Federated learning for 6G-enabled secure communication systems: a comprehensive survey

Deepika Sirohi[1] · Neeraj Kumar[1,2,3,7] · Prashant Singh Rana[1] · Sudeep Tanwar[4] · Rahat Iqbal[5] · Mohammad Hijjii[6]

Abstract

Machine learning (ML) and Deep learning (DL) models are popular in many areas, from business, medicine, industries, healthcare, transportation, smart cities, and many more. However, the conventional centralized training techniques may not apply to upcoming distributed applications, which require high accuracy and quick response time. It is mainly due to limited storage and performance bottleneck problems on the centralized servers during the execution of various ML and DL-based models. However, federated learning (FL) is a developing approach to training ML models in a collaborative and distributed manner. It allows the full potential exploitation of these models with unlimited data and distributed computing power. In FL, edge computing devices collaborate to train a global model on their private data and computational power without sharing their private data on the network, thereby offering privacy preservation by default. But the distributed nature of FL faces various challenges related to data heterogeneity, client mobility, scalability, and seamless data aggregation. Moreover, the communication channels, clients, and central servers are also vulnerable to attacks which may give various security threats. Thus, a structured vulnerability and risk assessment are needed to deploy FL successfully in real-life scenarios. Furthermore, the scope of FL is expanding in terms of its application areas, with each area facing different threats. In this paper, we analyze various vulnerabilities present in the FL environment and design a literature survey of possible threats from the perspective of different application areas. Also, we review the most recent defensive algorithms and strategies used to guard against security and privacy threats in those areas. For a systematic coverage of the topic, we considered various applications under four main categories: space, air, ground, and underwater communications. We also compared the proposed methodologies regarding the underlying approach, base model, datasets, evaluation matrices, and achievements. Lastly, various approaches' future directions and existing drawbacks are discussed in detail.

Keywords Blockchains · Distributed computing · Encryption · Federated learning · Machine learning · Privacy · Security

✉ Neeraj Kumar
neeraj.kumar@thapar.edu

Extended author information available on the last page of the article

1 Introduction

Machine Learning (ML) has revolutionized modern computing by allowing computers to learn without explicit programming. An ML algorithm trained on massive data can learn, self-teach, and evolve as intelligent entity. The essence of achieving this intelligence is hidden in the data provided to the model for training. The more versatile the data better is the learning. Today, data availability is not an issue anymore because most people carry their smart personal computing devices, such as smartphones, tablets, etc., all the time, equipped with sensors (cameras, GPS chips, microphones, etc.) continuously producing a bulk amount of data. Hence, access to a huge amount of data is needed to build a reliable ML model.

Conventionally, ML models are trained in a centralized manner, where algorithm and training data are stored on a single machine or server. But, this approach has challenges, like the computational power of the central machine and security and privacy concerns of the data collected from various users or organizations. Harvesting this massive amount of data to a central server is a costly process involving risks and responsibilities. Moreover, the risk of central server failure and data breaches is also there. Also, this centralized system needs to be more transparent to the end-users, leading to a lack of trust in the system.

Recently, few companies have been found listening to the conversation of their end-users for collecting datasets to analyze their client's behaviors. After such practices by these organizations, end-users are now very much concerned with their data's security and privacy. Therefore, they are only willing to share it with guaranteed assurance. Federated Learning (FL) has recently emerged as a solution proposed by Google Research (Konečnỳ et al. 2016) to overcome all the challenges mentioned above in the traditional ML training approach. FL is a distributed training framework for ML and DL models, where the model is shared with all the clients or edge devices participating in the training of a model on their local and private data (Bonawitz et al. 2019; Yang et al. 2019). After training, all clients send their model updates to the cloud-based central server for aggregation into a trained global model. This process continues in rounds till the model converges or achieves the required accuracy.

In this way, clients' private data do not leave their devices, and it assures them security and privacy. However, FL is still in its initial stages and needs more research to be carried out to confirm the assurance it is offering and pave a pathway for its mass application (Ma et al. 2020a).

Because of the unknown security and privacy implication, FL still needs more trust in the community for its widespread use in various applications. On the other hand, because of the privacy-preserving offers made by FL, it attracts multiple domains dealing with sensitive data, like banks, pharmaceutical companies, medicine, hospitals, etc. Organizations today want to keep their private data private and wish to exploit the capabilities of ML models. Therefore, the primary focus is on investigating all these possible privacy and security attacks in this new FL environment to ensure that it gets a fair chance to show its true potential in various domains (Li et al. 2019). Research work based on FL has recently gained much attention in providing solutions for the above concerns in many different application areas. Several survey papers are also available, focusing on security, privacy, or both. So, our survey paper is useful because it is not restricted to any specific field, area, or domain. Instead, it explores security and privacy concerns in FL deployed in space (satellites), air (UAV, radios, etc.), ground (IoT, mobile devices, etc.), and underwater (sea, rivers, etc.) communications Fig. 1.
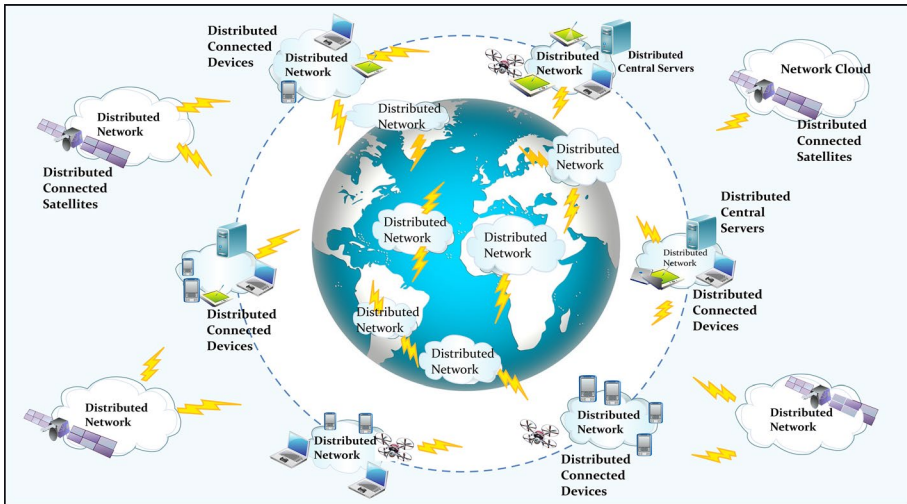
Fig. 1 FL is an evolving training framework for ML and DL models where smart computing devices such as a tablet, smartphones, laptops, etc., connected in a distributed manner via the internet or WiFi, come together in collaborative learning. It is attracting lots of attention from industry and researchers in various application areas giving it universal applicability

Figure 2 highlights some potential application domains currently deploying FL. It is evident from the diagram that the scope of FL is widespread, including industries, telecommunications, IoTs, pharmaceuticals, healthcare, smart farming, defense, smart city, satellite/terrestrial communication, ground and air-based transportation, ocean management, and many more Kumari et al. (2021). From the diagram, we can understand the global scope of FL, and it is impossible to capture the entire scenario in simple words. Therefore, we categorized the applications into four major domains, namely, space, air, ground, and underwater application areas. The significant applications belong to the ground domain. The air, space, and underwater domains still need to be explored, but research is also happening in these domains. The applications in one domain communicate and coordinate with other domains, such as satellites sending and receiving communications from earth stations. Similarly, drones communicate with their base stations on the ground. Air-based transportation is also controlled from the ground, and unmanned aerial vehicles can be used for disaster management on earth and at sea. Smart sensors play a crucial role in implementing FL, which can be installed anywhere, from the sea, rivers, industrial chimneys, homes, buildings, vehicles, roadsides, and many more, to collect huge amounts of information. With the huge amount of useful information and processing from edge devices, FL is overcoming many issues present in earlier systems. One of the major issues is the security and privacy of the participating participants in FL. This article comprehensively explored the majority of the work done by the researchers in resolving major privacy and security concerns in the FL environment.

1.1 Research contributions

FL has recently attracted a lot of attention and has scope in various application areas, as shown in Fig. 2. But, being a new technology, a considerable gap exists between the

theoretical concept and its actual realization. Much research is going on to fill this gap and its successful realization with trust. In this paper, we focused on security and privacy in FL to enhance the trust factor in this new technology. Therefore, researchers are working in this direction to fill these gaps for its successful realization with trust. This paper explores the basic concepts of FL, major threats, vulnerabilities, and various defenses proposed by the researchers to cope with them. Figure 4 shows the introductory terminology covered. And the major contributions of the paper are as follows.

- We discuss the basic concept of FL, its architecture, needs, platforms, approaches, and techniques for introducing and understanding the topic.
- We explore and analyze major vulnerabilities, attacks, and threats in FL that hinders its successful mass adoption.
- We investigate and present an in-depth systematic survey of various privacy and security threats and the recent defensive strategies proposed to defend against them. We covered as many applications as possible and sorted them under the broad spectrum of space-based, air-based, ground-based, and underwater-based domains.
- Finally, we discuss the significant challenges and future research directions in the security and privacy of FL.

1.2 Organization

The proposed survey is organized as follows. Section 1 gives the introduction to the article. Section 2 discusses the research approach used for this comprehensive survey. Section 3 covers the basic concept, architecture, approaches, and technologies that need to understand before going into depth. Also, this section discusses the major vulnerabilities that FL is facing in its deployment. Section 4 explores security and privacy concerns in FL. Section 5 discusses the work done by various researchers over the years to defend against security breaches and privacy threats in FL, covering almost every application area in space, air, ground, and underwater. Finally, Sect. 6 concludes the paper with future directions for further enhancing security and privacy in FL. Figure 3 shows the section-wise distribution of the paper.

2 Materials and methods

This section discusses the statistics and research questions that helped and inspired me to carry out and shape this survey article. The inclusion and exclusion criteria followed to finalize the research papers and search strings are also discussed. Finally, compare our work with a few other survey articles in the area.

2.1 Some statistics

FL has attracted a lot of attention from researchers in recent years. Figure 5 shows the pattern of the publications in the leading journals during the last decade, and the distribution of the publications based on security and privacy in various application areas deploying FL followed in this article.

2.2 Research questions

Google Scholar, IEEE Xplore, SpringerLink, and ACM digital libraries have been used to find research articles. The process to identify the potential research articles, screening, and eligibility criteria are followed as shown in Fig. 6. Furthermore, Table 2 lists the research questions followed to search the articles. More than two hundred research papers have been included in our survey from January 2016 to September 2022.

2.3 Search string

For the comprehensive analysis of the security and privacy in FL, the search was based on keywords like "security in federated learning," "privacy in federated learning," "federated learning in space," "federated learning for terrestrial communication," "federated learning in oceans/rivers," "federated learning in healthcare" and so on. Initially, 650 research articles in FL were shortlisted. Figure 6 shows the screening criteria followed for the final selection of the papers for our survey article. Table 1 lists the major abbreviations used in the article.

2.4 Comparison with other survey articles

FL is a new research area with several survey papers that focus on introducing the concept and the direction in which the research is going. A few papers also focus on the privacy and security aspects of FL. Mothukuri et al. (2021) provided a comprehensive study on privacy and security issues and their impact on the FL environment. They listed the major privacy and security threats and their proposed countermeasures. They included the basic introduction to this new concept, including definition, architecture, vulnerabilities, and frameworks. They also discussed the future directions for the mass adoption of FL in real-life scenarios. In another work, Blanco-Justicia et al. (2020) surveyed the proposed privacy and security solutions and evaluated them to compare their performance. They also analyzed the privacy and security issues independently as well as together. They concluded that achieving them together is challenging and an open problem in FL.

On the other hand, Truong et al. (2020) focused only on privacy preservation in FL regarding GDPR requirements. They examined the existing challenges in deploying different approaches in FL to comply with GDPR guidelines. These guidelines suggested that strong cryptographic privacy primitives must be developed to make the FL system fair, interpretable, and unbiased. Similarly, Enthoven and Al-Ars (2020) also focused on privacy and discussed the FL system's vulnerabilities to insider attacks. They also identified the major threats in the literature and categorized them based on their characteristics, such as active/passive, white/black box, and goals. And finally, they listed the defensive mechanisms to protect the system against those attacks. Lyu et al. (2020b) also provided an overview of privacy and robustness threats to FL, along with their defense strategies. They aimed to provide a concise summary of the topic that can help guide the research community toward robust privacy-preserving FL system design. In contrast, Mao et al. (2021) discussed security and privacy concerns in FL. The article briefly listed the major privacy-preserving techniques and suggestions for future work. Bouacida and Mohapatra (2021) also comprehensively surveyed vulnerabilities in the

Table 1 List of Key Abbreviations

Abbreviation	Definition
AI	Artificial Intelligence
CFL	Centralized Federated Learning
CNN	Convolutional Neural Network
DFL	Decentralized Federated Learning
DL	Deep Learning
DNN	Deep Neural Network
DP	Differential Privacy
FL	Federated Learning
FTL	Federated Transfer Learning
GDPR	General Data Protection Regulations
GAN	Generative Adversarial Networks
HE	Homomorphic Encryption
HRL	Horizontal Federated Learning
IID	Independent and Identically Distributed Data
IIoT	Industrial Internet of Things
ISTN	Intelligent Satellite Terrestrial Network
IoT	Internet of Things
IoUT	Internet of Underwater Things
IoV	Internet of Vehicles
LSTM	Long-short Term Memory
ML	Machine Learning
MEC	Mobile Edge Computing
NIDS	Network Intrusion Detection System
NN	Neural Network
non-IID	Non-independent and Identically Distributed Data
P2PFL	Peer-to-Peer Federated Learning
RNN	Recurrent Neural Networks
SMC	Secure Multiparty Computation
UAV	Unmanned Aerial Vehicle
VFL	Vertical Federated Learning

FL ecosystem. They systematically classified the major threats and discussed them in detail. Although the above-reviewed survey papers provide a comprehensive introduction to FL with a promising analysis of various threats with the existing solutions, they have yet to consider different applications' perspectives for security and privacy. Our survey paper introduces the concept of FL, its architecture, frameworks, vulnerabilities, adversaries, and threats. Then provide a comprehensive survey of the proposed solutions in various applications areas categorized as space-based, air-based, ground-based, and underwater-based areas. Table 3 compares our work with other survey articles based on the research questions listed in Table 2.
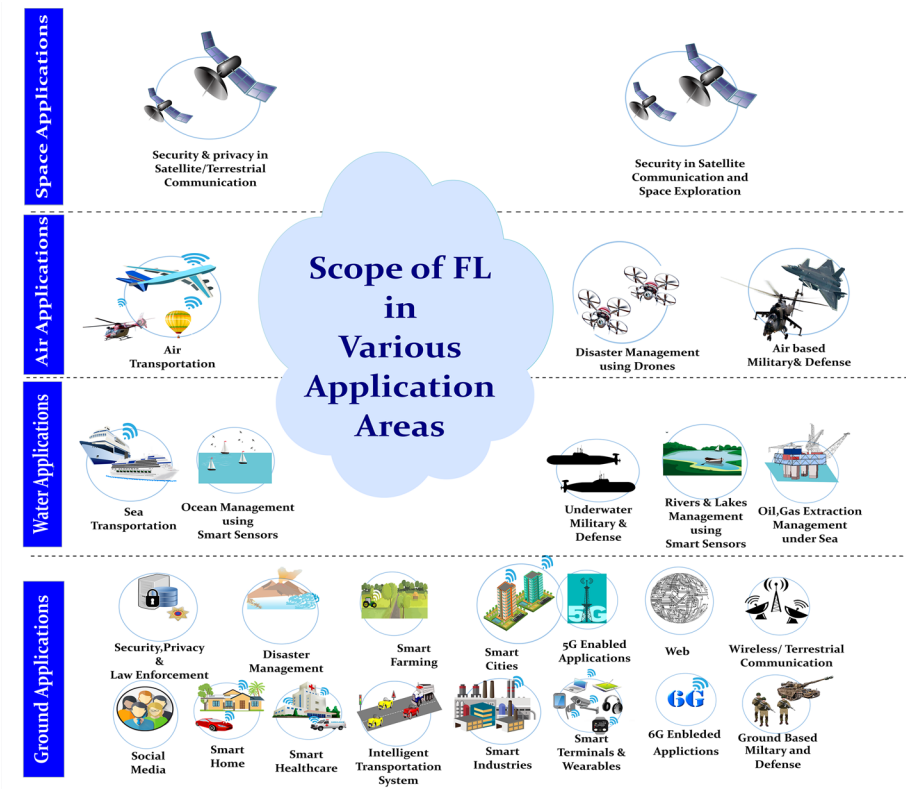
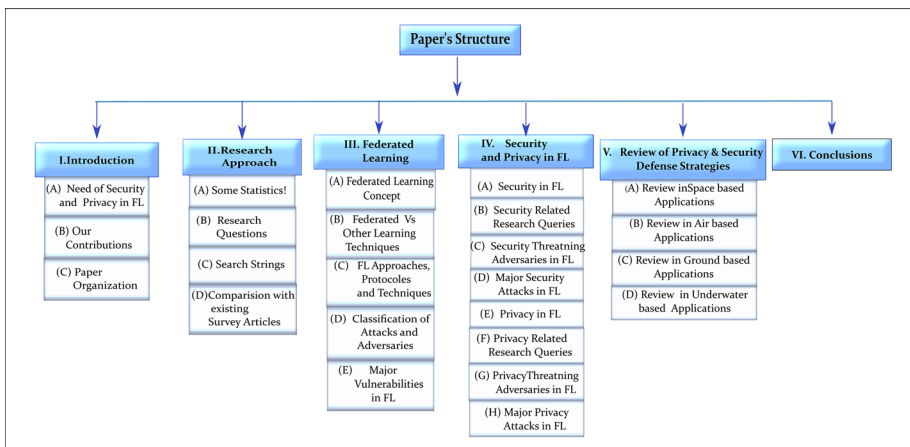**Fig. 2** Potential applications that are deploying FL
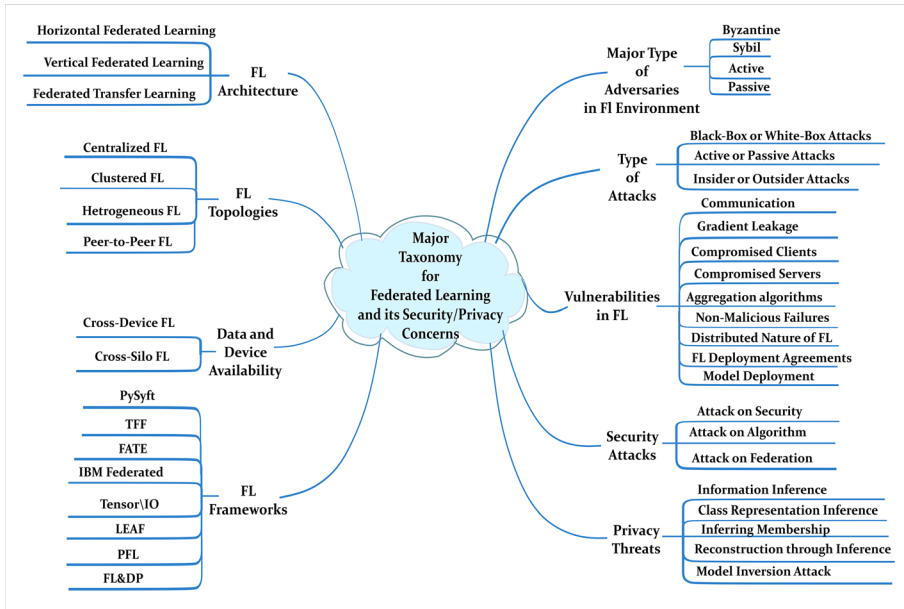

Fig. 3 Section-wise organization of the paper

Fig. 4 The major taxonomy for the basic FL concept, vulnerabilities, threats
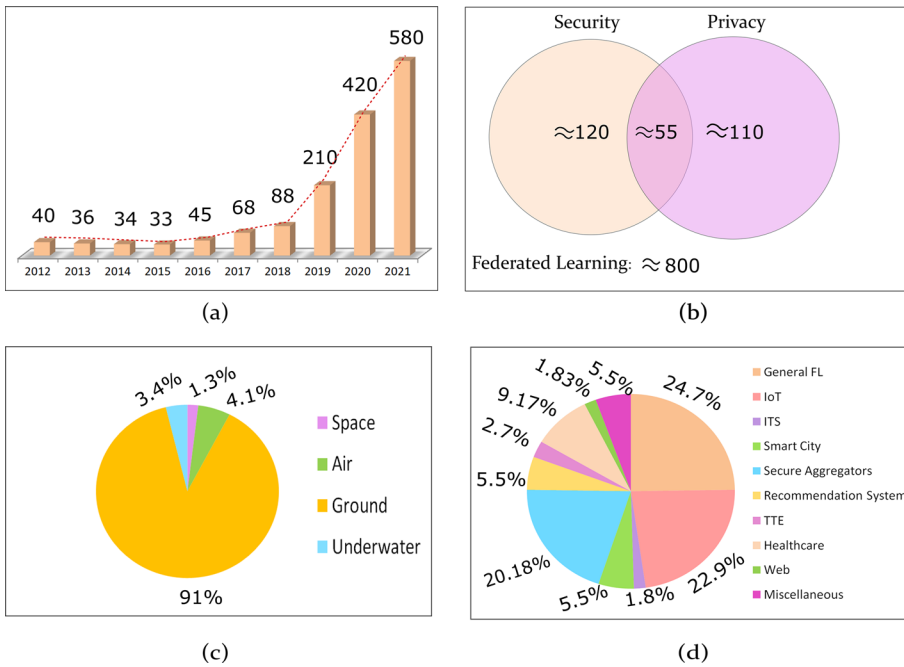

Fig. 5 **a** Publication pattern in FL over recent years. **b** Vann diagram represents the distribution of publication in security and privacy in FL. **c** Distributions of papers in various domains deploying FL in this survey. **d** Further distribution of publications in security and privacy in ground-based application areas deploying FL in this article

Fig. 6 Inclusion and exclusion criteria followed to finalize research papers for the article
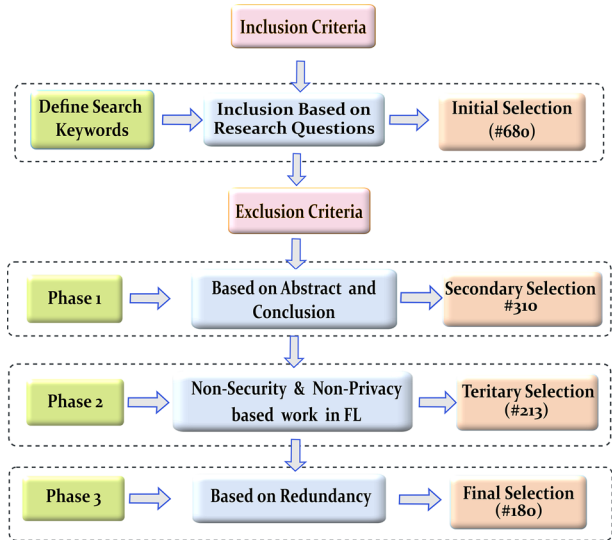
3 Basics of federated learning

This section discusses the basic concept of FL, its comparision with other distributed learning approaches, the underlying topologies, major architecture, and frameworks for a better understanding. The major security and privacy threats, adversaries, and vulnerabilities are discussed before diving deep into security and privacy discussions.

3.1 Federated learning: concept

FL (also known as collaborative learning) is an emerging, fast-growing research field that provides a distributed training framework for ML and DL models while preserving privacy (Rahman et al. 2020a). FL has attracted much attention from researchers working in different domains to exploit its potential and applicability. FL has emerged as a solution to all the challenges in training ML and DL models using a traditional centralized approach. It involves uploading the model and data to a centralized server and performing the training process. This approach comes with many burdens on the centralized server to store enormous data for training, powerful computation capabilities, and world-class security measures to protect data from breaches. A single central server machine for training can be a bottleneck for the entire system in case of failure.

In contrast to this, FL offers a way to train the model in a distributed manner by decentralizing the data and computation capabilities from a central server to the edge-computing devices (such as tablets, IoT devices, smartphones, PCs, smart wearables, etc.) and giving an additional benefit of providing privacy to the data (no need to transfer data to the central server now). In FL, the model is trained at the device level, where a central server orchestrates the entire training process. The selected model with initial parameters is distributed among a selected group of clients (edge devices) for training on their private data (Li et al. 2019). After completing the training, the parameters of

Table 2 Research questions and their objectives

S. no.	Research questions	Objectives
Q1	What is FL and its need?	The purpose is to understand the FL concept
Q2	How FL is different from distributed learning or shared memory learning?	It aims to provide a better understanding of the underlying concept
Q3	How FL approach is useful for ML and DL models?	This helps to understand the scope of FL in exploiting the full potential of ML and DL models
Q4	What are the major architectures, topologies, frameworks used for implementing FL?	The purpose is to provide the readers proper details of all the necessary concepts and terminology related to FL necessary to understand before going into depth
Q5	What are the major vulnerabilities in the FL environment?	It aims to explore the FL environment for the weakness in the system that helps to manage and defend against the threats
Q6	What are the major security threatening adversaries in FL environment?	Its main purpose is to know and be aware of the agents who are part of the system yet can carry out attacks on the system
Q7	What are the major security attacks/threats in FL environment?	To get aware of the majority of the security threats that surfaced in the FL the environment that is necessary to safety against them
Q8	What are the major privacy threatening adversaries in FL?	To be aware of all the adversaries that can be a threat to the privacy of FL clients
Q9	What are the major privacy threats in FL environment?	Its aim is to understand the privacy threats that are possible in FL environment
Q10	What are the major application areas that are deploying FL in space, air, ground, and underwater communications?	The purpose is to explore all possible application areas in which FL has a scope for deployability
Q11	What are the major security and privacy issues faced by various applications deploying FL and the measures employed to tackle them?	The aim is to explore all possible security and privacy threats surfaced in FL the environment in various applications to design more secure and privacy-preserving system
Q12	What are the challenges and future directions for further enhancing security and privacy in the FL environment?	The purpose is to provide challenges and future research directions to further enhance security and privacy of FL environment

Table 3 Comparision with existing surveys based on the research question in Table 2

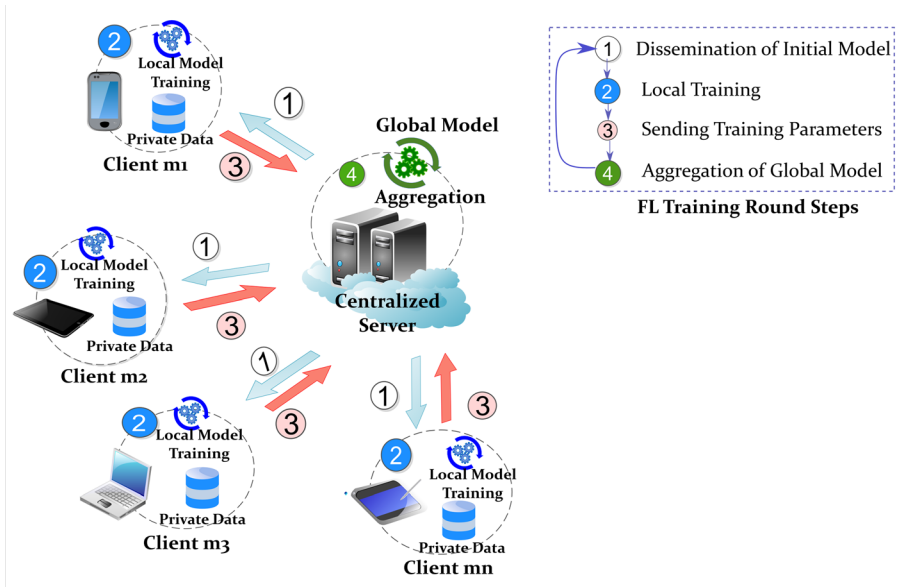| Survey paper	Year	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12
Mothukuri et al. (2021)	2021	●	●	○	●	●	○	●	○	●	○	○	○
Blanco-Justicia et al. (2020)	2020	●	○	○	○	○	●	●	●	●	○	○	○
Truong et al. (2020)	2020	●	●	○	○	○	○	○	○	●	○	○	○
Mao et al. (2021)	2021	●	○	○	○	○	○	●	○	●	○	○	○
Bouacida and Mohapatra (2021)	2021	●	●	○	●	●	○	●	●	◯	○	○	○
Enthoven and Al-Ars (2020)	2020	●	●	○	○	○	○	○	●	●	○	○	○
Lyu et al. (2020b)	2020	●	●	○	○	○	○	○	●	●	○	○	○
Ours	–	●	●	●	●	●	●	●	●	●	●	●	●

Fig. 7 Centralized FL training process

trained models are sent back to the central server for aggregation into a global model, making it one complete round of the training process. This consolidated model is distributed again to another set of clients for the next round of training. The entire process is repeated until the model either converges or gives the desired results. Figure 7 and Fig. 8 shows the training process for centralized and peer-to-peer FL environments, respectively.

FL training process is carried out iteratively in rounds, where each round typically consists of the following steps.

1. *Selection and Initialization of Global Model* In this first step, the central global model (DL model, regression model, etc.) is selected and initialized with initial parameters ready to be shared with the clients in the FL network.
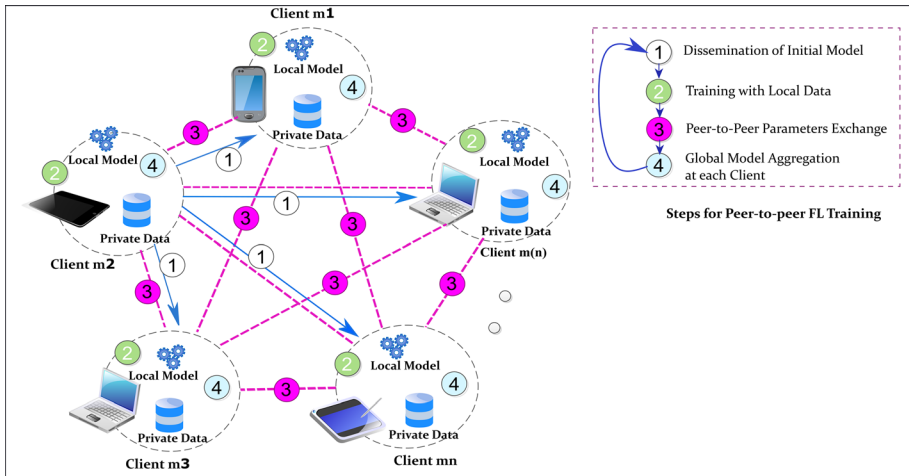
Fig. 8 Peer-to-Peer FL training

2. *Participants/Client Selection* The clients are selected based on the trust factor, meeting some eligibility criteria or client selection strategies (Tao and Li 2018) among the clients willing to contribute. The remaining clients wait for the next round.

3. *Dissemination of the Initial Model* Central cloud-based server broadcasts the model to the selected clients in the FL network.

4. *Local Training* Selected clients undergo training on their local dataset and update the model.

5. *Aggregation or Reporting of the Local Models* Each client sends their local model updates to the central server for global aggregation. Once the aggregation is done, this improved model is shared with the clients for further improvement in the next round. The next round takes us back to the second step, i.e., client selection.

6. *Final Update and Termination* The above steps (2–5) are iteratively carried out till either model converges, reaches some desired accuracy level, or meets some termination criteria.

The number of clients participating in each round is referred to as concurrency. The FL training proceeds in rounds and can be either synchronous or asynchronous. In synchronous FL (synFL), once all client updates are received, the server computes the new model aggregation. But it faces two major challenges, heterogeneity and concurrency size. The clients participating in training have cross-device heterogeneity (varying memory size, processor speed, etc.) and imbalanced data that results in stragglers (slowest-responding clients). They slow down the overall round completion. So, an over-selection method is used to discard the stragglers, which may result in biased training. Another challenge in synFL is the concurrency size. Increasing the size of participating clients slows down the model convergence, and reducing the size results in biased and non-generalized training.

Asynchronous FL (asynFL) can be a potential solution to alleviate the challenges with synFL. The client can send the updates as soon as they are ready, and a new client may then begin computing updates immediately. The clients are decoupled from the server model updates, thereby not affected by stragglers. But, it faces the challenge of staleness, where slow updates received later in training may not provide any valuable

information for training. The authors in Huba et al. (2022) proposed a system design to alleviate the challenges of synFL and compared it with another asynFL system design. They demonstrated that asynFL converges faster than synFL in a system with nearly a million devices. Few other authors have focused their work in this direction to propose different FL architectures to overcome major issues (Kulkarni et al. 2020; Geiping et al. 2020b; Yang et al. 2019; Feng and Yu 2020). There is also a middle-ground solution called semi-synchronous FL. The participating devices train the ML model locally up to a certain synchronization point where the global model is calculated, resulting in lower communication costs and better resource utilization. In another work, Qin and Kondo (2021) proposed a novel multi-local and multi-global model aggregation mechanism (MLMG) in FL. They used non-iid user data with clustering methods for training and a matching algorithm for appropriate exchanges between local and global models.

3.2 Federated learning vs. other learning techniques

3.2.1 Distributed learning

FL is a distributed approach for ML training, then the question arises: How is FL different from distributed learning? Well, distributed learning focuses on parallelizing the computing power by training a model on multiple servers (typically data centers) with powerful computational capabilities connected via high-speed links, which are available at all times, making it a reliable system. The important thing to notice here is that the datasets are identically distributed (iid) throughout the network, roughly having the same size.

On the other hand, FL involves a network of unreliable clients subjected to dropouts or failure at any time, as they are small devices with less computational power, battery-powered systems (tablets, smartphones, etc.), and are on less powerful communication media (like WiFi). In FL, the underlying dataset on these clients is heterogeneous and varies in size, i.e., datasets are non-identically distributed (non-iid) throughout the FL network. These are the fundamental differences between the FL and distributed learning concepts necessary to understand before going into depth.

3.2.2 Shared machine learning

Shared machine learning (SML) is another recent learning paradigm that protects participants' data differently than FL. FL is based on a "federation," where the identities and statuses of the participants are the same. On the other hand, in SML, the participants work in scenarios where they do not trust each other, and different participants have different roles. In FL, data does not leave the clients' side, thereby providing default privacy by design. But, in SML, data is transferred to cloud storage in an encrypted form using special encryption tools Verma et al. (2022). SML uses two main data sharing technologies, trusted execution environment (TEE) and multi-party computation (MPC), to solve privacy leakage and data abuse. TEE-based SML uses a third-party hardware environment for secure data transfer and training of ML models Khatri et al. (2021). On the other hand, MPC-based SML provides secure sharing, operations, and algorithms through a layered framework. Both distributed solutions based on MPC and centralized solutions based on TEE are available for model training and predictions.
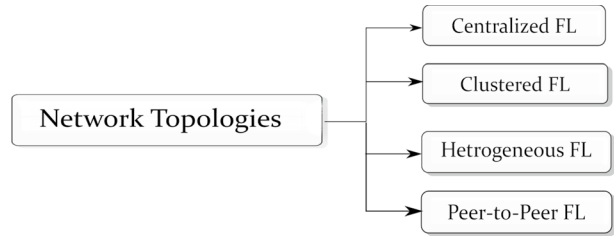
3.3 Federated learning underlying approaches, protocols, and techniques

FL is a recently introduced technology with its true potential yet to be discovered. Nevertheless, it has attracted a lot of attention from different fields. Numerous researchers have been deploying it in a variety of applications ranging from medical (Rieke et al. 2020; Schneble and Thamilarasu 2019), mobile applications (Beaufays et al. 2019; Hard et al. 2018; Yang et al. 2018; Ramaswamy et al. 2019), IoTs (Nguyen et al. 2021b), transportations (Lu et al. 2020d; Samarakoon et al. 2018), defense (Cirincione and Verma 2019) and many more.

Now, before we go deeper into the privacy and security aspects and explore the big picture, it is necessary to understand the underlying framework, architecture, techniques, and various approaches that make FL implementation possible. This section gives a thorough overview of the FL implementation aspects to help us understand all the basic terminologies needed to go deeper in later sections.

3.3.1 Network topologies

Network topology defines the underlying architecture of the FL networks and how various components are interlinked together to form the FL environment. Some of the widely used network topologies are shown in Fig. 9 and discussed.

(a) *Centralized FL* In this setting, a centralized server is responsible for organizing, managing, and coordinating the entire training process among all the participants, as shown in Fig. 7. All the clients respond to this central server. Being the main controlling authority, any failure to it results in the collapse of the entire FL network, thereby becoming a bottleneck for the whole system (Kairouz et al. 2019). The central node also suffers from high communication costs.

(b) *Clustered FL* Clustered FL addresses the data heterogeneity among different clients in a centralized topology, where the server creates clusters of clients with similar data distributions. Furthermore, an intermediate model is created for each cluster to jointly participate in training and help in faster global model convergence (Sattler et al. 2020; Ghosh et al. 2020). The main challenge in clustered FL is to identify the cluster membership, as the cluster identities of the users are unknown, which is necessary information to optimize models for clusters in distributed settings.

(c) *Decentralized FL or Peer-to-Peer FL* In decentralized FL, clients directly communicate with one another instead of any central authority, as shown in Fig. 8. A group of clients with a common goal collaborate to improve their models by sharing information from peer to peer. There is no single-point failure, but the performance may be affected by

Fig. 10 Data and device availability in FL
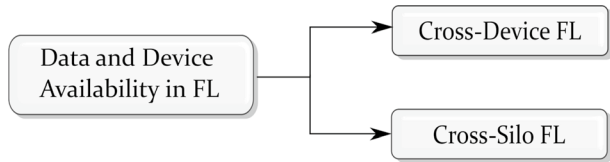
how clients are interconnected (Vanhaesebrouck et al. 2017; Lalitha et al. 2019). Lian et al. (2017) demonstrate the advantage of decentralized topology in terms of speed-ups and scalability over centralized topology. The potential challenge with the decentralization approach lies in the synchronization cost, which needs further exploration.

(d) *Heterogeneous FL* FL faces the challenge of heterogeneity in the network and suffers an accuracy drop in the aggregated global model. This is because FL networks have to deal with highly non-iid (non-identically distributed) data with varying computational and communication capabilities across the nodes. Recently, a new federated framework known as HetroFL (Diao et al. 2020) was introduced to deal with heterogeneity in the FL environment. The HetroFL-based techniques are regulation methods that dynamically adjust the task distribution and local model architecture according to the feature-level data distributions and computational capability of heterogeneous clients at the early training stages. This new framework showed enhanced performance and applicability of FL even in extensive heterogeneous settings (Yu et al. 2020b).

3.3.2 Data and devices availability

FL employs a central server architecture where the server acts as the orchestrator of the entire training process. After training on the client's local data, the server iteratively collects the model updates from remote and distributed clients and finally aggregates them into a refined model. Based on the availability of data and remote devices, two major settings for FL are cross-device FL and cross-silo FL, as shown in Fig. 10.

(a) *Cross-device FL* The cross-device FL consists of a large number (in millions) of unreliable clients (mobile or edge computing devices) with limited computation capability but with similar interests in similar domains. "unreliable clients" means they can drop out of the training process anytime. Also, they share a slow and unreliable communication channel between them. Due to the large number of clients involved, tracking and maintaining all the clients is quite challenging. This setting is generally utilized in IoT-based or mobile-based applications (Yang et al. 2018). Due to the unreliable behaviors of clients, different incentive mechanisms are used to encourage clients to participate in the training (Zhan et al. 2021). Along with client selection strategies (Tao and Li 2018), different device-scheduling algorithms (Chen et al. 2019) are also used for choosing the best-contributing clients among all.

(b) *Cross-silo FL* Cross-silo setting is considered more flexible than cross-device. It consists of a small range (approx. 2–150) of reliable clients (data silos) with powerful computation capability and high-speed connectivity among them that are available almost all the time (that is why reliable). This setting is mainly used within an organization or in organizations interested in training an ML model on their confidential data without sharing it, e.g., banks, pharmaceutical laboratories, hospitals (Silva et al. 2019), etc. In cross-silo, reliable clients with better computing power and high-speed links enjoy faster information exchange than the central server, which initiated the
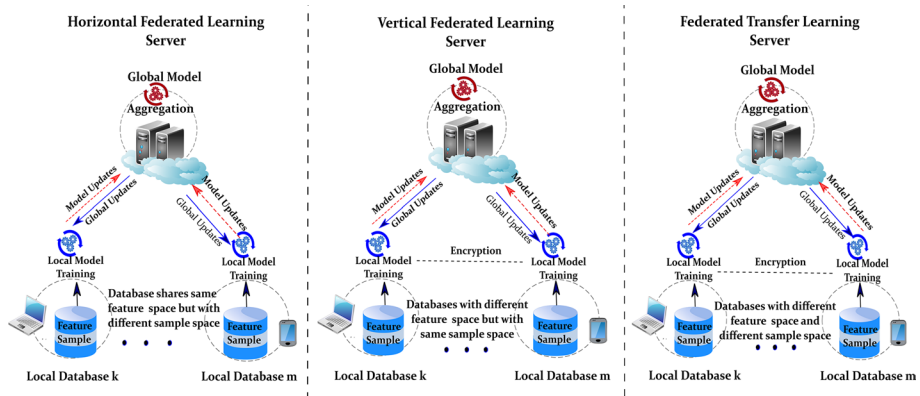
Fig. 11 Major FL architecture

training, making the entire setting inefficient and a candidate for congestion. Marfoq et al. (2020) proposed a throughout-optimal topology design for cross-silo FL, which guarantees better throughput. In another work, Zhang et al. (2020d) used homomorphic encryption (HE) to propose a batch encryption algorithm for reduced communication and computation cost in cross-silo FL.

3.3.3 Major architecture and platforms of federated learning

Despite being a new technology, only some platforms and architectures are available in FL. Many medical institutions and leading universities like Intel and the University of Pennsylvania are trying to develop an efficient FL architecture (Bonawitz et al. 2019; Cheng et al. 2021). FL is a distributed approach; client data distribution is critical. Yang et al. (2019) categorized FL architectures into three major categories as, Horizontal FL (HFL), Vertical FL (VFL), and Federated Transfer Learning (FTL), as shown in Fig. 11. HFL (also known as sample-based FL or Homogeneous Horizontal FL), datasets on different clients share similar features but vary in terms of instances. In other words, when there exists a large overlap in feature space between data sets, HFL architecture is used. The best utilization of this architecture is shown by Google (Hard et al. 2018), where they have used it to predict the next work in a virtual smartphone keyboard.

On the other hand, in VFL (or Feature-based FL), common data with different features (from unrelated domains) is used to train the global model. VFL is used when considerable overlap exists in the sample space between datasets. A third party (not mandatory) can be used that provides encryption logic to ensure that only the common datasets are used for training. Another important architecture is FTL, which uses a similar concept of transfer learning as in ML (Saha and Ahmad 2020). It is a concept in which a pre-trained model trained on some dataset is used to be trained again on a new requirement for solving an entirely different problem. Unlike HFL and VFL, FTL is used only when a small overlap exists between the datasets in both the sample and the feature space. One of the major benefits FTL offers, apart from privacy, is higher accuracy by a minimized error in predicting the target domain. That is the reason FTL is gaining huge attraction from wearable devices (Sun et al. 2020a), electro-encephalographic signal classification (EEG) (Ju et al. 2020),

autonomous driving (Liu et al. 2017; Sirohi et al. 2020; Parekh et al. 2023) to image stega-analysis (Yang et al. 2020).

Indent VFL has yet to be explored. Currently, it can handle two participants and perform binary classification only (Kairouz et al. 2019). Working in this direction, Feng and Yu (2020) proposed a new architecture based on VFL called Multi-Participant Multi-Class Vertical FL (MMVFL), making it suitable for applications involving complex classification tasks and multiple participants. In another work, Cao et al. (2020) proposed a distributed deep-learning framework called FEDF to train powerful DL algorithms geared towards privacy preservation and parallel training on geographically-distributed datasets having the same data distribution. Their proposed architecture consists of a master and worker type of setting. The master handles the training process, and workers are responsible for training a model instance on their data. During training, each worker is responsible for setting parameters such as learning rate, epochs, batch size, etc. These parameters are kept secret from the master and other workers. They developed a terrorizing approach in which workers only inform the master about the evolution of the model without revealing the data samples or gradients, thereby providing enhanced privacy and improved training speed.

Apart from these architecture discussed above, researchers have proposed few other architectures in (Zhao et al. 2020d; Chai et al. 2020; Lu et al. 2020e; Zhou et al. 2020; Hu et al. 2020; Liu 2020; Li et al. 2020b; Kim et al. 2019).

3.3.4 Personalized federated learning

Among many challenges of FL, heterogeneous data is one of the fundamental challenges, a universal characteristic inherent in all real-world datasets in the FL environment. It affects the training process, resulting in poor convergence, deteriorated performance of the global model, and even disincentivizes the clients from joining the training. The performance degradation is attributed to the client drift, in which the server updates move towards the average of client optima. Therefore, the averaged model drifts away from the global optimum and does not converge to its true optimum. Personalized FL (PFL) is the approach focused on handling data heterogeneity in the FL environment (Kulkarni et al. 2020). The goal of learning personalized models is to train a model for each client based on both client's dataset and the datasets of other clients. A model trained by general FL training would predict the same states for every client, which would only be considered an efficient model by some clients. Therefore, PFL gives a personalized touch to the trained model for every client. It is mainly categorized based on two strategies, global model personalization, and learning personalization models, as shown in Fig. 12.

1. *Global Model Personalization* In this strategy, once a global model is trained through general FL training, it is again trained on the local dataset of each client as an FL personalization strategy. Therefore, personalization is a two-step process involving FL training and local adaptation. It is further categorized into two types.

   (i) Data-based approach: It aims to reduce the statistical heterogeneity among clients' datasets, thereby reducing the effects of client drift in global model convergence. A few techniques, such as data augmentation and client selection mechanisms with homogeneous data distributions, are used to reduce the heterogeneity in FL training.

   (ii) Model-based approach: This approach focuses on the improvement of the local adaptation process for a strong future personalization. Regularized local loss, meta-learning, and transfer learning are techniques to improve model personalization.

2 *Learning personalized Models* This strategy is more focused towards training individual personalized FL models instead of personalizing single global models. And this is achieved by modifying the model aggregation process by applying different learning paradigms in FL settings. In this category, personalization can be achieved by following the architecture-based or similarity-based approach.

(i) Architecture-based approach: Personalization is achieved through the customization of the model design tailored to the requirement of each client. This customization is achieved either by layers personalization for each client using the parameter decoupling method or by personalized model architecture using the knowledge distillation method.

(ii) Similarity-based approach: This approach achieves personalization through modeling client relationships with related clients and learning similar models. Model interpolation, multi-task learning, and clusterings are techniques used to identify and group related clients.

Learning a personalized model in an FL environment allows the clients to train models with vast amounts of data for better generalization and privacy protection (Tan et al. 2022; Mansour et al. 2020).

3.3.5 Major frameworks in federated learning

Several popular frameworks exist for researchers and programmers to continue their research in FL.

- Tensorflow Federated (TFF): Google's TFF is one of the first attempts toward bringing FL into actual implementation. It provides a flexible and open framework in Tensorflow API (Federated 2019).
- PySyft: Pysyft is written in Pytorch, a Python library. It provides a virtual hook for connecting clients that uses encryption strategies for enhancing privacy in FL implementation (Openmined).
- FATE: Federated AI Technology Enablers (FATE) is another open-source framework that provides a visual approach (FATE Board) for implementing FL. It allows FedFL implementation in vertical, horizontal, and transfer learning settings (W. A. Department).
- IBM FL: This is another framework in the Python library. The main key point of this framework is its ease to use. It has an extensive library for ML and deep neural network (DNN) implementations (IBM).
- Tensor I/O: This platform helps implement and deploy FL on mobile devices, like Android, iOS and React native applications, etc., using the power of Tensorflow. It can run on Android and iOS phones with multi-language support like Swift, Kotlin, Java, or Javascript (Tensor/IO).
- LEAF: It is another Python-based framework that supports multitasking in FL. This framework provides many datasets for experimentation (LEAF).
- PaddleFL: It is an open-source framework specifically for industrial applications. It offers FL implementation in computer vision (CV), natural language processing(NLP), etc., (PaddlePaddle).

Table 4 Summary of major frameworks and their features for implementing FL

Framework		Focus	Data partitioning	Supporting software/platform	Setting
PySyft (Openmined)	Open-source	Privacy	Horizontal, vertical	Python library	Cross-silo, cross-device
TFF (Federated 2019)	Open-source	Federated learning	Horizontal	Tenser flow	Cross-silo
FATE (W. A. Department)	Open-source	Federated learning	Horizontal, vertical	FATE board	Cross-silo
IBM Federated Learning Fredrikson et al. (2015)	–	Privacy, neural networks	–	Python, Tenser flow	–
Tensor\IO (Tensor/IO)	Open-source	Mobile devices	Horizontal	Tenser flow	–
LEAF (LEAF)	–	Multitasking	Horizontal	Python library	–
Paddle Federated Learning (PFL) (PaddlePaddle)	Open-source	Privacy, deep learning	Horizontal, Vertical	PaddlePaddle	Cross-silo, Cross-Device (in future)
FL and Differential Privacy (FL& DP) (A. A. for everyone)	Open-source	Deep learning	Horizontal	Tenser flow, Scikit-Learn Library	Cross-silo

- FL &DP: The federated learning & differential privacy (FL &DP) framework is another open-source framework. It integrates Tensorflow for DL and the SciKit-Learn library for training linear models and clustering (A. A. for everyone).

Table 4 highlights the main features of these frameworks.

3.3.6 Aggregation algorithm

The aggregation algorithm plays a significant role in the FL environment. These algorithms combine or bind the local updates received from distributed clients after completing their local training in each round. The aggregation algorithm ensures the proper learning of global model parameters from all the clients. Furthermore, the anomaly detection mechanisms incorporated within the aggregation algorithm ensure the convergence of the global model with fairness in a heterogeneous environment (Karimireddy et al. 2020; Li et al. 2018).

3.4 Classification of attacks and adversaries

In general, there are numerous ways and patterns to carry out attacks by different adversaries, as shown in Figs. 13 and 14. Based on this, both attacks and adversaries are classified. This subsection discusses the main categories.

(1) *Types of Attacks* There are three major categories to classify attacks as follows.
    (a) Black-box or White-box Attack If the attacker has complete knowledge of the underlying FL system with full access to the model, it is considered a white-box attack.

In this case, the adversary knows the clear-text model without stored feature vectors. On the other hand, Black-box attacks work without knowing the system, and they can only query the model with inputs and collect the responses. An adversary can reconstruct the model in clear-text form using equation solving attack based on these responses. Theoretically, the adversary can extract knowledge of the complete model in N+1 queries for an N-dimensional linear model. In FL, clients have access to private data and the global model. Therefore a compromised client is vulnerable to white-box attacks. Similarly, the server has access to updated gradients and model descriptions, making it prone to white-box attacks. But in peer-to-peer FL, sometimes the aggregator does not know the model, making the aggregator more towards black-box attacks.

(b) Active and Passive Attacks Active attacks work by changing model parameters or system properties, affecting the normal working of the system. These attacks can corrupt the entire functioning of the system. In addition, these attacks disrupt the normal behavior of the model, creating doubt and, in a sense, are detectable. Passive attacks, on the other hand, do not require any modifications. These attacks leave no traces of their execution, making them dangerous.

(c) Insider vs. Outsider Attacks In an FL environment, an attack can be launched by an insider or an outsider. When an attack is carried out by the clients or the centralized server aggregator, it is considered an insider attack. On the other hand, an outsider attack is carried out by an outside entity of the FL system via a communicational channel such as eavesdropping (silently watching the traffic) or by the end-users of the deployed model.

Types of Adversaries The adversaries carrying out these attacks are further classified into the following categories.

(a) Byzantine Adversary These adversaries have complete knowledge of the system, with unpredictable behavior from passive eavesdropping to an active attack to corrupt the convergence of the global model.

(b) Sybil Adversary: The Sybil adversary in the FL system can counterfeit multiple peers participants or select previously compromised participants to launch a more powerful attack to compromise the global model.

(c) Active Adversary These are malicious adversaries who try to learn participants' private information and manipulate or delete updates/parameters/gradients to deviate the model from its purpose.

(d) Passive adversary These are semi-honest or honest but curious adversaries to observe the received information and infer some useful and private information.

3.5 Major vulnerabilities in federated learning

FL is a new paradigm that emerged as collaborative learning by using data from different organizations to train ML and DL models without sharing their private data. But before taking its applicability to an extensive scale, the FL environment must be analyzed in-depth to discover all the possible attacks and address all the vulnerabilities in the system. A "vulnerability" is the weakness of the system that an attacker can exploit to take advantage of and perform an unauthorized action (Ma et al. 2020a; ISO 2018). Knowledge of FL

Table 5 Major sources of vulnerabilities in FL environment

| Source of vulnerability	Description
Communication channel	An unsafe communicational channel can become a source of easy eavesdropping, attacks and security breaches
Compromised clients	Compromised clients can corrupt the model parameters or poison the training samples
Compromised servers	A compromised server can be a target of several attacks, like denial-of-service, tempering with the aggregation, corruption of received gradients, etc
Gradient leakage	The gradient can leak private information about the local data of the clients
Non-malicious failure	These are non-adversarial factors that affect the system like low bandwidth or limited computation power etc
Aggregation algorithms	A non-robust aggregation make the global model untrustworthy and vulnerable
Distributed nature of FL	The distributed environment is prone to various distributed attacks and colluding attacks to launch a coordinated attack
Model deployment	Adversaries can launch inference-time attacks or create perturbations in test inputs to lower the accuracy of the global model
FL deployment agreements	FL deployment agreements should be pre-decided to deploy FL in real world
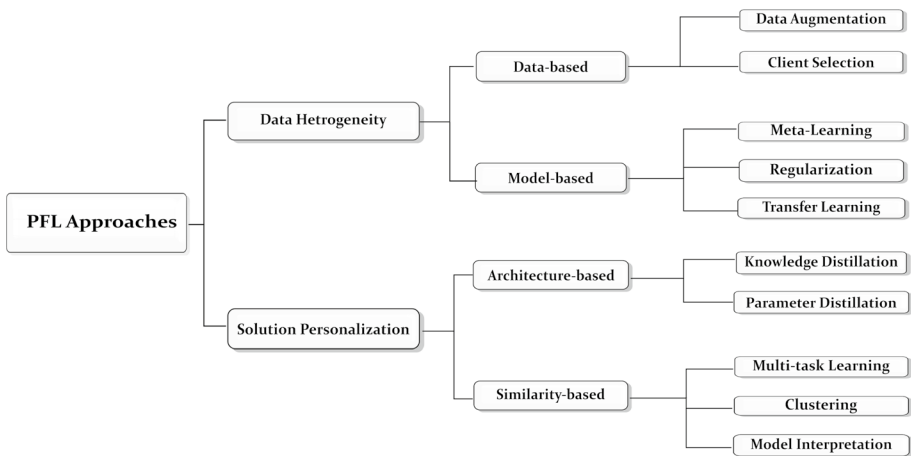
Fig. 12 The main personalized FL strategies

Fig. 13 Major adversaries that act as threat to security/privacy in FL
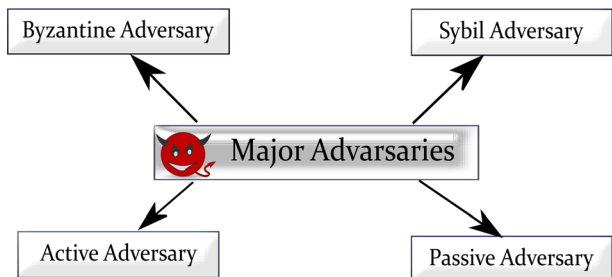
Fig. 14 Major types of attacks in FL
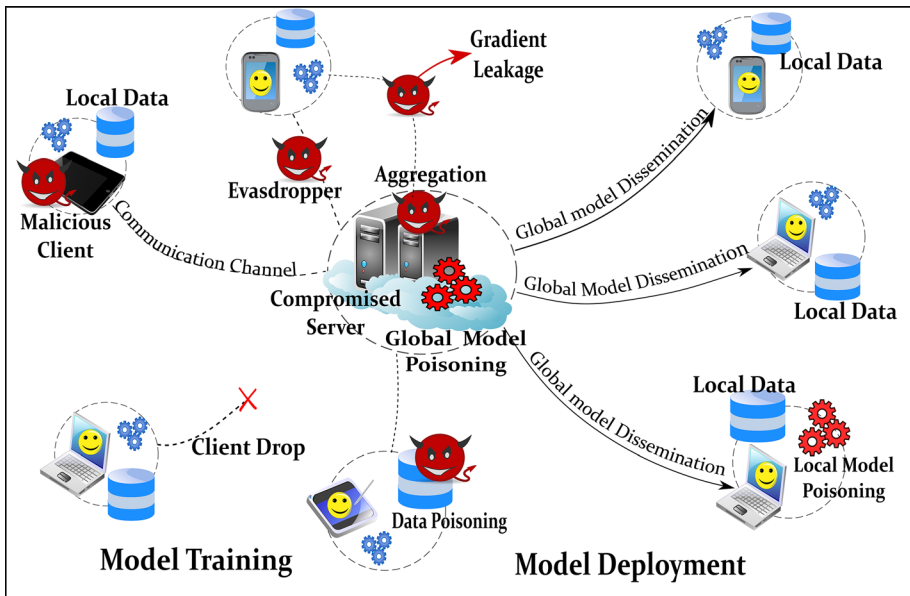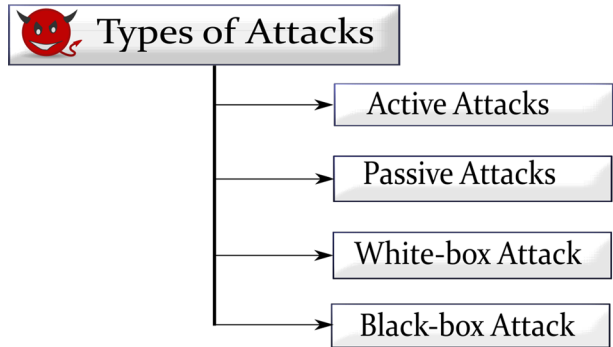
Fig. 15 Major vulnerabilities present in FL

vulnerabilities helps manage and defend against possible attacks due to various adversaries in the FL environment (Zhao et al. 2020f). Failure to identify FL vulnerabilities will result in weak defenses against attackers (Nguyen et al. 2021c). Therefore, the first step is to examine the different sources of vulnerabilities in the FL. Because a better understanding of possible vulnerabilities would help to defend against them. This section discusses some of the main sources of vulnerabilities in FL. Table 5 summarizes the major vulnerabilities in FL, and Fig. 15 shows them diagrammatically.

(1) *Communication* FL training takes place in rounds over the communication channel where model parameters are shared either with a central server or in a peer-to-peer

manner with other participants. Therefore, adversaries can intercept this exchange over an unsecured channel, modify the parameters, or replace them with malicious values. In general, some encryption algorithms, such as homomorphic encryption (HE), are employed to protect clients' data through model updates exchange between the clients and the server (Papernot et al. 2016; Zhang et al. 2020d). Besides, a slow internet connection can result in clients' dropout, resulting in unstable training, unwanted bias in the global model, and slow convergence.

(2) *Compromised Clients* In an FL environment, clients are inherent and significant components. They participate in the training and can observe the global model's intermediate states and contribute to model updates. This creates an opportunity for the compromised client to corrupt the entire training process. A malicious client can pretend genuine and corrupt the whole model training.

(3) *Gradient Leakage* FL provides privacy by not sharing user's data; instead model updates and gradients are shared in the training process. Geiping et al. (2020a) demonstrated in their work that sharing gradients and updates can reveal sensitive and private information, known as "gradient leakage."

(4) *Compromised Servers* In FL, a centralized server or cloud-based servers are vulnerable to hacking or distributed denial-of-service (DDOS) attack (Jabir et al. 2016; Mahjabin et al. 2017). Therefore, a compromised server can readily temper with the global model and the aggregation process leading to the weakening of the training process.

(5) *Non-Malicious Failures* Even if we assume no adversaries are in the system, factors still affect the FL process. Such factors include low communicational bandwidth, sudden client drop out of the training process, or limited computational power resulting in a low-quality-based model. Some other factors may include noisy features or labels in clients' datasets, compression of gradients of the global model, etc.

(6) *Aggregation Algorithms* An aggregation algorithm plays a significant role in FL training. It ensures the global model's overall convergence and maintains the trust factor in the FL process. Therefore, it becomes very crucial to incorporate an anomaly detection mechanism within the aggregation algorithm. Otherwise, a corrupted aggregator will make the global model vulnerable and an untrustworthy FL architecture.

(7) *Distributed Nature of FL* FL is based on the distributed approach, so the FL environment would also be prone to all those attacks found in a distributed environment. The major attacks and the mitigation strategies in a distributed environment are discussed in (Suri 2019). Furthermore, Xie et al. (2019) experimented with their proposed distributed backdoor attack (DBA) to show its effectiveness and persistence in a distributed FL environment than in a centralized one.

(8) *Model Deployment* Once the model is fully trained and ready to serve the clients, the next important step is to test the performance and accuracy of the global model. Attackers can manipulate, and craft perturbed variations to the test inputs so that even a correctly trained model gives lower accuracy on the test dataset. Therefore, it becomes crucial not to leave the deployed model vulnerable to some form of adversarial noise.

(9) *FL Deployment Agreement* The primary goal of FL is to learn through collaboration between competing companies through their private database without sharing them. Therefore, before the real-time deployment of such collaboration, some pre-agreement must be established. The terms and conditions of sharing, security requirements, rules, etc., should be negotiated beforehand. Otherwise, this collaboration would become an attack out of confusion, lack of understanding, and curious behaviors of participants. Working in this direction, "Melloddy" (Machine Learning Ledger Orchestration for Drug Discovery) is an FL-based project with a consortium of 10 pharma companies to

Table 6 Main threatning
advarsaries in FL with their
capabilities

Adversary	Capabilities
Client	Simply Observe
	Corrupt or Modify Updates
	Can control parameters and hyperparameters of training
	Carry out Backdoor attacks with other adversarial clients
Aggregator	Examine all model updates
	Inject attack through Aggregation Algorithm
	Modify or corrupt global model updates
	Allows malicious outsiders to participate in training
Outsider	Can carry out Inference-time-attack
	Eavesdropping

develop an accurate model to predict compounds for drug discoveries and development
(David et al. 2019).

4 Security and privacy in federated learning

After understanding the FL environment from the above discussion, this section focuses
on the security and privacy concerns, attacks, and vulnerabilities in the FL environment.
This section discusses the main research questions and their answers that helped shape the
article.

4.1 Security in federated learning

Security means to guard against any attack; an attack means a malicious attacker has
exploited some system vulnerability. The goal of an attacker could be manipulating the
global model and clients' data, inserting backdoors, etc. (Liu et al. 2020c, d).

4.2 Security-related research questions

- Research Question 1: Who are the major adversaries exploiting the security of FL?
- Research Question 2: What are FL's main security threats/attacks?
- Research Question 3: What current defense mechanisms are used in different
  application areas to defend against security threats?

Research Questions 1 and 2 are discussed in this section, and Research Question 3 is
discussed in the next section, i.e., Sect. 5.

4.3 Security threatening adversaries in federated learning

Unlike the conventional centralized ML approach, where the central server is the only way
to attack the system, FL works distributedly with various actors playing different roles.
Table 6 lists the significant activities that an adversary can carry out. Keeping that in mind,
the FL environment should guard against three major potential adversaries: the clients, the
aggregators, and the outsiders.

(1) *Client as an Adversaries* An attacker can get complete control over one or more participants by compromising the operating system (OS) or application software of the client's device. Thereby acquiring full control over the training process to carry out activities on their accord. Moreover, a malicious client can participate as a genuine client and launch various attacks during training.

(2) *Aggregator as an Adversary* Aggregator has direct access to the global model. If an adversary gets control of the aggregator, it can infer the data features and private information through the updates and gradients received in the rounds.

(3) *Outsider as an Adversary* End-users of the final trained model are considered "outsiders." Even an outsider can be an adversary with access to the final trained model in the deployment phase. An outsider can perform inference time (runtime) attacks (Ma et al. 2020b). Inference time (also exploratory attack) attack does not temper with the target model. It just collects the evidence regarding model characteristics causing a confidentiality attack. Besides this, outsiders, clients, and even the aggregator can launch a collusion attack opening a whole new dimension to security threats.

4.4 Major security attacks in federated learning

This subsection discusses and classifies major attackers possible in the FL environment. By sharing the model parameters and gradients instead of data, the FL environment is exposed to a new set of attacks surface at training time (Ma et al. 2020b). Therefore, it becomes crucial to provide security in the FL environment. Understanding all the possible attacks is necessary first, then discussing safeguards against them.

To begin with, the first/initial categorization of attacks is based on the "goal of the attack." The attack can be either a "targeted attack" or an "unauthorized attack." Targeted Attacks are focused attacks because they specifically target some subtask or sub-activity instead of corrupting the entire model. A targeted attack on a classification model may force it to "misclassify" instances of some class X to class Y; for example, a model classifies all dogs to the correct category, except the "black and white" dog is classified as zebra. On the other hand, untargeted attacks are "intentional threats" with the intent to cause major damage to the entire system. From the FL perspective, the focus is either on reducing the accuracy of the global model or "fully-break" it. Apart from this, attacks can also be focused on data, models, aggregators, or the federation itself.

(1) *Attack on Data* These attacks compromise the integrity of the training data, thereby corrupting the global model. This attack is also called "poisoning attacks," where poisoning means "polluting" or "corrupting" anything.

    (a) Poisoning Attacks It focuses on corrupting either the training samples or the model updates. Based on that, poisoning attacks are further of two types: data poisoning and model poisoning.

    (i) Model Poisoning This attack focuses on corrupting the local model updates before sending them to the aggregator, targeting the global model directly. This attack is effective and more common in the FL environment, as thousands or millions of clients participate in the training, and the global model is exposed to all of them in each round

of training. A malicious client can change or replace the local model updates to cause maximum damage to the global model and its overall performance.

(ii) Data Poisoning These attacks compromise the integrity of the training data to corrupt the global model. To carry out a data-poisoning attack, attackers can either change the labels of any class in the training set (like changing the label of digit 5 to 8 in the MNIST handwritten dataset) or introduce random samples with target class labels on them. It will cause the correctly trained model to behave abnormally. One another attack is called "backdoor poisoning," in which adversaries can modify features or add watermarks to the images of training data, resulting in biased training.

(b) Backdoor Attacks Backdoor attacks are "hidden" or "less transparent" attacks. These works by inserting backdoors or injecting a malicious task into the existing model without compromising the accuracy of the main task. Backdoor attacks are triggered depending upon some event or condition during the normal working of the trained model. These attacks are hard to detect and confuse the ML model to predict false positives with high confidence.

(c) Evasion Attacks In this attack, the attacker tries to evade a deployed model by carefully crafting new test samples. It deceives a correctly trained model, showing poor performance in testing. Besides, the attackers can generate perturbation in the dataset, making the model more prone to misclassification or class change.

(2) *Attack on Algorithm* In FL, the training is orchestrated by an aggregator algorithm either in a centralized or a peer-to-peer setting. This attack causes the violation of the integrity of the system. This attack can be launched through an aggregator or by changing training parameters. It can be further classified into three major categories. para *(a) Model Parameter Manipulation* In ML and DL, the parameters, hyper-parameters, and optimization techniques play a crucial role. So, in this attack, the adversaries manipulate and play with crucial parameters, such as learning rate, epochs, batch size, etc., through some compromised clients. Thus forcing the global model to converge into a failure or preventing the model from learning.

(b) Non-Robust Aggregation The aggregation algorithm is also prone to attacks. With several challenges, such as non-iid data distribution, data poisoning, model poisoning, sudden dropout of clients, etc., a non-robust aggregator will produce a compromised model. Therefore, a thoroughly inspected and robust aggregator is a must for an FL environment against adversaries.

(c) Compromised FL Distributed Computation A thousand or millions of geographically distributed clients participate in the training process. Clients are also contributing computation power along with their private data. So, it becomes a concern to the clients whether their computation is used for genuine, agreed-upon model training. Otherwise, a compromised server can take advantage of distributed computation in FL.

(3) *Attack on Federation* FL's distributed or decentralized approach opens up many fronts for FL security. Creating a secure federation is challenging for the developer when attacks can be possible from anywhere, such as communication channels, network topologies, data poisoning, and model corruption. Several possible attacks on the federation are as follows.

(a) Malicious Server A malicious server can easily extract participants' private information, manipulate the global model through received updates from clients, and even use the shared computation to build some malicious task while training a model.

(b) GANs Attack GANs pose both security and privacy threat to FL. Being generative models, GANs can produce samples similar to training sets obtained through inference

from a compromised client. These generated samples can be used later to poison the training set and compromise the global model.

(c) Inference Attack It is more of a privacy attack but similar to a poisoning attack. Therefore, it is a security threat too. An adversary can infer private information about participants and datasets using shared updates and gradient information over the communication channel.

(d) Communication Bottlenecks Training an ML or DL model involves millions of parameters. Transferring this much of parameters iteratively in rounds over the communication channel to the central aggregator is a big challenge. So, communicational bottlenecks can severely disrupt the FL environment significantly. Various compression techniques have been tried to reduce the communication cost, but it, in turn, degrades the overall quality and performance of the model. In addition, asynchronous aggregation-based algorithms have also been tried for performance even with low bandwidth.

(e) Man-in-the-Middle Attacks Man-in-the-middle eavesdrops on the exchanges between client and server through weaker communication channels to perform some malicious activities. They look for clients with fragile security to obtain knowledge about the model parameters.

(f) Free-Riding Attacks Free-Riders are passive clients who intentionally participate in the FL training but do not contribute. They either do not update the local parameters or insert some random dummy values without performing any training on their private data. The impact of this attack is medium in a large FL setup but is a major challenge for a smaller federation environment, where data is scarce, and the model has high commercial value. Lin et al. (2019) proposed an anomaly detection technique using autoencoders to identify free-riders in the system.

(g) Dropouts of Clients/Un-availability of Clients Un-availability or dropout of the participants may occur due to many reasons, such as lower communicational bandwidth, power loss at the client-side (discharged battery), an internet issue, etc. Client dropout may cause fairness issues and unproductive results in the training process. It is similar to a free-riding attack; it's just unintentional here. A robust aggregation algorithm is needed to overcome this attack that can work asynchronously.

Table 7 summarizes the major attacks in the FL environment and their sources of vulnerabilities.

4.5 Privacy in federated learning

This section is focused on the privacy concerns in FL, basic concepts, overview, categorization of attacks, and vulnerabilities. In the next section, we provide a comprehensive literature survey of the defense strategies proposed by various researchers to ensure privacy.

FL facilitates collaborative training of a shared model and promotes privacy preservation by not sharing the clients' private data. This concept sounds ideal in theory, but it is far from reality (Li et al. 2020c). FL is still in its infancy, so the primary concern is tackling this new set of privacy issues in a new environment. But thanks to, technological advances allow higher computing power, increased storage capacities, and a massive amount of data availability, making FL deployability possible.

When we talk about privacy, several factors come into play, such as increasing awareness towards privacy-preservation, client's consent before using their private data, the

Table 7 Summary of major aattacks in FL

Category of attack	Type of attack	Description	Source of vulnerabilities
Attack on data	Data poisoning	Manipulation of training datasets like modifying features or flipping labels	Compromised client
	Model poisoning	Manipulation of model updates to introduce bias in the global mode	Compromised client Compromised serve
	Backdoor attack	Insertion of backdoor into the global model while maintaining the overall accuracy	Compromised client
	Evasion attack	Circumventing a deployed model through manipulated data samples	Model deployment Compromised client
Attack on algorithm	Model parameters manipulation	Manipulation of parameters to either introduce bias or prevent convergence	Distributed nature of FL Compromised client
	Non-robust aggregation	Aggregation algorithm with weak defenses	Aggregation algorithm
Attack on federation	Malicious server	Exploiting the client's information or manipulating model parameters for some malicious task	Compromised server
	GAN attack	Poisoning the training with fake generated samples through GAN	Compromised client Communication
	Inference attack	Analyzing the private information of clients or gradients information to craft an attack	Compromised server Communication
	Communication bottlenecks	To reduce the communication cost in FL training applied techniques can disrupt the FL process	Communication Distributed nature of FL
	Man-in-the-middle attack	Eavesdropper take advantage of weak commun- ication channel to extract information exchanged	Communication
	Free-riding attacks	Passive client who takes part in the FL training to reap the benefits of final global model	Compromised client
	Dropout of clients	Unavailability of the participants in training either due to network issues or power loss	Non-malicious failure Communication

emergence of legal laws and regulations, such as General Data Protection Regulation (GDPR) (Hoofnagle et al. 2019), etc. After the promulgation of GDPR by the European Union in the year 2018, it is illegal to directly consolidate data-crossing enterprises due to security and other concerns, especially for privacy-sensitive industries. Therefore, it becomes necessary to guarantee that FL is secure enough to convince the clients to collaboration in these scenarios. Even though FL promises privacy by not sharing clients' data on the network, it can be exposed to the risk of a new set of privacy and security threats by sharing model parameters and local gradients. An adversary can track and extract private information from shared gradient information. Recent studies have shown various attacks and vulnerabilities in the privacy-preserving capabilities of the FL environment (Jere et al. 2020). Therefore, a detailed and structured analysis is required to analyze the major vulnerabilities and attacks on privacy in FL.

4.6 Privacy-related research questions

- Research Question 1: Who are the major Adversaries threatening the privacy of FL?
- Research Question 2: What are FL's main privacy threats/attacks?
- Research Question 3: What are the current defense mechanisms available in different application areas to defend against privacy threats?

Research Questions 1 and 2 are discussed in this section, and Research Question 3 is discussed in the next section.

4.7 Privacy threatening adversaries in federated learning

In general, an adversary's major goals in FL are to extract private information somehow and compromise the global model to behave abnormally. The main components of the FL environment are servers or aggregator algorithms, clients, and the communication channel. A privacy-preserving FL environment assumes trustworthy clients, honest servers, and secure communication channels, but this is not the case. Curious and malicious clients or servers attack to threaten privacy in the FL environment. Therefore, the main culprit of privacy threats in the FL environment is the components themselves, i.e., malicious participants, malicious servers or aggregators (insider attack), and unsecured communication channels (outsider attack).

(a) Client-side Threats A malicious client can act as a genuine participant and pose several threats like arbitrary model updates without participating in the training process or affecting the global aggregated model. Furthermore, an adversary can compromise some clients to manipulate the overall training process.

(b) Server-side Threats These are the threats by some malicious insider. The adversary can adapt the global model to some other target from this side. They can regulate participants and access their private information through updates (passive attack). Moreover, a compromised server, if aggregated, the model can carry out an inference attack.

(c) Communicational Threats As such, communication channels are assumed to be secure. But still, recent researchers showed various threats like eavesdropping, man-in-the-middle attack; tempering are launched via unsecured communication channels.

4.8 Major privacy threats in federated learning

This sub-section discusses the privacy threats in FL. While dealing with privacy, the primary concern is protecting clients' private information and data from leakage or any other adversarial activity. Although FL prevents sharing clients' private data over the network, recent work has demonstrated that sharing updates and gradients can be a prime source for the leakage of private information. So, it becomes crucial to identify the vulnerabilities first and devise a defense against them. Privacy threats, in general, are categorized as follows.

(1) *Information Inference* This threat exploits the shared gradient in FL training to infer the private information of the participants. The gradients are vulnerable to attack because they are derived through a training model on participants' private data. In DL models, gradients of weights are the inner product of the layer's learned features, and the error is backpropagated from the next layer during backpropagation. The features that sequential layers of a model learns are from the training dataset. So, suppose the entire training process is formulated mathematically. Is it possible to retrieve or extract useful information by performing reverse operations on intermediate updates or shared gradients between participants and the servers?

(2) *Inferring Class Representation* Here, the attacker tries to generate new training samples that appear to belong to the same data distribution as the training dataset. If successful, the adversary can learn a lot about the underlying dataset. This inference attack can be carried out with generative adversarial networks (GANs), which can be trained in real-time to generate samples of the targeted participant's training set and observe the loss function value. If the value decreases in the next round, generated samples are similar to the original dataset samples.

(3) *Inferring Membership* This inference attack focuses on determining whether a given data point or record was used in training the model or not. For example, an adversary can infer the words used during an NLP model training on a text-based dataset. To infer the membership, an adversary takes the help of a duplicate model of the original one and tests the sample on the duplicate model. The sample belongs to the original dataset if the prediction has high confidence. This inference attack tries to figure out meta-characteristics of other participants' training datasets. For example, if an adversary wants to know whether or not the target data set mainly consists of blue-colored cars.

(4) *Reconstruction through inference* In this attack, the adversary tries to reconstruct the training dataset used by the participants. To avoid this attack, the gradient update should not be shared in plaintext, making the system vulnerable. Some encryption techniques, such as homomorphic encryption, protect the gradients. Moreover, ML models that store feature values such as k-nearest neighbors (KNN) or support vector machine (SVM) should be avoided. Furthermore, only black-box access to the model should be granted to protect against inference.

(5) *Model Inversion Attack* Model inversion attack formalized by Frederickson et al. (2015), in which trained model is available in a black-box fashion to the adversary. The adversary queries the model with its input and collects the respective responses as outputs. Later, use these input–outputs to find the correlations between unknown and known inputs. A "brute force" approach is used to find all possible variations of unknown input to predict the most likely features of the training dataset. Fortunately,

the model inversion attack is only successful in the case of linear models. This attack becomes computationally infeasible for significant input.

Table 8 summarizes the above-discussed privacy threats in FL.

5 Security and privacy concerns of federated learning in space, air, ground, and underwater communications

This section provides a comprehensive literature survey of the defense strategies proposed by various researchers against the above-discussed security and privacy threats concerning different application areas in four main domains, i.e., Space, air, underwater, and ground. For a better understanding, the proposed works are discussed and compared in tables. Finally, take-away sections are also included to summarize the domain-wise discussion in terms of conclusions, challenges, future scopes, etc.

5.1 Security and privacy in FL-based applications covering space

The new generation of communicational standards (i.e., 5G, 6G) promises broad prospects in communicational technology, such as massive connections, enhanced capacity, fast speed, etc. But still, it is a ground-level-based technology, facing many issues and challenges like terrestrial networks have. On the other hand, space communication networks provide widespread coverage, covering almost every from roads, vehicles, cities, remote rural areas, oceans, etc. Therefore, it is evident that the integration of space networks with terrestrial networks is the future of information networks. This integration is generally called integrated Space and terrestrial networks (ISTN) or satellite-territorial integrated networks (STIN). It results in a massive amount of transmissions between two networks, which are pretty different in terms of resource allocations, security, privacy, computation capabilities, etc.

The data generated by satellites is more sensitive and of a high priority than terrestrial networks. Therefore, it has high privacy and security needs. With the advancement in satellite network technologies over recent years, billions of devices have been connected through satellites, creating an urgent need for higher security and privacy measures. Various security and privacy measures used in territorial networks are not successful. Because terrestrial networks do not face resource shortages, upgrading the hardware and other resources are challenging once a satellite is launched. Even if the space networks have

Table 8 Major privacy threats in FL environment

| Privacy attack	Description
Information inference	inferring private information from the shared gradients
Inferring class representation	generation of a fake training data sample that appears to belong to the training dataset
Inferring class membership	finding out whether a given data point or record is part of the training dataset
Reconstruction through Inference	trying to reconstruct the training dataset using GANs
Model inversion	Finding out the input–output correlations using brute force technique
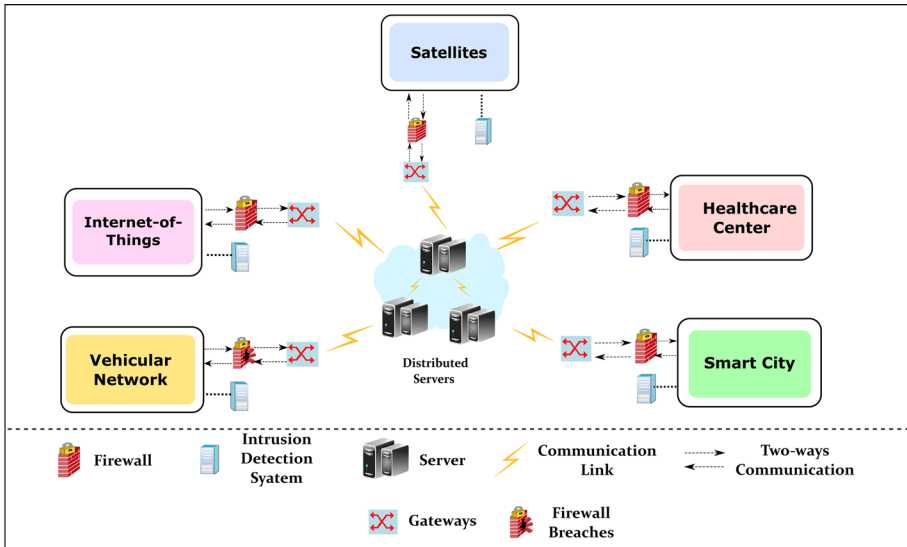
Fig. 16 Intrusion detection systems (IDS) for the collaboration of different applications with heterogeneous environments using FL

some intrusion detection system (IDS) or firewalls, etc., they are not necessarily strong enough against modern attacks that are getting stronger day by day, shown in Fig. 16. Once a satellite network is attacked, all the satellite network resources will exhaust quickly. Besides, another primary concern is the availability of standard datasets for satellites-terrestrial networks containing both normal and abnormal traffic to train a robust defense system and evaluate the performance. FL appears very convincing in this case due to its privacy-preserving and distributed nature.

Not much research is available in this area, but still, some research is going on to overcome all the abovementioned issues. Motivated by this new technology, Li et al. (2020a) proposed a distributed networks-IDS (NIDS) in a satellite-terrestrial integrated network using FL. NIDS are used to identify malicious traffic and avoid intrusions into the system. Their proposed system meets both privacy and security requirements in heterogeneous networks. To make an efficient system, they first created a security dataset conforming to the characteristics of both heterogeneous networks and collected all available attacks between them. They proposed an algorithm for STIN using FL adaptability to combine the HFL method within a network. Furthermore, they evaluated their proposed NIDS on their dataset and showed higher accuracy in identifying malicious traffic with reduced CPU utilization. Table 9 lists and compares the major work done in the space-based application areas.

Solar power is free and the best source of renewable energy. Nowadays, the integration of solar energy into the electrical network is in practice, making solar irradiance forecasting essential. Solar irradiance forecasting involves collecting and analyzing data to predict solar power generation on different time horizons. ML and DL models are the best practices for predicting and analyzing data. To further enhance the learning capabilities of the model, Zhang et al. (2020a) proposed a novel federated probabilistic solar irradiation forecasting scheme using DL, differential privacy (DP), and FL. With FL, they achieved data-privacy protection by not sharing the data and still achieved competitive performance compared to state-of-the-act forecasting methods.

Table 9 Survey and comparison of security and privacy measures in space-based application areas

References	Application area	Proposed work	Privacy/security approach	Base model	Data set	EM	Achievements
Li et al. (2020a)	Satellites	IDS for Satellite-terrestrial networks communication	Paillier encryption system, HFL	CNN	**	TTC, Acc, TA,	Security against malicious traffic,and DoS attack Enhanced privacy, Achieved higher accuracy rates Lower CPU utilization
Zhang et al. (2020a)	Solar power	Solar radiation forecasting based on Variational bayesian inference with secure FL	DP	Bayes LSTM NN	SolarGIS, NSRDB, Folsom	Acc	Enhanced security, Data privacy Enhanced forecasting, performance
Fang et al. (2021)	Space-air- ground integrated network (SGAIN)	Privacy-protected data transmission in SGAIN	Data-drivan AI solution for 6G	CNN	MNIST, Fashion-MNIST, CIFAR-10 (non-iid)	TC, Acc	Privacy preserved by design
Xia et al. (2014)	LEO based Satellites clouds	Utility-awareFL problem in LEO-based clouds	Double auction mechanism	Jobs	–	LDA	Privacy preserved by design

EP evaluation parameters, *HFL* horizontal federated learning, *DP* differential privacy, *LSTM* long short term memory, *BC* blockchain, *CNN* convolutional neural network, *NN* neural network, *LSTM* long short term memory, *DP* differential privacy, *Acc* accuracy, *TTC* total time cost, *LDA* local data accuracy, *TC* time cost

**Dataset collected and designed for tracking malicious traffic in STIN network

In another work, Fang et al. (2021) claimed to be the first to propose a novel configurable FL-based approach for privacy-preserved and effective data transmission in the space-air-ground integrated network (SGAIN), named olive branch learning (OBL). The OBL framework consists of three layers in space, air, and ground, respectively, where devices from each other collaborate to train a powerful model on their local data. Specifically, the space layer consisted of the ring structure of LEO constellations, a two-tier star structure imposed on air nodes, and internet-of-remote things (IoT) in the air and ground layer. Similarly, Xia et al. (2014) formulated a utility-aware FL problem in low-earth-orbit (LEO) based satellite edge clouds (SEC). They designed a double-auction mechanism for a fixed and variable number of participants. They achieved privacy by training the model locally on each LEO satellite and sending the trained model to data centers via ground stations.

5.1.1 Take away

Satellite-based communication is the only broadband vast area network (WAN) technology available everywhere, covering the entire world. But it has challenges, like a huge amount of satellite data that cannot be transferred to earth for model training, communication overheads, idle connectivity issues, and is vulnerable to strong security and privacy threats. FL is a promising approach showing scope in overcoming these challenges. But, it needs specially designed FL algorithms and techniques instead of existing terrestrial-based FL algorithms. Moreover, 5G and 6G communications would bring a new level of challenges and constant threats. Only a little work is available in this domain. Indeed, it requires further research is to be carried out in this area. This paper covered most of the initial work in this area listed in Table 9. Tables 26 and 27 show the majority of security and privacy defenses discussed in this section. The next subsection is focused on air-based application areas that are deploying FL.

5.2 Security and privacy in FL-based applications covering air

Unmanned Aerial Vehicles (UAVs), commonly known as drones, were initially developed for the military and aerospace industry. But now, they have found their way into our daily life. UAVs are used in numerous applications ranging from dangerous to dumb tasks such as surveillance, filming, journalism, shipping and delivery, disaster management, rescue operations, healthcare, law enforcement, agriculture, etc Chhikara et al. (2021). With the next generation of wireless communication (5G, 6G), their scope will increase further. UAVs have unique characteristics such as comprehensive coverage, mobility, wireless, flexibility, capacity, etc. These characteristics are the main reasons behind its rapid fame. With the increasing number of UAVs in the air, new challenges came to light, such as their management, trajectory decisions, scheduling, etc. Besides these, security and privacy are also of significant concern. UAVs are prone to accidental attacks, intentional hacking, and privacy threats as they fly in various situations like disaster areas, enemy territories, crossing borders, etc.

With the growing interest in ML-based approaches in multiple fields, researchers are also motivated to apply them in wireless networks. However, conventional, cloud-centric ML schemes are unsuitable for UAV-based wireless networks Iqbal et al. (2019). The main reasons are privacy concerns, latency, and the need for high bandwidth in dealing with the central authority. Therefore, the real solution is to move towards decentralized approaches. Recently, FL has been proposed to investigate distributed learning possibilities on IoT
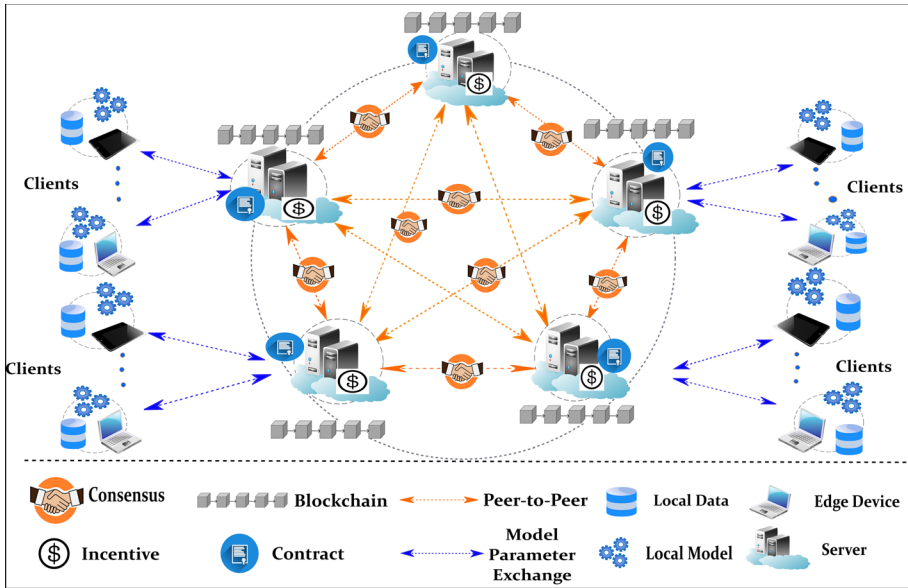
Fig. 17 Blockchain-enabled Federated Learning architecture

devices with better privacy, increased computations, and lesser need for network bandwidth. Being a new approach, not much research work is available in this domain. But still, researchers are motivated by the promises made by this new approach and trying to explore FL, its strengths and weakness, for its mass adoption.

Blockchains (BC) are used to ensure the integrity of the data and the safety of model aggregation, as shown in Fig. 17 (Gupta et al. 2021a). Saraswat et al. (2022), in their survey article, discussed the open problems in beyond 5G (B5G) networks for UAVs. They presented a taxonomy of blockchain-based FL solutions for B5G network issues. Furthermore, they discussed a case study for UAVs in a 6G network using BC-based FL as a future technology. Islam et al. (2022) proposed FL based blockchain embedded data accumulation scheme that combines drones and remote IoT devices that are prone to cyber threats and network scarcity. To further enhance the privacy of the proposed scheme, they employed DP before sharing model updates. In another work, He et al. (2022) used blockchains to design an efficient IDS for a UAV network. They proposed a conditional GAN-based intrusion detection algorithm with blockchain-empowered distributed FL for security. For privacy, they used the DP technique. A recent study in the context of FL for UAV-enabled wireless networks is presented by Brik et al. (2020) to deal with the challenges of UAV-based wireless networks. They discussed the key challenges and future directions for FL in UAV-based wireless networks.

During disasters such as floods, fire, earthquakes, or COVID-19 pandemic (social-distancing-based) zones, working communications services is crucial for disaster mitigation strategies. Because these disasters cause severe disruptions and damage to equipment, networks, etc., that result in the loss of emergency communication services. Along with communication, another critical concern is privacy leakage during disasters, as any sensitive information leakage into the media or public can further worsen the situation. To overcome such problems, Ma et al. (2020c) proposed a privacy-preserving FL-based infrastructure

(PPFL-Aid Life) network using mobile buses and drones as edge devices for emergency communication services during disasters. Their proposed work combined various aspects of different technologies to make it a robust infrastructure. A bus-and-drones network adds flexibility to the network, reusability of the public bus system, and the reachability of drones to any dangerous situation Gupta et al. (2021b). Furthermore, privacy-preserving capability protects the network from "privacy leakage."

Yao and Ansari (2021), investigated power-control of drones for increasing their security consideration which is restricted due to their battery capacities. The proposed power control in secure FL (PCSF) to counteract eavesdropping in internet-of-drones (IoD) networks. In another work, Zhang et al. (2020e) focussed on privacy concerns in cognitive radio networks using VFL. In cognitive radio networks, secondary users (SUs) are allowed to sense and access the white space primary user's (PU) license channels spectrum to reuse the spectrum. But spectrum sensing suffers from severe security and privacy threats. Therefore, the authors proposed VFL-based cooperative sensing (VFL-CS), in which SU's data is kept local during the training and evaluation process while encrypted in data exchanges.

Last but not least, FANets are considered the most efficient solution for UAV-based networks. But still, UAVs (uncrewed aerial vehicles) are considered vulnerable to various privacy and security threats in FANets. Mowla et al. (2019) proposed FL based solution to defend against on-device jamming attacks. They used client-group prioritization using the "dempster-Shafer theory" to identify the best clients and use their updates for global updates. Wang et al. (2020a) proposed secure federated UAV-assisted mobile crowdsensing (SFAC) for both privacy and security of the exchange of local model updates between the UAV and to verify their contributions. Their proposed method uses DP for privacy preservation and a two-tier reinforcement learning-based incentive mechanism for optimal task publishing without any central curator.

5.2.1 Take away

This subsection discussed FL privacy and security measures in air-based application areas. UAVs, Radio, and IoDs (Internet-of-Drones) are a few application areas covering this domain. The application areas of UAVs and IoDs are evolving at a tremendous rate, and with new technologies, they will be much more efficient in the future with small size and less power consumption. Their application areas are expanding, ranging from delivery, industrial inspections, agriculture, disaster management, and surveillance. These networks are highly dynamic, with limited resources, energy constraints, storage, processing capabilities, signaling overhead, computation, and communication costs. Different research works have revealed that FL can be an optimal solution for the various challenges faced in this application domain. With computation and data distributed among UAVs and drones in FL, it is possible to use them with fewer energy constraints and more intelligent purposes. But at the same time, a secure and privacy-preserving UAV-FL ecosystem would require new techniques, algorithms, and approaches for reliable UAVs selection, accommodating scalability, handling heterogeneous computing systems, dropouts, data privacy, and protection of gradients in transmission for aggregation, etc. Furthermore, advanced privacy and security measures are needed with upcoming 5G and 6G communications. Therefore, further research is needed to be carried out in this domain to explore the scope of FL in air-based application areas. Table 10 describes and compares the recently proposed defense mechanisms in this area. Tables 26 and 27 show the majority of security and privacy defenses

Table 10 Survey and comparison of security and privacy measures in Air-based applications areas

References	Proposed work	Privacy/security approach	Base model	Dataset	EP	Achievements
Brik et al. (2020)	FL for UAVs enabled wireless networks	Privacy preservation by design	DL Based Model	–	–	Discussed usefulness, challenges, open problems, and use cases of FL in UAV-enabled networks
Ma et al. (2020c)	Privacy-preserving buses-and drones FL networks in disaster management	Privacy preservation by design	DL Based Model	@		Privacy-preservation; Better data utilization; Emergency communicational services
Yao and Ansari (2021)	Secure FL by power control for drones	Privacy preservation by design	–	–		Analyzed eavesdropping rates; Optimized drone's wireless transmission power; Reduced FL training time
Zhang et al. (2020e)	Vertical-FL cooperative sensing for secure radios networks using Additively HE	Additively HE for intermediate results	RNN	–	AUC, ROC	Higher privacy-preserving capabilities; Improved sensing performance
Wang et al. (2020a)	Secure FL for UAV-assisted crowdsensing	BC for mobile updates, Local DP	CNN	MNIST	PBU, AE	Privacy-preservation; Secure; Improved utilization of UAVs; Improved quality of local model updates
Mowla et al. (2019)	FL-based on-device jamming attack detection in FANETs	Dempster-shafer theory for client group prioritization	NN	CRAWDAD	Acc	Enhanced security; Achieved promising performance in detecting jamming attacks
Islam et al. (2022)	Secure embedded data accumulation scheme using drones for IoTs	BC, Secure accumulation using Hampel filter, DP	–	–	MAE, POC	Privacy-preservation; Secure
He et al. (2022)	Intrusion detection for UAV networks	BC, DP	LSTM	CIC-IDS 2017	Acc, P,R, Fs	Secure against intrusion attack

EP evaluation parameters, *DL* deep learning, *DP* differential privacy, *BC* blockchain, *HE* homomorphic encryption, *RNN* recurrent neural network, *NN* neural network, *LSTM* long short-term memory, *Acc* accuracy, *P* precision, *R* recall, *Fs* F1-Score, *AE* aggregation error, *AUC* area under curve, *ROC* receiver operating characteristic, *PBU* Privacy budget of UAVs, *MAE* mean absolute error, *POC* proof of concept

@Collected from remote-radio head-mounted UAVs and buses

discussed in this section. In the next subsection, we will be exploring various ground-based application areas deploying FL.

5.3 Security and privacy in FL-based applications covering ground

Recently, the concept of FL has been proposed, giving opportunities to build intelligent and privacy-enhanced ML-based applications in almost every domain. In this section, we have tried to cover as many application areas as possible, according to the inclusion/exclusion criteria followed in this work, as shown in Fig. 6 for finalizing the research papers. Many applications, such as IoT, healthcare, transport, and fractures, are deploying FL to exploit ML and DL capabilities with enhanced trust. Various research work in different areas has been carried out to enhance security and privacy in the FL environment, discussed as follows.

5.3.1 General federated learning

Majeed et al. (2021) applied secured FTL in a cross-silo HFL configuration for network traffic classification using secure aggregation protocol. Paul et al. (2020) proposed FLaPS, an FL and privately scaling architecture for improving scalability, privacy, and security in FL. They used the clustering approach to increase the system's scalability and improve robustness. They used DP with FL for privacy preservation.

Zhao et al. (2020g) discussed generic security and operation considerations of the FL platform for communication service providers among different parties. They discussed and provided viable solutions for the efficient and secure delivery of FL services. They proposed a cryptographic infrastructure for authenticity and data protection for trusted connections between communications parties. FL deals with the heterogeneous environment having heterogeneous devices and data. Therefore, ensuring cybersecurity, privacy, and stability of the entire system becomes necessary.

In traditional cloud computing, data from millions of IoTs is sent to the cloud-based computing center for processing. These IoT devices generate a huge amount of data daily. Therefore, data transmission or uploading to the cloud center results in processing delays and congestion. Edge computing came to light as a solution, but with an issue of security and privacy. Lu et al. (2020a) focussed their work on ensuring security and privacy by proposing a privacy-preserving synchronous FL mechanism (PAFLM) for edge network computing. The proposed design allowed distributed collaborative learning of discrete nodes in edge networks without sharing private data. Furthermore, their design also incorporated two more aspects, self-adaptive threshold gradient compression, and asynchronous FL. The proposed compression method automatically adapts to the changing gradients by computing a threshold to compress gradient communications. Thereby, the possibility of privacy leakage through gradients is reduced. They also explored asynchronous FL and proposed a dual-weight correction method for better performance in asynchronous learning.

Among many security attacks in FL, a poisoning attack is an acute attack in which malicious clients submit random updates, thereby introducing bias or preventing model convergence. The anti-poisoning techniques used to avoid attack are based on identifying outlying values in the client updates. This might lead to the discrimination of some minority groups whose updates significantly and legitimately differ from the majority of the participants. Therefore, this approach results in an unfairly trained model. Singh

et al. (2020) suggested two approaches to distinguish between updates from minority groups and malicious ones, using micro-aggregations (Domingo-Ferrer and Torra 2005) and gaussian mixture models. In the micro-aggregation approach, clients belonging to minority anonymous groups with some attributes. So, peer entity creates clusters based on these attributes, resulting in the majority and minority groups. Now FL training is carried out on a cluster basis. As a result, it becomes a little bit easier to identify outliers within minority clusters. Their second approach based on gaussian mixture models helps to spot outliers more sophisticatedly.

Li et al. (2021a) also used blockchains for their proposed byzantine-resistant secure FL framework named BytoChain. Additionally, Shejwalkar and Houmansadr (2021) centered their work on model poisoning in FL. They carried out the work in two parts. In the first part, they mounted a model poisoning attack on FL, outperforming known state-of-the-art model poisoning attacks and defeating all byzantine-robust FL algorithms. In the second part, they proposed a novel robust aggregation algorithm, divide-and-conquer(DNC), to defend against their proposed poisoning attacks. Backdoor attacks are attacks where an adversary embeds an adversarial trigger to misclassify on some particular input while performing well on others. To defend against backdoor attacks, FL needs access to the updates received from the clients, which in turn results in privacy threats. To overcome this, secure aggregation (SecAgg) cryptographic protocol is used to keep updates uninspectable.

Similarly, Aramoon et al. (2021) proposed a framework called Meta-FL, which facilitates defense against backdoor attacks, along with protecting the privacy of clients through secure aggregation, both working in a compatible manner. Around the world, the general practice is establishing LANs within organizations, universities, laboratories, and research institutes. Keeping in mind the unpredictability in patterns of recent cyber attacks, Sun et al. (2020b) proposed segmented FL for intrusion detection in large-scale multiple LANs. Their proposed learning varied from traditional FL because it manages multiple global models instead of a single global model. These multiple global models allowed segments of participants to learn collaboratively and even rearrange the segments dynamically. These multiple global models interact with each other to update parameters. Because of parameter sharing and LAN structure transformation, their proposed approach performed well in intrusion detection in large-scale LANs with the privacy preservation of participants. Furthermore, Lyu et al. (2020a) addressed the fairness and privacy-preservation issues in FL. They proposed local credibility and transaction points for collaborative fairness and further investigated the approach. They designed a three-layer onion-style encryption scheme for privacy preservation and enhanced accuracy. Experimental results showed balanced fairness, accuracy, and privacy.

Nasar et al. (2019) designed and evaluated novel white-box-membership-inference attacks against DL algorithms in both standalone and federated settings by exploiting the privacy vulnerabilities of stochastic gradient descent algorithm. Their work investigated the reason for training information leakage in DL models. They showed the effectiveness of the white-box-inference attack on various publicly available state-of-the-art models.

In contrast, Qin et al. (2020) focused their work on anomaly detection using selective model aggregation approach where local models showing unsatisfying performances are excluded from FL training. They measured the performance of the models using the prediction errors shown by models on the observed datasets. Experimental results showed improved anomaly detection accuracy compared to the state-of-the-art federated averaging methods.

In an FL system, distributed clients have heterogeneous computational, communication, and storage resources. Hence, deploying cumbersome DNNs with many model parameters

on these devices is challenging. Allowing heterogeneous models and reduced communication overhead has motivated the development of federated distillation (FD) using a concept called knowledge distillation (KD) that enables effective and low-cost information exchange in FL Seo et al. (2020). It is based on exchanging only the local model outputs whose dimensions are much smaller than the model sizes. It effectively transfers knowledge from a large teacher model to a small, lightweight student model. The student model mimics the teacher model's output, i.e., logits, on the same training data. The parent and student's model architectures may differ, and the communication cost depends only on the logit size instead of the model weights. However, since KD is data-dependent, considering the privacy regulation in FL, FD needs to achieve distillation without sharing the local private data. On the other hand, federated model distillation (FedMD) shares the knowledge of FL parties' models via their predictions on an unlabeled public set. But, sharing the predictions may still leak the privacy of the local data as there is no reasonable privacy guarantee for sharing model predictions in the FL environment. Hence, KD is also proving an effective way as a security measure.

Working in this direction, Sun and Lyu (2020) proposed a federated model distillation framework with a novel noise-free DP (NEDP) mechanism. The proposed framework showed the feasibility of heterogeneous model architectures in both iid and non-iid settings of multi-labeled public datasets. Experiments showed the framework to be communication efficient and guaranteed privacy-preserving. Similarly, Gong et al. (2022) proposed another federated framework with ensembled one-way KD (FedKD) on cross-domains, unlabelled, and non-sensitive public datasets. They focused on the issues like communicational bottlenecks and preserving privacy without sacrificing accuracy.

Zheng et al. (2020) conducted a comparative study on the effectiveness of local DP and federated ML in tackling privacy risks and security breaches. Zhang et al. (2019) in their work studied and evaluated the effectiveness of poisoning attack on FL setup using GANs to mimic the samples from other participants. Their proposed novel poisoning attack differs from conventional poisoning attacks as it doesn't require forced entry into any participant's device or any struggle with intrusion detection within the local system. They demonstrated the vulnerability of FL architecture to poisoning attacks. Triastcyn and Faltings (2019) proposed augmentation to FL through bayesian-differential privacy (BDP), a relaxation of differential privacy, for tighter and guaranteed privacy preservation. They also introduced a novel technique of joint accounting to guarantee privacy at an instance and client levels jointly from only instance-level noise. Jiang et al. (2019) proposed PruneFL, a novel approach that allows parameter pruning to reduce the neural network model size during FL training. Their proposed approach is adaptive and suitable for distributed FL. The authors suggested fine-turning and model pruning as a solution to defend against backdoor attacks. The experiments showed that computation time, communication overhead, and training time were minimized in FL settings. In a similar work, Liu et al. (2018) analyzed the efficacy of fine-tuning and pruning defense mechanisms against backdoor attacks. They found that neither is strong enough against backdoor attacks. Therefore, they proposed a solution fine-pruning by combining the strengths of both techniques that effectively nullified backdoor attacks. They tested the proposed solution on three prior attacks.

AI-based techniques are popular approaches used to classify malwares (Ahmadi et al. 2016; Suarez-Tangil et al. 2017). Combined with FL, it further enhances the overall system and privacy preservations by providing secure data transfer between distributed clients. Lin and Huang (2020) proposed a malware classification with decentralized data collection using FL. It is a common issue of unbalanced computations and communication resources in FL among the parties and clients. The best approach to deal with such a scenario is using

asynchronous FL. Gu et al. (2021) contributed their efforts in this direction and proposed asynchronous approaches to deal with unstable situations. The proposed asynchronous federated stochastic gradient descent (AFSAD-VP) for vertically partitioned (VP) data. Furthermore, they also proposed its two variants, stochastic variance reduced gradient (SVRG) and SAGA. Results verified better convergence rates, higher efficiency, model, and data privacy in vertically partitioned data sets.

Zhu et al. (2020) in their work introduced a new notion of named weighted FL (wFL) within the secret sharing framework. In wFL, participants' private data is split into random shares and distributed among predefined computing servers, providing the best security to state-of-the-art security approaches. The authors investigated the relationship between multiparty computations (MPC) and FL. Their work guaranteed security within the secret share framework. In another work, Bai and Fan (2021) focused on achieving security and privacy in FL settings. They used homomorphic encryption (HE) to encrypt the parameter updates for security. To achieve privacy, they added a parameter selection method to choose updates from specific participants with certain probabilities reaching a threshold value.

In contrast to the above-discussed work for achieving privacy and security via DP or secure MPC, Domingo-Ferrer et al. (2021) used Co-Utility property (Domingo-Ferrer et al. 2017), a self-enforcing protocol for mutual benefits of the participants. Incentives would be given to protocol-abiding participants and punishment to the rule-breakers. In (Wainakh et al. 2020), the author discussed HFL architecture for a flexible, decentralized, controlled training process and better privacy preservations. Xu et al. (2020), through their work, addressed the issue of the irregular user (who shares low-quality data) in the federated training process, which severely affects the global model convergence. In another work, Xin et al. (2020) tried to generate synthetic training data without compromising client privacy using FL-GAN. And used this fake data to train another GAN model. GAN's training is challenging and requires lots of training data for better learning.

Song et al. (2020a) proposed a framework for a multi-task GAN auxiliary identification (mGAN-AI) to analyze user-level privacy leakage attack in FL by a malicious server that can simultaneously discriminate the client identity and category of the input sample. This enables the recovery of the private data of a specific client. Their proposed attack turned out to be stronger than state-of-the-art attacks on the server side.

For assured and strong privacy preservation, Chamikara et al. (2021) used a data perturbation mechanism named DISTPAB, which introduces perturbs into the data before communication and enforcing privacy preservation. A central authority controls the global perturbation parameter generation on the server side. On the client side, a distributed entity introduces perturbs in the local data. Results showed that the angry data generated by DISTPAB is resistant to strong attacks, thereby providing excellent privacy preservation.

FL is inherently vulnerable to poisoning attacks. Focusing work in this direction, Cao et al. (2019) implemented an FL system and invested poisoning attacks in the system in various scenarios. The authors proposed a novel defense mechanism named, Sniper that can filter out poisoned local models from malicious participants during the training and reduce the success rate of poisoning attacks. In their proposed mechanism, they measured the distance between the models, where honest models had a smaller distance among them, and the poisoned local model had a large distance measured from honest models. Poisoned models change the global model divergence in other directions. Therefore, distance measures help in identifying the poisoned model among honest ones. To avoid attacks from malicious clients, Zhao et al. (2020a) proposed a secure member selection strategy (SMSS) that evaluated the data quality of the clients before allowing them to participate. In this

Table 11 Survey and comparison of security and privacy measures in general FL environment

References	Proposed work	Privacy/security approach	Base model	Data-sets	EP	Achievements
Majeed et al. (2021)	Secure FTL for flow based Traffic Classification	Cross-silo model-based secure FTL	Federated model	–	P, R, Acc, Fs, TT	Enhanced security Privacy-preserving Validation accuracy Training time efficiency
Paul et al. (2020)	FLaPS: FL and PrivatelyScaling	Balancing utility and DP by shuffling algorithm (BUDS), Aggregated RAPPOR and Analysis (ARA)	Pre-trained CNN, Inception ResNetV2, MobileNetV2	MNIST, CIFAR10, and TINY-IMAGENET-200	Loss, AUC, Fs	Scaled privacy using DP Scalable using clustered approach Robust
Zhao et al. (2020g)	Discussed security and operations considerations for FL service providers	Added security domain	–	–	–	Enhanced Security Trusted infrastructure
Moustafa et al. (2020)	FL-IoT Testbed Architecture	Utilized hacking scenarios for strong security	–	DARPA 98, KDD-99, ADFA-LD, NGIDS-DS, SSENet-2014 AWSCTD, ADFA-WD	CM	Launched and tested nineattacks in FL setting.
Lu et al. (2020a)	Privacy-Preserving for Edge Network Computing	Asynchronous FL mechanism, designed improved gradient compression algorithm.		MNIST	Acc, CR, CBI	Privacy preservation
Singh et al. (2020)	Malicious updates identification in FL	Microaggregation-based approach forfair detection of attacks, Gaussian mixture models (GMM)	Microaggregation-based FL model	Adult Income Dataset	Acc, ROC- AUC, FNR	Distinguish abnormal/ malicious behavior of clients. Fair attack detection.

Table 11 (continued)

References	Proposed work	Privacy/security approach	Base model	Data-sets	EP	Achievements
Shejwalkar and Houmansadr (2021)	Model Poisoning attack	A novel robust aggregation algorithm, divide-and-conquer (DnC), to defend against model poisoning attacks	Alexnet, VGGI1	MNIST, CIFAR10, Purchase, non-iid FEMNIST Dataset	AI	Launched strong poisoning attack Proposed robust aggregation algorithm to defend against launched poisoning attack on FL.
Aramoon et al. (2021)	defend against backdoor attacks (Meta-FL)	Secure aggregation protocol	–	SVHN, GTSRB	BSR, ASR	Defense against backdoor attack Robust to adversarial attacks and utility.
Sun et al. (2020b)	IDS in FL	Intrusion Detection with segmented FL for Large-scale multiple LANs	CNN	–	Acc	Enhanced Security Privacy Preservation
Lyu et al. (2020a)	Privacy in General FL	a three-layer onion-style encryption scheme, including DP, HE, and BC	CNN, MLP	MNIST, SVHN	Acc	Fair collaboration Privacy-preservation
Nasr et al. (2019)	General FL setting	Design and evaluation of active and passive white-box-inference on DL models in FL setting	CNN, FCN, Alexnet, ResNet, DenseNet	CIFAR100, Purchase100, Texas100	AA, TFP, PU	Showed the effectiveness of white-box-inference attack in leaking training data information
Qin et al. (2020)	Anomaly Detection in FL	Selective model aggregation approach	ONLAD [MOD1], OS-ELM [MOD2], Autoencoder	MNIST, Fashion MNIST with anomalies)	P, R, Acc, Fs	High anomaly detection accuracy Improved training

Table 11 (continued)

References	Proposed work	Privacy/security approach	Base model	Data-sets	EP	Achievements
Zheng et al. (2020)	Privacy in FL	Comparative experimental study of Local DP and FL in handling security breaches and privacy risks	NN	NYC Taxi, BR2000, Adult	MR, IA, ODT	Lower misclassification
Sun and Lyu (2020)	Privacy in FL	A noise-free DP mechanism, Model distillation framework (FEDMD-NFDP)	–	MNIST/FEDMNIST, CIFAR10/CIFAR-100 (iid/non-iid)	Acc, CR	Effective comparable utility; Communication efficiency; Guarantee privacy
Gong et al. (2022)	Privacy in FL	Quantized and noisy ensemble for privacy, One-shot logits ensemble distillation	Res Net-8	NIH CXR14, CheXpert, CIFAR10/100	Acc	Privacy guarantee; Feasible with cross-domain and heterogeneous data distributions

EP evaluation parameters, *DP* differential privacy, *BC* blockchain, *CNN* convolutional neural network, *MLP* multi layer perceptron, *NN* neural network, *Acc* accuracy, *P* precision, *R* recall, *Fs* F1-Score, *TP* test performance, *PA* predictive accuracy, *DA* detection accuracy, *TT* training time, *AUC* area under the curve, *CM* correlation matrix, *CR* compression ratio, *CBI* compression balance index, *ROC-AUC* area under the ROC curve, *FNR* false negative rate, *AI* attack impact, *BSR* backdoor success rate, *ASR* attack success rate, *AA* attack accuracy, *TFR* true/false positive, *IA* inference accuracy, *MR* misclassification rate, *PA* prediction uncertainty, *ODT* overall data transferred

Table 12 Survey and comparison of security and privacy measures in general FL environment

References	Proposed work	Privacy/security approach	Base model	Data sets	EP	Achievements
Zhang et al. (2019)	Poisoning attack in FL	Launched poisoning attack using GANs	GAN, CNN	MNIST, AT &T	Acc	Successfully launched a poisoning attack on FL Architecture
Triastcyn and Faltings (2019)	Malicious updates identification, anti-poisoning techniques	Micro-aggregation-based approach for fair detection of attacks, GMM	Federated learning model	Adult Income	Acc, ROC- AOC, FNR	Distinguish abnormal/malicious behavior of clients Fair attack detection.
Li et al. (2021a)	Secure FL (BytoChain)	Byzantine Resistant SecureBlockchained FL at the Edge	Lightweight (CNN)	MNIST	FDR, MDR	Byzantine resistant secure BC FL Bytochain can mitigate five types of attacks
Zhao et al. (2020a)	Security against attacks on Server in FL	Secure member selection strategy using polynomial based solution(PBS), and Shamir's secret sharing	–	–	AL, TO	Proposed and analyzed strong attacks on server
Xin et al. (2020)	Synthetic training data generation for efficient FL training	GAN for synthetic data generation with DP	GAN	MNIST, CelebA	IS	Satisfactory data generation without compromising privacy
Xu et al. (2020)	Privacy preserving FL with irregular users	Yao's garbled circuits and additively homomorphic cryptosystems	CNN	MNIST	Acc, CO, CommC	Robust to dropouts Higher accuracy Reduced computation overheads Reduced communication overhead
Wainakh et al. (2020)	Hierarchical FL (HFL)	Privacy preservation via Hierarchical FL	–	–	–	Flexible framework Privacy-preserving Enhanced trust between participants

Table 12 (continued)

References	Proposed work	Privacy/security approach	Base model	Data sets	EP	Achievements
Domingo-Ferrer et al. (2021)	Secure and privacy FL protect from Byzantine and poisoning attacks	Co-utility framework	–	–	–	Enhanced Security Privacy-preserving Lower computational over-heads
Bai and Fan (2021)	Secure and privacy-preserved in FL	DP and SMC	CNN	CIFAR-10	AA	Defense against member-ship inference attack Defense against poisoning attack Achieved higher accuracy rates
Jiang et al. (2019)	Secure FL (PruneFL)	Model pruning for efficient FL and defense against attacks	VGG-11, ResNet-18, Mobile-NetV3	FEMNIST,CIFAR-10, ImageNet-100, CelebA	–	Defense against Backdoor attack EfficientCommunication Reduced computation overhead Minimized training timings
Cao et al. (2019)	Sniper:protection against poisoning attack	Distributed poisoning model identification in FL, poisoned local models elimination	CNN	MNIST	ASR, ED	Observed poisoning attacks in various scenarios and their success rate
Lin and Huang (2020)	Malware in FL	Malware classification method	SVM, LSTM	Virustotal api	Acc	Achieved higher accuracy Security Privacy-preservation

Table 12 (continued)

References	Proposed work	Privacy/security approach	Base model	Data sets	EP	Achievements
Gu et al. (2021)	Privacy preserved VerticalFL	Asynchronous Vertical FL algorithm for multiparty collaborative learning	–	UCICreditCard, GiveMeSome Credit	Acc	Better convergence Privacy Preservation Achieved higher efficiency than synchronous algorithms.
Zhu et al. (2020)	Secure FL Framework	Weighted FL within secretsharing framework, MPC, anovel encryption method	–	–	–	Guaranteed Security Privacy-preserving
Liu et al. (2018)	Defense Against Backdoor	Fine-pruning, a combination of pruning and, fine-tuning	AlexNet, DeepID, Faster-RCNN	YouTube Aligned Face Dataset	BA PAA	Effective defense against DNN backdoor attacks.

EP evaluation parameters, *DP* differential privacy, *SMC* secure multiparty computation, *BC* blockchain, *CNN* convolutional neural network, *MLP* multi layer perceptron, *GAN* generative adversarial network, *GMM* gaussian mixture models, *Acc* accuracy, *ROC-AUC* area under the ROC curve, *FNR* false negative rate, *FDR* false detection rate, *MDR* missed detection rate, *AA* attack accuracy, *accuracy* loss, *TO* time overhead, *IS* inception score, *CO* communication overhead, *CommC* communication cost, *ASR* attack success rate, *EU* euclidean distance, *BA* baseline attack, *PAA* pruning aware attack

way, malicious clients could not acquire any information regarding the model. Tables 11 and 12 summarized and compared the above-discussed papers.

5.3.2 Internet-of-things (IoTs)

IoT-based networks and their operating systems are vulnerable to massive cyber attacks. Therefore, high-quality data is vital to propose and investigate a solution against this attack, representing various behavioral scenarios. Moustafa et al. (2020) proposed a new IoT-tested architecture for collecting versatile federated data from heterogeneous sources in various malicious scenarios. They employed nine attacks in the dataset, such as scanning, DoS attack, ransomware attack, distributed-DoS (DDoS) attack, injection attack, cross-site scripting attack, password attack, and man-in-the-middle attack, thereby helping the evaluation of AI-based cyber solutions, including privacy- preservation, intrusion detection threat intelligence, etc.

Industrial Internet-of-things (IIoTs) offer promising opportunities to transform future industries. Integrating Artificial Intelligence (AI) with intelligent IIoT is widely employed in realizing IIoT applications. However, to make this scenario highly feasible and reliable, confidentiality, data security, and privacy are crucial requirements (Song et al. 2020b; Khoa et al. 2020). Nguyen et al. (2021a) presented a comprehensive discussion of the use cases to demonstrate the feasibility of FL in IIoT. Along with this, they highlighted major concerns and future directions for the full realization of FL-IIoT in industries (Wang et al. 2020b). But, with the plorification of this integration comes side effects of adversarial attacks and security and privacy threats. To address these issues, Song et al. (2020b) presented a practical cloud-based defense approach against adversarial attacks, FDA3, by distributing the defense capabilities among IIoT devices using FL architecture. On the other hand, Zhang et al. (2020b) used asynchronous DL based on proxy re-encryption and group dynamic management in IIoT-based FL for privacy preservation.

Zhou (2022) designed a verifiable FL framework to deal with a malicious aggregator in IIoT-based application scenarios. Initially, a reliable aggregator is selected using a multi-weight subjective logic model to calculate reputation. And later used a Chinese remainder theorem (CRT) and homomorphic hash function for a secured and variable gradient aggregation. In another work, Wei et al. (2022) proposed a novel chameleon hash scheme with a changeable trapdoor (CHCT) to construct a redactable blockchain for secure FL in IIoT settings. Li et al. (2022) presented a tentacle distribution-based algorithm to identify adaptive poisoning attacks in software-defined IIoT settings. They also proposed a stochastic tentacle data exchanging protocol (STDE) to minimize the impact of adaptive poisoning attacks. In their scheme, the participants with similar learning tasks are assigned to the same tentacle group using cluster analysis. Therefore, the parameter updates outside the clusters are considered "poisoned." Furthermore, they also designed an adaptive DP superposition algorithm to add gaussian noise to average data for the robustness and privacy of the global FL model.

Due to the complex distributed nature of IIoT, it is vulnerable to a wide range of stealthy and evolving cyber-attacks. Abdel-Basset et al. (2022) proposed an integrated. FL framework with distributed temporal convolutional GAN for semi-supervised cyber attack detection in IIoT. They also proposed a novel BC-orchestrated edge intelligence (BOEI) for a privacy-preserved aggregation of distributed local updates. In another work, Han et al. (2022) proposed PCFed, a novel framework with higher accuracy, communicational

efficiency, and guaranteed privacy in IIoTs. They used the de-facto privacy standard DP with the Laplace mechanism.

Energy harvesting (EH) is a very critical and promising technology in the internet of everything (IoE), where edge devices have limited battery capacity and increasing energy consumption. It also suffers from energy information cross threats, energy deprivation, and privacy leakage. Pan et al. (2021) proposed FL based solution for detecting malicious energy user detection method. They also proposed a DP-based private information-preserving scheme. They also designed an incentive mechanism for EH nodes to enhance security. Additionally, Lu et al. (2019a) proposed privacy-preserved data sharing in IIoT using blockchains and FL. The authors designed blockchain-enabled architecture to reduce the risk of data leakage in distributed multiparty data sharing. They integrated DP into FL for data privacy.

In line with this discussion, Kong et al. (2019) used FL for industrial knowledge mining in a secure manner. They proposed federated tensor mining (FTM) framework (Kong et al. 2019) to bring multiple factories within an alliance to share their data, which is encrypted using HE in a centralized FL manner. This allowed raw data within the factory but still allowed a good amount of data for knowledge mining. With the rapid development of communicational technologies, internet-of-vehicles (IoVs) is a new paradigm integrating intelligent vehicle networks in a distributed manner. In IoVs, moving vehicles constantly generate huge amounts of diverse data like traffic information and multimedia-based data, vulnerable to numerous threats Maniak et al. (2018). Lu et al. (2020b) addressed this issue and proposed hybrid blockchain architecture, using permissioned blockchain and locally directed acyclic graphs (DAG) for efficient data sharing in IoV. The IoVs are maintained by roadside units (RSUs), and local DAGs are handled by the vehicles. Furthermore, they used asynchronous FL for efficient learning models and two-stage parameter verification for the reliability of the learned model.

Similarly, Lu et al. (2019b) incorporated local DP into FL and proposed DP-AFL to enhance the privacy of updated local models in vehicular networks. They further proposed a randomly distributed update scheme to protect against security threats to centralized curators. Providing personalized services to clients in an intelligent transportation system (ITS) requires data sharing among vehicles. In IoV scenarios where edge devices are mobile, they need enhanced data-sharing schemes for efficiency and reliability. The overall learning system is such an AI-based novel approach that helps to improve training efficiency on the data set. Using the broad learning system approach, Yuan et al. (2021) proposed FeBBLS, a federated bidirectional connection broad learning scheme to share data securely. They used a bi-directional connection overall learning system (BiBLS) model for training the vehicular nodes.

Issa et al. (2022) reviewed blockchain-based FL methods and techniques to present the current state of research on the security and privacy of IoT ecosystems. The study focused on the security perspective, challenges, and open research questions associated with integrating blockchain and FL in IoT applications. In recent work, Qu et al. (2020) also used blockchains in FL to resolve the security concerns of fog-based IoT networks. Wang et al. (2021) focused on the anomaly detection in IIoT using FL.

Few authors focused on privacy concerns in distributed vehicular networks. Lu et al. (2020c) presented a novel privacy-preserving FL mechanism for data privacy preservation in vehicular IoT networks using a two-phase mitigation scheme. Similarly, Zhao et al. (2020b) integrated local-DP with FL crowdsourcing applications in an IoV-based network. Crowdsourcing application owners can infer users' location, vehicle information, traffic information, etc. The proposed approach assured the vehicles' generated gradients' privacy

to prevent attackers from deducing original data even after obtaining the gradients. Vehicular ad-hoc Network (VANet) for IoV suffers a data falsification attack in which false information, such as position falsification, is exchanged between the vehicle nodes. Uprety et al. (2021) focused on detecting position falsification attacks in the federated setting of IoV. Vehicles in VANet periodically broadcast information as basic safety messages (BSM).

But attackers can exploit this information and launch a falsification attack by corrupting BSMs. Therefore, the authors used FL, where the model is trained on the edge vehicles on their private information and avoids information exchange between vehicles, thereby prohibiting the attackers from corrupting the training data.

Apart from the numerous capabilities of FL, it also facilitates anomaly detection in IoT-based FL networks. Nguyen et al. (2019) proposed distributed IoT (DIoT), an autonomous self-learning distributed system for compromised IoT-device detection. Every IoT device in the network shares its local detection profile with the security gateway, providing access to a massive dataset with various features to build an efficient anomaly detection model for the IoT network. DIoT does not require any human intervention or labeled data to operate. Khoa et al. (2020), presented a collaborative learning intrusion detection system for IoT industry (4.0) network (4th industrial revolution), i.e., smart factory, smart industry. They used deep neural network (DNN) trained filters to identify and prevent cyber-attacks at IoT gateways in industry 4.0. These filters are trained on the local data of its subnetwork. The server aggregates the massive updates from distributed IoT gateways and achieves high learning accuracy without compromising data privacy. To further evaluate FL support for intrusion detection systems, Cetin et al. (2019) conducted experiments in an FL-based simulated environment that allows edge devices to collaborate in the training of a global anomaly detection model without sharing their sensitive data. Results showed higher classification accuracy and reduced computation and communication cost.

In an another work, by Athba et al. (2020) proposed ML-based IDS for IoT devices using federated mimic learning (Shafee et al. 2020) for privacy preservation. In mimic learning, a student model learns from the teacher model, and in this way, knowledge is passed on. On the other hand, Arachchige et al. (2020) amalgamated DP, Ethereum blockchains, and smart contracts with FL for enhanced safety, security privacy, and resilience in IIoT systems. Wu et al. (2021) applied an incentive mechanism in IoT-based FL to ensure privacy. The incentive mechanism is based on the client's task expenditure, including privacy, computation, and communication costs. They also used the DP mechanism for privacy preservation. Furthermore, they designed a multi-dimensional contract for optimal rewards, making the users abide by privacy and security norms. In another work, Tabassum et al. (2022) proposed a novel federated DL-based IDS system using GAN (FEDGAN-IDS) to detect cyber threats in smart IoT systems. They used GAN to augment and create a balanced training dataset that helped better generalize model training. Similarly, Kalapaaking et al. (2022) proposed a BC-based secure aggregation using Intel-SGX-based TEE for IoTs. Continuous authentication is necessary for mobile devices like smartphones and IoTs for analyzing their behavioral interactions. But this may increase the chances of privacy leakage as authentication requires the participants' personal data. Wazzah et al. (2022) proposed a novel warm-up FL-based continuous authentication mechanism with privacy-preserving assurances for mobile and IoT-based distributed networks.

On the other hand, Zhang et al. (2020c) proposed a novel poisoning attack and experimentally demonstrated the effectiveness of this attack on IoT-based FL settings. They used GANs for poisoned data generation. To effectively launched this attack, they created a fake dataset named Data_Gen, that mimics the participant training data to explore an active and powerful poisoning attack in IoT-based FL. Working with IoT attacks, one more attack is

known as a "zero-day botnet" attack. Zero-day botnet attacks exploit unknown vulnerabilities that exist in a system. It got its name because this attack occurred one day before the first day the unknown vulnerability became public. DL-based methods are generally used to detect botnet attacks in IoT networks. But in the centralized approach, botnet attacks cannot be detected without compromising the users' privacy.

Popoola et al. (2021) focused on detecting botnet attacks to avoid data privacy leakage in IoT edge devices using FL. The authors employed an optimal DNN architecture for network traffic classification. They achieved satisfactory results to guarantee privacy and security, lower communication overhead, and lower network latency. Results showed federated DL methods outperformed centralized, localized, and distributed application scenarios. Malware is one serious security threat in the internet world. Taheri et al. (2020) presented a robust FL-based architecture, namely, Fed-IIoT, for malware detection for android applications in IIoT both at participants and server-sides. Tables 13, 14, and 15 listed and compared the major work done in the security and privacy of FL-IoTs. Soon, 5G technology will connect all walks of life. But deploying 5G in IoT needs special techniques and consideration because of the heterogeneity and diversity of IoT networks. Fan et al. (2020a) proposed IoTDefender, an intrusion detection framework for 5G IoT-based FTL.

5.3.3 Intelligent transportation system

In Intelligent Transportation System (ITS), FL can provide adaptable and efficient training of ML and DL models for traffic flows prediction, traffic sign detection and classification, pedestrian detection, behavior forecasting, traffic congestion detection, and many more. Because of the availability of the versatile and massive amount of training data distributed across the IoVs (Manias and Shami 2021). But again, this distributed setting opens new attack fronts that must be tackled. Elbir et al. (2020) investigated the usage and FL over ML in vehicular networks to develop an efficient ITS Patel et al. (2022a). They investigated the learning and communicational perspective along with security and privacy concerns. Cars have become one of the most computationally powerful mobile edge devices, and their low cross-device communication bandwidth needs could potentially help overcome the current network limitations.

Research in the autonomous driving domain shows a huge scope of improvements and enhancements through FL. In this direction, Claas Brüß (2021) used FL for pedestrian behavior forecasting and analyzed whether the training of these forecasting models could be federated. Results showed an opportunity for improvements through this scheme due to the availability of huge training data volumes and highly paralleled training. Liu et al. (2020b) proposed FedGRU, an FL aggregation algorithm using FedAvg (Canetti et al. 1996) aggregator and gated recurrent neural network (RNN) for traffic flow prediction. The recurrent unit enabled the global model to capture spatiotemporal correlation for traffic flow. Their work in traffic flow prediction is pioneering and achieved comparable results with competing techniques with little accuracy degradation and privacy preservation. Nuding and Mayer (2020) studied and evaluated the effectiveness of poisoning attacks in the FL settings for traffic sign classification. They manipulated the training process to embed a backdoor and evaluated the possibilities of creating a backdoor, its effectiveness, and its contribution to learning the classification model. The IoVs interconnect smart vehicles, allowing them to share useful information for independent decision-making by an autonomous vehicle. Moulahi et al. (2022) used FL to protect vehicle privacy. On the other hand, using blockchains ensured the integrity of the data and the safety of model aggregation.

Table 13 Survey and comparison of FL security and privacy measures in IoT-based application areas

References	Area	Proposed work	Privacy/security approach used	Base model	Dataset	EP	Achievements
Song et al. (2020b)	IIoT	Defense against adversarial attacks for cloud-based IIoT (Fda3)	ModifiedFL Framework, A novel Loss function	LeNet ResNet	MNIST CIFAR10	Acc	Defense against maliciousattacks and adversarial attacks
Wang et al. (2021)	IIoT	Anomaly detection in IIoT	Deep deterministic policy gradient (DDPG)	DRL	–	Th, AL, ADA	Higheranomaly detection accuracy Privacy-preservation Higher throughput Lower latency
Lu et al. (2019a)	IIoT	Privacy in data sharing in IIoT	DP, consensus process of permissioned BC	Text GCN	Reuters, 20 newsgroup	ROC, ROC-AUC	Privacy preservation Enhanced security, efficiency and accuracy
Kong et al. (2019)	IIoT	Federated tensor mining for secure IIoT (FTM)	Encryption, HE, Knowledge Decryption	–	@@	RA, OR, AE	Defense against eavesdroppers and hackers Data privacy Increased mining accuracy
Lu et al. (2020b)	IoV	AsynchronousFL for secure data sharing in IoV (PermiDAG)	Hybrid BC architecture, Two-stage (DAG) verification	DRL, CNN	MNIST, ***	Acc, CR	Higher accuracy Faster convergence
Lu et al. (2019b)	IoV	FLfor secure IoV data sharing (DP-AFL)	Local DP for local model update, GBDT for local training	–	Reuters, 20 news- groups, Ohsumed	ROC, ROC- AUC	Privacy preservation Enhanced security, -Convergence boosting through updates verification and weighted aggregation
Qu et al. (2020)	Fog- IoT	Decentralized privacy in FL–based fog computing	BC	CNN	Fashion-MINIST, CIFAR-10	Acc, ToD, CSR	Decentralized privacy High efficiency Resistance to poisoning attack proof
Lu et al. (2020c)	IoV	Vehicular cyber- physical-systems (VCPS) inIoV	New random sub-gossip updating scheme	CNN	Real-time	Acc	Privacy preservation Mitigate data leakage, Not safe against eaves-dropping

Table 13 (continued)

References	Area	Proposed work	Privacy/security approach used	Base model	Dataset	EP	Achievements
Zhao et al. (2020b)	IoV	Privacy in IoV	Local DP, Federated SGD algorithm	–	##, WISDM Human Activity Recognition, WO public datasets	PB	Privacy preservation
Uprety et al. (2021)	IoV	Vehicle misbehavior detection in IoV using FL	Locally model training in the vehicle, no data-sharing	ANN	BSM, VeReMi	P, R, Acc	Privacy preservation Better position falsification attack detection in FLsettings than a centralized approach
Nguyen et al. (2019)	IoT	FL-based IDS for IoT (DÏoT)	Self-learning distributed system for device-type detection models for anomalous behavior	GRU	Mirai (IoT Malware)	FPR, TPR	Higher anomaly detection rate
Khoa et al. (2020)	IIoT	Intrusion detection in IoT	Design smart "filters" at the IoT gateways to promptly detect and prevent cyberattacks	DBN	KDD, NSLKDD, UNSW-NB15, N-BaIoT	RMSE, Mar, Acc	Enhanced privacy Increased detection accuracy Reduce network traffic
Cetin et al. (2019)	IoT	Intrusion detection in IoT	Federated Wireless Network	SAE	Aegean Wi-Fi Intrusion	CB, Acc	Strong defense against ID Effective in terms of classification accuracy, computation cost, communication cost

EP evaluation parameter, *DP* differential privacy, *ADA* anomaly detection accuracy, *Text GCN* text graph convolutional networks, *HE* homomorphic encryption, *GBDT* gradient boosting decision tree, *GRU* gated recurrent units, *IDS* intrusion detection system, *ID* intrusion detection, *DBN* deep belief network, *SGD* stochastic gradient descent, *ROC* receiver operating characteristic, *SAE* stacked autoencoders, *Acc* accuracy, *Th* throughput, *AL* average latency, *ROC-AUC* area under the ROC curve, *RA* reconstruction accuracy, *OR* outlier ratio, *CB* convergence behavior, *DRL* deep reinforcement learning, *AE* average error, *CR* cumulative reward, *ToD* the turbulance of data, *CHR* cost of hash-rate, *PB* privacy budget, *P* precision, *R* recall, *FPR* false positive rate, *TPR* true positive rate, *RMSE* root mean square error, *M* margin

@@Real-time data collected, ***Dataset of Uber pickups in New York City, ##Real-world and synthetic Datasets

They performed classification tasks in VANets and cyber-threat detection at the vehicles. Table 16 highlights the proposed security measures in ITS areas.

5.3.4 Smart cities/homes

The main reasons behind the surging popularity of IoT are their quality of service, easy installation, and inexpensive. Hence, IoTs are used in smart cities, buildings, infrastructures, etc., to make life efficient and sustainable. They are ubiquitous everywhere, from lighting and air conditioning to surveillance and management (Wang and Qiao 2019; Fraboni et al. 2021). Earlier work in smart infrastructure generally focuses on centralized approaches using IoT sensors. IoT-based infrastructures are also exposed to cyber threats and privacy leakage despite their numerous benefits. Therefore, to make smart infrastructures robust and secure, researchers are deploying FL to leverage its benefits (Jiang et al. 2020a). Working in this area, Dasari et al. (2021) proposed an FL-based framework for smart building energy prediction. Energy management is a very crucial component of a smart building. Therefore, predicting energy consumption using ML models is a general approach. They presented the architectural details of their proposed framework and compared it with centralized ML methods for the achieved benefits along with privacy preservation.

In addition, Yu et al. (2020a) proposed, LoFTI, a federated multitask learning framework that learns general features to capture contextual access patterns of users from smart homes in a privacy-preserving manner. These contextual patterns are necessary to be identified to form contextual policies. Because if we allow IoT devices in our homes, these contextual policies should be pre-decided to protect against security, privacy leakage, and physical hazards. In addition, Otoum et al. (2021) proposed an integrated adaptive framework that combines blockchain and FL for a secure and trustworthy network for IoT-based smart city services and applications.

Similarly, Sater and Hamza (2020) introduced an FL-based LSTM model on time series data generated by smart-IoT sensors for energy usage prediction such as lighting, fault detention, and better energy management system. Their proposed model showed fast model convergence of model along with the default inherited privacy and security capabilities of FL. In another work, Zhao et al. (2020c) focused their work on privacy preservation in IoT-based smart home systems with mobile phones as clients. They used DP and blockchains to prevent malicious model updates in their proposed hierarchical crowdsourcing FL system for training ML models. Their proposed system can help home appliance manufacturers improve their products' quality and services. Table 17 describes and compares the major security and privacy defense mechanisms proposed in FL-based smart city infrastructure.

5.3.5 Aggregaation algorithm

Aggregation algorithms need to be efficient in dealing with the various challenges in FL, such as heterogeneity in data, clients, models, communication issues, anomalies in received gradients and parameters, privacy preservation, and handling asynchronous updates. Several algorithms have been proposed to tackle the abovementioned challenges, summarized in Tables 18 and 19. Konečnỳ et al. (2016) proposed federated average (FedAvg) used in a centralized FL setting in which the central server is responsible for orchestrating the training process. It shares the global model with all the clients and collects respective model

Table 14 Survey and comparison of proposed FL security and privacy measures in IoT-based application areas

References	Area	Proposed work	Privacy/security approach used	Base Model	Dataset	EP	Achievements
Wei et al. (2022)	IIoT	Secure FL	Chameleon hash scheme with a changeable trapdoor (CHCT), Redactable medical blockchain with CHCT (RMB)	LeNet, ResNet model	MNIST, CIFAR10	Acc	Trapdoor restricted and can be abolished at any time Security and efficient scheme
Li et al. (2022)	IIoT	Poisoning attacks in IIoT	Multi-tentacle FL scheme (MTFL), Stochastic tentacle data exchanging (STDE), Adaptive DP superposition algorithm	–	MNIST, Cifar10	Acc	Robustness of global FL model Improve model accuracy under adaptive poisoning attacks
Abdel-Basset et al. (2022)	IIoT	Cyberattack Detection in (IEoT)	BC-orchestrated edge intelligence (BoEI) framework	TCGAN	TON_IOT, LITNET-2020	Acc, P, R, Fs	Secure framework
Han et al. (2022)	IIoT	PCFed, a novel privacy-enhanced and communication-efficient FL framework	DP and Laplace *Mechanism*	SVM, k-means-based clustering	*WM-811K, *Surveil Edge	Acc	Higher model accuracy Rigorous privacy guarantees Communication efficiency
Kalapaaking et al. (2022)	IoT	Secure FL environment for IoT	BC-powered trustworthy aggregated model using Intel-SGX based TEE	AlexNet, LeNet, VGG16	Fashion MNIST, CIFAR-10, MNIST	Acc	Achieved a good balance between privacy and model performance
Wazzeh et al. (2022)	Mobile, IoT	Continuous authentication mechanism for mobile and IoT devices for privacy	Warmup FL approach, for continuous authentication on mobile and IoT devices	CNN	MNIST, CIFAR-10, FEMNIST	Acc, CR	Increased the accuracy of FL process

EP evaluation parameters, *CNN* convolutional neural network, *TCGAN* temporal convolutional generative adversarial network, *IoET* internet-of-edge-of-things, *BC* blockchain, *DP* differential privacy, *Intel-SGX* Intel Software Guard Extension, *TEE* trusted execution environment, *SVM* support vector machine, *CR* communication rounds, *Acc* accuracy, *Fs* F1-Score

updates and parameters from them to get the final trained global model. FedAvg uses the averaging logic for calculating the weighted sum of all received local model parameters from clients. But FedAvg cannot tackle the heterogeneity present in the FL environment (Nilsson et al. 2018).

To handle heterogeneity in FL Li et al. (2018) proposed a modified version of FedAvg, known as FedProx (Li et al. 2018) that showed better performance in a heterogeneous environment. FedProx algorithm can assign a different amount of work to the clients based on the client's capabilities (computational power or other factors) and performance over various rounds. To deal with non-uniformity in the model updates from the clients, FedProx allows partial work instead of uniform work. To address the challenges of a mobile-devices-based FL environment, Canetti et al. (1996) proposed the secure multiparty computation (SMC) algorithm that ensures privacy-preserving aggregation of the updates from unreliable clients. Because unreliable clients can drop out at any time from the training. This algorithm showed fault tolerance, which means the system will work well even if one-third of the clients fail to participate.

Wang et al. (2020c) proposed a federated matched averaging (FedMA) algorithm for training DL models, e.g., CNNs and LSTM, in a heterogeneous federated environment. In standard aggregation, the parameters of local models are averaged element-wise with weight proportional to the sizes of the client dataset. However, this averaging logic may affect the overall model's performance and also put a significant communicational burden. To overcome this, FedMA performs the aggregation by matching and averaging the hidden elements, such as neurons and channels with the same features. Experiments showed that FedMA outperformed FedAvg and FedProx within a few initial training rounds. Zhang et al. (2022) proposed a verifiable secure aggregator, G-VCFL, a group-verifiable chained privacy-preserving FL scheme. It used a grouped chained training structure to improve training efficiency and verify the correctness of the aggregation results. Instead of any complex cryptographic technique, they utilized lightweight pseudo-random generators for the privacy preservation of users.

Due to the non-identical distributed (non-iid) nature of data in the FL environment, client drift or gradient dissimilarity results in unstable training and slow convergence. To address this issue, Karimireddy et al. (2020) proposed a stochastic controlled averaging algorithm (Scaffold) that used control variates (variance reduction) to ensure that client updates are moving in the right direction (both at client and server-side). Scaffold showed fast model convergence in a heterogeneous environment in significantly fewer rounds. Several works aim at improving data privacy in FL. They typically prevent access to local updates using secret sharing techniques and encryption to reduce information leakage by applying noise. Bonawitz et al. (2017) proposed another secure aggregation algorithm in an FL environment. The authors used Shamir's secret sharing (SSS) combined with symmetric encryption to protect local models and can tolerate dropouts. However, their proposed aggregation algorithm increased the communicational overhead of training rounds.

Xu et al. (2019a) extended the work of Bonawitz et al. (2017) and proposed, Veri-fyNet, by adding verifiability on top of it using the double-masking protocol for users' confidentiality. In a similar work, Gou et al. (2020) proposed VeriFL, a communication-efficient verifiable aggregation protocol that can efficiently handle dropouts. Both rely on a trusted party to generate public/private key pairs for all clients. Kadhe et al. proposed FastSecAgg (Kadhe et al. 2020), a multi-secret sharing secure aggregation protocol based on fast Fourier transform (FFT). Their proposed protocol is robust against dropouts and guarantees security against colluding server attacks and adaptive adversaries. Furthermore,

Table 15 Survey and comparison of proposed FL security and privacy measures in IoT-based application areas

References	Area	Proposed work	Privacy/security approach used	Base model	Dataset	EP	Achievements
Zhang et al. (2020c)	FL-IoT	Generative poisoning attack on FL	Poison Data Generation using GANs for fake training sample generation, and a novel poisoning attack model (PoisonGAN)	Res Net-18, CNN	MNIST, Fashion-MNIST, CIFAR-10, Data_Gen	Acc	Launched strong poisoning attack Designed poison data generation method Effectively compromised global model
Popoola et al. (2021)	IoT-FL	Avoid data privacy leakage in IoT Edge Devices	Zero-day botnet attack detection using FDL	DNN	Bot-IoT, N-BaIoT data set	Acc, P, R, Fs	Detects zero-day botnet attacks with high classification performance Guarantees data privacy and security Low communication overhead Requires low-memory space for storage of training data Low network latency.
Fan et al. (2020a)	5G-IoT	ID framework for 5G IoT (IoTDefender)	Customized detection models by FTL	CNN	CICIDS2017, NSL-KDD,$^{\$\$}$	Acc, TPR, FPR	Personalized model for privacy-preservation Unknown attacks detection with excellent generalization
Wu et al. (2021)	IoT-FL	Private FL	3-D contract-based Incentivizing differentially private mechanism	LeNet	MNIST (iid)	PB, TA	Optimal reward for different types of data owners
Arachchige et al. (2020)	IIoT	Trustworthy framework for ML in IIoT	Amalgamation of DP, federated ML, Ethereum BC, and Smart contracts	CNN	MNIST	Acc	Privacy-preservation Enhanced security

Table 15 (continued)

References	Area	Proposed work	Privacy/security approach used	Base model	Dataset	EP	Achievements
Al-Marri et al. (2020)	IoT	IDS for FL–IoT	Combination of the advantages of FL and Mimiclearning	MLP	NSL-KDD dataset	DA, Acc, P, R, FA, Fs	Efficient IDS
Zhang et al. (2020b)	IIoT	Two Privacy-preserving Asynchronous DL schemes	Proxy re-encryption technique, Dynamic update secrecy inherently group key management method using Additive HE	–	MNIST	–	Secure Efficient Privacy-preserving
Pan et al. (2021)	IoT	Secure Energy harvesting (EH) in IoT	DP-empowered information preservation scheme, Noncooperative-game-enabled incentive mechanism for participation	–	–	TAR, TPR, FPR	Enables secure and privacy-preserving Avoid privacy leakage Encourage participation in proposed joint protection system
Chamikara et al. (2021)	IoT	Privacy preservation in IoT-FL	Distributed perturbation algorithm (DISTPAB)	ANN	SSDS dataset	CA, AR	Strong privacy-preservation
Yuan et al. (2021)	IoV	Secure data sharing in FL- IoV (FeBBLS)	Federated bidirectional connection broad learning scheme for secure model aggregation, Transfer Learning for V2V	CNN	MNIST	Acc	Improved the average accuracy of prediction on the server Reduced the size of parameters sharing between server and vehicle nodes

Table 15 (continued)

References	Area	Proposed work	Privacy/security approach used	Base model	Dataset	EP	Achievements
Taheri et al. (2020)	IIoT	Malware Detection in IIoT	Byzantine Median (BM) and Byzantine Krum, Aggregation of FL, and GAN algorithms for adversaries detection in server-side components. GAN-based attack algorithm		Drebin, Genome, Contagio Dataset	Acc	Outperformed existing defense-based schemes in terms of accuracy
Tabassum et al. (2022)	IoT	IDS for smart IoT	Used GAN to augment and create a balanced training dataset	CNN, AC- GAN	NSL-KDD, KDD-CUP, UNSW-NB15 (non-iid)	Acc, P, R, Fs, AUC	Enhanced security
Zhou (2022)	IIoT	Secured and variable gradient aggregation	Homomorphic hash function, Chinese remainder theorem and blinding method	CNN	–	Acc, RT	Secured and variable gradient aggregation

EP evaluation parameter, *FTL* federated transfer learning, *CNN* convolutional neural network, *DP* differential privacy, *DNN* deep neural network, *MLP* multi-layer perceptron, *ANN* artificial neural network, *RT* running time, *P* precision, *R* recall, *AUC* area under the curve, *Fs* F1 score, *TAR* test accuracy rate, *FPR* false positive rate, *TPR* true positive rate, *CA* classification accuracy, *AR* attack resistance, *PB* privacy budget, *TA* test accuracy, *DA* detection accuracy, *FA* false alarm, *RT* running time

$SPrivate datasets from two different smart home networks

Table 16 Survey and comparison of proposed FL security and privacy measures in intelligent transportation system

References	Area	Proposed work	Privacy/security approach	Base model	Data sets	EP	Achievements
Nuding and Mayer (2020)	Traffic-Sign Classification (TSC)	Launched Poisoning Attack in TSC using FL	Manipulation of the training process to embed a backdoor	CNN	European Traffic Signs Dataset	TA	Confirmed that FL settings are vulnerable to adversaries Successfully installed backdoors in FL
Liu et al. (2020b)	Traffic-Flow Prediction (TFP)	Privacy Preserving aggregator for TFP (FedGRU)	Secure parameter aggregation mechanism using enhanced FedAvg with Joint Announcement Protocol	GRU	Caltrans (PeMS) Dataset	MAE, MSE, RMSE, MAPE	Privacy Preserving, Enhanced Prediction Accuracy
Moulahi et al. (2022)	Classification task at vehicle	Cyber Threat detection at vehicle	BC	SVM, RF, NB, KNN	VeReMi Dataset	Acc,P, R, Fs	Enhance Security Privacy by design

EP evaluation parameters, *TA* test accuracy, *BC* blockchain, *GRU* gated reccurent unit, *CNN* convolutional neural network, *SVM* support vector machine, *RF* random forest, *NB* naive, bayesian, *KNN* K-nearest neighbour, *RMSE* root mean square error, *P* precision, *R* recall, *Acc* accuracy, *MAE* mean absolute error, *MSE* mean square error, *RMSE* root mean square error, *MAPE* mean absolute percentage error

Table 17 Survey and comparison of proposed FL security and privacy measures in Smart City/Building applications

References	Area	Proposed work	Privacy/security approach	Base model	Data sets	EP	Achievements
Dasari et al. (2021)	Smart Buildings	Privacy Enhanced EnergyPrediction in Smart Buildings using FL	TTP server for secure aggreg-ation	DNN		RMSLE	Privacy Preservation Better predictions than centralized Approach
Yu et al. (2020a)	Smart Homes	Proposed solution for privacy leakage threats to smart homes from IoT devices in FLA	Learning Context-Aware Policies from Multiple homes via multitask FL	DNN	@ CASAS	P,R, Acc, Fs	Privacy-Preservation Security Achieved Lower FP/FN rate than state-of-the-art mechanisms
Otoum et al. (2021)	Smart City	Securing Critical IoT infrastructure with Blockchain-supported FL	Blockchain, adaptive FL-based trust evaluation (AFL-TE)	RL	Traffic Dataset	Acc, DR	Enhanced security and Trust Efficient energy consumption Higher accuracy and detection rates of system
Sater and Hamza (2020)	Smart Building	An FL approach for Anomaly Detection in Smart Buildings (FSLSTM)	Pattern learner process, pattern recognizer, threshold determinator, and anomaly classifier for anomaly detection	Federated Stacked LSTM	**	BA,P, R,ROC, AUC	Fast model convergence than centralized approach Privacy Security Superior performance in anomaly detection
Zhao et al. (2020c)	Smart Home Appliances	Privacy-Preserving FL for crowdsourcing system	DP, BC(prevents malicious model updates)	CNN	MNIST Dataset	TA	Privacy-Preserving Blockchain-FL for crowdsourcing system
Aïvodji et al. (2019)	Smart Home	Proposed a secured and privacy-preserving smart home (IoT-FLA)	IoT-FL Architecture, ECIPAPprotocol for secure data aggregation, IDS	–	–	–	Privacy Security

EP evaluation parameters, *RL* reinforcement learning, *TTP* trusted third party, *DNN* deep neural network, *CNN* convolutional neural network, *LSTM* long short term memory, *RMSLE* root mean square log error, *Acc* accuracy, *DR* detection rate, *BA* balanced accuracy, *P* precision, *R* recall, *ROC-AUC* area under the ROC curve, *TA* test accuracy, *Fs* F1 score

**Real-world datasets generated, @ Public large-scale IoT historical record dataset

Table 18 Survey and comparison of proposed FL security and privacy using Secure Aggregators

References	Local updates sharing approach	Methodology	Achievements
SMC Canetti et al. (1996)	Secret sharing Based approach	Encrypt uploaded parameters	Dropout tolerance Privacy preserving, Efficiency loss due to encryption
FedAvg McMahan et al. (2017)	–	Parameters averaging	Dropout tolerance Model convergence in hetrogeneous environment
Bonawitz et al. (2017)	Secret sharing Based approach	Shamir's Secret Sharing	Secure Aggragation Guranteed Privacy, but with extra rounds
VerifyNet Xu et al. (2019a)	Secret sharing Based approach	Zero-knowledge Prooof Double Masking Homomorphic Hash	High Security Verification of Server's result Robust
VeriFL Guo et al. (2020)	Secret sharing Based approach	Linear Homomorphic Hash	Privacy Verification of Server's result, Reduced Communication and Communicational overhead
FastSecCAGG Kadhe et al. (2020)	Secret sharing Based approach	Fast Fourier Transform	Privacy Dropouts Tolerance Secure Against Colluding Attack Security against Adaptive Adversries Reduced Communication Cost
TurboAgg So et al. (2021)	Secret sharing Based approach	Multi-Group Circular Strategy	Tolerate 50% Dropouts Guranteed User Privacy Secure Against Colluding Attack Fast Computation
Safer Beguier and Tramel (2020)	Secret sharing Based approach	Model Updates Compression Technique	Guranteed Privacy Secure Aggregation
SafeLearn Tabassum et al. (2022)	Secret sharing Based approach	Secure Two Party Communication	Guranteed Privacy Secure Aggregation Dropouts Tolerance, No expansive computations Reduced Computation and communicational overhead

Table 18 (continued)

References	Local updates sharing approach	Methodology	Achievements
Truex et al. (2019)	Encryption	Differential Privacy	Protection against Inferrence Attack,
Wu et al. (2020)	Encryption	Threshold Homomorphic Encryption	Achieved higher accuracy Reduced Noise, End-to-End Private FL
Madi et al. (2021)	Encryption	Partial encryption of model updates	Security Privacy
Li et al. (2020d)	–	Homomorphic Encryption (HE) Verifiable computing (VE)	Security Privacy
Zhao et al. (2021a)	–	Differential Privacy Gaussian noise	Secure Maintained convergence rates Better Communication efficiency High testing accuracy.
Shayan et al. (2021)	Intel SGX	Trusted Execution Environment (TEE)	Secure
	P2P-FL Aggregatoor	Blockchain	Robust to Byzantine adversaries computationally efficient Privacy-preserving
		Cryptographic techniques	Secure Privacy-preserving

FastSecAgg, significantly reduced the communication cost of the aggregation to make the system efficient and secure. In another, So et al. (2021) proposed Turbo-Aggregate, another fast aggregation algorithm suitable for wireless topologies with unreliable users. Therefore, Turbo-Aggregate can handle unreliable wireless networks with reduced communication and computation overhead but at the cost of increased round complexity.

Similarly, Beguier et al. proposed SAFER (Beguier and Tramel 2020), another privacy-preserving secure aggregation protocol based on compression of the model updates and use them for aggregation for security. SAFER is more suitable for FL's healthcare, medical, and application areas. However, this protocol assumes a small number of clients without any dropouts with identical distributed (iid) data. To overcome the limitations of the previously discussed aggregator, Tabassum et al. (2022) proposed another secure aggregation protocol named SAFELearn. It is a generic private secure aggregator that defends against inference attacks for private FL that does not rely on any trusted third party. It is robust, does not requires any complex cryptographic operations, and is computation efficient.

All the above-discussed aggregation algorithms are based on the secret-sharing approach for ensuring the secrecy of the model updates sharing. In some other works, authors used encryption to achieve security. Truex et al. (2019) proposed an algorithm that uses DP and threshold homomorphic encryption to achieve privacy and security. Their proposed method ensured secrecy and privacy but could not tolerate dropouts and added significant runtime overhead to the system, making it impractical for the real-time scenario. EaSTFfly (Dong et al. 2020) algorithm is another encryption-based approach using pallier-homomorphic encryption or SSS along with quantization. EaSTFfly offers secure aggregation with privacy preservation. Furthermore, the authors designed an attack strategy to analyze the privacy of ternary gradients.

In general, encryption of the local gradients increases the computational and communicational overhead of the overall FL system. BatchCrypt (Zhang et al. 2020) proposed a system solution for cross-silo FL to reduce this overhead by encoding a batch of gradients and then encrypting them instead of encrypting individual gradients. HybridAlpha (Xu et al. 2019b) uses DP with multiparty computations and encryption to guarantee security and privacy. POSEIDON (Sav et al. 2020) encrypts the complete FL process using zero-knowledge proof and lattice-based multiparty HE. Additionally, the authors used a tree-like network instead of classical star topology to reduce computational overhead. Last but not least, BaFFLe (Andreina et al. 2020) and FLGUARD (Nguyen et al. 2021c) are secure aggregation protocols that provide security and a strong defense against backdoor attacks.

Li et al. (2020d) proposed an enhanced version of the FedAvg algorithm using DP gaussian noise for secure aggregation. Madi et al. (Madi et al. 2021) combined HE with verifiable computing to perform aggregation in the encrypted domain and then verified the results to confirm the valid updates. Their proposed approach showed secured and privacy-preserving global model aggregation. Shayan et al. (2021) proposed another aggregation algorithm for fully decentralized peer-to-peer (P2P) FL settings. It uses blockchains and cryptographic techniques for peer-client coordination and privacy preservation. In (Wu et al. 2020), authors achieved secure aggregation by encrypting only the inner product of model updates instead of encrypting entire updates altogether. They achieved efficient and secure aggregation of the model. Zhao et al. (2021a) is a secure and efficient aggregation framework for robust byzantine FL. SEAR relies on the trusted execution environment (TEE), Intel SGX, to protect clients' privacy.

5.3.6 Recommendation systems

Recommendation systems are now integral to various applications we use on the internet, such as social media, e-commerce, or any other online activity. These systems are trained on users' internet behavior, choices, interests, and search patterns. Therefore, it becomes crucial to protect users' data and private information from malicious activity. FL is a suitable framework for training a recommendation system without compromising users' privacy. Here, we have discussed the major work done by researchers for an efficient recommendation system using FL.

Li et al. (2020e) proposed an FL-based wireless recommendation system for consumers using a combination of DP and multiagent bandit learning. They experimented in both "master-worker" and "fully decentralized" FL setting to maintain privacy and explored how the addition of noise affects the learning and decision of an aggregator to the following recommendation. In another work, Zhao et al. (2020e) proposed Fed4Rec, a privacy-preserving online page recommendation system using FL and model-agnostic meta-learning. In model-agnostic meta-learning, the model is trained on data from public users (who share data with servers) and private users (who do not share data with users). Fed4Rec aggregates recommendations for public users on the servers and the local devices for private users. Results showed that Fed4Rec outperformed the baseline recommendation system.

Similarly, Lin et al. (2020) proposed FedRec, a federated recommendation system for rating predictions of items for customers from explicit feedback without sharing any rating behaviors or records of users with the centralized server or other users. They proposed and utilized user averaging (UA) and hybrid filling (HF) to protect users' privacy. In another work, Zhou et al. (2019) proposed a privacy-preserving distributed personalized social recommendations system in a centralized FL setting to avoid unreliable network connections in the distributed FL approach. They used DP to handle the users' privacy. Blockchain is not limited to banking and financial sectors only. It is now used in several other application areas, such as IoT, smart grids, UAVs, and healthcare. Hai et al. (2022) used Blockchain in the healthcare management system to ensure the privacy and security of electronic medical and health records. Their proposed BVFLEMR, a blockchain vertical FL e-medical recommendation system, recommends a tailored treatment to patients after analyzing their health records in an electronic health record database.

In a similar work, Ammad et al. (Ammad-Ud-Din et al. 2019) proposed a personalized recommendation system using federated collaborative filtering (Fed-CF) to protect users' privacy. The authors claimed to be the first to use collaborative filtering for privacy preservation that models interactions between uses and sets of items. Experiments showed Fed-CF achieved similar recommendation performance with state-of-the-act systems without compromising users' privacy. In contrast to the above work Jian et al. (2020) focussed on the security threat caused by shilling attack (Lam and Riedl 2004) in the FL environment and proposed FSAD, a federated shilling attack detector. It is a well-known and studied attack in the recommendation system that influences the prediction of the recommendations system by generating fake or malicious user accounts that assign random or predecided ratings to an item to increase or decrease its sale. They utilized a semi-supervised Bayes classifier to identify malicious attackers among genuine users. Table 20 compared the above-discussed research in recommendation systems using FL.

Table 19 Survey and comparison of proposed FL security and privacy using Secure Aggregators

References	Local updates sharing approach	Methodology	Achievements
EaSTFly Dong et al. (2020)	Encryption and secret sharing	Shamir's threshold secret sharing Piallier homomorphic encryption	Analyzed Privacy of TernGrand Protection against Semi-honest adversary Privacy-preserving Higher accuracy Communication and Computa-tionoverhead reduced
BatchCrypt Zhang et al. (2020)	Encryption	Encoded gradients with batch encryption Homomorphic encryption	Privacy preservation -Reduced Encryption communi-cation overhead in cross-silo FL
HybridAlpha Xu et al. (2019b)	Encryption	Secure multi-party computation with functional encryption Differential privacy	Privacy preservation Guaranteed Security Dropout Tolerance -Reduced Training Time
POSIDON Sav et al. (2020)	Encryption	Zero-knowledge proof Lattice-based multiparty Homomorphic Encryption	Privacy-preserving Increased Accuracy Reduced computational and communicational overheads
FLGUARD Nguyen et al. (2021c)	Encryption	Secure two-party computation technique	Secure and Privacy preserving Defense against Backdoor attacks
Baffle Andreina et al. (2020)	Encryption	Round based feedback	Secure and Privacy preserving Defense against Backdoor attacks
FedMa Wang et al. (2020c)	–	Layer-wise matched averaging for CNN and LSTM	Fast model convergence Reduced communicational overhead

Table 20 Survey and comparison of proposed FL security and privacy measures in recommendation systems

References	Proposed work	Privacy/security approach	Base model	Data-sets	EP	Achievements
Li et al. (2020e)	Consumer recommendation system	DP, Multiagent Bandit Learning	–	–	RA, RP	AchievedAccuracy Tradeoff between Privacy and Regret
Zhao et al. (2020e)	Privacy-AwareFL for Page Recommendation (Fed4Rec)	Encryption, ModelAgnostic Meta-Learning (MAML)	BiGRU	Globo Dataset	RA	Outperformed baseline recommendation systems
Lin et al. (2020)	Privacy-Preserving Federated Recommendation for item rating Prediction (Fed-Rec)	UserAveraging and Hybrid Filling	–	MovieLens 100K/1 M	MAE, RMSE	Enhanced privacy, Efficiency, accuracy in predictio
Zhou et al. (2019)	Personalized Recommendation System with privacy(pp-DRS)	DP, Centralized model on TTP (Secure aggregation)	–	YFCC 100 M	PL, AR	Privacy preservation for user's context and agent's repository Suitable item recommendation
Ammad-Ud-Din et al. (2019)	Privacy-Preserving Personalized Recommendation System (Fed-CF)	Collaborative Filtering	Collaborative Filtering	MovieLens, In-house Production Dataset	P, R, MAP, RMSE	Achieved higher accuracy and privacy
Hai et al. (2022)	Recommendation System in Healthcare Records(BVFLEMR)	BC with Hyper- ledger fabric	–	–	P, R,Fs	Data Privacy -Security using secure aggregation
Jiang et al. (2020b)	Federated Shilling Attack Detector (FSAD)	Federated Collaborative Filtering (Fed-CF)	Semi-supervised Bayes classifier	Real-world datasets (Netflix, MovieLens)	P,R, Fs, RMSE	Slightly lower detection than traditional algorithms on user's item rating

EP evaluation parameters, *TTP* trusted third party, *BiGRU* bi-directional gated recurrent unit, *DP* differential privacy, *BC* blockchain, *RP* regret performance, *RA* recommendation accuracy, *MAE* mean absolute error, *RMSE* root mean square error, *R* recall, *P* precision, *Fs* F1-Score, *Acc* accuracy, *MAP* mean average precision, *PL* privacy loss, *AR* average regret
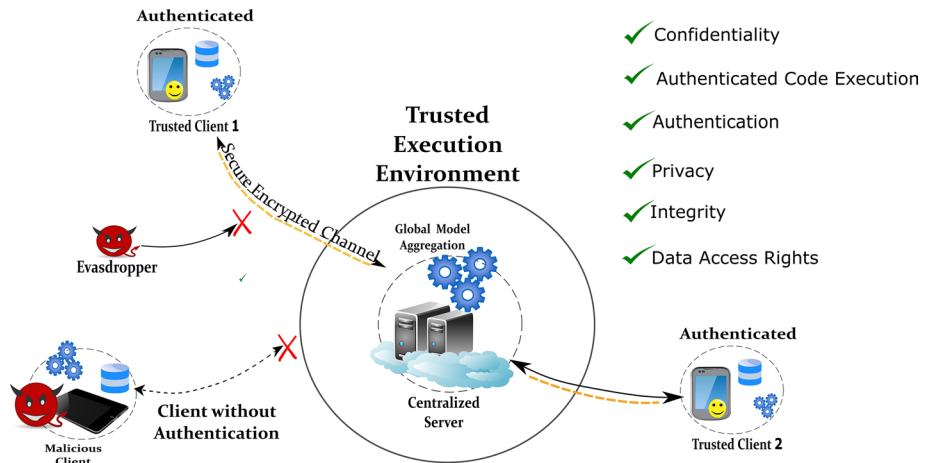
Fig. 18 Trusted execution environment

5.3.7 Trusted execution environment

A trusted execution environment (TEE) is a defense mechanism in FL for security. TEE is a secure and trusted environment for execution. It is a secure hardware technique for computation in an untrusted environment without exposing sensitive data or processing to threats. From the FL scenario, TEE establishes a digitally secure end-to-end connection between connected devices (between client, server) (Sabt et al. 2015). It protects against malware, data breaches, and hacking attacks on servers or clients. TEE uses cryptographic encryptions for end-to-end security. Last but not least, it provides a tamper-resistant isolated processing environment ensuring confidentiality, privacy, authenticity, integrity, and data access rights, as shown in Fig. 18. Zhang et al. (2021) proposed shuffleFL, a gradient preserving system that uses a TEE through SGX-processors to combat side-channel attacks.

In another work, Mo et al. (2021) proposed and implemented PPFL, a privacy-preserving FL framework for mobile systems to protect against privacy leakage. They utilized TEEs on mobile clients for local training and on the server for secure aggregation. Similarly, Mo and Haddadi (2019) proposed TEE implementation for edge devices such as mobile phones or other devices with limited computing resources using FL. They used DP for privacy protection and a data-oblivious algorithm to defend against tracking. In another work, Keto et al. (2022) analyzed and proposed countermeasures against the vulnerability of TEE on the server side. They proposed OLIVE, oblivious differentially private FL on TEE, to ensure secure mode aggregation on an untrusted server. It makes sure that only differentially private models are observable by the server. They also designed an attack that violated the privacy of training data and used the proposed system to justify the risk through experiments on real-world datasets. The oblivious algorithm also guaranteed security on TEE. Table 21 summarizes the proposed work using TEE.

Table 21 Survey and comparison of proposed FL security and privacy measures in trusted execution environment

References	Area	Proposed work	Privacy/security approach	Base model	Data sets	EP	Achievements
Zhang et al. (2021)	SGX Processors Environment	ShuffleFL: Gradient-preserving FL using TEE	Secure Enclave Aggregation, Encryption, Random Grouping Structure	–	–	CpC, CmC	Enhanced security and Privacy in hardware, protocol and networks
Mo et al. (2021)	Mobile Devices	PPFL: Privacy-Preserving FL with TEE	TEE on client/Server side with Intel SGX, Layer-wise training and aggregation	DNN	MNIST, CIFAR-10	TAcc, CR, AC	Defense against Data Reconstruction, Property Inference, Member Inference attacks Enhanced Privacy But increased small system overhead at client-side
Mo and Haddadi (2019)	Mobile Devices	Efficient and Private FL with TEE	Trust zone with TEE using IntelSGX, DP, Data obliviousness	LeNet, DarkNet	MNIST, CIFAR-10	–	Defense against Tracking, Privacy-Preserving
Kato et al. (2022)	FL Environment	Proposed counter measures against vulnerabilities of TEE	Oblivious Algorithm, Oblivious DP	NN, JAC	MNIST, CIFAR 10/100, Purchase 100	ISP, SR, Ob	Designed an attack to test proposed countermeasures Achieved security and privacy

EP evaluation parameters, *TEE* trusted execution environment, *DP* differential privacy, *DNN* deep neural network, *NN* neural network, *JAC* Jaccard similarity, *Intel-SGX* Intel Software Guard Extension, *CpC* computation cost, *CmC* communication cost, *TAcc* test accuracy, *CR* communication rounds, *AC* amount of communication, *ISR* Index Set Privacy, *SR* success rate, *Ob* obliviousness

5.3.8 Healthcare

The healthcare industry is being revolutionized by technological development such as smart wearables, wristbands, smartphones, etc. They have the potential for early detection of several diseases Chaudjary et al. (2022). Furthermore, ML models enable doctors to detect and predict severe diseases like cancers, tumors, and Parkinson's at an early stage. Chen et al. (2020a) conducted their research in integrating FL with healthcare and proposed FedHealth, an FTL framework for wearable healthcare. Fedhealth aggregates data from various organizations to achieve personalized model learning without compromising the privacy and security of users Patel et al. (2022b).

In an another work, Aich et al. (2021) proposed a robust AI-based model during the COVID-19 pandemic. The authors used blockchain and AI-based FL to build a generalized prediction model for predicting COVID symptoms, reasons for the spread, and treatments from patients' data across various healthcare organizations that do not want to share their private data. Their proposed model offers real-time application use. One of the major concerns in FL schemes is irrelevant updates affecting the model's global convergence. To deal with this issue, Chen et al. (2020b) proposed PFL-IU, a privacy-preserving FL framework, to deal with these irrelevant updates, thereby accelerating the model convergence and improving model accuracy. They proposed a *sign*-method to identify the relevant local updates and a secure aggregation protocol.

In another work, Passerat-Palmbach et al. (2020) presented a novel framework for FL using a blockchain-orchestrated ML platform. Their proposed platform uses blockchains and can track the incentives for good quality data and best model contribution for enhanced security, improved health outcomes, and patient trust in the learning healthcare system. Similarly, Schneble and Thamilarasu (2019) designed and implemented an IDS using FL for a medical cyber-physical system (MCPS). It is a networked system of medical devices that enables continuous monitoring and treatment for patients in healthcare Iqbal et al. (2020). The proposed design protects against attacks such as DoS, data modifications, and injection. It achieved a high detection accuracy of 99.6% with reduced network communication overhead Gupta et al. (2020).

Shah et al. (2021) presented FL as a technological solution to data security and privacy concerns for patients' private medical data as electronic medical records are vulnerable to various attacks. The authors showed the potential of FL in this domain when stringent laws do not allow the collection and sharing of the patient's data. Similarly, Ma et al. (2021) presented a secure and privacy-preserving FL for collaboration between multiple health institutions for any time diagnosis to the patients, known as "pocket-diagnosis." It is installed on smart devices like smartphones to help users all the time. Rahman et al. (2020b) used blockchain-managed lightweight hybrid FL framework on the internet-of-health things (IoHT) devices used in daily health management. They also employed DP and noise addition to avoid data leakage.

Li et al. (2021b) exploited FL capabilities for early-stage detection of dementia disease with IoT devices installed at the patient side in their smart homes. The authors use DP to enhance the privacy of data shared among IoT devices. On the other hand, Xing et al. (2020) proposed Jupiter, an easy-to-use and secure FL platform for regional medical care. It provides a high-performance infrastructure for secure parameter aggregations with dedicated links between aggregators and hospitals. For secure aggregation, they used Intel SGX, a popular TEE technology, to guarantee confidentiality for end-to-end parameter

Table 22 Survey and comparison of proposed FL security and privacy measures in Healthcare

References	Area	Proposed work	Privacy/security approach	Base model	Data-sets	EP	Achievements
Chen et al. (2020a)	HealthCare	A FTL framework for healthcare using smart wearable (FedHealth)	HE	CNN	UCI Smart Phone	Acc, Fs	Security User's Privacy Personalized Model Learning
Aich et al. (2021)	Personal Healthcare	Protecting Personal Healthcare using FL and Blockchain	BC, No datasharing	–	–	–	Privacy Preserving Robust AI Based model
Chen et al. (2020b)	E-Health Applications	Privacy-Preserving FL with Irrelevant Updates(PFL-IU)	Secure aggrega-tion, Non-interac-tivekey generation	CNN	MNIST	PA, TP	Secure Aggregation Protect Privacy Dropout Tolerance Achieved better accuracy, convergence
Schneble and Thamilarasu (2019)	Medical Cyber Physical System (MCPS)	Intrusion Detection System in MCPS using FL (FLIDS)	IDS	MLModel	MIMIC	DA, FPR, R,Fs, TT	Lower False Positive Rate Protection against Data modification and Data injections
Xing et al. (2020)	Medical Care	Jupiter: Platform for FL	Intel SGX on TEE	DLModel	–	–	Accelerated Secure Aggregation Confidentiality of parameters
Passerat-Palmbach et al. (2020)	Medicine and utilities in e-Healthcare	ML for privacy-preserving FL in e-Healthcare	BC, HE, SMPC	–	–	–	Security Incentive mechanism for better contributors Privacy-preservation

Table 22 (continued)

References	Area	Proposed work	Privacy/security approach	Base model	Data-sets	EP	Achievements
Shah et al. (2021)	Medical Imaging	Proposed privacy preservations in Medical Imaging using FL	DP, HE, Secure Aggregation	NN	–	Acc	Enhanced Security Privacy-preservation
Ma et al. (2021)	Pocket Diagnosis	Proposed secure and privacy-preserving random-forest based FL used for pocket diagnosis on Smart mobile devices	Multikey secure computation, Encryption	–	Heart Disease, Thyroid Disease Dataset	Acc, MSE	Defense against Poisoning attacks Guaranteed confidentiality
Rahman et al. (2020b)	IoHT	Proposed BC enhanced IoHT framework	Light-weight DP,BC withmultiplicative encryption, Intel SGX, TEE	CNN	–	Acc	Privacy-preserving Enhanced Security
Li et al. (2021b)	IoT based smart Health Care	Proposed FL based privacy preserved Smart Healthcare system (ADDetector)	DP, Unique 3-level FL Architecture, Novel Privacy- preserving Aggregation Framework	Logistic Regession Model	ADRess Dataset	Acc, Fs, TO	Privacy-preservation in Early-stage
Hai et al. (2022)	Healthcare Record System	Recommendation System in Healthcare Record	BC with Hyperledger Febric (BVFLE-MER)	–	–	P, R, Fs	Privacy-preserving Enhanced Security

EP evaluation parameters, *HE* homomorphic encryption, *BC* blockchain, *IoHT* internet of health things, *IDS* intrusion detection system, *SMPC* secure multi-party computation, *Intel-SGX* Intel Software Guard Extension, *TEE* trusted execution environment, *CNN* convolutional neural network, *NN* neural network, *DP* differential privacy, *Acc* accuracy, *TP* test performance, *PA* predictive accuracy, *DA* detection accuracy, *FPR* false positive rate, *TT* training time, *TO* time overhead, *MSE* mean sqaure error, *Fs* F1-Score

Table 23 Survey and comparison of proposed FL security and privacy measures in Web/Internet applications deploying FL

References	Area	Proposed work	Privacy/security approach	Base model	Data-sets	EP	Achievements
Khramtsova et al. (2020)	Web	FL for Cyber Security	Malicious URL Detection	NN	**	TAcc,	Higher Detection Rates Suitable for Real-world scenarios
Fan et al. (2020b)	Web	Smart Ponzi Scheme Detection using FL	DP, Secure Aggregation	–	Real time	Acc, P, R,Fs	Data Privacy Security using secure aggregation

EP evaluation parameters, *URL* uniform resource locators, *NN* neural network, *DP* differential privacy, *Acc* accuracy, *P* precision, *R* recall, *TAcc* test accuracy, *Fs* F1-Score

**Dataset collected (from URL Hans, OpenPhish, and HackerNews Post URLs)

sharing. All the above-discussed research work has been compared and summarized in Table 22.

5.3.9 Web/internet services

To provide security-as-a-service (SaaS), ML models are in trend, but they rely on lots of data. Small organizations need to improve in this scenario. Because with insufficient data, a machine-learned threat-detection system will not perform as efficiently as in the case of a larger organization. Khramtsova et al. (2020) used FL to detect malicious URLs in the network traffic. So, in this collaborative environment, a model can learn better and improve performance for small service providers.

In another work, in web services, Fan et al. (2020b) proposed SPSD-FL, a novel smart Ponzi scheme detection framework using FL. Ponzi is a form of fraud launched on websites to lure investors. Detecting a Ponzi scheme requires lots of data to learn the patterns of the schemes. But websites do not share their data out of data security and privacy norms. Therefore, the authors proposed FL based solution framework that allowed secure aggregation and no sharing of data for smart Ponzi detection. Table 23 describes security and privacy measures in web-based application areas.

5.3.10 Bank services

As discussed above, FL has attracted lots of attention from various business organizations such as banks, pharmaceuticals, smart industries, etc. Liu et al. (2021) focused their work on secure data sharing of client's information with distributed banks to enhance the quality of service while preserving the privacy of the clients. The authors proposed secure and distributed privacy-preserving FL solutions for banks by combining cryptographic and blockchain techniques. They used the MPC algorithm with multi-key fully-HE and allowed blockchain consensus protocol. Zhao et al. (2021b) proposed anonymous and privacy-preserving FL with big industrial data. They tried to leverage the gaussian mechanism DP. Furthermore, employed proxy servers as the middle layer between participants and servers to achieve anonymity, thereby preserving strict privacy with Industrial Big Data.

5.3.11 Miscellaneous

Smart farming is an emerging field that refers to managing and performing farming with the help of technology such as drones, IoT, and robotics. Smart farming focuses mainly on better production and efficient human labor utilization. In the farming context, timely data analysis is crucial for efficient production. Vimalajeewa et al. (2021) deployed FL in the context of smart farming. They jointly used neural networks with FL for better predictions and sustainable farming practices. They proposed a neural network and partial least square-based joint FL model (FL-NNPLS) for milk quality analysis. The proposed model performed efficiently better than centralized state-of-the-art approaches. In another work, Friha et al. (2022) proposed FELIDS, an FL-based IDS system for a secured agricultural-IoT (Agri-IoT) network, which is an essential part of the "smart agriculture" system. They used blockchain to enhance the system's security and encryption for privacy preservation. To evaluate the performance, three real-time datasets have been used, including both malicious and benign network traffic.

Smart Mobile devices are one of the edge devices used in FL. So, it's quite obvious that they are also vulnerable to security breaches and privacy threats. Wang et al. (2019) launched a reconstruction attack named mGAN-AI, using GANs on the federation of mobile devices to infer class representations of victim clients. In another work, Hsu et al. (2020) focused their work on malware detection for android devices using FL. They build their detection system using a support vector machine (SVM) and secure MPC method. Khazbak et al. (2020) proposed MLGuard, an FL-based poisoning attack mitigation technique for a network with many mobile edge devices. Their proposed model is suitable for security and privacy in resource-constrained mobile devices. Malware is one serious security threat in the internet world. Therefore, researchers are experimenting with FL for malware detection, like Gâlvez et al. (2020) deployed FL on android devices and proposed Lim, an FL-based malware classification framework to detect and classify malicious applications without compromising privacy. Table 24 summarizes these remaining few application areas.

5.3.12 Take Away

This subsection discussed security and privacy in ground-based FL applications, including IoT networks, vehicular networks, healthcare, smart city infrastructure, agriculture, TEE, recommendation systems, and others. It is evident from the survey that the FL architecture is a secure and optimal solution for applications involving multiple clients. Many research efforts are dedicated to DP, HE, and authentication protocols (AP) for privacy protection, but at the expense of performance and computational efficiency and cannot sustain complex operations Banerjee et al. (2018). Blockchain has also been incorporated into various applications for privacy and security, but it also has research gaps and challenges that need further research. In IoT-based application areas, researchers highlighted the design of the asynchronous FL model for a more scalable, adaptable, and secure IoT-federated ecosystem. The ML models are trained on client data, and research has shown that using diverse, real-world data has a considerable positive impact on the model's performance. Therefore, new secure incentive mechanisms are needed to encourage users to participate with their high-quality data in supervised and unsupervised scenarios. And, of course, that would further need more robust privacy preservation techniques. Studies suggested that ML models must be redesigned to have inherent privacy and security capabilities. Adversarial attacks

Table 24 Survey and comparison of FL security and privacy measures in few miscellaneous application areas

References	Application area	Proposed work	Privacy/security approach	Base Model	Datasets	EP	Achievements
Zhao et al. (2021b)	Industrial Big Data	Proposed Anonymous and privacy-preserving FL with Industrial Big Data	DP with GNM, Reduced parameter sharing, Proxy Servers (Anonymity)	MLP, CNN	MNIST	Acc, RT, CC	Privacy preservation
Liu et al. (2021)	Banks	Distributed Banks Privacy-Preserving Data Sharing Scheme with FL	BC, Two-round MPC with multikey-fully-HE(MFHE), Anonymity Mechanism	–	–	TC, MSE	Strong privacy / Reduced computat-ional overhead / Enhanced security
Vimalajeewa et al. (2021)	Smart farming	FL model for milk quality analysis	No data sharing	CNN	FOSS MilkScan	RSS, Acc, CoD	Better predictions / Privacy preservation
Khazbak et al. (2020)	Mobile devices	Proposed poisoning attack mitigation on Mobile devices	Lightweight SSS, Cosine similarity for parameters updates	CNN	MNIST CIFAR-10	ASR, TA, ADR	Privacy-preserving / Mitigating poisoning attacks / Reduced communicat-ional overheads
Wang et al. (2019)	Mobile devices	Proposed and demonstrated a generic reconstruction attack on the Federation	GAN based reconstruction attack	–	MNIST, AT &T	Acc	Strong attack proposed / Successfully launched attack on user's privacy
Hsu et al. (2020)	Android devices	Proposed FL based for Android Edge Malware Detection computing	SMC by sharing additive secrets,Crypto protocols secure NN	SVM	@@	Acc, P,R, Fm	Privacy-preserving / Better detection than centralized approaches
Friha et al. (2022)	Smart farming	Proposed IDS system for secured agricultural-IoTs	BC, Encryption and Authentication	CNN, RNN	CSE-, CIC-, IDS2018, MQTTest, InSDN	Acc, P,R, Fs	Privacy-preserving / Secure against IDS

EP evaluation parameters, *CNN* convolutional neural network, *BC* blockchain, *MLP* multi layer perceptron, *DP* differential privacy, *SVM* support vector machine, *RNN* recurrent neural network, *RSS* residual sum of square, *CoD* coefficient of determination, *Acc* accuracy, *RT* running time, *CC* computation cost, *TC* time consumption, *MSE* mean square error, *P* precision, *R* recall, *Fs* F1-Score, *Fm* F-measures, *ASR* attack success rate, *TA* test accuracy, *ADR* attack detection rate
@@Collected APK files from Opera Mobile Store

are another issue that needs further research beyond existing countermeasures (secure aggregators), as a single malicious client in the federation can ruin the entire model. A proper evaluation of their impact in unsupervised scenarios should be a research focus. Many research works highlighted the importance of understanding the attacks by launching the attack through a client, communication channel, or server, then formalizing a countermeasure for that attack. Furthermore, fifth-generation (5G) and beyond (6G) networks bring new levels of privacy and security vulnerabilities (zero-day attacks) to the system. Thus addressing these issues is essential for the future federation. Thus, further research is needed to exploit FL capabilities in real-life applications to their full potential. Tables 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23 and 24 summarizes most of the proposed work in FL security and privacy preservation in various application areas. Tables 26 and 27 show the majority of security and privacy defenses discussed in this section. In the following subsection, we have discussed underwater-based applications deploying FL.

5.4 Security and privacy in FL-based applications covering underwater

In the last few decades, advancements in communicational technologies allowed researchers to conduct research in extreme-area such as deep underwater oceans, deep inside the earth, spaces, etc. To tackle these challenges, researchers take the help of intelligent sensors, the internet-of-things (IoT), etc. Our planet's surface is covered with several water bodies: oceans, seas, lakes, rivers, ponds, and wetlands. The world is facing "Global Water Crises" for several reasons, especially climate change, droughts, water wastage, groundwater depletion, water pollution, and many more. Similarly, when discussing oceans, the most significant resource of life on the planet, sadly face numerous challenges, such as overfishing, garbage, acidification, mercury pollution, ocean warming, habitat destruction, and coral reefs. Therefore, there is an urgent need for an efficient system that can cover the entire planet and help us overcome these challenges and save our planet.

We are talking about vast geographical areas here, so IoTs-based smart sensors are used to monitor and collect the necessary samples in various situations. ML and DL-based research solutions efficiently analyze different environmental situations trained on the data collected from distributedly installed IoT sensors. FL is the best approach to enhance the overall system's capability. FL is not yet explored much in this area despite offering many capabilities. Researchers are exploring and trying its capabilities with enhanced security and privacy features. Very recently, Kwon et al. (2020) proposed a novel multiagent DDPG-based algorithm for deep reinforcement learning with internet-of-underwater-things (IoUTs) devices using FL. To work in the ocean environment, with a communication fading effect compared to air- communications, the authors proposed a multiagent deep deterministic policy gradient (DDPG) for resource allocation and reliable delivery of parameters from IoT devices to the central FL server. Their proposed FL approach showed improved performance and privacy preservation.

In another work, Moubayed et al. (2021) discussed FL-based architectures for water leakage detection problems in pipelines, especially in manufacturing and industry settings. Leakage detection is a major concern for various industrial and governmental stakeholders. The authors suggested FL deployment due to its privacy-preserving and distributed approach. Sensors installed within the transmission pipelines or colling pipes of furnaces provide a massive amount of data for training a global leakage detection model from various local model updates, allowing the knowledge to be distributed to a wide area while maintaining the privacy of the data.

Additionally, Park et al. (2021) proposed an FL-based network model for large-scale water quality prediction to predict green-tide phenomena. Green tide is one of the severe water pollution problems due to the overpopulation of algae, directly affecting human health and the underwater ecosystem. To train a model, the authors collected a huge amount of data through smart sensors distributed across rivers and lakes in South Korea to collect water-quality-related indicators. Furthermore, they presented an optimal fair scheduling algorithm for efficient data transmissions between sensors and servers to avoid overfitting in a privacy-preserving manner. Zhou et al. (2020) used FL in water demand forecasting in a smart water grid. To achieve privacy, the author used zero-knowledge proof to verify users. Blockchain (BC) has been used to prevent malicious updates in the model to ensure security. On the contrary, Chen et al. (2021) used FL in oil–water layer identification, a vital process for petroleum explorations. They proposed an FL-based dynamic weighted fusion strategy for ensuring data security.

For a secure aggregation deep under the ocean's difficult circumstances, Meng et al. (2020) proposed FedMONN, Meta Operation Neural Network, that performs basic operations in an encrypted way and generates results in plaintext. They used neural networks for encryption and decryption using an encoder and meta-operation decoder. Experiments showed that their approach provides higher security than state-of-the-art aggregation methods.

5.4.1 Take away

This subsection discussed the major privacy and security concerns and the proposed solutions in underwater-based applications covering oceans, rivers, lakes, petroleum extraction, and pipelines having wide geographical coverage. In these applications, to collect information, a large number of sensors or edge devices are installed to cover the whole area. Moreover, they may be placed in difficult positions, such as deep under the sea, in furnaces, pipelines, or strong-flow rivers. In such scenarios, gathering this huge amount of data to train an ML/DL model is challenging. Due to its privacy-preserving capabilities and distributed nature, the FL paradigm can be a desirable characteristic to handle the situation. The beauty of this architecture is that it leverages the capacities of its participating edge devices to train a deep and generalized model in a distributed manner. FL shows a huge scope in this area but needs to handle the difficult conditions discussed above. Therefore, new approaches, like cluster-based or hierarchical distributed muli-level based, are needed to group the geographically distributed devices to have balanced participation in the training of global ML models. Similarly, future work could be focused on secure global aggregation schemes, positioning network components, communication channel qualities, and balanced data, together with their safe and reliable operations. Additionally, special methods for the privacy of real-time data of clients/edge devices, the security of local parameters, and gradients sent for model aggregation in FL for water-based areas under difficult scenarios are needed. Table 25 summarizes the work done for safe and secure working with FL in this area. Tables 26 and 27 show the majority of security and privacy defenses discussed in this section. Table 28 listed the reference papers focused on the specific type of attack/threat. Figure 19 shows the year-wise distribution of the papers included in this survey paper.

Table 25 Survey and comparison of proposed FL security and privacy measures in underwater-based application areas

References	Area	Proposed work	Privacy/security approach	Base model	Data-sets	EP	Achievements
Kwon et al. (2020)	Ocean	MultiagentDDGP based DL for Smart Ocean FL IoUT N/W	Privacy by Design	DNN	Real Time	–	Privacy-Preserving First to considerFL for smart Ocean Application Enhanced Performance
Moubayed et al. (2021)	Pipelines for Fluid, Gas Transmission	FL Based Water Leakage Detection	Privacy by Design	–	Real Time	–	Secure and Privacy Preserving Water Leakage Detection System
Park et al. (2021)	Rivers, Lake	Large-ScaleWater Quality Prediction (Water-Pollution)	No Data Sharing	DNN	Real Time Big Data	Acc	Increased Privacy, Secure Aggregation, Higher Accuracy Rates, Fair Scheduling
Meng et al. (2020)	Ocean	MetaOperation Neural Network in FL	Secure Federated Aggregation, Encryption	CNN	MNIST, CIFAR-10	Acc	Increased Data Privacy, -secure than state-of-the art aggregators
Zhou et al. (2020)	Smart Water Grid	Water Demand Forecasting	ZKP, BC	Bi-direct-ional LSTM (B-LSTM)	Public Dataset	MSE	Security Privacy Preservation
Chena et al. (2021)	Petroleum Exploration	Oil–water layer identification	Dynamic weighted fusion strategy (DWFS)	Transfor-mers, Fusion Method	3W Dataset	Acc, Fs, TS	Ensured Data security Privacy Preservation

EP: evaluation parameters, *CNN* convolutional neural network, *LSTM* long short term memory, *BC* blockchain, *ZKP* zero-knowledge proof, *Acc* accuracy, *Fs* F1-Score, *MSE* mean square error, *TS* training speed

Table 26 Summarization of major privacy-preservation approaches in FL

Defense approach	Methodology	Defense against
Secure multiparty	Encryption of the parameters uploaded by clients	Inference Attack
		Reconstruction
Computation		
Differential privacy	Adding random noise to the uploaded parameters.	Evasion Attack
		Poisoning Attack
		Inference Attack
VerifyNet	Achieving privacy preservation using double-masking, encryption, secret sharing, and verification of aggregated results.	Evasion Attack
		Poisoning Attack
		Inference Attack
		Reconstruction Attack
Adversarial training	Including adversarial training samples for training and alternatively updating the model parameters.	Evasion Attack
Homomorphic	Encryption technique that allows computations on encrypted data thereby allowing model updates exchanges between clients and servers in encrypted form.	Poisoning Attack
		Inference Attack Encryption
Gradient compression	Encoding and Decoding of every gradient updates on client and server sides respectively.	Poisoning Attack
		Inference Attack
		Reconstruction Attack
Data perturbation	Adding noise to the data and avoiding original data transmissions on both client and server sides respectively.	Poisoning Attack
		Inference Attack
		Reconstruction Attack Mechanism

Table 27 Summarization of major security defenses in FL

Defense approach	Methodology	Defense against
Anomaly detection	Explicitly monitoring and detecting suspicious client updates	Poisoning Attacks, Free-riding Attacks
Trusted environment	A high-level and trusted environment for executions on servers that provides privacy, integrity, authenticity and confidentiality	Compromised Servers, Model Parameters manipulation, Compromised FL Distributed computations Execution
Pruning	Reducing neural network's model size to improve overall accuracy and to disable backdoors	Communicational bolltenecks, Backdoors Attacks
Robust aggregation	Secure and robust aggregation algorithm for a fair, reliable global model	Poisoning Attacks, Backdoors Attacks, Client's Dropout, Non-Robust Aggregation
Zero-knowledge proofs	Cryptographic approaches to verify client updates	Man-in-the middle, Poisoning Attacks, Backdoors Attacks
Moving target defense	Introducing randomization to the FL system modules to avoid attacks on FL	Inference Attacks, Reconstruction Attack, Man-in-the middle
Recognizing valid clients	To identify the genuine clients among all the participants that are actually contributing to the global model training	Poisoning Attacks, Backdoors Attacks
Federation distillation	This approach includes knowledge sharing through model predictions rather than gradients or parameters. sharing	Inference Attacks, Reconstruction Attack, Man-in-the middle, Communicational bolltenecks
Blockchain	Blockchain is a complete risk management system incorporating cybersecurity frameworks, assurance services, and best practices to mitigate the risks of fraud and cyber-attacks	Inference Attacks, Backdoor Attack, Model Parameter Manipulation, Poisoning Attacks

Table 28 Threat specific categorization of the research papers surveyed in Sect. 5

Attack/threat	References
Intrusion detection system	Li et al. (2020c), Fang et al. (2021), Zhao et al. (2020f), Lu et al. (2019b), Yuan et al. (2021), Issa et al. (2022), Zhao et al. (2020b), Khoa et al. (2020), Jiang et al. (2020b), Chen et al. (2020a)
Poisoning attack	Mowla et al. (2019), Wang et al. (2020a), Sun et al. (2020b), Lyu et al. (2020b), Triastcyn and Faltings (2019), Jiang et al. (2019), Bai and Fan (2021), Song et al. (2020b), Pan et al. (2021), Khoa et al. (2020), Wazzeh et al. (2022), Iqbal et al. (2020)
Backdoor attack	Mowla et al. (2019), Paul et al. (2020), Nasr et al. (2019), Qin et al. (2020), Xu et al. (2019a), Guo et al. (2020)
Anomaly detection	Domingo-Ferrer and Torra (2005), Lu et al. (2019a), Brüß (2021)
Inference attack	Triastcyn and Faltings 2019), Li et al. (2018), McMahan et al. (2017)
Malicious updates identification	Yao and Ansari (2021), Lyu et al. (2020b)
Adversarial attacks	Song et al. (2020a), Zhao et al. (2020c), Wang et al. (2020c), Truex et al. (2019)
Malware detection	Al-Marri et al. 2020), Schneble and Thamilarasu (2019)
Jamming attack	Saraswat et al. (2022)
Anomalous behavior	Maniak et al. (2018), Lu et al. (2020b)
Server attack	Domingo-Ferrer et al. (2021)
Data reconstruction/modification	McMahan et al. (2017), Jiang et al. (2020b)
Cyber attack	Khoa et al. (2020), Zhang et al. (2020c), Kato et al. (2022)
DoS attacks	Li et al. (2020c), Mowla et al. (2019), Majeed et al. (2021), Jiang et al. (2020a)
Trapdoor	Zhao et al. (2020a)
Free-riding	Mowla et al. (2019)
Eavesdropper and hackers	Pan et al. (2021)
Data leakage	Kong et al. (2019), Khoa et al. (2020)
Device tracking attack	Li et al. (2020e)

Fig. 19 Year-wise papers count included in the Sect. 5
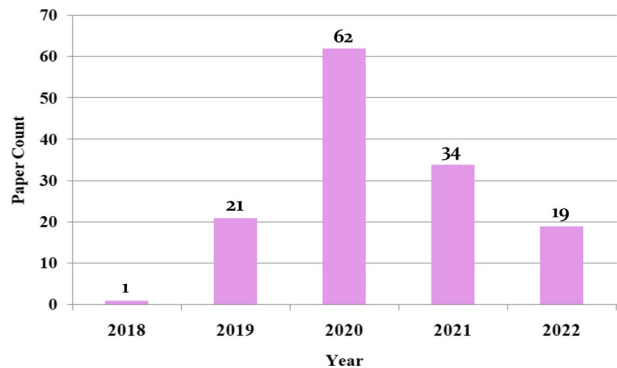
6 Conclusion

FL is a new learning paradigm for ML models that allow access to unlimited and versatile data in a distributed and privacy-preserving manner. This survey paper presents the

basics of the FL concept, major vulnerabilities, attacks, and threats in the FL environment to air, space, ground, and underwater communication scenarios. Moreover, we conduct a detailed, comprehensive survey of the FL landscape's privacy and security issues and defenses. Because identifying these threats, mass adoption of FL is easier in the aforementioned environments. Therefore, our work is dedicated to comprehensively surveying the majority of the research done in security and mitigating privacy techniques proposed over the years; without restricting ourselves to any specific field, area, or domain, we included FL-based applications areas in space, air, ground, and underwater. Subsequently, we provide a discussion on the latest deployments of the FL in various applications in different domains and proposed privacy and security measures in them, including smart cities, smart buildings, transportation, smart healthcare, internet/web, internet-of-things (IoT), UAVs, internet-of-underwater devices, etc. FL adoption to a wide range of smart applications is also explored in detail to various constraints. To further optimize the learning process in FL, secure and robust aggregators must be designed to handle various situations like disasters, deep under oceans, space, etc. Lastly, we highlight the limitations and challenges for various FL techniques' applicability in a wide range of applications.

References

A.A. for everyone, We research and build artificial intelligence technology and services. https://sherpa.ai/

Abdel-Basset M, Moustafa N, Hawash H (2022) Privacy-preserved cyberattack detection in industrial edge of things (IEOT): a blockchain-orchestrated federated learning approach. IEEE Trans Ind Inform 8(11):7920–7934

Ahmadi M, Ulyanov D, Semenov S, Trofimov M, Giacinto G (2016) Novel feature extraction, selection and fusion for effective malware family classification. In: Proceedings of the sixth ACM conference on data and application security and privacy, pp 183–194

Aich S, Sinai NK, Kumar S, Ali M, Choi YR, Joo M-I, Kim H-C (2021) Protecting personal healthcare record using blockchain & federated learning technologies. In: 2021 23rd international conference on advanced communication technology (ICACT), pp 109–112. IEEE

Aïvodji UM, Gambs S, Martin A (2019) Iotfla: a secured and privacy-preserving smart home architecture implementing federated learning. In: 2019 IEEE security and privacy workshops (SPW), pp 175–180. IEEE

Al-Marri NAA-A, Ciftler BS, Abdallah MM (2020) Federated mimic learning for privacy preserving intrusion detection. In: 2020 IEEE international black sea conference on communications and networking (BlackSeaCom), pp 1–6. IEEE

Ammad-Ud-Din M, Ivannikova E, Khan SA, Oyomno W, Fu Q, Tan KE, Flanagan A (2019) Federated collaborative filtering for privacy-preserving personalized recommendation system, arXiv preprint arXiv:1901.09888

Andreina S, Marson GA, Möllering H, Karame G (2020) Baffle: backdoor detection via feedback-based federated learning, arXiv preprint arXiv:2011.02167

Arachchige PCM, Bertok P, Khalil I, Liu D, Camtepe S, Atiquzzaman M (2020) A trustworthy privacy preserving framework for machine learning in industrial IoT systems. IEEE Trans Ind Inform 16(9):6092–6102

Aramoon O, Chen P-Y, Qu G, Tian Y (2021) Meta federated learning, arXiv preprint arXiv:2102.05561

Bai Y, Fan M (2021) A method to improve the privacy and security for federated learning. In: 2021 IEEE 6th international conference on computer and communication systems (ICCCS), pp 704–708. IEEE

Banerjee S, Odelu V, Das AK, Chattopadhyay S, Kumar N, Park Y, Tanwar S (2018) Design of an anonymity-preserving group formation based authentication protocol in global mobility networks. IEEE Access 6:20673–20693

Beaufays FS, Chen M, Mathews R, Ouyang T (2019) Federated learning of out-of-vocabulary words

Beguier C, Tramel EW (2020) Safer: sparse secure aggregation for federated learning, arXiv preprint arXiv:2007.14861

Blanco-Justicia A, Domingo-Ferrer J, Martínez S, Sánchez D, Flanagan A, Tan KE (2020) Achieving security and privacy in federated learning systems: survey, research challenges and future directions, arXiv preprint arXiv:2012.06810

Bonawitz K, Ivanov V, Kreuter B, Marcedone A, McMahan HB, Patel S, Ramage D, Segal A, Seth K (2017) Practical secure aggregation for privacy-preserving machine learning. In: Proceedings of the 2017 ACM SIGSAC conference on computer and communications security, pp 1175–1191

Bonawitz K, Eichner H, Grieskamp W, Huba D, Ingerman A, Ivanov V, Kiddon C, Konečnỳ J, Mazzocchi J, McMahan HB et al (2019) Towards federated learning at scale: system design, arXiv preprint arXiv:1902.01046

Bouacida N, Mohapatra P (2021) Vulnerabilities in federated learning. IEEE Access 9:63229–63249

Brik B, Ksentini A, Bouaziz M (2020) Federated learning for UAVs-enabled wireless networks: Use cases, challenges, and open problems. IEEE Access 8:53841–53849

Brüß C (2021) Federated learning in pedestrian trajectory prediction tasks, in Master Thesis, Lehrstuhl für Datenverarbeitung Technische Universität München

Canetti R, Feige U, Goldreich O, Naor M (1996) Adaptively secure multi-party computation. In: Proceedings of the twenty-eighth annual ACM symposium on theory of computing, pp 639–648

Cao D, Chang S, Lin Z, Liu G, Sun D (2019) Understanding distributed poisoning attack in federated learning. In: 2019 IEEE 25th international conference on parallel and distributed systems (ICPADS), pp 233–239. IEEE

Cao T-D, Truong-Huu T, Tran H, Tran K (2020) A federated learning framework for privacy-preserving and parallel training, arXiv preprint arXiv:2001.09782

Cetin B, Lazar A, Kim J, Sim A, Wu K (2019) Federated wireless network intrusion detection. In: 2019 IEEE international conference on Big Data (Big Data), pp 6004–6006. IEEE

Chai Z, Ali A, Zawad S, Truex S, Anwar A, Baracaldo A, Zhou Y, Ludwig H, Yan F, Cheng Y (2020) Tifl: a tier-based federated learning system. In: Proceedings of the 29th international symposium on high-performance parallel and distributed computing, pp 125–136

Chamikara MAP, Bertok P, Khalil I, Liu D, Camtepe S (2021) Privacy preserving distributed machine learning with federated learning. Comput Commun 171:112–125

Chaudjary S, Kakkar R, Gupta R, Tanwar S, Agrawal S, Sharma R (2022) Blockchain and federated learning-based security solutions for telesurgery system: a comprehensive review. Turk J Electr Eng Comput Sci 30(7):2446–2488

Chen M, Yang Z, Saad W, Yin C, Poor HV, Cui S (2019) Performance optimization of federated learning over wireless networks. In: 2019 IEEE global communications conference (GLOBECOM), pp 1–6. IEEE

Chen Y, Qin X, Wang J, Yu C, Gao W (2020a) Fedhealth: a federated transfer learning framework for wearable healthcare. IEEE Intell Syst 35(4):83–93

Chen H, Li H, Xu G, Zhang Y, Luo X (2020b) Achieving privacy-preserving federated learning with irrelevant updates over e-health applications. In: ICC 2020-2020 IEEE international conference on communications (ICC), pp 1–6. IEEE

Chena B, Zenga X, Zhang W (2021) Federated learning for cross-block oil-water layer identification, arXiv preprint arXiv:2112.14359

Cheng K, Fan T, Jin Y, Liu Y, Chen T, Papadopoulos D, Yang Q (2021) Secureboost: a lossless federated learning framework. IEEE Intell Syst 36(6):87–98

Chhikara P, Tekchandani R, Kumar N, Tanwar S, Rodrigues JJPC (2021) Federated learning for air quality index prediction using UAV swarm networks. In 2021 IEEE global communications conference (GLOBECOM), pp 1–6

Cirincione G, Verma D (2019) Federated machine learning for multi-domain operations at the tactical edge. In: Artificial intelligence and machine learning for multi-domain operations applications, vol 11006. International Society for Optics and Photonics, p 1100606

Dasari SV, Mittal K, Sasirekha G, Bapat J, Das D (2021) Privacy enhanced energy prediction in smart building using federated learning. In 2021 IEEE international IOT, electronics and mechatronics conference (IEMTRONICS), pp 1–6. IEEE

David L, Arús-Pous J, Karlsson J, Engkvist O, Bjerrum EJ, Kogej T, Kriegl JM, Beck B, Chen H (2019) Applications of deep-learning in exploiting large-scale and heterogeneous compound data in industrial pharmaceutical research. Front Pharmacol 10:1303

Department WA. An industrial grade federated learning framework. FATE. https://fate.fedai.org/

Diao E, Ding J, Tarokh V (2020) Heterofl: computation and communication efficient federated learning for heterogeneous clients, arXiv preprint arXiv:2010.01264

Domingo-Ferrer J, Torra V (2005) Ordinal, continuous and heterogeneous k-anonymity through microaggregation. Data Min Knowl Disc 11(2):195–212

Domingo-Ferrer J, Martínez S, Sánchez D, Soria-Comas J (2017) Co-utility: self-enforcing protocols for the mutual benefit of participants. Eng Appl Artif Intell 59:148–158

Domingo-Ferrer J, Blanco-Justicia A, Manjón J, Sánchez D (2021) Secure and privacy-preserving federated learning via co-utility. IEEE Internet Things J 9(5):3988–4000

Dong Y, Chen X, Shen L, Wang D (2020) Eastfly: efficient and secure ternary federated learning. Comput Secur 94:101824

Elbir AM, Soner B, Coleri S (2020) Federated learning in vehicular networks, arXiv preprint arXiv:2006.01412

Enthoven D, Al-Ars Z (2020) An overview of federated deep learning privacy attacks and defensive strategies, arXiv preprint arXiv:2004.04676

Fan Y, Li Y, Zhan M, Cui H, Zhang Y (2020a) Iotdefender: a federated transfer learning intrusion detection framework for 5g IoT. In: 2020 IEEE 14th international conference on big data science and engineering (BigDataSE), pp 88–95

Fan S, Xu H, Fu S, Xu M (2020b) Smart ponzi scheme detection using federated learning. In: 2020 IEEE 22nd international conference on high performance computing and communications; IEEE 18th international conference on smart city; IEEE 6th international conference on data science and systems (HPCC/SmartCity/DSS), pp 881–888. IEEE

Fang Q, Yu S, Chen X (2021) Olive branch learning: a novel federated learning framework for space-air-ground integrated network In: 2021 international conference on space-air-ground computing (SAGC), pp 44–50. IEEE

Federated T (2019) Machine learning on decentralized data, TensorFlow. https://www.tensorflow.org/federated. Accessed 13 Oct 2020

Feng S, Yu H (2020) Multi-participant multi-class vertical federated learning, arXiv preprint arXiv:2001.11154

Fereidooni H, Marchal S, Miettinen M, Mirhoseini A, Möllering H, Rieger TDNP, Sadeghi A-R, Schneider T, Yalame H, Zeitouni S (2021) Safelearn: secure aggregation for private federated learning

Fraboni Y, Vidal R, Lorenzi M (2021) Free-rider attacks on model aggregation in federated learning. In: International conference on artificial intelligence and statistics, PMLR, pp 1846–1854

Fredrikson M, Jha S, Ristenpart T (2015) Model inversion attacks that exploit confidence information and basic countermeasures. In: Proceedings of the 22nd ACM SIGSAC conference on computer and communications security, pp 1322–1333

Friha O, Ferrag MA, Shu L, Maglaras L, Choo K-KR, Nafaa M (2022) Felids: federated learning-based intrusion detection system for agricultural internet of things. J Parallel Distrib Comput 165:17–31

Gâlvez R, Moonsamy V, Diaz C (2020) Less is more: a privacy-respecting android malware classifier using federated learning, arXiv preprint arXiv:2007.08319

Geiping J, Bauermeister H, Dröge H, Moeller M (2020a) Inverting gradients-how easy is it to break privacy in federated learning? Adv Neural Inf Process Syst 33:16937–16947

Geiping J, Bauermeister H, Dröge H, Moeller M (2020b) Inverting gradients—how easy is it to break privacy in federated learning?, arXiv preprint arXiv:2003.14053

Ghosh A, Chung J, Yin D, Ramchandran K (2020) An efficient framework for clustered federated learning, arXiv preprint arXiv:2006.04088

Gong X, Sharma A, Karanam S, Wu Z, Chen T, Doermann D, Innanje A (2022) Preserving privacy in federated learning with ensemble cross-domain knowledge distillation

Gu B, Xu A, Huo Z, Deng C, Huang H (2021) Privacy-preserving asynchronous vertical federated learning algorithms for multiparty collaborative learning. IEEE Trans Neural Netw Learn Syst 33(11):6103–6115

Guo X, Liu Z, Li J, Gao J, Hou B, Dong C, Baker T (2020) V eri fl: communication-efficient and fast verifiable aggregation for federated learning. IEEE Trans Inf Forensics Secur 16:1736–1751

Gupta R, Shukla A, Tanwar S (2020) Aayush: a smart contract-based telesurgery system for healthcare 4.0. In: 2020 IEEE international conference on communications workshops (ICC Workshops), pp 1–6

Gupta R, Nair A, Tanwar S, Kumar N (2021a) Blockchain-assisted secure UAV communication in 6g environment: architecture, opportunities, and challenges. IET Commun 15(10):1352–1367

Gupta R, Kumari A, Tanwar S (2021b) Fusion of blockchain and artificial intelligence for secure drone networking underlying 5g communications. Trans Emerg Telecommun Technol 32(1):e4176

Hai T, Zhou J, Srividhya S, Jain SK, Young P, Agrawal S (2022) Bvflemr: an integrated federated learning and blockchain technology for cloud-based medical records recommendation system. J Cloud Comput 11(1):1–11

Han Q, Yang S, Ren X, Zhao P, Zhao C, Wang Y (2022) Pcfed: privacy-enhanced and communication-efficient federated learning for industrial iots. IEEE Trans Ind Inf 18(9):6181–6191

Hard A, Rao K, Mathews R, Ramaswamy S, Beaufays F, Augenstein S, Eichner H, Kiddon C, Ramage D (2018) Federated learning for mobile keyboard prediction, arXiv preprint arXiv:1811.03604

He X, Chen Q, Tang L, Wang W, Liu T (2022) Cgan-based collaborative intrusion detection for UAV networks: a blockchain empowered distributed federated learning approach. IEEE Internet Things J

Hoofnagle CJ, van der Sloot B, Borgesius FZ (2019) The European union general data protection regulation: what it is and what it means. Inf Commun Technol Law 28(1):65–98

Hsu R-H, Wang Y-C, Fan C-I, Sun B, Ban T, Takahashi T, Wu T-W, Kao S-W (2020) A privacy-preserving federated learning system for android malware detection based on edge computing. In: 2020 15th Asia Joint Conference on Information Security (AsiaJCIS), pp 128–136. IEEE

Hu R, Gong Y, Guo Y (2020) Cpfed: communication-efficient and privacy-preserving federated learning, arXiv preprint arXiv:2003.13761

Huba D, Nguyen J, Malik K, Zhu R, Rabbat M, Yousefpour A, Wu C-J, Zhan H, Ustinov P, Srinivas H et al (2022) Papaya: practical, private, and scalable federated learning. Proc Mach Learn Syst 4:814–832

IBM. Ibm federated learning, https://ibmfl.mybluemix.net/

Iqbal R, Maniak T, Karyotis C (2019) Intelligent remote monitoring of parking spaces using licensed and unlicensed wireless technologies. IEEE Netw 33(4):23–29

Iqbal R, Doctor F, More B, Mahmud S, Yousuf U (2020) Big data analytics and computational intelligence for cyber-physical systems: recent trends and state of the art applications. Futur Gener Comput Syst 105:766–778

Islam A, Al Amin A, Shin SY (2022) Fbi: a federated learning-based blockchain-embedded data accumulation scheme using drones for internet of things. IEEE Wirel Commun Lett 11(5):972–976

ISO (2018) Information technology security techniques information security risk management. In: Standard ISO/IEC 27005

Issa W, Moustafa N, Turnbull B, Sohrabi N, Tari Z (2022) Blockchain-based federated learning for securing internet of things: a comprehensive survey. ACM Comput Surv

Jabir RM, Khanji SIR, Ahmad LA, Alfandi O, Said H (2016) Analysis of cloud computing attacks and countermeasures. In: 2016 18th international conference on advanced communication technology (ICACT), pp 117–123. IEEE

Jere MS, Farnan T, Koushanfar F (2020) A taxonomy of attacks on federated learning. IEEE Secur Privacy 19(2):20–28

Jiang Y, Wang S, Valls V, Ko BJ, Lee W-H, Leung KK, Tassiulas L (2019) Model pruning enables efficient federated learning on edge devices, arXiv preprint arXiv:1909.12326

Jiang JC, Kantarci B, Oktug S, Soyata T (2020a) Federated learning in smart city sensing: challenges and opportunities. Sensors 20(21):6230

Jiang Y, Zhou Y, Wu D, Li C, Wang Y (2020b) On the detection of shilling attacks in federated collaborative filtering. In: 2020 international symposium on reliable distributed systems (SRDS), pp 185–194. IEEE

Ju C, Gao D, Mane R, Tan B, Liu Y, Guan C (2020) Federated transfer learning for EEG signal classification. In: 2020 42nd annual international conference of the IEEE engineering in medicine & biology society (EMBC), pp 3040–3045. IEEE

Kadhe S, Rajaraman N, Koyluoglu OO, Ramchandran K (2020) Fastsecagg: scalable secure aggregation for privacy-preserving federated learning, arXiv preprint arXiv:2009.11248

Kairouz P, McMahan HB, Avent B, Bellet A, Bennis M, Bhagoji AN, Bonawitz K, Charles Z, Cormode G, Cummings R et al (2019) Advances and open problems in federated learning, arXiv preprint arXiv:1912.04977

Kalapaaking AP, Khalil I, Rahman MS, Atiquzzaman M, Yi X, Almashor M (2022) Blockchain-based federated learning with secure aggregation in trusted execution environment for internet-of-things. IEEE Trans Ind Inform

Karimireddy SP, Kale S, Mohri M, Reddi S, Stich S, Suresh AT (2020) Scaffold: stochastic controlled averaging for federated learning. In: International conference on machine learning, PMLR, pp 5132–5143

Kato F, Cao Y, Yoshikawa M (2022) Olive: oblivious and differentially private federated learning on trusted execution environment, arXiv preprint arXiv:2202.07165

Khatri S, Vachhani H, Shah S, Bhatia J, Chaturvedi M, Tanwar S, Kumar N (2021) Machine learning models and techniques for Vanet based traffic management: implementation issues and challenges. Peer-to-Peer Netw Appl 14(3):1778–1805

Khazbak Y, Tan T, Cao G (2020) Mlguard: mitigating poisoning attacks in privacy preserving distributed collaborative learning. In: 2020 29th international conference on computer communications and networks (ICCCN), pp 1–9

Khoa TV, Saputra YM, Hoang DT, Trung NL, Nguyen D, Ha NV, Dutkiewicz E (2020) Collaborative learning model for cyberattack detection systems in IoT industry 4.0. In: 2020 IEEE wireless communications and networking conference (WCNC), pp 1–6, IEEE

Khramtsova E, Hammerschmidt C, Lagraa S, State R (2020) Federated learning for cyber security: soc collaboration for malicious url detection. In: 2020 IEEE 40th international conference on distributed computing systems (ICDCS), pp 1316–1321. IEEE

Kim H, Park J, Bennis M, Kim S-L (2019) Blockchained on-device federated learning. IEEE Commun Lett 24(6):1279–1283

Konečný J, McMahan HB, Ramage HB, Richtárik P (2016) Federated optimization: Distributed machine learning for on-device intelligence, arXiv preprint arXiv:1610.02527

Kong L, Liu X-Y, Sheng H, Zeng P, Chen G (2019) Federated tensor mining for secure industrial internet of things. IEEE Trans Ind Inform 16(3):2144–2153

Kulkarni V, Kulkarni M, Pant A (2020) Survey of personalization techniques for federated learning. In: 2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4), pp 794–797. IEEE

Kumari A, Gupta R, Tanwar S (2021) Amalgamation of blockchain and IoT for smart cities underlying 6g communication: a comprehensive review. Comput Commun 172:102–118

Kwon D, Jeon J, Park S, Kim J, Cho S (2020) Multiagent ddpg-based deep learning for smart ocean federated learning IoT networks. IEEE Internet Things J 7(10):9895–9903

Lalitha A, Kilinc OC, Javidi OC, Koushanfar F (2019) Peer-to-peer federated learning on graphs, arXiv preprint arXiv:1901.11173

Lalle Y, Fourati M, Fourati LC, Barraca JP. A hierarchical clustering federated learning-based blockchain scheme for privacy-preserving in water demand prediction, Available at SSRN 4108575

Lam SK, Riedl J (2004) Shilling recommender systems for fun and profit. In: Proceedings of the 13th international conference on World Wide Web, pp 393–402

LEAF. Leaf—light enterprise application framework, https://www.krminc.com/portfolio/leaf/

Li T, Sahu AK, Zaheer M, Sanjabi M, Talwalkar A, Smith V (2018) Federated optimization in heterogeneous networks, arXiv preprint arXiv:1812.06127

Li T, Sanjabi M, Beirami A, Smith V (2019a) Fair resource allocation in federated learning, arXiv preprint arXiv:1905.10497

Li Q, Wen Z, He B (2019b) Federated learning systems: vision, hype and reality for data privacy and protection

Li K, Zhou H, Tu Z, Wang W, Zhang H (2020a) Distributed network intrusion detection system in satellite-terrestrial integrated networks using federated learning. IEEE Access 8:214852–214865

Li Y, Chen C, Liu N, Huang H, Zheng Z, Yan Q (2020b) A blockchain-based decentralized federated learning framework with committee consensus. IEEE Netw 35(1):234–241

Li Z, Sharma V, Mohanty SP (2020c) Preserving data privacy via federated learning: challenges and solutions. IEEE Consumer Electron Mag 9(3):8–16

Li Y, Chang T-H, Chi C-Y (2020d) Secure federated averaging algorithm with differential privacy. In: 2020 IEEE 30th international workshop on machine learning for signal processing (MLSP), pp 1–6

Li T, Song L, Fragouli C (2020e) Federated recommendation system via differential privacy. In: 2020 IEEE international symposium on information theory (ISIT), pp 2592–2597. IEEE

Li Z, Yu H, Zhou T, Luo L, Fan M, Xu Z, Sun G (2021a) Byzantine resistant secure blockchained federated learning at the edge. IEEE Netw 35(4):295–301

Li J, Meng Y, Ma L, Du S, Zhu H, Pei Q, Shen S (2021b) A federated learning based privacy-preserving smart healthcare system. IEEE Trans Ind Inform

Li G, Wu J, Li S, Yang W, Li C (2022) Multi-tentacle federated learning over software-defined industrial internet of things against adaptive poisoning attacks. IEEE Trans Ind Inform 19(2):1260–1269

Lian X, Zhang C, Zhang H, Hsieh C-J, Zhang W, Liu J (2017) Can decentralized algorithms outperform centralized algorithms? a case study for decentralized parallel stochastic gradient descent, arXiv preprint arXiv:1705.09056

Lin J, Du M, Liu J (2019) Free-riders in federated learning: attacks and defenses, arXiv preprint arXiv:1911.12560

Lin K-Y, Huang W-R (2020a) Using federated learning on malware classification. In: 2020 22nd international conference on advanced communication technology (ICACT), pp 585–589. IEEE

Lin G, Liang F, Pan W, Ming Z (2020b) Fedrec: federated recommendation with explicit feedback. IEEE Intell Syst 36(5):21–30

Liu S, Tang J, Wang C, Wang Q, Gaudiot J-L (2017) Implementing a cloud platform for autonomous driving, arXiv preprint arXiv:1704.02696

Liu K, Dolan-Gavitt B, Garg S (2018) Fine-pruning: Defending against backdooring attacks on deep neural networks. In: International symposium on research in attacks, intrusions, and defenses, pp 273–294. Springer

Liu Y, Ai Z, Sun S, Zhang S, Liu Z, Yu H (2020a) Fedcoin: a peer-to-peer payment system for federated learning. In: Federated learning. Springer, pp 125–138

Liu Y, James J, Kang J, Niyato D, Zhang S (2020b) Privacy-preserving traffic flow prediction: a federated learning approach. IEEE Internet Things J 7(8):7751–7763

Liu Y, Peng J, Kang J, Iliyasu AM, Niyato D, Abd El-Latif AA (2020c) A secure federated learning framework for 5g networks. IEEE Wirel Commun 27(4):24–31

Liu Y, Yuan X, Xiong Z, Kang J, Wang X, Niyato D (2020d) Federated learning for 6g communications: challenges, methods, and future directions. China Commun 17(9):105–118

Liu J, He X, Sun R, Du X, Guizani M (2021) Privacy-preserving data sharing scheme with fl via mpc in financial permissioned blockchain. In: ICC 2021-IEEE international conference on communications, pp 1–6. IEEE

Lu Y, Huang X, Dai Y, Maharjan S, Zhang Y (2019a) Blockchain and federated learning for privacy-preserved data sharing in industrial iot. IEEE Trans Ind Inform 16(6):4177–4186

Lu Y, Huang X, Dai Y, Maharjan S, Zhang Y (2019b) Differentially private asynchronous federated learning for mobile edge computing in urban informatics. IEEE Trans Ind Inform 16(3):2134–2143

Lu X, Liao Y, Lio P, Hui P (2020a) Privacy-preserving asynchronous federated learning mechanism for edge network computing. IEEE Access 8:48970–48981

Lu Y, Huang X, Zhang K, Maharjan S, Zhang Y (2020b) Blockchain empowered asynchronous federated learning for secure data sharing in internet of vehicles. IEEE Trans Veh Technol 69(4):4298–4311

Lu Y, Huang X, Dai Y, Maharjan S, Zhang Y (2020c) Federated learning for data privacy preservation in vehicular cyber-physical systems. IEEE Netw 34(3):50–56

Lu Y, Huang X, Zhang K, Maharjan S, Zhang Y (2020d) Blockchain empowered asynchronous federated learning for secure data sharing in internet of vehicles. IEEE Trans Veh Technol 69(4):4298–4311

Lu Y, Huang X, Zhang K, Maharjan S, Zhang Y (2020e) Blockchain empowered asynchronous federated learning for secure data sharing in internet of vehicles. IEEE Trans Veh Technol 69(4):4298–4311

Lyu L, Yu J, Nandakumar K, Li Y, Ma X, Jin J, Yu H, Ng KS (2020a) Towards fair and privacy-preserving federated deep models. IEEE Trans Parallel Distrib Syst 31(11):2524–2541

Lyu L, Yu H, Ma X, Sun L, Zhao J, Yang Q, Yu PS (2020b) Privacy and robustness in federated learning: attacks and defenses, arXiv preprint arXiv:2012.06337

Ma C, Li J, Ding M, Yang HH, Shu F, Quek TQ, Poor HV (2020a) On safeguarding privacy and security in the framework of federated learning. IEEE Netw 34(4):242–248

Ma C, Li J, Ding M, Yang HH, Shu F, Quek TQ, Poor HV (2020b) On safeguarding privacy and security in the framework of federated learning. IEEE Netw 34(4):242–248

Ma B, Wu J, Liu W, Chiaraviglio L, Ming X (2020c) Combating hard or soft disasters with privacy-preserving federated mobile buses-and-drones based networks. In: 2020 IEEE 21st international conference on information reuse and integration for data science (IRI), pp 31–36. IEEE

Ma Z, Ma J, Miao Y, Liu X, Choo K-KR, Deng R (2021) Pocket diagnosis: secure federated learning against poisoning attack in the cloud. IEEE Trans Serv Comput

Madi A, Stan O, Mayoue A, Grivet-Sébert A, Gouy-Pailler C, Sirdey R (2021) A secure federated learning framework using homomorphic encryption and verifiable computing. In: 2021 reconciling data analytics, automation, privacy, and security: a big data challenge (RDAAPS), pp 1–8

Mahjabin T, Xiao Y, Sun G, Jiang W (2017) A survey of distributed denial-of-service attack, prevention, and mitigation techniques. Int J Distrib Sens Netw 13(12):1550147717741463

Majeed U, Hassan SS, Hong CS (2021) Cross-silo model-based secure federated transfer learning for flow-based traffic classification. In: 2021 international conference on information networking (ICOIN), pp 588–593. IEEE

Maniak T, Iqbal R, Doctor F (2018) Traffic modelling, visualisation and prediction for urban mobility management. In: Advances in hybridization of intelligent methods. Springer, pp 57–70

Manias DM, Shami A (2021) Making a case for federated learning in the internet of vehicles and intelligent transportation systems. IEEE Netw 35(3):88–94

Mansour Y, Mohri M, Ro J, Suresh AT (2020) Three approaches for personalization with applications to federated learning, arXiv preprint arXiv:2002.10619

Mao J, Cao C, Wang L, Ye J, Zhong W (2021) Research on the security technology of federated learning privacy preserving. J Phys 1757:012192

Marfoq O, Xu C, Neglia G, Vidal R (2020) Throughput-optimal topology design for cross-silo federated learning, arXiv preprint arXiv:2010.12229

McMahan B, Moore E, Ramage D, Hampson S, Arcas BAY (2017) Communication-efficient learning of deep networks from decentralized data. In: Artificial intelligence and statistics, PMLR, pp 1273–1282

Meng D, Li H, Zhu F, Li X (2020) Fedmonn: meta operation neural network for secure federated aggregation. In: 2020 IEEE 22nd international conference on high performance computing and communications; IEEE 18th international conference on smart city; IEEE 6th international conference on data science and systems (HPCC/SmartCity/DSS), pp 579–584. IEEE

Mo F, Haddadi H (2019) Efficient and private federated learning using tee In: Proc. EuroSys Conf

Mo F, Haddadi H, Katevas K, Marin E, Perino D, Kourtellis N (2021) Ppfl: privacy-preserving federated learning with trusted execution environments, arXiv preprint arXiv:2104.14380

Mothukuri V, Parizi RM, Pouriyeh S, Huang Y, Dehghantanha A, Srivastava G (2021) A survey on security and privacy of federated learning. Future Gener Comput Syst 115:619–640

Moubayed A, Sharif M, Luccini M, Primak S, Shami A (2021) Water leak detection survey: challenges & research opportunities using data fusion & federated learning. IEEE Access 9:40595–40611

Moulahi T, Jabbar R, Alabdulatif A, Abbas S, El Khediri S, Zidi S, Rizwan M (2022) Privacy-preserving federated learning cyber-threat detection for intelligent transport systems with blockchain-based security. Expert Syst e13103

Moustafa N, Keshk N, Debie N, Janicke H (2020) Federated ton_iot windows datasets for evaluating ai-based security applications. In: 2020 IEEE 19th international conference on trust, security and privacy in computing and communications (TrustCom), pp 848–855. IEEE

Mowla NI, Tran NH, Doh I, Chae K (2019) Federated learning-based cognitive detection of jamming attack in flying ad-hoc network. IEEE Access 8:4338–4350

Nasr M, Shokri R, Houmansadr A (2019) Comprehensive privacy analysis of deep learning: passive and active white-box inference attacks against centralized and federated learning. In: 2019 IEEE symposium on security and privacy (SP), pp 739–753. IEEE

Nguyen TD, Marchal S, Miettinen M, Fereidooni H, Asokan N, Sadeghi A-R (2019) Dïot: a federated self-learning anomaly detection system for iot. In: 2019 IEEE 39th international conference on distributed computing systems (ICDCS), pp 756–767. IEEE

Nguyen DC, Ding M, Pathirana PN, Seneviratne A, Li J, Niyato D, Poor HV (2021a) Federated learning for industrial internet of things in future industries, arXiv preprint arXiv:2105.14659

Nguyen DC, Ding M, Pathirana PN, Seneviratne A, Li J, Poor HV (2021b) Federated learning for internet of things: a comprehensive survey, arXiv preprint arXiv:2104.07914

Nguyen TD, Rieger P, Yalame H, Möllering H, Fereidooni H, Marchal S, Miettinen M, Mirhoseini A, Sadeghi A-R, Schneider T et al (2021c) Flguard: secure and private federated learning, arXiv preprint arXiv:2101.02281

Nilsson A, Smith S, Ulm G, Gustavsson E, Jirstrand M (2018) A performance evaluation of federated learning algorithms. In: Proceedings of the second workshop on distributed infrastructures for deep learning, pp 1–8

Nuding F, Mayer R (2020) Poisoning attacks in federated learning: an evaluation on traffic sign classification. In: Proceedings of the tenth ACM conference on data and application security and privacy, pp 168–170

Openmined, Let's solve privacy. https://www.openmined.org/

Otoum S, Ridhawi I Al, Mouftah H (2021) Securing critical iot infrastructures with blockchain-supported federated learning. IEEE Internet Things J

PaddlePaddle. Baidu paddlepaddle releases 21 new capabilities to accelerate industry-grade model development. http://research.baidu.com/Blog/index-view?id=126

Pan Q, Wu J, Bashir AK, Li J, Yang W, Al-Otaibi YD (2021) Joint protection of energy security and information privacy for energy harvesting: an incentive federated learning approach. IEEE Trans Ind Inform

Papernot N, Abadi M, Erlingsson U, Goodfellow I, Talwar K (2016) Semi-supervised knowledge transfer for deep learning from private training data, arXiv preprint arXiv:1610.05755

Parekh R, Patel N, Gupta R, Jadav NK, Tanwar S, Alharbi A, Tolba A, Neagu B-C, Raboaca MS (2023) Gefl: gradient encryption-aided privacy preserved federated learning for autonomous vehicles. IEEE Access 11:1825–1839

Park S, Jung S, Lee H, Kim J, Kim J-H (2021) Large-scale water quality prediction using federated sensing and learning: a case study with real-world sensing big-data. Sensors 21(4):1462

Passerat-Palmbach J, Farnan T, McCoy M, Harris JD, Manion ST, Flannery HL, Gleim B (2020) Blockchain-orchestrated machine learning for privacy preserving federated learning in electronic health data. In: 2020 IEEE international conference on blockchain (Blockchain), pp 550–555. IEEE

Patel VA, Bhattacharya P, Tanwar S, Jadav NK, Gupta R (2022a) Bfledge: blockchain based federated edge learning scheme in v2x underlying 6g communications. In: 2022 12th international conference on cloud computing, data science & engineering (Confluence), pp 146–152

Patel VA, Bhattacharya P, Tanwar S, Gupta R, Sharma G, Bokoro PN, Sharma R (2022b) Adoption of federated learning for healthcare informatics: emerging applications and future directions. IEEE Access 10:90792–90826

Paul S, Sengupta P, Mishra S (2020) Flaps: federated learning and privately scaling. In: 2020 IEEE 17th international conference on mobile ad hoc and sensor systems (MASS), pp 13–19. IEEE

Popoola SI, Ande R, Adebisi B, Gui G, Hammoudeh M, Jogunola O (2021) Federated deep learning for zero-day botnet attack detection in IoT edge devices. IEEE Internet Things J 9(5):3930–3944

Qin Y, Kondo M (2021) Mlmg: multi-local and multi-global model aggregation for federated learning. In: 2021 IEEE international conference on pervasive computing and communications workshops and other affiliated events (PerCom Workshops), pp 565–571. IEEE

Qin Y, Matsutani H, Kondo M (2020) A selective model aggregation approach in federated learning for online anomaly detection. In: 2020 International Conferences on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData) and IEEE Congress on Cybermatics (Cybermatics), pp 684–691. IEEE

Qu Y, Gao L, Luan TH, Xiang Y, Yu S, Li B, Zheng G (2020) Decentralized privacy using blockchain-enabled federated learning in fog computing. IEEE Internet Things J 7(6):5171–5183

Rahman SA, Tout H, Ould-Slimane H, Mourad A, Talhi C, Guizani M (2020a) A survey on federated learning: the journey from centralized to distributed on-site learning and beyond. IEEE Internet Things J 8(7):5476–5497

Rahman MA, Hossain MS, Islam MS, Alrajeh NA, Muhammad G (2020) Secure and provenance enhanced internet of health things framework: a blockchain managed federated learning approach. IEEE Access 8:205071–205087

Ramaswamy S, Mathews R, Rao K, Beaufays F (2019) Federated learning for emoji prediction in a mobile keyboard, arXiv preprint arXiv:1906.04329

Rieke N, Hancox J, Li W, Milletari F, Roth HR, Albarqouni S, Bakas S, Galtier MN, Landman BA, Maier-Hein K et al (2020) The future of digital health with federated learning. NPJ Digital Med 3(1):1–7

Sabt M, Achemlal M, Bouabdallah A (2015) Trusted execution environment: what it is, and what it is not. In: 2015 IEEE Trustcom/BigDataSE/ISPA, vol 1, pp 57–64. IEEE

Saha S, Ahmad T (2020) Federated transfer learning: concept and applications, arXiv preprint arXiv:2010.15561

Samarakoon S, Bennis M, Saad W, Debbah M (2018) Federated learning for ultra-reliable low-latency v2v communications. In: 2018 IEEE global communications conference (GLOBECOM), pp 1–7. IEEE

Saraswat D, Verma A, Bhattacharya P, Tanwar S, Sharma G, Bokoro PN, Sharma R (2022) Blockchain-based federated learning in UAVs beyond 5g networks: a solution taxonomy and future directions. IEEE Access 10:33154–33182

Sater RA, Hamza AB (2020) A federated learning approach to anomaly detection in smart buildings, arXiv preprint arXiv:2010.10293

Sattler F, Müller K-R, Samek W (2020) Clustered federated learning: model-agnostic distributed multitask optimization under privacy constraints. IEEE Trans Neural Netw Learn Syst 32(8):3710–3722

Sav S, Pyrgelis A, Troncoso-Pastoriza JR, Froelicher D, Bossuat J-P, Sousa JS, Hubaux J-P (2020) Poseidon: privacy-preserving federated neural network learning, arXiv preprint arXiv:2009.00349

Schneble W, Thamilarasu G (2019) Attack detection using federated learning in medical cyber-physical systems. In: 2019 28th international conference on computer communication and networks, ICCCN, pp 1–8

Seo H, Park J, Oh S, Bennis M, Kim S-L (2020) Federated knowledge distillation, arXiv preprint arXiv:2011.02367

Shafee A, Baza M, Talbert DA, Fouda MM, Nabil M, Mahmoud M (2020) Mimic learning to generate a shareable network intrusion detection model. In: 2020 IEEE 17th annual consumer communications & networking conference (CCNC), pp 1–6. IEEE

Shah U, Dave I, Malde J, Mehta J, Kodeboyina S (2021) Maintaining privacy in medical imaging with federated learning, deep learning, differential privacy, and encrypted computation. In: 2021 6th international conference for convergence in technology (I2CT), pp 1–6. IEEE

Shayan M, Fung C, Yoon CJM, Beschastnikh I (2021) Biscotti: a blockchain system for private and secure federated learning. IEEE Trans Parallel Distrib Syst 32(7):1513–1525

Shejwalkar V, Houmansadr A (2021) Manipulating the byzantine: optimizing model poisoning attacks and defenses for federated learning. Internet Society, p 18

Silva S, Gutman BA, Romero E, Thompson PM, Altmann A, Lorenzi M (2019) Federated learning in distributed medical databases: meta-analysis of large-scale subcortical brain data. In: 2019 IEEE 16th international symposium on biomedical imaging (ISBI 2019), pp 270–274. IEEE

Singh AK, Blanco-Justicia A, Domingo-Ferrer J, Sánchez D, Rebollo-Monedero D (2020) Fair detection of poisoning attacks in federated learning. In: 2020 IEEE 32nd international conference on tools with artificial intelligence (ICTAI), pp 224–229. IEEE

Sirohi D, Kumar N, Rana PS (2020) Convolutional neural networks for 5g-enabled intelligent transportation system: a systematic review. Comput Commun 153:459–498

So J, Güler B, Avestimehr AS (2021) Turbo-aggregate: breaking the quadratic aggregation barrier in secure federated learning. IEEE J Sel Areas Inf Theory 2(1):479–489

Song M, Wang Z, Zhang Z, Song Y, Wang Q, Ren J, Qi H (2020a) Analyzing user-level privacy attack against federated learning. IEEE J Sel Areas Commun 38(10):2430–2444

Song Y, Liu T, Wei T, Wang X, Tao Z, Chen M (2020) Fda3: federated defense against adversarial attacks for cloud-based IIoT applications. IEEE Trans Ind Inform 17(11):7830–7838

Suarez-Tangil G, Dash SK, Ahmadi M, Kinder J, Giacinto G, Cavallaro G (2017) Droidsieve: fast and accurate classification of obfuscated android malware. In: Proceedings of the seventh ACM on conference on data and application security and privacy, pp 309–320

Sun L, Lyu L (2020) Federated model distillation with noise-free differential privacy, arXiv preprint arXiv: 2009.05537

Sun F, Zang W, Gravina R, Fortino G, Li Y (2020a) Gait-based identification for elderly users in wearable healthcare systems. Inf Fusion 53:134–144

Sun Y, Ochiai H, Esaki H (2020b) Intrusion detection with segmented federated learning for large-scale multiple lans. In: 2020 international joint conference on neural networks (IJCNN), pp 1–8. IEEE

Suri N (2019) Distributed systems security knowledge area issue. The Cyber Security Body Of Knowledge

Tabassum A, Erbad A, Lebda W, Mohamed A, Guizani M (2022) Fedgan-ids: privacy-preserving ids using gan and federated learning. Comput Commun 192:299–310

Taheri R, Shojafar M, Alazab M, Tafazolli R (2020) Fed-IIoT: a robust federated malware detection architecture in industrial IoT. IEEE Trans Ind Inform 17(12):8442–8452

Tan AZ, Yu H, Cui L, Yang Q (2022) Towards personalized federated learning. IEEE Trans Neural Netw Learning Syst

Tao Z, Li Q (2018) esgd: communication efficient distributed deep learning on the edge. In: USENIX Workshop on Hot Topics in Edge Computing (HotEdge 18)

Tensor/IO. Tensor/io, https://doc-ai.github.io/tensorio/

Triastcyn A, Faltings B (2019) Federated learning with bayesian differential privacy. In: 2019 IEEE international conference on Big Data (Big Data), pp 2587–2596. IEEE

Truex S, Baracaldo N, Anwar A, Steinke T, Ludwig H, Zhang R, Zhou Y (2019) A hybrid approach to privacy-preserving federated learning. In: Proceedings of the 12th ACM workshop on artificial intelligence and security, pp 1–11

Truong N, Sun K, Wang S, Guitton F, Guo Y (2020) Privacy preservation in federated learning: an insightful survey from the gdpr perspective, arXiv preprint arXiv:2011.05411

Uprety A, Rawat DB, Li J (2021) Privacy preserving misbehavior detection in iov using federated machine learning. In: 2021 IEEE 18th annual consumer communications & networking conference (CCNC), pp 1–6. IEEE

Vanhaesebrouck P, Bellet A, Tommasi M (2017) Decentralized collaborative learning of personalized models over networks. In: Artificial Intelligence and Statistics. PMLR, pp 509–517

Verma A, Bhattacharya P, Bodkhe U, Saraswat D, Tanwar S, Dev K (2022) Fedrec: trusted rank-based recommender scheme for service provisioning in federated cloud environment. Digital Commun Netw

Vimalajeewa D, Kulatunga C, Berry D, Balasubramaniam S (2021) A service-based joint model used for distributed learning: application for smart agriculture. IEEE Trans Emerg Topics Comput 10(2):838–854

Wainakh A, Guinea AS, Grube T, Mühlhäuser M (2020) Enhancing privacy via hierarchical federated learning. In: 2020 IEEE European symposium on security and privacy workshops (EuroS &PW), pp 344–347. IEEE

Wang S, Qiao Z (2019) Robust pervasive detection for adversarial samples of artificial intelligence in IoT environments. IEEE Access 7:88693–88704

Wang Z, Song M, Zhang Z, Song Y, Wang Q, Qi H (2019) Beyond inferring class representatives: user-level privacy leakage from federated learning. In: IEEE INFOCOM 2019-IEEE conference on computer communications, pp 2512–2520. IEEE

Wang Y, Su Z, Zhang N, Benslimane A (2020a) Learning in the air: secure federated learning for UAV-assisted crowdsensing. IEEE Trans Netw Sci Eng 8(2):1055–1069

Wang H, Sreenivasan K, Rajput S, Vishwakarma H, Agarwal S, Sohn J-Y, Lee K, Papailiopoulos D (2020b) Attack of the tails: yes, you really can backdoor federated learning, arXiv preprint arXiv: 2007.05084

Wang H, Yurochkin M, Sun Y, Papailiopoulos D, Khazaeni Y (2020c) Federated learning with matched averaging, arXiv preprint arXiv:2002.06440

Wang X, Garg S, Lin H, Hu J, Kaddoum G, Piran MJ, Hossain MS (2021) Towards accurate anomaly detection in industrial internet-of-things using hierarchical federated learning. IEEE Internet Things J 9(10):7110–7119

Wazzeh M, Ould-Slimane H, Talhi C, Mourad A, Guizani M (2022) Privacy-preserving continuous authentication for mobile and iot systems using warmup-based federated learning. IEEE Netw

Wei J, Zhu Q, Li Q, Nie L, Shen Z, Choo K-K R, Yu K (2022) A redactable blockchain framework for secure federated learning in industrial internet-of-things. IEEE Internet Things J

Wu D, Pan M, Xu Z, Zhang Y, Han Z (2020) Towards efficient secure aggregation for model update in federated learning. In: GLOBECOM 2020–2020 IEEE global communications conference, pp 1–6

Wu M, Ye D, Ding J, Guo Y, Yu R, Pan M (2021) Incentivizing differentially private federated learning: a multidimensional contract approach. IEEE Internet Things J 8(13):10639–10651

Xia Q, Gao X, Xu Z (2014) Double auctions for federated learning in satellite edge clouds. Available at SSRN 4220613

Xie C, Huang K, Chen P-Y, Li B (2019) Dba: distributed backdoor attacks against federated learning. In: International Conference on Learning Representations

Xing J, Jiang Z, Yin H (2020) Jupiter: a modern federated learning platform for regional medical care. In: 2020 ieee international conference on joint cloud computing, pp 21–21. IEEE

Xin B, Yang W, Geng Y, Chen S, Wang S, Huang L (2020) Private fl-gan: differential privacy synthetic data generation based on federated learning. In: ICASSP 2020–2020 IEEE international conference on acoustics, speech and signal processing (ICASSP), pp 2927–2931, IEEE

Xu G, Li H, Liu S, Yang K, Lin X (2019a) Verifynet: secure and verifiable federated learning. IEEE Trans Inf Forensics Secur 15:911–926

Xu R, Baracaldo N, Zhou Y, Anwar A, Ludwig H (2019b) Hybridalpha: an efficient approach for privacy-preserving federated learning. In: Proceedings of the 12th ACM workshop on artificial intelligence and security, pp 13–23

Xu G, Li H, Zhang Y, Xu S, Ning J, Deng R (2020) Privacy-preserving federated deep learning with irregular users. IEEE Trans Dependable Secure Comput 19(2):1364–1381

Yang T, Andrew G, Eichner H, Sun H, Li W, Kong N, Ramage D, Beaufays F (2018) Applied federated learning: Improving google keyboard query suggestions, arXiv preprint arXiv:1812.02903

Yang Q, Liu Y, Chen T, Tong Y (2019) Federated machine learning: concept and applications. ACM Trans Intell Syst Technol 10(2):1–19

Yang H, He H, Zhang W, Cao X (2020) Fedsteg: a federated transfer learning framework for secure image steganalysis. IEEE Trans Netw Sci Eng 8(2):1084–1094

Yao J, Ansari N (2021) Secure federated learning by power control for internet of drones. IEEE Trans Cognitive Commun Netw 7(4):1021–1031

Yu T, Li T, Sun Y, Nanda S, Smith V, Sekar V, Seshan S (2020a) Learning context-aware policies from multiple smart homes via federated multi-task learning. In: 2020 IEEE/ACM fifth international conference on internet-of-things design and implementation (IoTDI), pp 104–115. IEEE

Yu F, Zhang W, Qin Z, Xu Z, Wang D, Liu C, Tian Z, Chen X (2020b) Heterogeneous federated learning, arXiv preprint arXiv:2008.06767

Yuan X, Chen J, Zhang N, Fang X, Liu D (2021) A federated bidirectional connection broad learning scheme for secure data sharing in internet of vehicles. China Commun 18(7):117–133

Zhan Y, Zhang J, Hong Z, Wu L, Li P, Guo S (2021) A survey of incentive mechanism design for federated learning. IEEE Trans Emerg Topics Comput 10(2):1035–1044

Zhang J, Chen J, Wu D, Chen B, Yu S (2019) Poisoning attack in federated learning using generative adversarial nets. In: 2019 18th IEEE international conference on trust, security and privacy in computing and communications/13th IEEE international conference on big data science and engineering (TrustCom/BigDataSE), pp 374–380. IEEE

Zhang X, Fang F, Wang J (2020a) Probabilistic solar irradiation forecasting based on variational Bayesian inference with secure federated learning. IEEE Trans Ind Inform 17(11):7849–7859

Zhang X, Chen X, Liu JK, Xiang Y (2020b) Deeppar and deepdpa: privacy preserving and asynchronous deep learning for industrial iot. IEEE Trans Ind Inf 16(3):2081–2090

Zhang J, Chen B, Cheng X, Binh HTT, Yu S (2020c) Poisongan: generative poisoning attacks against federated learning in edge computing systems. IEEE Internet Things J 8(5):3310–3322

Zhang C, Li S, Xia J, Wang W, Yan F, Liu Y (2020d) Batchcrypt: efficient homomorphic encryption for cross-silo federated learning. In: 2020 USENIX annual technical conference (USENIXATC 20), pp 493–506

Zhang Y, Wu Q, Shikh-Bahaei M (2020e) Vertical federated learning based privacy-preserving cooperative sensing in cognitive radio networks. In: 2020 IEEE globecom workshops (GC Wkshps), pp 1–6. IEEE

Zhang Y, Wang Z, Cao J, Hou R, Meng D (2021) Shufflefl: gradient-preserving federated learning using trusted execution environment. In: Proceedings of the 18th ACM international conference on computing frontiers, pp 161–168

Zhang Z, Wu L, He D, Wang Q, Wu D, Shi X, Ma C (2022) G-vcfl: grouped verifiable chained privacy-preserving federated learning. IEEE Trans Netw Serv Manag

Zhao K, Xi W, Wang Z, Zhao J, Wang R, Jiang Z (2020a) Smss: secure member selection strategy in federated learning. IEEE Intell Syst 35(4):37–49

Zhao Y, Zhao J, Yang M, Wang T, Wang N, Lyu L, Niyato D, Lam K-Y (2020b) Local differential privacy-based federated learning for internet of things. IEEE Internet Things J 8(11):8836–8853

Zhao Y, Zhao J, Jiang L, Tan R, Niyato D, Li Z, Lyu L, Liu Y (2020c) Privacy-preserving blockchain-based federated learning for IoT devices. IEEE Internet Things J 8(3):1817–1829

Zhao Y, Zhao J, Jiang L, Tan R, Niyato D, Li Z, Lyu L, Liu Y (2020d) Privacy-preserving blockchain-based federated learning for IoT devices. IEEE Internet Things J 8(3):1817–1829

Zhao S, Bharati R, Borcea C, Chen Y (2020e) Privacy-aware federated learning for page recommendation. In: 2020 IEEE international conference on Big Data (Big Data), pp 1071–1080. IEEE

Zhao L, Tang X, You Z, Pang Y, Xue H, Zhu L (2020f) Operation and security considerations of federated learning platform based on compute first network. In: 2020 IEEE/CIC international conference on communications in China (ICCC Workshops), pp 117–121. IEEE

Zhao L, Tang X, You Z, Pang Y, Xue H, Zhu L (2020g) Operation and security considerations of federated learning platform based on compute first network. In: 2020 IEEE/CIC international conference on communications in China (ICCC Workshops), pp 117–121. IEEE

Zhao L, Jiang J, Feng B, Wang Q, Shen C, Li Q (2021a) Sear: secure and efficient aggregation for byzantine-robust federated learning. IEEE Trans Dependable Secur Comput 19(5):3329–3342

Zhao B, Fan K, Yang K, Wang Z, Li H, Yang Y (2021b) Anonymous and privacy-preserving federated learning with industrial big data. IEEE Trans Ind Inform 17(9):6314–6323

Zheng H, Hu H, Han Z (2020) Preserving user privacy for machine learning: local differential privacy or federated machine learning? IEEE Intell Syst 35(4):5–14

Zhou P, Wang K, Guo L, Gong S, Zheng B (2019) A privacy-preserving distributed contextual federated online learning framework with big data support in social recommender systems. IEEE Trans Knowl Data Eng 33(3):824–838

Zhou Z, Yang S, Pu L, Yu S (2020) Cefl: online admission control, data scheduling, and accuracy tuning for cost-efficient federated learning across edge nodes. IEEE Internet Things J 7(10):9341–9356

Zhou Z, Tian Y, Peng C, Yang N, Long S (2022) Vflf: a verifiable federated learning framework against malicious aggregators in industrial internet of things. Concurr Comput e7193

Zhu H, Goh RSM, Ng W-K (2020) Privacy-preserving weighted federated learning within the secret sharing framework. IEEE Access 8:198275–198284

Authors and Affiliations

Deepika Sirohi[1] · Neeraj Kumar[1,2,3,7] (ID) · Prashant Singh Rana[1] · Sudeep Tanwar[4] · Rahat Iqbal[5] · Mohammad Hijjii[6]

Deepika Sirohi
ddeepika1_phd18@thapar.edu

Prashant Singh Rana
prashant.singh@thapar.edu

Sudeep Tanwar
sudeep.tanwar@nirmauni.ac.in

Rahat Iqbal
riqbal@ud.ac.ae

Mohammad Hijjii
m.hijji@ut.edu.sa

1   Department of Computer Science and Engineering, Thapar Institute of Engineering and Technology, Patiala, Punjab, India

2   Department of Electrical and Computer Engineering, Lebanese American University, Beirut, Lebanon

3   Faculty of Computing and IT, King Abdulaziz University, Jeddah, Saudi Arabia

4   Department of Computer Science and Engineering, Institute of Technology, Nirma University, Ahmedabad, Gujarat, India

5   University of Dubai, Dubai, UAE

6   Computer Science Department, Faculty of Computers & Information Technology, University of Tabuk, Tabuk, Saudi Arabia

7   Department of Computer Science and Engineering, University of Petroleum and Energy Studies, Dehradun, 248001, India