosystems is to improve the quality of life of residents by facilitating the seamless supply of food, water and energy to end users. FL-IoT is a revolutionary technology that is revolutionizing smart cities, especially in the area of urban transportation. Table 5 shows the various performance metrics related to FL-IoT.

Table 5: Details of performance measures used in FL-IoT applications

Reference	Base model with FL	Data distribution type	Performance measures	IoT application domain
[68]	CNN	Distributed	Acc = 96, Precision = 97, recall = 97 and F1-Score = 97	Health
[69]	CNN	Distributed	Acc = 91.05, AUC = 0.908, Sensitivity = 0.910, Specificity = 0.909	Health
[72]	YOLOv3	Distributed	Recall = 60 and acc = 85	Smart city
[57]	CNN	Distributed	Acc-97–98	Social media
[88]	ANN	Distributed	ACC = 99	Health
[86]	Synthetic minority over-sampling technique	Distributed	Acc = 94.0, precision = 0.95, recall=0.94, f1–score = 0.91	Loan prediction
[89]	CNN-LSTM	Distributed (IID and Non-IID)	Val_acc = 90-92, val_loss = 0.04-0.96, CPU utilization = 60-80, RAM utilization = Stable	Fake news detection
[90]	CNN-LSTM	Distributed (IID-Non-IID)	Val_acc = 87, Val_loss = 0.09	IOV
[77]	InceptionResnetV2	Distributed (IID and Non-IID)	Val-acc = 74, Val-loss = 1.16	Internet of UAVs
[83]	CNN	Distributed	ACC = 75.6%	Smart agriculture
[84]	MobileNetV2, EfficientNetB3	Distributed (IID and Non-IID)	Acc = 99, loss = 0.1	Smart agriculture
[28]	EfficientNetB3	Distributed (IID and Non-IID)	Val_Acc = 95, val_loss = 0.08	Smart agriculture

6.2.1 Data and Traffic Management

FL-IoT offers a revolutionary approach to managing data and traffic in smart cities. This decentralized solution offers privacy protection while effectively managing huge amounts of data generated by the IoT. Data is processed locally by the devices, which promotes collaborative learning to develop predictive models for urban features such as traffic patterns and environmental monitoring. Procedures to protect the privacy of individuals, such as FL, guarantee the confidentiality of the information recorded. A FL-based approach known as FedSem is also proposed by various authors

[70]. FedSem was evaluated in a smart city context with intelligent vehicles that learn from traffic sign datasets. It shows high accuracy and minimal test losses, demonstrating its effectiveness in processing unlabeled data in a smart city environment. FL is applied in reference [71] to organize data streams from IoT devices, serving as FL clients. This approach enables local learning on devices without the need to exchange data externally. It offers the potential to transform smart cities with innovative services such as intelligent urban communication, collaborative sharing in the social economy, monitoring social activities and establishing connectivity between global citizens [72]. The research outlined in reference [73] recommends the application of FL to develop a platform for managing video data in smart city environments. To address the issues of non-IID data, the authors introduce a solution known as the Fed Swap operation.

6.2.2 Smart Grid

Smart grids enhanced by FL-IoT are revolutionizing energy distribution systems through decentralized learning between networked devices. In this framework, collaboration between IoT devices such as smart meters and sensors optimizes energy consumption, increases grid reliability and facilitates real-time decision making. The application of FL-IoT enables adaptive ML models that respond to dynamic energy demand and changes in the grid while maintaining data privacy. In reference [74], the authors have proposed a novel framework to help IoT users. First, they developed a framework that provides an agreement between locally varying privacy and resource consumption. Then, they classify users according to the level of privacy they need and preserve privacy for sensitive users.

6.3 FL-IoT for Smart Transportation

A variety of clients, such as vehicles, are involved in the process of cooperatively training globally shared AI models through the use of FL, which was recently developed to bring AI capabilities to the network edges to enable intelligent transportation. This eliminates the need for lengthy data transfer and protects user privacy.

6.3.1 Autonomous Vehicles

Recent advances in sensor and communication technology, as well as the amount of data coming in from in-vehicle sensors, embedded devices and road cameras, have helped to increase the robustness of vehicle networks. It is becoming more common to use AI and ML techniques in the transportation sector to develop intelligent transportation systems. There are many different types of IoT applications that can be developed using FL in cars. For example, in autonomous driving systems, each car is trained online by observing a single vehicle, resulting in a limited understanding of the environment. By using communication between vehicles, FL can provide additional details for each vehicle [75]. Zeng et al. [76] present a unique FL framework enabled by large-scale wireless connectivity for the development of autonomous control units for connected and autonomous vehicles. FL is an essential component in the ongoing development of autonomous vehicle systems. It serves as a means of facilitating communication between vehicles and enhances a variety of functions [77].

6.4 FL-IoT for Smart Industry

FL can also provide realistic solutions to update the knowledge of industrial intelligent systems with different application areas such as automation and Industry 4.0 or Industry 5.0 without jeopardising data sharing or privacy. These solutions can be implemented without jeopardising the

integrity of the data. For managing data exchange between robots for industrial activities, such as traffic routing, FL is an appealing technique. This is because it eliminates the possibility of unforeseen delays in network transmission [78,79].

6.4.1 Industrial IoT (IIoT)

The IIoT is revolutionized by FL, which makes it possible to implement AI applications without compromising the confidentiality of private data. The ideals of Industry 4.0 are reconciled with the decentralized approach that allows collaborative models to be trained across remote devices. Efficiency, data protection and the implementation of intelligent applications for industry are improved by this connection with EC in IoT networks [80].

6.4.2 Resource Efficient FL for IIoT

FL in dispersed edge networks requires efficient management and allocation of network resources to be resilient and successful. It is important to implement strategies that minimize latency, reduce communication overhead and prudently manage resources in distributed edge networks. The researchers in reference [81] proposes a framework for the distribution of network resources in wireless networks, with particular attention to edge networks built with the FL environment. The goal of the study is to develop a method that is both fair and effective in terms of allocation to facilitate collaborative development in FL-based edge networks. In reference [82], a study introduces an FL model that may speed the learning process by examining client behaviors and exploiting local computer resources. This model is particularly useful for resource-constrained IoT devices such as mobile robots [73,74].

6.5 FL-IoT for Smart Agriculture

FL-IoT can bring about a revolutionary change in the field of smart agriculture by improving a variety of elements of agricultural practices. In the field of agriculture, FL refers to the process of training ML models by utilizing data collected from a variety of decentralized sources, such as fields and sensors. This strategy facilitates the implementation of precision agriculture, which in turn improves crop yields, resource allocation and long-term sustainability, while maintaining the confidentiality of harvested data. Researchers like Antico et al. and Aggarwal et al. [28,83,84] classify maize and rice leaf crop diseases using FL-IoT by keeping the leaf image information at the farmer's location [85].

6.6 FL-IoT for Finance

The use of FL in finance improves data protection by enabling companies to work together on training models without having to share sensitive financial data. It not only ensures compliance with strict regulatory requirements, but also enables the construction of more accurate fraud detection models, risk assessment algorithms and customized financial services. However, the application of FL in banking requires customized enhancements to address real-world challenges. To effectively address these difficulties, user incentives need to be managed efficiently and access to personal data needs to be restricted. In reference [75], authors discuss all of the possible obstacles and problems that might arise while adopting FL in the banking sector, as well as the solutions to these problems. In reference [86] highlights issues in the bank loan approval process, where manual approval is often required due to insufficient data for automating decision-making through ML models. FL proves beneficial in overcoming data scarcity challenges by involving multiple financial institutions in global model

training. In reference [87], the authors analyze the credit risk assessment process, proposing an FL-based model for predicting credit risks.

7 Challenges Related to FL-IoT

FL involves sharing the trained model with the central server and requires multiple rounds of communication between the clients and servers. When sharing the models, lower communication costs and better efficiency are crucial. Therefore, it is important to overcome challenges such as limited energy and storage capacities, ensuring data privacy on the client side and ensuring hardware specifications on the edge devices. In this section, we have discussed various issues and challenges related to the FL-IoT environment as shown in Fig. 6.

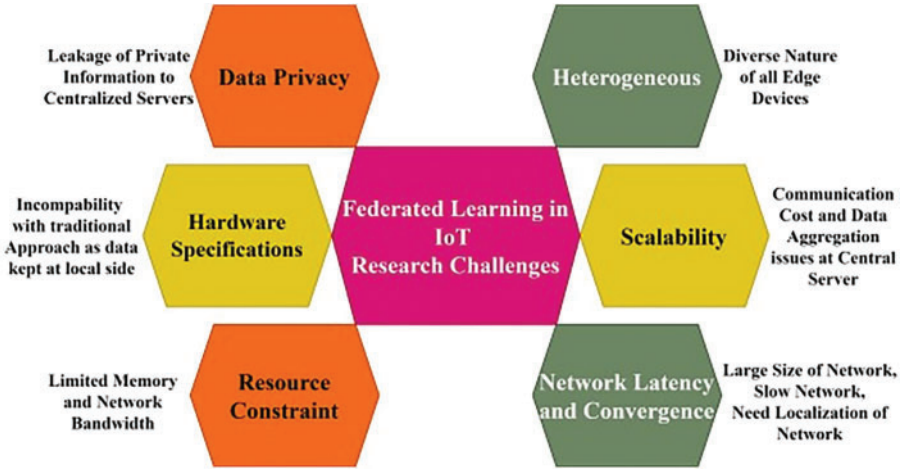

Figure 6: Core challenges of FL-IoT

7.1 Resource Constraint in FL-IoT

When it comes to dealing with the edge nodes of a network, there are a lot of challenges that can arise with FL from the resources. Various FL clients can pose particular challenges due to their limited performance or memory capacity, as well as their high energy consumption. A client with more memory may be able to perform more demanding calculations than a client with less memory. In addition, the energy budgets FL clients set during training may not be sufficient to meet the demands placed on the system. The combination of these characteristics leads to an increase in communication overhead and a decrease in system efficiency, both of which can lead to major difficulties when conducting model training. Utilizing EC for local computation on IoT devices proves to be a solution to reduce the resource burden and enable successful FL integration into various IoT ecosystems.

In FL environments, the inclusion of multiple devices offers performance benefits by training ML models on large datasets. However, there are also challenges, such as communication bottlenecks and increased computational costs, especially with a large number of clients. To address these issues, Hard et al. [91] focused on essential hardware prerequisites, required memory capacity, and computational capabilities for next-word prediction on a keyboard. Nishio et al. [40] addressed heterogeneous devices with varying computational power, aiming to optimize the computations on these devices, reducing processing times for lower-performance devices and minimizing upload times in poorer connection quality scenarios. Reference [92] shows a resource-aware FL architecture for

mobile devices that addresses computational power constraints. The proposal includes a soft training technique to accelerate the training of straggler devices. These can partially train the model locally by hiding resource-intensive neurons that are later restored in the aggregation phase.

7.2 Network Latency and Convergence Challenges

Network latency and convergence challenges in FL-IoT arise from delays in communication and model synchronization between distributed IoT devices. Limited computing capacity, energy constraints and bandwidth limitations contribute to these challenges. Managing network latency and ensuring timely convergence are critical to effective FL implementation in IoT, which includes strategies such as reducing device participation and optimizing communication rounds. Tackling communication overhead involves model compression techniques such as quantization and partitioning. Although this is effective, resource-constrained clients can face issues such as unsuccessful connections during training [93].

Wu et al. [94] presented a FL framework, FedKD, that focuses on adaptive mutual distillation of knowledge and dynamic compression gradient techniques. The authors conclude that the proposed framework reduces the communication cost by up to 94.8% and achieves better results by preserving the privacy of the data. An innovative approach is introduced in reference [95], Momentum FL by adding a momentum gradient framework at the aggregation server for accelerated convergence. Experimental results using the MNIST dataset are used to evaluate the convergence performance of MFL for a variety of machine-learning models.

Liu et al. [96] explore the approach applied to vehicular task offloading by discussing the various issues and challenges involved in edge servers with wireless networks.

7.3 Data Privacy Concerns in FL-IoT

Maintaining the confidentiality, integrity and privacy of data during model training on IoT devices is an important concern. However, due to the limited resources available, the privacy protection algorithms of the FL system may not work properly on these IoT devices [97]. Therefore, not only robust privacy safeguards need to be provided, but also new methods that are able to deal with fancy participants,that are efficient in terms of communication and that are frugal in terms of data processing. There are many studies that focus on the problems associated with peripheral devices that do not have sufficient computing capabilities. In order to build trust in FL-IoT applications, comply with privacy standards and develop effective communication and computing techniques for devices with limited power, it is essential to find solutions to these difficulties.

Zhang et al. [58] address security concerns in mobile and peripheral devices, proposing a Verifiable Privacy-preserving FL scheme to prevent gradient leakage and an online/offline method for lightweight gradient integrity verification. Reference [98] deploys privacy-aware Internet of Vehicles (IoV) services with FL in cloud-EC, utilizing distributed edge servers for model aggregation and homomorphic encryption for enhanced privacy.

7.4 Hardware Specifications Issues in FL-IoT

Resource-constrained IoT devices, characterized by limited computing, storage and power resources, pose scalability challenges influenced by factors such as physical size and cost considerations. These devices, including drones and smartphones, are an essential part of applications such as environmental monitoring in smart cities and factories [99]. Their role in tasks like environmental monitoring and EC applications is significant [4]. Before integrating the FL into the IoT environment,

it is important to close the gaps that currently exist and identify the latest hardware requirements for the IoT environment. Various hardware devices used in the FL-IoT EC scenario are listed in Table 6.

Table 6: Hardware devices used in FL-IoT computing scenario

S.no.	Hardware device	Definition
1	Raraspberry Pi	A compact and affordable single-board computer commonly utilized in IoT projects
2	NVIDIA Jetson series	Specialized EC platforms designed for AI workloads, offering GPU acceleration for ML tasks
3	Edge servers:	Powerful computing servers deployed at the edge of the network to process data locally, reducing the need for centralized processing
4	Intel NUC (Next unit of computing)	Small form-factor computers suitable for EC applications, offering a range of processors and configurations
5	Arduino edge boards	Microcontroller-based boards optimized for EC tasks, offering a balance between power consumption and processing capability
6	Google Coral Dev Board	A development board with an Edge TPU (Tensor Processing Unit) for accelerating ML tasks at the edge
7	AWS IoT greengrass	A software service that extends cloud capabilities to edge devices, enabling local processing and communication
8	Qualcomm edge AI platforms	Snapdragon processors and AI accelerators integrated into the platforms for edge AI applications
9	Movidius neural compute stick	USB stick with a dedicated neural processing unit, suitable for edge devices with limited computing power
10	ESP32/ESP8266	Low-cost and low-power Wi-Fi modules commonly used in IoT applications, offering EC capabilities
11	Samsung ARTIK modules	Compact and modular IoT modules designed for EC and connectivity
12	Helium atom development kit	Hardware kit for building decentralized IoT networks, enabling EC at scale

These above-mentioned hardware devices play a very important role in the FL-IoT computing environment and contribute to the distributive nature of FL.

7.5 Heterogeneous Environment

In a heterogeneous environment, each device has different specifications, computing capacities, operating conditions, energy and storage capacities and data processing capabilities. The FL-IoT

method can incorporate a wide range of heterogeneous devices in different ways. These may not only be alternative device performances, but also different platforms, different generations of devices or different amounts of data on which the local model is informed in this scenario. As a result, the duration of the training session can vary greatly from one customer to the next, and it would not be productive to assume that all participants have the same coverage [1]. The FL must be familiar with the various hardware configurations and be able to provide training on different platforms. In order to meet their system requirements, it is always necessary to select only the most trustworthy customers from among the connected customers. When it comes to successful FL collaboration, selective choice of participants that can be relied upon is absolutely essential. He et al. [100] explore training variation possibilities for heterogeneous devices in their paper. They present a formulation to maximize the efficiency of training, resource utilization, and heterogeneity. Feng et al. [101] examine the utilization of wireless power transfer and heterogeneous computing in FL. Their study suggests a framework for resource allocation and heterogeneous computing.

Effectively managing variations in heterogeneous hardware and non-IID data distribution is crucial for the success of FL systems, impacting the overall training procedure and global model accuracy. In 2022, Tahir et al. [102] offer a detailed analysis and overview of challenges associated with systematic and statistical heterogeneity. The study delves into various algorithms, including FedAvg, FedProx, FedPD, SCAFFOLD, and Fedmed, discussing their implications in addressing heterogeneity-related issues. Karimireddy et al. [103] focus on minimizing variance in local updates during data collection. Through experimental demonstrations, they find that SCAFFOLD exhibits a remarkable reduction in required communication rounds and proves resilient to data heterogeneity and client sampling issues, ultimately leading to faster convergence.

7.6 Scalability Issue in FL-IoT

The scalability challenges of FL for IoT (FL-IoT) relate to difficulties in efficiently expanding the system. This is a major problem in terms of communication costs and aggregation of models on the central server with IoT devices. We need appropriate algorithms for aggregated models and communication protocols to overcome this scalability problem. In the FL environment, client selection is a very tedious task due to limited bandwidth and battery resources. Therefore, efficient client selection methods are essential to overcome these problems. Many researchers have explored these scalability issues with appropriate client selection mechanisms.

Zhang et al. [104] proposed a framework to solve the problem of scalability in order to minimize the communication costs between client and server. The authors presented a cooperative federated edge learning framework for high accuracy and low latency between mobile edge devices. Ye et al. [105] has addressed the problem of model aggregation and introduced an approach to model aggregation in vehicle clients, where a local model is selected and sent to the aggregation server while preserving the confidentiality of image quality and computational capability. FL-IoT thus needs to address scalability issues to successfully manage the growing network of IoT devices and maintain algorithms based on ML algorithms that are reliable and effective across different platforms.

8 Discussion

Many data services and applications have emerged from the remarkable proliferation of IoT and the data it generates. On the other hand, traditional approaches using classical AI and ML techniques for IoT face significant challenges, including data privacy, data diversity, energy efficiency in transmission and scalability. FL is an AI revolution in the deployment of IoT services and

applications in this environment. As a result, the purpose of this study is to provide a complete overview of the use of FL for a variety of IoT services and applications.

To summarize, FL has the remarkable potential to solve several problems that arise in IoT applications. These challenges include maintaining privacy, managing resources to handle large amounts of data, the cost of communication and scalability involved in transferring data to the central server for training ML models, real-time analytics and customized decisions based on geographical locations and heterogeneity of data. However, to fully realize the potential of FL in IoT applications, some obstacles still need to be overcome. These obstacles include limited computing resources and network bandwidth, the heterogeneity of devices and privacy concerns. The advantages of using FL in IoT applications over traditional ML approaches are listed in Table 7.

Table 7: Existing challenges and benefits of FL in IoT applications

Applications	Challenges faced	Advantages with FL
Smart healthcare	Need a wide variety of data from a variety of medical institutions to train the ML models	Through FL, it is possible to collaborate across numerous hospitals without revealing the confidential and sensitive information of patients. This is made possible by the fact that the global model may be performed at specific hospital locations Without sharing patient data.
	Real-time analysis is difficult during a pandemic	In a situation like a pandemic, FL can give analytics in a manner that is very close to real-time since the local device does not have to wait for the receipt of data from other devices.
	Protection of patient's sensitive information	In the FL framework, the ML model may be implemented on local devices, ensuring that the privacy of patients' data is maintained.
	Communication and storage costs increased due to the distribution of substantial amounts of medical information from IoT devices.	In FL, only locally trained model is shared so, it decreases the communication and storage cost.
Smart city	Managing resources	In FL local model is trained at the local site, so the burden of resource management at the cloud is reduced.
	High communication cost for transferring huge amounts of data	As only the trained model is shared so, the cost of communication decreases.

(Continued)

Table 7 (continued)

Applications	Challenges faced	Advantages with FL
	Protection of citizen's and vehicle's private information	The trained model is shared with the cloud instead of the user's private information.
	During an emergency, it might be challenging to broadcast unique solutions that are relevant to the diverse demographic maps in real-time	Using FL, appropriate solutions may be supplied to meet the different requirements of various regions of the city, based on the data that is essential to the situation.
Smart transportation	Protection of driver and vehicle private information.	FL ensures data privacy as only the model is shared
	The high levels of latency and communication costs are associated with the process of sending massive amounts of data from the vehicles to the cloud	It reduces the latency and communication cost as instead of data only model is shared.
	Customized solutions that are based on the facts on the traffic in a certain region	FL is trained based on the data from the local region, it can make individualized recommendations based on the knowledge about the traffic in that particular location.
Smart industry	Security concerns arise due to the centralized approach	Due to its decentralized nature, security is achieved with FL.
	Protection of sensitive data/information related to business plans	Data/Information is protected with FL.
	Difficulties in using collective intelligent edge devices	Each edge device has its own data and trained model locally
Smart agriculture	Communication costs involved in transferring a large amount of data	With FL, communication cost is reduced as the model is trained at a local farmer's site.
	Data privacy/security issues	Farmer's data is protected with FL.
Smart finance	High security/data privacy risk related to financial information	Data privacy is assured with FL as raw data is kept at the local site.
	Data storage and communication cost issues	In the FL model parameter is shared with the cloud server so, it reduces the data storage and communication cost.

8.1 Comparative Analysis of ML and FL

ML methods have proven their effectiveness in various applications, but due to the centralized approach of traditional machine learning methods, they raise the problem of data privacy, have high communication costs and require more computational resources. The FL approach overcomes these problems by preserving the data on the client side and reducing communication costs as only the trained models are shared with the aggregation server. Many researchers have demonstrated the effectiveness of the FL approach over traditional ML algorithms. In Table 8 and Fig. 7, we have discussed some manuscripts that implement the FL approach and achieve better accuracy in training the model.

Table 8: Comparative analysis of ML and FL approaches

Reference	Approach used	ML centralized	FL decentralized	Data privacy	Reduced communication cost
[68]	CNN + FL	94%	96%	√	√
[69]	CNN + FL	96.8%	91%	√	√
[77]	InceptionResNet + FL	75%	74%	√	√
[83]	CNN + FL	97.29%	96.87%	√	√
[84]	EfficientNetB3 + FL	100%	99%	√	√
[28]	EfficientNetB3 + FL	99%	99%	√	√
[86]	ML algorithm + FL	93%	94%	√	√
[58]	LSTM + FL	95%	92%	√	√

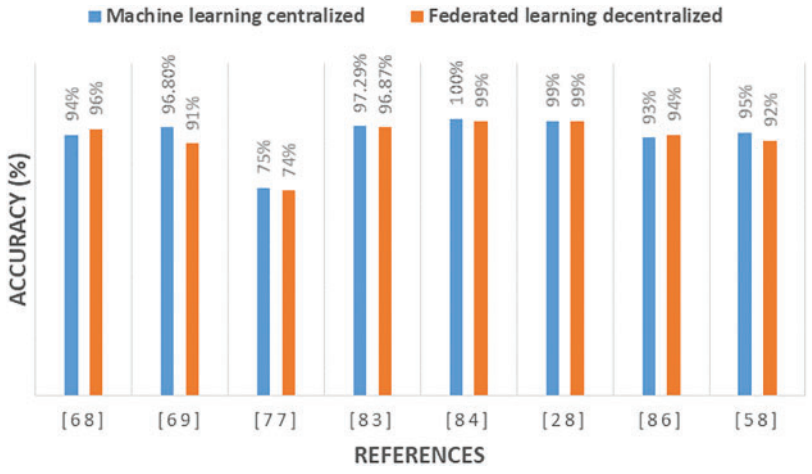

Figure 7: Comparative analysis of ML and FL approaches

As it is clear from Fig. 7, there is a slight difference between the accuracies of ML and FL. In [69], the accuracy with the base ML approach is 96.8%, the accuracy with the FL approach is 91%, and in [28], the accuracy is 99% with both approaches. So, we conclude that with FL, we achieved almost the same results as with ML models by preserving data and reducing communication cost.

8.2 Comparative Analysis of IID and Non-IIDs Approaches

IID and non-IID mean the distribution of different data patterns to different devices. It is difficult to evaluate the actual non-IID performance of models because FL has a considerable number of hyperparameters, such as the number of clients, epochs, and the probability of a client failing. These hyperparameters change drastically from method to method, making it difficult to compare the performance of these algorithms. Dealing with non-IID data (device heterogeneity) is a major problem when implementing FL algorithms. In Table 9 and Fig. 8, we have discussed some manuscripts that implement the FL approach with IID and non-ID datasets and achieve better accuracy in training the non-ID data.

Table 9: Comparative analysis of IID and Non-IID approaches

Reference	Approached used	FL-IID	FL-NonIID	Centralized DL approach	Resource utilization	Data privacy	Less communication cost
[90]	CNN-LSTM + FL	87.8	87.7	87	√	√	√
[28]	EfficientNetB3 + FL	99.7	97.4	99	√	√	√
[84]	EfficientNetB3 + FL	99	98	99	√	√	√
[84]	MobileNetB3	98	90	99	√	√	√
[106]	DenseNet + FL	82	82	84	√	√	√
[107]	DenseNet201 + FL	96.39	94.44	99	√	√	√

In Fig. 8, we compare the accuracy of the FL approach (IID and Non-ID) with the centralized approach and conclude that all three approaches have almost similar accuracy in terms of model accuracy, but with the FL approach we solve problems such as privacy, resource utilization and high communication costs. FL is an emerging distributed AI technique that has attracted great interest in realizing IoT services and applications that enhance privacy and are scalable.

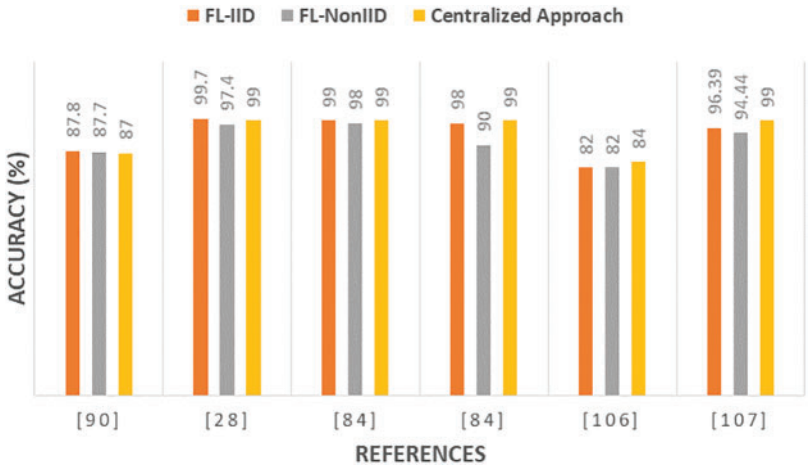

Figure 8: FL-IID and Non IID approach comparison

9 Emerging Trends and Future Directions in FL-IoT

Decentralized learning environments will benefit from innovation, scalability, privacy, and security thanks to these new emerging trends and directions in FL and IoT that will influence the development of intelligent IoT applications in the future. After analyzing the various implementation challenges related to FL-IoT [4,5,22], we figure out some possible future directions such as:

Data Privacy Mechanism: The aim of the research is to improve privacy preserving methods in FL-IoT systems to preserve private information while enabling cooperative model training. This includes developments in secure aggregation protocols, FL with encrypted gradients, homomorphic encryption, and differential privacy. There is a need to develop and improve sophisticated privacy preserving methods specifically designed for FL in the IoT context.

Federated Learning with Multiple Modes: Future FL systems will provide multi-modal data gathering and model training due to the widespread use of several sensor kinds in the IoT devices. This makes it possible to create extensive models that can concurrently handle and analyze several kinds of data streams.

Adversarial Robustness: To protect against adversarial assaults and efforts at data poisoning, FL-IoT systems will utilize robustness techniques. The goal of this research is to improve security and reliability by creating adversarial training strategies, anomaly detection algorithms, and model verification processes.

Resource Constraint Optimization: Lightweight ML models, compression strategies, and energy-efficient algorithms that are ideal for implementation on resource-constrained IoT devices should be the main areas of future study to get beyond these devices' restrictions.

Heterogeneity Management: To manage heterogeneity while preserving model fairness and accuracy, future work should focus on FTL approaches and adaptive learning algorithms, as IoT devices and data sources differ in their capabilities and formats.

Scalability: To cope with the growing number of IoT devices, research into scalable solutions should be a top priority in the future of FL-IoT. This means that distributed optimization algorithms and communication protocols need to be developed specifically for large FL installations.

Future developments in FL-IoT applications will be tailored to specific use cases. In healthcare, FL can enable collaborative model training across distributed medical devices, improving diagnostic accuracy while protecting patient privacy. It has the potential to increase productivity and save maintenance costs in smart cities by enabling proactive infrastructure maintenance through the consolidation of sensor data from edge devices. It could also help predict defects and detect anomalies in manufacturing processes as part of the industrial IoT, maximizing production and reducing downtime. To enhance navigation and safety in autonomous vehicles while ensuring data privacy, FL-IoT can support cooperative learning between vehicles. These applications show how FL can use distributed learning to solve real-world problems in a variety of IoT domains.

10 Review Summary

This investigation examines numerous fascinating and valuable articles about the state-of-the-art in FL-IoT. This article is organized based on FL and IoT approaches, protocols, architecture, application areas, and challenges. Fig. 1 depicts the PRISMA flow diagram for conducting the systematic review. Table 1 shows the summary of the related articles of literature reviewed.

10.1 Limitations

Despite a thorough search across databases, some relevant publications may be missing because of the inclusion of only English-published studies, chosen search keywords, and database constraints.

11 Conclusions

The realization of IoT services and applications that enhance privacy and are scalable has been greatly influenced by an emerging distributed AI technique known as FL. We have explored the potential of FL to facilitate IoT networks through a comprehensive review of the current state of the art and in-depth discussions based on recent research in the field. FL enables the training of collaborative ML models on decentralized devices, contributing to a privacy-friendly approach where sensitive data remains in its original location. The novelty lies in decentralized model training. Centralization of raw data is no longer necessary, which protects the privacy of the individual. In addition, FL proves its ability to extend to multiple devices without interruption, providing a gateway to intelligent and efficient solutions for numerous applications in the IoT. FL is a key enabler for the use of AI in decentralized and connected contexts as the IoT evolves. This will ensure that there is a balance between innovation and privacy protection. In this manuscript, we have first provided an overview of the latest developments in IoT and FL and made suggestions for improving their integration. We then looked at recent developments in FL-IoT applications in various industries, including smart healthcare, transportation, city government, manufacturing, financial services and architecture. To conclude a comprehensive review, we have also examined the implementation framework with performance metrics and communication protocols relevant to FL-IoT. Finally, we also discussed various open research challenges and future directions related to FL-IoT. In summary, an analysis was conducted to compare FL (IID and Non-IID) with centralized methods, confirming the superiority of FL in preserving privacy and minimizing communication overhead. We hope that this study will serve as a springboard for further research projects aimed at the widespread use of FL-IoT, promoting awareness and progress in this rapidly evolving sector.

Acknowledgement: Not applicable.

Funding Statement: The authors received no specific funding for this study.

Author Contributions: Study conception and design: M.A., V.K., N.G., S.M.S.; data collection: M.A., V.K., S.R., T.A.P., S.M.S.; analysis and interpretation of results: M.A., V.K., S.R., S.B.B., S.M.S.; draft manuscript preparation: M.A., V.K., N.G., S.M.S., T.A.P., S.B.B. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: Not applicable.

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

References

[1] A. Brecko, E. Kajati, J. Koziorek, and I. Zolotova, "Federated learning for edge computing: A survey," *Appl. Sci.*, vol. 12, no. 18, pp. 1–36, 2022. doi: 10.3390/app12189124.

[2] M. Venkatasubramanian, A. H. Lashkari, and S. Hakak, "IoT malware analysis using federated learning: A comprehensive survey," *IEEE Access*, vol. 11, pp. 5004–5018, 2023. doi: 10.1109/ACCESS.2023.3235389.

[3] Z. Du, C. Wu, T. Yoshinaga, K. L. A. Yau, Y. Ji and J. Li, "Federated learning for vehicular internet of things: Recent advances and open issues," *IEEE Open J. Comput. Soc.*, vol. 1, no. 1, pp. 45–61, 2020. doi: 10.1109/OJCS.2020.2992630.

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

[5] D. Sirohi, N. Kumar, P. S. Rana, S. Tanwar, R. Iqbal and M. Hijjii, *Federated Learning for 6G-Enabled Secure Communication Systems: A Comprehensive Survey*, vol. 56, no. 10. Netherlands: Springer, 2023.

[6] Y. Chen, S. Huang, W. Gan, G. Huang, and Y. Wu, "Federated learning for metaverse: A survey," in *Companion Proc. ACM Web Conf.*, 2023, pp. 1151–1160.

[7] A. Rahman *et al.*, "On the ICN-IoT with federated learning integration of communication: Concepts, security-privacy issues, applications, and future perspectives," *Futur. Gen. Comput. Syst.*, vol. 138, pp. 61–88, 2023.

[8] A. Qammar, A. Karim, H. Ning, and J. Ding, "Securing federated learning with blockchain: A systematic literature review," *Artif. Intell. Rev.*, vol. 56, no. 5, pp. 3951–3985, 2023. doi: 10.1007/s10462-022-10271-9.

[9] M. Aledhari, R. Razzak, R. M. Parizi, and F. Saeed, "Federated learning: A survey on enabling technologies, protocols, and applications," *IEEE Access*, vol. 8, pp. 140699–140725, 2020. doi: 10.1109/ACCESS.2020.3013541.

[10] Z. Yang, M. Chen, K. K. Wong, H. V. Poor, and S. Cui, "Federated learning for 6G: Applications, challenges, and opportunities," *Engineering*, vol. 8, pp. 33–41, 2022.

[11] Y. Liu, X. Yuan, Z. Xiong, J. Kang, X. Wang and D. Niyato, "Federated learning for 6G communications: Challenges, methods, and future directions," *China Commun.*, vol. 17, no. 9, pp. 105–118, 2020.

[12] K. M. J. Rahman *et al.*, "Applications and design aspects of federated learning: A survey," *IEEE Access*, vol. 9, pp. 124682–124700, 2021. doi: 10.1109/ACCESS.2021.3111118.

[13] D. C. Nguyen *et al.*, "Federated learning meets blockchain in edge computing: Opportunities and challenges," *IEEE Internet Things J.*, vol. 8, no. 16, pp. 12806–12825, 2021. doi: 10.1109/JIOT.2021.3072611.

[14] W. Issa, N. Moustafa, B. Turnbull, N. Sohrabi, and Z. Tari, "Blockchain-based federated learning for securing internet of things: A comprehensive survey," *ACM Comput. Surv.*, vol. 55, no. 9, pp. 1–43, 2023. doi: 10.1145/3560816.

[15] H. G. Abreha, H. Mohamed, and M. Adel, "Federated learning in edge computing: A systematic survey," *Sensors*, vol. 22, no. 2, pp. 1–45, 2022. doi: 10.3390/s22020450.

[16] I. Kholod *et al.*, "Open-source federated learning frameworks for IoT: A comparative review and analysis," *Sensors*, vol. 21, no. 1, pp. 1–22, 2021.
[17] P. Zeng, A. Liu, N. N. Xiong, S. Zhang, and M. Dong, "TD-MDB: A truth-discovery-based multidimensional bidding strategy for federated learning in industrial IoT systems," *IEEE Internet Things J.*, vol. 11, no. 3, pp. 4274–4288, 2024. doi: 10.1109/JIOT.2023.3298814.
[18] R. Liu, M. Xie, A. Liu, and H. Song, "Joint optimization risk factor and energy consumption in IoT networks with TinyML-enabled internet of UAVs," *IEEE Internet Things J.*, pp. 1–1, 2024. doi: 10.1109/JIOT.2023.3348837.
[19] V. Mothukuri *et al.*, "A survey on security and privacy of federated learning," *Futur. Gener. Comput. Syst.*, vol. 115, no. 4, pp. 619–640, 2021. doi: 10.1016/j.future.2020.10.007.
[20] Q. Li *et al.*, "A survey on federated learning systems: Vision, hype and reality for data privacy and protection," *IEEE Trans. Knowl. Data Eng.*, vol. 35, no. 4, pp. 3347–3366, 2023. doi: 10.1109/TKDE.2021.3124599.
[21] P. Cruz, N. Achir, and A. C. Viana, "On the edge of the deployment: A survey on multi-access edge computing," *ACM Comput. Surv.*, vol. 55, no. 5, pp. 1–35, 2022.
[22] L. Kong *et al.*, "Edge-computing-driven internet of things: A survey," *ACM Comput. Surv.*, vol. 55, no. 8, pp. 1–41, 2022.
[23] N. Victor, C. R., M. Alazab, S. M. Sweta Bhattacharya, P. K. R. Maddikunta, and T. R. G. Kadiyala Ramana, "Federated learning for IoUT: Concepts, applications, challenges and opportunities," arXiv:2207.13976v1, 2022, pp. 1–7.
[24] L. U. Khan, W. Saad, Z. Han, E. Hossain, and C. S. Hong, "Federated learning for internet of things: Recent advances, taxonomy, and open challenges," *IEEE Commun. Surv. Tutorials*, vol. 23, no. 3, pp. 1759–1799, 2021. doi: 10.1109/COMST.2021.3090430.
[25] R. Gosselin, L. Vieu, F. Loukil, and A. Benoit, "Privacy and security in federated learning: A survey," *Appl. Sci.*, vol. 12, no. 19, pp. 1–15, 2022. doi: 10.3390/app12199901.
[26] R. T. Hameed, "Federated learning in IoT: A survey on distributed decision making," *BJIoT*, vol. 2023, pp. 1–7, 2023.
[27] P. Boobalan *et al.*, "Fusion of federated learning and industrial internet of things: A survey," *Comput. Netw.*, vol. 212, no. 11, pp. 1–24, 2022. doi: 10.1016/j.comnet.2022.109048.
[28] M. Aggarwal, V. Khullar, N. Goyal, A. Alammari, M. A. Albahar and A. Singh, "Lightweight federated learning for rice leaf disease classification using non independent and identically distributed images," *Sustainability*, vol. 15, no. 16, pp. 1–20, 2023. doi: 10.3390/su151612149.
[29] S. Sharma and K. Guleria, "A comprehensive review on federated learning based models for healthcare applications," *Artif. Intell. Med.*, vol. 146, pp. 102691, 2023. doi: 10.1016/j.artmed.2023.102691.
[30] Q. Yang, Y. Liu, T. Chen, and Y. Tong, "Federated machine learning: Concept and application," *ACM Trans. Intell. Syst. Technol.*, vol. 10, no. 2, pp. 1–19, 2019. doi: 10.1145/3339474.
[31] S. K. Das and S. Bebortta, "Heralding the future of federated learning framework: Architecture, tools and future directions," in *Proc. 11th Int. Conf. Cloud Comput. Data Sci.*, Eng., Noida, India, 2021, pp. 698–703.
[32] S. K. Lo, Q. Lu, C. Wang, H. Y. Paik, and L. Zhu, "A systematic literature review on federated machine learning," *ACM Comput. Surv.*, vol. 54, no. 5, pp. 1–39, 2022.
[33] R. Akhter and S. A. Sofi, "Precision agriculture using IoT data analytics and machine learning," *J. King Saud Univ.—Comput. Inf. Sci.*, vol. 34, no. 8, pp. 5602–5618, 2022. doi: 10.1016/j.jksuci.2021.05.013.
[34] S. Rani, S. H. Ahmed, and R. Rastogi, "Dynamic clustering approach based on wireless sensor networks genetic algorithm for IoT applications," *Wirel. Netw.*, vol. 26, no. 4, pp. 2307–2316, 2020. doi: 10.1007/s11276-019-02083-7.
[35] A. A. Laghari, K. Wu, R. A. Laghari, M. Ali, and A. A. Khan, "A review and state of art of internet of things (IoT)," *Arch. Comput. Methods Eng.*, vol. 29, no. 3, pp. 1395–1413, 2022. doi: 10.1007/s11831-021-09622-6.

[36] V. Khullar, H. P. Singh, and M. Bala, "IoT based assistive companion for hypersensitive individuals (ACHI) with autism spectrum disorder," *Asian J. Psychiatr.*, vol. 46, pp. 92–102, 2019. doi: 10.1016/j.ajp.2019.09.030.
[37] M. S. Farooq, S. Riaz, A. Abid, T. Umer, and Y. Bin Zikria, "Role of IoT technology in agriculture: A systematic literature review," *Electronics*, vol. 9, no. 2, pp. 1–41, 2020.
[38] W. Y. B. Lim *et al.*, "Federated learning in mobile edge networks: A comprehensive survey," *IEEE Commun. Surv. Tutorials*, vol. 22, no. 3, pp. 2031–2063, 2020. doi: 10.1109/COMST.2020.2986024.
[39] K. Bonawitz *et al.*, "Towards federated learning at scale: System design," 2019. Accessed: Dec. 16, 2023. [Online]. Available: http://arxiv.org/abs/1902.01046
[40] T. Nishio and R. Yonetani, "Client selection for federated learning with heterogeneous resources in mobile edge," *IEEE Int. Conf. Commun.*, pp. 1–7, 2019. doi: 10.1109/ICC.2019.8761315.
[41] Z. Zhao *et al.*, "Towards efficient communications in federated learning: A contemporary survey," *J. Franklin Inst.*, vol. 360, no. 12, pp. 8669–8703, 2023. doi: 10.1016/j.jfranklin.2022.12.053.
[42] R. Yu and P. Li, "Toward resource-efficient federated learning in mobile edge computing," *IEEE Netw.*, vol. 35, no. 1, pp. 148–155, 2021. doi: 10.1109/MNET.011.2000295.
[43] K. Ostrowski, "TensorFlow Federated: Machine learning on decentralized data," *TensorFlow*, 2019. Accessed: Dec. 24, 2023. [Online]. Available: https://www.tensorflow.org/federated
[44] J. Mancuso, "Introducing Pysyft Tensorflow," *Open Mined*, 2021. Accessed: Dec. 20, 2023. [Online]. Available: https://blog.openmined.org/introducing-pysyft-tensorflow/
[45] C. Beauville, "Federated Learning with fast AI and Flower," *Flower*, 2023. Accessed: Dec. 10, 2023. [Online]. Available: https://flower.ai/blog/2023-02-21-federated-learning-with-flower-and-fastai/
[46] K. Martineau, "IBM federated learning," *IBM*, 2022. Accessed: Dec. 22, 2023. [Online]. Available: https://research.ibm.com/blog/what-is-federated-learning
[47] M. Roehm, "Frameworks for federated learning," *APEHRIS*, 2022. Accessed: Dec. 19, 2023. [Online]. Available: https://www.apheris.com/resources/blog/top-7-open-source-frameworks-for-federated-learning
[48] H. T. Truong *et al.*, "Light-weight federated learning-based anomaly detection for time-series data in industrial control systems," *Comput. Ind.*, vol. 140, pp. 1–35, 2022. doi: 10.1016/j.compind.2022.103692.
[49] G. Wu, Z. Xu, H. Zhang, S. Shen, and S. Yu, "Multi-agent DRL for joint completion delay and energy consumption with queuing theory in MEC-based IIoT," *J. Parallel Distrib. Comput.*, vol. 176, no. 1, pp. 80–94, 2023. doi: 10.1016/j.jpdc.2023.02.008.
[50] S. Shen, X. Wu, P. Sun, H. Zhou, Z. Wu and S. Yu, "Optimal privacy preservation strategies with signaling Q-learning for edge-computing-based IoT resource grant systems," *Expert. Syst. Appl.*, vol. 225, no. 3, pp. 120192, 2023. doi: 10.1016/j.eswa.2023.120192.
[51] S. Pouriyeh *et al.*, "Secure smart communication efficiency in federated learning: Achievements and challenges," *Appl. Sci.*, vol. 12, no. 18, pp. 1–22, 2022. doi: 10.3390/app12188980.
[52] D. Leroy, A. Coucke, T. Lavril, T. Gisselbrecht, and J. Dureau, "Federated learning for keyword spotting," in *Proc. Int. Conf. Acoust. Speech Signal Process (ICASSP)*, Brighton, UK, IEEE, 2019, pp. 6341–6345.
[53] S. Feng and H. Yu, "Multi-participant multi-class vertical federated learning," 2020. Accessed: Dec. 12, 2023. [Online]. Available: http://arxiv.org/abs/2001.11154.
[54] 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, 2020. doi: 10.1109/MIS.2020.2988525.
[55] Y. Li, C. Chen, N. Liu, H. Huang, Z. Zheng and Q. Yan, "A blockchain-based decentralized federated learning framework with committee consensus," *IEEE Netw.*, vol. 35, no. 1, pp. 234–241, 2021. doi: 10.1109/MNET.011.2000263.
[56] A. Reisizadeh, A. Jadbabaie, A. Mokhtari, H. Hassani, and R. Pedarsani, "FedPAQ: A communication-efficient federated learning method with periodic averaging and quantization," in *Proc. Mach. Learn. Res.*, vol. 108, no. 2, pp. 2021–2031, 2020.
[57] A. Heidari, N. J. Navimipour, H. Dag, S. Talebi, and M. Unal, "A novel blockchain-based deepfake detection method using federated and deep learning models," *Cogn. Comput.*, vol. 9, pp. 1–19, 2024. doi: 10.1007/s12559-024-10255-7.

[58] J. Zhang, Y. Liu, D. Wu, S. Lou, B. Chen and S. Yu, "VPFL: A verifiable privacy-preserving federated learning scheme for edge computing systems," *Digit. Commun. Netw.*, vol. 9, no. 4, pp. 981–989, 2023. doi: 10.1016/j.dcan.2022.05.010.

[59] G. Wu, X. Chen, Z. Gao, H. Zhang, S. Yu and S. Shen, "Privacy-preserving offloading scheme in multi-access mobile edge computing based on MADRL," *J. Parallel Distrib. Comput.*, vol. 183, pp. 104775, 2024. doi: 10.1016/j.jpdc.2023.104775.

[60] B. C. Drolet, J. S. Marwaha, B. Hyatt, P. E. Blazar, and S. D. Lifchez, "Electronic communication of protected health information: Privacy, security, and HIPAA compliance," *J. Hand Surg. Am.*, vol. 42, no. 6, pp. 411–416, 2017. doi: 10.1016/j.jhsa.2017.03.023.

[61] N. Rieke *et al.*, "The future of digital health with federated learning," *npj Digit. Med.*, vol. 3, no. 1, pp. 1–7, 2020.

[62] B. Yuan, S. Ge, and W. Xing, "A federated learning framework for healthcare IoT devices," vol. 1, 2020. Accessed: Dec. 12, 2023. [Online]. Available: http://arxiv.org/abs/2005.05083

[63] L. Huang, Y. Yin, Z. Fu, S. Zhang, H. Deng and D. Liu, "LoadaBoost: Loss-based AdaBoost federated machine learning with reduced computational complexity on IID and non-IID intensive care data," *PLoS One*, vol. 15, no. 4, pp. 1–16, 2020. doi: 10.1371/journal.pone.0230706.

[64] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, "BEdgeHealth: A decentralized architecture for edge-based IoMT networks using blockchain," *IEEE Internet Things J.*, vol. 8, no. 14, pp. 11743–11757, 2021. doi: 10.1109/JIOT.2021.3058953.

[65] A. G. Roy, S. Siddiqui, S. Pölsterl, N. Navab, and C. Wachinger, "BrainTorrent: A peer-to-peer environment for decentralized federated learning," 2019. Accessed: Dec. 04, 2023. [Online]. Available: http://arxiv.org/abs/1905.06731

[66] T. S. Brisimi, R. Chen, T. Mela, A. Olshevsky, I. C. Paschalidis, and W. Shi, "Federated learning of predictive models from federated electronic health records," *Int. J. Med. Inform.*, vol. 112, pp. 59–67, 2018. doi: 10.1016/j.ijmedinf.2018.01.007.

[67] M. J. Sheller, G. A. Reina, B. Edwards, J. Martin, and S. Bakas, "Multi-institutional deep learning modeling without sharing patient data: A feasibility study on brain tumor segmentation," in *4th Int. Workshop*, Granada, Spain, 2018, vol. 11383, pp. 92–104.

[68] D. H. Mahlool and M. H. Abed, "Distributed brain tumor diagnosis using a federated learning environment," *Bull Electr. Eng. Inform.*, vol. 11, no. 6, pp. 3313–3321, 2022. doi: 10.11591/eei.v11i6.4131.

[69] M. Islam, M. T. Reza, M. Kaosar, and M. Z. Parvez, "Effectiveness of federated learning and CNN ensemble architectures for identifying brain tumors using MRI images," *Neural Process Lett.*, vol. 55, pp. 3779–3809, 2023.

[70] A. Albaseer, B. S. C. M. Abdallah, and A. Al-Fuqaha, "Exploiting unlabeled data in smart cities using federated edge learning," in *Int. Wirel. Commun. Mobile Comput. Conf., IWCMC*, Limassol, Cyprus, 2020.

[71] D. R. Mukhametov, "Ubiquitous computing and distributed machine learning in smart cities," in *Proc. Wave Electron. Appl. Inf. Telecommun. Syst.*, St. Petersburg, Russia, 2020, pp. 7–11.

[72] Y. Liu *et al.*, "Fedvision: An online visual object detection platform powered by federated learning," in *Proc. 34th AAAI Conf.*, Washington DC, USA, 2020, pp. 13172–13179.

[73] H. Chai, S. Leng, Y. Chen, and K. Zhang, "A hierarchical blockchain-enabled federated learning algorithm for knowledge sharing in internet of vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 7, pp. 3975–3986, 2021. doi: 10.1109/TITS.2020.3002712.

[74] H. Cao, S. Liu, R. Zhao, and X. Xiong, "IFed: A novel federated learning framework for local differential privacy in power internet of things," *Int. J. Distrib. Sens. Netw.*, vol. 16, no. 5, pp. 155014772091969, 2020. doi: 10.1177/1550147720919698.

[75] J. H. Chen, M. R. Chen, G. Q. Zeng, and J. S. Weng, "BDFL: A byzantine-fault-tolerance decentralized federated learning method for autonomous vehicle," *IEEE Trans. Veh. Technol.*, vol. 70, no. 9, pp. 8639–8652, 2021. doi: 10.1109/TVT.2021.3102121.

[76] T. Zeng, O. Semiari, M. Chen, W. Saad, and M. Bennis, "Federated Learning on the road autonomous controller design for connected and autonomous vehicles," *IEEE Trans. Wirel. Commun.*, vol. 21, no. 12, pp. 10407–10423, 2022. doi: 10.1109/TWC.2022.3183996.

[77] V. Khullar and H. P. Singh, "Privacy protected internet of unmanned aerial vehicles for disastrous site identification," *Concurr. Comput. Pract. Exp.*, vol. 34, no. 19, pp. 1–10, 2022. doi: 10.1002/cpe.7040.

[78] Q. Li, Y. Diao, Q. Chen, and B. He, "Federated learning on non-IID data silos: An experimental study," in *Proc. Int. Conf.*, Kuala Lumpur, Malaysia, 2022, pp. 965–978.

[79] H. Zhu, J. Xu, S. Liu, and Y. Jin, "Federated learning on non-IID data: A survey," *Neurocomput.*, vol. 465, pp. 371–390, 2021. doi: 10.1016/j.neucom.2021.07.098.

[80] S. Shen, L. Xie, Y. Zhang, G. Wu, H. Zhang and S. Yu, "Joint differential game and double deep Q-networks for suppressing malware spread in industrial internet of things," *IEEE Trans. Inf. Forensics Secur.*, vol. 18, pp. 5302–5315, 2023. doi: 10.1109/TIFS.2023.3307956.

[81] L. Wang, W. Wang, and B. Li, "CMFL: Mitigating communication overhead for federated learning," in *Proc. Int. Conf. Distrib. Comput.*, Syst., Dallas, TX, USA, 2019, pp. 954–964.

[82] A. Imteaj and M. Hadi Amini, "FedAR: Activity and resource-aware federated learning model for distributed mobile robots," in *Proc. 19th IEEE Int. Conf. Mach. Learn. Appl. ICMLA*, Miami, FL, USA, 2020, pp. 1153–1160.

[83] T. M. Antico, L. F. R. Moreira, and R. Moreira, "Evaluating the potential of federated learning for maize leaf disease prediction," in *Proc. Natl Meet. Artif. Comput. Intell. (ENIAC)*, Campinas/SP, 2023, pp. 282–293.

[84] M. Aggarwal *et al.*, "Federated transfer learning for rice-leaf disease classification across multiclient cross-silo datasets," *Agron.*, vol. 13, no. 10, pp. 1–25, 2023. doi: 10.3390/agronomy13102483.

[85] D. Vimalajeewa, C. Kulatunga, D. P. Berry, and S. Balasubramaniam, "A service-based joint model used for distributed learning: Application for smart agriculture," *IEEE Trans. Emerg. Top. Comput.*, vol. 10, no. 2, pp. 838–854, 2022.

[86] G. Shingi, "A federated learning based approach for loan defaults prediction," in *IEEE Int. Conf. Data Min. Work.*, Sorrento, Italy, 2020, pp. 362–368.

[87] D. Kawa, S. Punyani, P. Nayak, A. Karkera, and V. Jyotinagar, "Credit risk assessment from combined bank records using federated learning," *Int. Res. J. Eng. Technol.*, pp.1–4, 2008.

[88] E. Ashraf, N. F. F. Areed, H. Salem, E. H. Abdelhay, and F. Ahmed, "FIDChain : Federated intrusion detection system for blockchain-enabled IoT healthcare applications," *Healthcare*, vol. 10, no. 6, pp. 1–20, 2022.

[89] V. Khullar and H. P. Singh, "f-FNC: Privacy concerned efficient federated approach for fake news classification," *Inf. Sci.*, vol. 639, pp. 1–15, 2023. doi: 10.1016/j.ins.2023.119017.

[90] R. Chhabra, S. Singh, and V. Khullar, "Privacy enabled driver behavior analysis in heterogeneous IoV using federated learning," *Eng. Appl. Artif. Intell.*, vol. 120, no. 5, pp. 1–34, 2023. doi: 10.1016/j.engappai.2023.105881.

[91] A. Hard *et al.*, "Federated learning for mobile keyboard prediction," 2018. Accessed: Oct. 23, 2023. [Online]. Available: http://arxiv.org/abs/1811.03604

[92] Z. Xu, F. Yu, J. Xiong, and X. Chen, "Helios: Heterogeneity-aware federated learning with dynamically balanced collaboration," in *Proc. Des. Autom. Conf.*, San Francisco, CA, USA, 2021, pp. 997–1002.

[93] J. Konečný, H. B. McMahan, F. X. Yu, P. Richtárik, A. T. Suresh, and D. Bacon, "Federated learning: Strategies for improving communication efficiency," 2016. Accessed: Oct. 23, 2023. [Online]. Available: http://arxiv.org/abs/1610.05492

[94] C. Wu, F. Wu, L. Lyu, Y. Huang, and X. Xie, "Communication-efficient federated learning via knowledge distillation," *Nat. Commun.*, vol. 13, no. 1, pp. 1–7, 2022. doi: 10.1038/s41467-022-29763-x.

[95] W. Liu, L. Chen, Y. Chen, and W. Zhang, "Accelerating federated learning via momentum gradient descent," *IEEE Trans. Parallel Distrib. Syst.*, vol. 31, no. 8, pp. 1754–1766, 2020. doi: 10.1109/TPDS.2020.2975189.

[96] J. Liu *et al.*, "RL/DRL meets vehicular task offloading using edge and vehicular cloudlet: A survey," *IEEE Internet Things J.*, vol. 9, no. 11, pp. 8315–8338, 2022. doi: 10.1109/JIOT.2022.3155667.

[97] Y. Shen, S. Shen, Q. Li, H. Zhou, Z. Wu and Y. Qu, "Evolutionary privacy-preserving learning strategies for edge-based IoT data sharing schemes," *Digi. Commun. Netw.*, vol. 9, no. 4, pp. 906–919, 2023. doi: 10.1016/j.dcan.2022.05.004.

[98] X. Xu *et al.*, "PSDF: Privacy-aware IoV service deployment with federated learning in cloud-edge computing," *ACM Trans. Intell. Syst. Technol.*, vol. 13, no. 5, pp. 1–22, 2022. doi: 10.1145/3501810.

[99] L. P. A. Brecko and I. Zolotová, "Brief overview of edge AI accelerators for energy-constrained edge," in *Int. Symp. Appl. Mach. Intell. Inf. (SAMI)*, Poprad, Slovakia, 2022.

[100] J. He, S. Guo, M. Li, and Y. Zhu, "AceFL: Federated learning accelerating in 6G-enabled mobile edge computing networks," *IEEE Trans. Netw. Sci. Eng.*, vol. 10, no. 3, pp. 1364–1375, 2023. doi: 10.1109/TNSE.2022.3190330.

[101] J. Feng, W. Zhang, Q. Pei, J. Wu, and X. Lin, "Heterogeneous computation and resource allocation for wireless powered federated edge learning systems," *IEEE Trans. Commun.*, vol. 70, no. 5, pp. 3220–3233, 2022. doi: 10.1109/TCOMM.2022.3163439.

[102] M. Tahir and M. I. Ali, "On the performance of federated learning algorithms for IoT," *Internet Things*, vol. 3, no. 2, pp. 273–284, 2022.

[103] S. P. Karimireddy, S. Kale, M. Mohri, S. J. Reddi, S. U. Stich and A. T. Suresh, "SCAFFOLD: Stochastic controlled averaging for federated learning," in *37th Int. Conf. Mach. Learn.*, 2020, vol. 119, pp. 5088–5099.

[104] Z. Zhang, Z. Gao, Y. Guo, and Y. Gong, "Scalable and low-latency federated learning with cooperative mobile edge networking," *IEEE Trans. Mob. Comput.*, vol. 41, no. 5, pp. 1–26, 2022. doi: 10.1109/TMC.2022.3230853.

[105] D. Ye, R. Yu, M. Pan, and Z. Han, "Federated learning in vehicular edge computing: A selective model aggregation approach," *IEEE Access*, vol. 8, pp. 23920–23935, 2020. doi: 10.1109/ACCESS.2020.2968399.

[106] M. Adnan, S. Kalra, J. C. Cresswell, G. W. Taylor, and H. R. Tizhoosh, "Federated learning and differential privacy for medical image analysis," *Sci. Rep.*, vol. 12, no. 1, pp. 1–10, 2022. doi: 10.1038/s41598-022-05539-7.

[107] M. Aggarwal *et al.*, "Privacy preserved collaborative transfer learning model with heterogeneous distributed data for brain tumor classification," *Int. J. Imaging Syst. Technol.*, vol. 34, pp. 1–16, 2023.