Archives available at journals.mriindia.com

International Journal of Recent Advances in Engineering and Technology

ISSN: 2347 - 2812

Volume 15 Issue 01, 2026

Federated Learning for Privacy-Preserving Optimization in Multi-Domain Optical Networks

[1]Mr. Vicky Kumar, [2]Mr. Sumit Dalal
[1]M. Tech, Research Scholar,ECE Department, Sant Kabir Institute of Technology and Management, Bahadurgarh
[2]Assistant professor, Ece department, SKITM, Bahadurgarh
Email: [1]vickysharma1067@gmail.com

Peer Review Information

Submission: 15 March 2026

Revision: 30 March 2026

Acceptance: 11 April 2026

Keywords

Federated Learning, Multi-Domain Optical Networks, Privacy-Preserving Optimization, Distributed Machine Learning, Network Resource Optimization

Abstract

Modern optical networks have been seriously challenged by new infrastructures and data intensive applications that have increased to an alarming rate. Intelligent, scalable, privacy-preserving optimization mechanisms are needed in multi-domain optical networks (MD-ONs), which entail multiple administrative and technological domains. Federated Learning (FL) is a promising novel decentralized machine learning model capable of addressing all these challenges by offering the possibility to jointly train models without sharing raw data. The work in this research paper explains how federated learning could be integrated to the multi-domain optical network to enable privacy-preserving optimization. It talks about architectural buildings, optimization techniques, communication boundaries, and practical applications, problems and research gaps. The paper sheds light on the ways in which FL can improve the efficiency, scalability and privacy of data on networks, and this makes it one of the enabling factors in the next generation of intelligent optical networks.

Introduction

The modern communication systems are based on optical networks whereby they are used to transmit large amount of data in metropolitan, regional and international networks via fiber-optic technology. These networks are turning into multi-domain environments where different operators have different segments and each of them has its own policies, data and control mechanisms. Conventional centralized optimization models demand the exchange of network data in large amounts of data across domains, which poses privacy and scalability issues and regulatory challenges (Ahmad Madni *et al.*, 2024). Federated Learning (FL) provides the paradigm shift as it allows distributed training on a variety of nodes without exchanging raw data, thereby protecting privacy and minimizing the overhead of communication. This paper will discuss how federated learning can be applied to maximize multi-domain optical networks without affecting privacy.

Background and Related Work

1. Optical Networks and Multi-Domain Architecture

The very basis of modern high-speed communication systems is optical networks, which allow sending the huge amounts of data across large distances with a minimum amount of latency and signal deterioration. Such networks are founded on light propagation in an optical fiber and technologies such as wavelength-division multiplexing (WDM) allow using a single-optical fiber to deliver simultaneous streams of data by assigning varying wavelengths of light (or varying colors) to different channels (Huang *et al.*, 2025). The functionality has significantly enhanced the bandwidth usage and the ever-increasing data-driven applications such as cloud computing, video streaming and scale out distributed applications.

Optical networks have developed over the last few years into multi-domain optical networks with high complexity (MD-ONs) as opposed to single-domain, centrally controlled networks. Multi-domain optical networks consist of two or more domains that are interconnected and each domain is managed by a distinct administrative unit such as Internet Service Providers (ISPs), telecommunication operators or enterprise networks. All of the domains are autonomous, having their control plane, routing policies, resource management strategies, and security constraints (Mir *et al*., 2026). Whereas such a form of decentralization results in improved scalability and flexibility in administration, it poses significant coordination and optimization challenges.

Lack of global visibility is one of the main difficulties in MD-ONs. The inability to be able to optimize the end-to-end across domains is complicated by the fact that the domains are not willing to provide the internal state information due to privacy, security or competitiveness. One example is that the information about the available wavelengths, the use of links or traffic routes might be limited to the domain boundaries (Liu *et al*., 2024). This results in the making of suboptimal routing decisions, inefficient use of resources and high latency.

The Routing and Wavelength Assignment (RWA) is a basic optimization problem in optical networks, in particular WDM-based networks. RWA: This is the procedure of selecting a route that is ideal to convey a data transmission request and place it on an appropriate wavelength on the route, such that wavelength continuity limits are followed. RWA in multi-domain environments is much more complicated because of the lack of information sharing, non-uniform policies, and changing network dynamics. In inter-domain RWA, there are a set of controllers which share the information incompletely, and therefore the information cannot be shared in a centralized fashion as in the traditional approaches.

To overcome these challenges, the literature has suggested a number of solutions such as hierarchical control planes, software-defined networking (SDN)-based orchestration, and path computation elements (PCEs). The hierarchical SDN architecture introduces a global orchestrator, communicating with domain-specific controllers that can coordinate in some way, but without domain autonomy (Xiang *et al*., 2019). Similarly, PCE based architectures can be used to compute network paths distributedly using standard protocols. Such approaches, however, also assume some extent of information exchange, and it is not always the case in the context of privacy issues.

Moreover, network technologies are heterogeneous in domains (differences in modulation formats, switching capability, and transmission standards) and it makes the optimization across domains even more complicated (Wang *et al*., 2025). As the scale and diversity of networks continue to rise, the need to have intelligent, adaptive as well as privacy-conscious optimization mechanisms that can effectively work in such contexts of decentralization increases. This has compelled scientists to think of machine based learning solutions particularly those ones that do not require a centralized data collection.

2. Fundamentals of Federated Learning

Federated Learning (FL) has become a revolutionary model in distributed machine learning that can help resolve the key issues of data privacy, communication efficiency, and decentralized model training. As opposed to the classical centralized learning frameworks where numerous data sources are collected into one central server to be trained, FL allows various clients (or nodes) to cooperatively train a common global model with their data being localized.

With regard to optical networks, the domains can be considered clients within the federated learning framework (Fan *et al*., 2025). These areas have data to train a local model (traffic statistics, network topology information, performance metrics, and so on) on their own and are independent. Instead of communication of raw data, each domain pushes the model updates (e.g. gradients or weights) to a central aggregator, which pushes them to the global model to update it. This is done iteratively until convergence of the model.

Federated learning can be mathematically defined as:

$$f(x) = \frac{1}{K} \sum_{i=1}^{K} f_i\,(x)$$

where Krep denotes the number of participating customers (domains) and f i (x) is the local objective function of the i-th customer, based on its information only. It is intended to minimize the global loss functional through a pooling of the local contributions without exposing any particular data.

A complex of characteristics of federated learning predisposes it towards multi-domain optical networks, in particular (Lai *et al*., 2024). To begin with, it is able to guarantee data privacy, which retains sensitive information in local fields. This would be valuable in the cases where the operators of the network do not desire or are unable to share proprietary or user related information. Second, FL helps in collaborative learning whereby several domains gain by sharing knowledge without interfering with autonomy. Third, it reduces the transfer of large volumes of crude data, therefore, communication overhead and scalability.

There can be different types of federated learning, cross-silo FL, and cross-device FL. With cross-device FL, many devices (e.g., smartphones or IoT nodes) are involved in training, usually having few or no computational resources and intermittent connectivity. On the other hand, cross-silo FL contains fewer high capacity entities (such as data centers or network domains) and can be better applied in optical networking situations.

Federated learning presents a number of challenges, despite its benefits. One of the main issues is the data heterogeneity (also called non-independent and identically distributed (non-IID) data). Changes in traffic patterns and network conditions across domains in optical networks can be extreme leading to biased local models and slower convergence (Hashemi *et al*., 2021). The other issue is efficiency of communication since the frequent updating of models can also be a burden to the network resources, especially when the model is large or when the model is encrypted to ensure security.

In order to solve these problems, several optimization techniques have been proposed including model compression, adaptive aggregation algorithms and asynchronous training techniques. Aggregation of model updates via techniques like Federated Averaging (FedAvg) has become widely used and more complex techniques include weighting schemes based on data quality or domain relevance.

Overall, federated learning can be viewed as an effective platform of distributed intelligence, providing collaboration optimization under the conditions of limited data sharing. Its use in optical networks is becoming more and more popular as scientists strive to come up with privacy-sensitive and scalable systems of the next generation of communication systems.

3. FL in Communication Networks

Federated learning has brought forth new possibilities in the domain of intelligent network management and optimization in that it is embedded in communication networks (Wang *et al*., 2025). The increasing complexity and data-focused characteristics of networks are rendering the traditional rule-based and centralized models ineffective to deal with dynamic trends of traffic, heterogeneous infrastructures, and high-performance needs. Federated learning provides a decentralized option, which suits well with the distributed aspect of contemporary communication systems.

One of the most remarkable applications of FL in the communication networks can be regarded as traffic prediction. In order to support the proper distribution of resources, congestion and quality of service (QoS) control, as well as correct traffic prediction is needed. The traffic patterns of multi-domain optical networks are at two levels, one domain level and the other level is at the local level and this is based on the local factors such as user behavior, type of application and time variation. With federated learning, each domain will have the opportunity to localize a model on its own traffic data and contribute to a global model that represents more general trends. It is a collaborative approach towards the effectiveness of prediction and data confidentiality.

Such models as Federated Multi-Objective Network (FedMON) are proposed to enhance traffic prediction in multi-domain environment (Ibrahimi *et al*., 2025). These structures have hierarchical aggregation methods, where local models are aggregated in regional scales and then in global scales. This reduces overheads on communication and increases scalability and hence would be applicable in large scale optical networks.

Other applications of federated learning include the resolution of resource allocation problems such as bandwidth allocation, spectrum control, and load balancing in addition to traffic forecasting. The FL-based models can utilize past data to predict the future resource demand and optimize allocation strategy on the basis of past data. This is quite useful particularly in optical networks where optimum usage of spectrum and wavelengths is vital in the maximization of throughput.

Fault detection and network monitoring is another significant usage. Optical networks are prone to numerous failures that include fiber cuts, failure of equipment and degradation of signals. The localization and early fault detection are essential in network reliability. Federated learning will enable sharing of fault detection across domains without sharing sensitive data on operation (Ibrahimi *et al*., 2025). Each domain can be trained on a local anomaly detector-model and be part of a global model that can identify patterns that can be an indicator of network failures.

Moreover, FL has been explored in routing optimization, where models are trained to select the most optimal routes based on the network conditions. This in multi-domain cases means predicting levels of congestion, availability of links and latency on various domains. Federated models are capable of utilizing several domains to gain more knowledge than local models isolated, thereby, making superior routing decisions.

Although the applications of federated learning are promising, its application in communication networks is still at its infancy. Problems such as lag in synchronization, overhead in communication and security risks ought to be addressed to ensure that it is a viable approach. However, current studies are still ongoing to improve the algorithms and architectures of FL and this is leading to their application in the real world optical networks.

Motivation for Privacy-Preserving Optimization

1. Challenges in Multi-Domain Optical Networks

The multi-domain optical networks pose a special set of challenges which are based on their distributed nature as well as independence of individual domains. One of the issues that are regarded as the most significant is the existence of data silos (Zhan *et al*., 2025). Data sets in the domains (like traffic logs, performance data, and network settings) are not shared across domains. Such fragmentation of data does not allow carrying out global optimization, and the traditional machine learning methods become less effective.

This issue is also compounded by privacy and security issues. Network data is prone to contain sensitive data about user behavior, use of the services and infrastructure information. The dissemination of such data in other fields may cause loss of privacy, breach of regulations, and competitiveness. As a result, domains are not eager to participate in collaborative optimization projects that are associated with the data share.

Heterogeneity is another major issue of multi-domain optical networks. Various fields might have different technologies, protocols and configurations of hardware, resulting in differences in the data format and behavioral nature. This makes it difficult to develop common optimization models that can be domain-generalized.

Limited inter-domain trust is significant, too. Since a domain is often operated by competitors, it is not believed that there is open cooperation. This restricts the exchange of information and coordination of optimization methods.

There is also high overhead of communication (Cloud *et al*., 2025). The traditional centralized schemes presuppose the interchange of information between the realms and a central controller on a regular basis that can strain the network resources and increase the latency. This overhead is also prohibitive in a large scale network and better solutions are needed that are more efficient and scalable.

2. Why Federated Learning?

The abovementioned problems can be resolved by federated learning which provides a scheme to optimize collectively without the need to share data. FL brings data close to every domain, which ensures the privacy protection and compliance with regulations. This is particularly important in optical networks where very sensitive information about operation should be confidential.

FL does not demand domains to share raw data but instead only model parameters or updates. These updates are usually pooled together with secure protocols, such that no one contribution can be reverse-engineered to disclose personal information (Madni *et al*., 2025). This will go a long way in reducing the risk of leaking the data and increasing confidence among domains involved.

FL can as well be used to do decentralized optimization in which every domain is allowed to independently train models, but all with a global objective. This is highly compatible with distributed nature of multi-domain optical networks and facilitates scalable and flexible deployment.

Moreover, federated learning enables cooperating without total trust among the participants. The domains are not required to share raw data with anyone since it is never shared, therefore, they are able to participate in the learning process without exposing sensitive data. This will result in cooperation and development of better and more accurate models.

The other advantage of FL is that it reduces overhead of communication. FL reduces bandwidth consumption and enhances efficiency by only transferring model changes rather than sending big datasets (Qian *et al*., 2023). More effective communication is also provided through the advanced techniques, such as model compression and selective update transmission.

Overall, federated learning is a powerful solution to aid privacy-preserving optimization in multi-domain optical networks that help resolve the significant issues of data silos, privacy, and scalability.

System Architecture for FL in Multi-Domain Optical Networks

1. Hierarchical FL Architecture

Multi-domain optical networks are particularly well suited to hierarchical federated learning architecture since it is a hierarchical structure of the systems. This architecture has local domain controllers as clients and they use domain-specific data to train models. The regional pooling of the local models is then consolidated into a global model by a central orchestrator.
The multi-level aggregation method has a number of benefits. It reduces overhead through communication by reducing direct communication with the global server and can be scaled by distributing the process of aggregation (Kholidy *et al*., 2022). It is also optimizable at regional levels and increases model sensitivity and accuracy.

2. Cross-Silo Federated Learning

The federated learning paradigm in optical networks is commonly cross-silo and there are few high-capacity domains in the training. Unlike cross-device FL, the participants in cross-silo FL may be unreliable, or resource-constrained, and involves stable and powerful nodes that are interconnected reliably.
This arrangement provides the possibility of a more efficient training and coordination as domains will be capable of making intricate calculations and regularly participate (Zhang *et al*., 2025). It also allows the creation of extremely advanced security, such as, but not restricted to, secure aggregation and encryption, with no significant performance impact.

3. Communication Model

In multi-domain optical networks, communication model of federated learning poses new challenges, in particular. Deep learning models may be large, leading to a higher bandwidth usage in model updates. In addition, privacy preservation via encryption can also lead to an increase of the size of data sent by several orders of magnitude.
Synchronization delays is another problem in cases where other domains may be differing in speed of processing and network conditions. To overcome this issue, asynchronous training has been proposed, by which realms can synchronize the global model without necessarily having to wait until all the participants are online.
The scalability and feasibility of FL in optical networks require effective communication schemes including update compression, sparsification, and adaptive transmission time (Chen *et al*., 2025). The multi-domain setting can also be fed with federated learning through the optimization of the communication model which enables the privacy-preserving and efficient optimization of the network.

Optimization Techniques Using Federated Learning

1. Traffic Prediction

One of the most crucial optimization processes in multi-domain optical networks is traffic forecasting, which dictates the effectiveness of routing and congestion control, and Quality of Service (QoS) on the whole. In conventional methods, to make accurate predictions about the traffic, it is necessary to have central access to the historically recorded traffic data on all domains, which is usually not feasible because of privacy limitations and administrative barriers (Liu *et al*., 2025). Federated Learning (FL) addresses this shortcoming by allowing collaboratively training models without exchanging raw data, thus ensuring privacy and enhancing prediction quality.
In an FL-based traffic prediction system, the domains are trained locally using their respective historic traffic data, including both time dynamics and peak-hour dynamics, service requirements, and user behavioral trends. These local models adopt domain specific traffic dynamics, otherwise unique in some geographic, demographic or application specific sense. The updates of the locally trained model are then exchanged with a central aggregator or hierarchical coordinator which integrates to create a global model (Mannaperumal *et al*., 2026). This cross-national paradigm means that there is increased generalization of traffic pattern in all the spheres involved.
One of the most significant advantages of FL in a traffic prediction is the possibility of FL to capture both local and global patterns at the same time. The global model, which is an aggregate form of the local model, unlike the local models, incorporates cross-domain correlations, leading to improved generalization and robustness. It has also been found particularly handy in multi-domain optical networks, where local variations and global trends may arise in traffic patterns.
The models of FL-based traffic prediction are usually based on the developed machine learning methods, including recurrent neural networks (RNNs), long short-term memory (LSTM) networks, and temporal convolutional networks (TCNs). The models can easily model the time-varying interactions of network traffic and they have time series forecasting capability. These models are not only applicable when integrated into a federated structure but also have privacy in the process of distributed training.
Scalability is another factor to consider. As the domains increase, the centralized approaches struggle to cope with the rising حجم of data and

complexity of computation (Iqbal *et al*., 2025). FL spreads training process over domains, eliminating the stress on any single entity and allows scaled deployment. Furthermore, hierarchical FL models can be scaled to become more scalable through consolidating the models at the intermediary level, and then form the global model.

In real-life applications, FL-based traffic forecasting has been demonstrated to cause a major decrease in congestions, as well as enhance network planning. When the traffic requirements are properly predicted, the network operators are able to make pre-emptive resource allocation, alter routing policies and prevent congestion points. This leads to the improved utilization of network, minimisation of latency and general improved user experience.

2. Routing and Wavelength Assignment (RWA)

Routing and Wavelength Assignment (RWA) is an essential issue in optical networks, especially in wavelength-division multiplexing (WDM) systems. It involves the selection of an optimum path where data transmission happens and allocation of an appropriate wavelength so that the data transmission constraints like the wavelength continuity and the non overlapping utilization is achieved. Multi-domain optical networks are far more complex to RWA due to low visibility, policy heterogeneity and dynamic traffic.

Federated learning is a recent solution to RWA optimization, where domains can figure out the best routing strategies collaboratively while not having access to sensitive network information (Hou *et al*., 2025). Training a local model is performed by each domain, and is informed by its network state, such as the use of links, the available wavelengths, past routing choices, and congestion. These local models are trained to predict the optimal routes and wavelengths assignment to such network conditions.

The models that are trained locally are then fed into a global model where inter-domain dependencies and broader dynamics of the network are captured, via federated aggregation. This world model can then be resorted to in making routing decisions in a distributed fashion enhancing the overall network efficiency.

Perhaps the most crucial benefits of FL in RWA is the possibility to predict congestion and dynamically make routing decisions. Traditional RWA algorithms are rather heuristic or statistic in nature and thus may not be useful in a fast changing traffic situation. On the other hand, FL-based models are able to use past and real-time information to predict congestion and choose alternative routes in advance.

Dynamic wavelength assignment is another important aspect (Zhao *et al*., 2023). FL models can predict the wavelength availability and allocate it optimally to minimize the blocking probability. These models can attain an improved utilization of resources by taking into account local and global information and lower the chances of connection failures.

Further, FL facilitates decentralized decision-making, which is appropriate in the context of multi-domain optical networks, which are distributed. The global model may be adopted to make informed routing decisions by each domain, as opposed to a central controller. This reduces the dependence on the centralized infrastructure and enhances the robustness of the systems.

3. Resource Allocation

Resource allocation within optical networks is important to ensure the best performance. The bandwidth, spectrum and network capacity should be dynamically distributed to meet the various load of traffic without resulting in congestion and also do justice. The problem of resource allocation is more complicated in multi-domain environments because of the lack of information sharing and the heterogeneous network conditions.

The federated learning can be employed to provide an advantageous model to optimize resource allocation in a decentralized privacy-conscious manner. Each domain trains a local model on its data, which may include demand pattern of traffic, resource use statistics, and performance data (Zheng *et al*., 2025). These models are learnt to predict the future demands on resources and how the resources should be used optimally.

Bandwidth management is one of the main uses of FL in the allocation of resources. The demand of traffic can be predicted by FL models which allocate bandwidth to different services or users dynamically so that it is used efficiently and the congestion is reduced. This is especially significant in optical networks where bandwidth is a very scarce and valuable resource.

The other one is the use of spectrum. FL models can optimize the optical spectrum allocation because they can forecast usage and avoiding fragmentations. This results in better spectral efficiency and network throughput.

FL also enhances load balancing. By reallocating traffic by the distribution of traffic over domains, FL models were able to absorb traffic over idle links, reducing congestion and improving the overall network performance (Sun *et al*., 2021). This can be especially useful in the context of multi-domain environment where the imbalance of traffic can lead to bottlenecks and low QoS.

FL may be deployed with dynamic bandwidth allocation (DBA) algorithms that may be utilized to prioritize the traffic that relates to model training and updates, and as a result, provide good communication within the federated system. This is significant in making sure that the latency and performance in FL-based systems are low.

Overall, FL enables intelligent and dynamic resource allocation by utilizing distributed data and distributed learning that leads to higher efficiency and scalability.

4. Fault Detection and Failure Localization

The most important in the reliability and strength of the optical networks is the failure localization and fault detection. Breakdowns like fiber cut, equipment failure and signal impairment may greatly affect network performance and availability of services. Multi-domain optical networks particularly are hard to monitor and detect faults due to low visibility and dissemination of information.

Federated learning is an inter-domain collaborative fault detecting privacy-preserving technique. Each domain develops a local anomaly detector model that is dependent upon the operation data of that domain, which consists of signal quality measures, error statistics and performance history (Wu *et al*., 2025). These models are trained to distinguish the patterns that are indicative of faults or anomalies.

The federated aggregation is the one that brings a global model which can take a wide range of failure patterns in domains. This enhances fault detection accuracy and strength of fault detection as opposed to isolated local models. It is interesting to note that this is achieved without sharing sensitive information about operations thus preserving privacy and security.

In this case, vertical federated learning (VFL) can be highly beneficial, as various areas can possess complementary characteristics instead of the same datasets. VFL allows learning across such heterogeneous data sources in a collaborative manner, providing increased fault detection.

FL-based fault detection systems can also be used in the support of real time monitoring and predictive maintenance. Such systems could also be employed to minimize downtime by identifying early warning signals of potential failures and taking proactive actions to avert failure, which make the network more dependable.

Privacy-Preserving Mechanisms

1. Differential Privacy

Federated learning has been widely applied in the privacy of sensitive data by applying differential privacy. It means that an intelligent noise is added to model updates prior to sharing them with the aggregator (Ahmad Madni *et al*., 2024). This guarantees that one cannot deduce individual data points based on the updates, even by an adversary that has access to the model.

Optical networks utilise differential privacy to help protect sensitive information such as network configurations and traffic pattern. Privacy and accuracy are however, trade offs, where excessive noise can adversely affect the performance of the model.

2. Secure Aggregation

Secure aggregation refers to a cryptographic technique that proves that single updates of a model cannot be accessed and reconstructed by the central server. Rather, the aggregate result is disclosed only. It is accomplished using encryption and decentralized multi-party computer protocols.

Mutual domain security in multi-domain optical networks enhances inter-domain trust, since it will ensure that contributions of domains are not revealed. It also safeguards against insider attacks and malicious aggregators.

3. Homomorphic Encryption

Homomorphic encryption allows performing computations on encrypted information without even having to decrypt it. This makes aggregation of models to be safe and has data confidentiality (Huang *et al*., 2025). However, homomorphic encryption involves high computation and communication costs, and it is challenging to apply homomorphic encryption to resource-constrained situations. This notwithstanding, current studies revolve around its efficiency to enhance its practical use.

4. Trust and Security Considerations

Ensuring trust and security in federated learning systems is critical for their successful deployment. Protection against inference attacks, in which opposing parties strive to understand sensitive information about model updates, and resistance to adversarial nodes which can deliver malicious updates are also key aspects.

The integrity and authenticity of model updates can be ensured with the help of secure communication protocols (TLS and blockchain-based mechanisms). Some of the techniques that may minimize the impact of malicious participants are also anomaly detection and robust aggregation.

Challenges and Limitations

Federated learning (FL) is a promising model of privacy-sensitive optimization in a multi-domain optical network; the model is not widely used due to a number of technical and operational challenges (Mir *et al.*, 2026). These are attributed to the characteristics of distributed environments, heterogeneity of domains and security risks, which should be properly mitigated to enable a sound and effective implementation.

1. Data Heterogeneity

One of the significant problems in federated learning is the data heterogeneity or non-independent and identically distributed (non-IID) data. Multi-domain optical networks possess various domains with varying conditions of the traffic, user behaviours, infrastructure setup and service requirements. This means that the local datasets that are used in the models training are vastly different in the distribution and statistics.

The outcome of such heterogeneity is that biased local updates are possible, and this also affects the quality of the final global model. Using the example of a domain with a high traffic volume can produce updates that overload control of that traffic but a domain with a steady traffic may produce less aggressive updates. When such updates are combined with the global model, it may not be able to generalize to all domains.

Also, non-IID data slows down convergence when training. The more traditional federated averaging algorithms assume relatively similar things about the data distributions and suffer relatively when these assumptions do not hold (Liu *et al.*, 2024). To overcome this problem, some sophisticated methods, including personalized federated learning, domain-adaptive aggregation, and clustering-based FL have been suggested. These solutions are to customize models to specific areas as they derive out of shared knowledge.

2. Communication Overhead

Another important constraint of federated learning is communication overhead, which is especially problematic in very large multi-domain optical networks. FL entails frequent model update between the domains involved and the central aggregator. Large updates can be made by deep learning models with millions of parameters, especially when using a smaller learning rate.

In addition, privacy-sensitive techniques such as encryption and secure aggregation also add to the growth in the size of the information being transmitted (Xiang *et al.*, 2019). This can lead to network congestion, increased latency, and poor utilization of bandwidth- in fact, the opposite of optimal optical networks.

In order to reduce the communication overhead, a number of methods have been suggested. Model compression is used to reduce the size of updates, which involves deleting unimportant parameters, and update scarification transmits only the most important updates. Overhead can also be minimized by adaptive communication strategies like reducing the number of updates or event-driven communication. In spite of the above developments, the challenge of balancing the effectiveness of communication and model accuracy remains.

3. Scalability Issues

With additional domains, the issue of scalability becomes a major challenge. Training coordination among many domains in a large multi-domain optical network is more and more complicated. A bottleneck may be a central aggregator, resulting in a slowing down of updating the models making the system inefficient.

Also, synchronization requirements may inhibit scalability. In synchronous FL, all domains should finish their local training before aggregation is possible, and this might be slow in practice when individual domains have limited resources or bad connectivity (Wang *et al.*, 2025). Asynchronous FL methods aim to address this issue, by allowing updates to be added independently, however, they are challenging in terms of model consistency and stability.

One of the possible solutions is hierarchical federated learning architectures which introduce intermediate levels of aggregation. Domains in these architectures are clustered and local aggregations are carried out prior to adding to the global model. Decentralized aggregation schemes such as peer-to-peer FL can also enhance scalability as the use of central server is not required.

4. System Heterogeneity

System heterogeneity is determined as the differences in the computation power, storage and network conditions between domains. Multi-domain optical networks can have domains with high-performance computing capabilities and reliable connectivity, and ones with limited processing power or bandwidth (Fan *et al.*, 2025).

This disparity affects the performance of federated learning, and stragglers or domain-resource-restrained spheres could slow down the training process. It can also lead to unequal contribution whereby learning process can be overcome by more powerful domains which may bias the global model.

The heterogeneity of the systems requires resource conscious training strategies. These may be adaptive workload distribution, and variable training epochs, and selective participation of domains which varies with their capabilities. Federated dropout and partial participation are methods which could also assist in balancing the training process and enhance efficiency.

5. Security Threats

An important aspect of federated learning system is security. Although FL is privacy-preserving in nature, it is susceptible to a number of attacks. In model poisoning attacks attackers strive to poison the global model by inserting malicious updates into it. The data inference attack aims at recovering sensitive data of commonly shared model parameters, which undermines privacy.

Failure in Byzantine, in which certain players act unpredictably or maliciously, may also cause more disturbances to learning (Lai *et al*., 2024). Such threats are especially worrisome in the multi-domain optical networks, where domains do not trust each other.

A robust defines mechanisms is required in order to ensure system integrity. Such risks may be mitigated through the assistance of such techniques as anomaly detection, resilient aggregation algorithms (such as median or trimmed mean) and secure multi-party computation. It is also necessary to introduce safe communication schemes and authentication measures that would guarantee that the model updates do not get on the wrong side and are modified.

Applications in Multi-Domain Optical Networks

Federated learning is facilitating a wide range of applications in multi-domain optical networks like the addition of intelligence, flexibility and privacy protection to the network activities.

1. Intelligent Optical Transceivers

FL simplifies development of intelligent optical transceivers which can dynamically adjust the parameters of transmission, such as modulation format, baud rate and power levels (Hashemi *et al*., 2021). These transceivers have the ability to exploit learned predictive models over other domains to achieve maximum performance depending on the prevailing and predicted network conditions, leading to reduced latency and increased spectral efficiency.

2. Network Slicing

Network slicing enables the establishment of a variety of virtual networks over a common physical base on the specifics of the application needs. The capability is boosted by federated learning, which predicts the traffic needs and dynamically allocates the resources, guaranteeing the efficient use of network slices and their isolation.

3. Edge Computing Integration

FL with edge computing also brings computation closer to the data source, reduces latency and increases responsiveness. It is especially useful in real-time applications like autonomous systems and smart cities where decisions are required to be made in a short period of time.

4. QoS Optimization

Constant Quality of Service (QoS) is a very important aspect in optical networks. Models based on FL have the capacity to forecast congestion, route optimization, and proactive resource allocation, which can guarantee stable performance and improved user experience in domains.

Emerging Trends and Future Directions

1. Integration with 6G Networks

Federated learning is probably the key to 6G networks, and it might be possible to have intelligent, autonomous, and self-optimizing communication systems that form the basis of advanced applications, such as immersive reality, and ultra-reliable low-latency communications (Wang *et al*., 2025).

2. Split and Hybrid Federated Learning

Hybrid approach of both centralized and decentralized learning paradigms are gaining popularity. Split FL, e.g., deploys model layers across clients and servers, enhancing efficiency and minimizing communication overhead.

3. AI-Driven Optical Networks

The interplay between FL and artificial intelligence technologies will allow self-healing and self-optimizing optical networks that will be able to respond to dynamic conditions without human intervention.

4. Energy-Efficient Federated Learning

Along with the advent of sustainability, research is now at work on how to reduce the energy consumption of the FL systems through efficient algorithms, hardware acceleration and optimal communication plans.

Case Study: Federated Learning in Passive Optical Networks

Passive optical networks (PONs) have been optimized to use federated learning to allocate bandwidth and improve network performance (Ibrahimi *et al*., 2025). Results show that scalable FL models are capable of maintaining a constant bandwidth usage whilst improving model accuracy by approximately 10%.

The algorithms of dynamic wavelength and bandwidth allocation give priority to FL traffic, resulting in efficient model training and minimized latency. The practicality and usefulness of FL in optical networks is proven by these results.

Performance Evaluation Metrics

The effectiveness of federated learning in multi-domain optical networks is measured based on a number of crucial metrics. Model accuracy is used to determine the effectiveness of the trained model whereas convergence time is used to determine the rate at which the model is able to achieve optimal performance. The cost of transmitting model updates is known as communication overhead and responsiveness of the system is known as latency. Privacy leakage risk is used to evaluate the risk of exposing sensitive information (Zhan *et al*., 2025). Collectively, these measures will give a holistic analysis framework to gauge the performance of FL-based optimization algorithms in optical networks.

Conclusion

Federated learning introduces a paradigm shift in terms of privacy-preserving optimization in the multi-domain optical networks. FL can address some of the most important problems of privacy, scalability and inter-domain trust because it allows training a model in a collaborative manner without sharing raw data. Its uses in traffic forecasting, optimization of routing and resource allocation show considerable enhancements in network efficiency and performance.

Nevertheless, such challenges as communication overhead, data heterogeneity, and the security risks are open research questions. The existing capabilities of federated learning in optical networks will be enhanced as the hierarchical architecture, hybrid learning models, and AI-based network management will be advanced.

Reference

Ahmad Madni, H., Muhammad Umer, R. and Luca Foresti, G., 2024. Exploiting data diversity in multi-domain federated learning. *Machine Learning: Science and Technology*, *5*(2), p.025041.

Huang, W., 2025. *Privacy-preserving federated learning framework* (Doctoral dissertation, University of Southampton).

Mir, B.A., Abbas, S.R. and Lee, S.W., 2026, January. Federated Learning in Healthcare Ethics: A Systematic Review of Privacy-Preserving and Equitable Medical AI. In *Healthcare* (Vol. 14, No. 3, p. 306). MDPI.

Liu, F., Ye, M. and Du, B., 2024. Domain generalized federated learning for person re-identification. *Computer Vision and Image Understanding*, *241*, p.103969.

Xiang, Q., Zhang, J.J., Wang, X.T., Liu, Y.J., Guok, C., Le, F., MacAuley, J., Newman, H. and Yang, Y.R., 2019. Toward fine-grained, privacy-preserving, efficient multi-domain network resource discovery. *IEEE Journal on Selected Areas in Communications*, *37*(8), pp.1924-1940.

Wang, S., Han, S., Cheng, Z., Wang, M. and Li, Y., 2025, September. Federated fine-tuning of large language models with privacy preservation and cross-domain semantic alignment. In *2025 6th International Conference on Computer Vision and Data Mining (ICCVDM)* (pp. 494-498). IEEE.

Fan, Y., Zhao, J. and Yue, M., 2025. Adaptive Privacy Preserving Federated Learning for Virtual Power Plant Cyberattack Detection. *IEEE Transactions on Smart Grid*.

Lai, H., Luo, Y., Li, B., Lu, J. and Yuan, J., 2024. Bilateral proxy federated domain generalization for privacy-preserving medical image diagnosis. *IEEE Journal of Biomedical and Health Informatics*, *29*(4), pp.2784-2797.

Hashemi, N., Safari, P., Shariati, B. and Fischer, J.K., 2021, September. Vertical federated learning for privacy-preserving ML model development in partially disaggregated networks. In *2021 European Conference on Optical Communication (ECOC)* (pp. 1-4). IEEE.

Wang, W., Zhang, S., Khan, Z., Liu, Z., Cai, D., Li, T., Huang, H., Khan, M.A. and Boulila, W., 2025. A Privacy-Preserving Authentication Scheme for Federated Learning in Drone-Assisted Vehicular Networks. *IEEE Transactions on Intelligent Transportation Systems*.

Ibrahimi, M., Temiz, F., Musumeci, F., Sticca, G., Sgambelluri, A., Castoldi, P. and Tornatore, M., 2025, May. Failure Localization in Disaggregated Optical Networks: Application of Vertical Federated Learning on Heterogeneous Data. In *2025 IEEE International Conference on*

Machine Learning for Communication and Networking (ICMLCN) (pp. 1-6). IEEE.

Zhan, S., Huang, L., Luo, G., Zheng, S., Gao, Z. and Chao, H.C., 2025. A review on federated learning architectures for privacy-preserving AI: Lightweight and secure cloud–edge–end collaboration. *Electronics*, *14*(13), p.2512.

Cloud, S., 2025, July. Privacy-Preserving Cross-Domain Personalization: Leveraging E-commerce Behavior for Adaptive E-learning Pathways using Federated Graph NetworksRahul Goel. In *2025 6th International Conference on Big Data & Artificial Intelligence & Software Engineering (ICBASE)* (pp. 330-342). IEEE.

Madni, H.A., 2025. Data and Model Privacy in Cloud Computing using Federated Learning.

Qian, L.P., Li, M., Ye, P., Wang, Q., Lin, B., Wu, Y. and Yang, X., 2023. Secrecy-driven energy minimization in federated-learning-assisted marine digital twin networks. *IEEE Internet of Things Journal*, *11*(3), pp.5155-5168.

Kholidy, H.A. and Kamaludeen, R., 2022, October. An innovative hashgraph-based federated learning approach for multi domain 5g network protection. In *2022 IEEE Future Networks World Forum (FNWF)* (pp. 139-146). IEEE.

Zhang, C., Shan, G., Roh, B.H. and Jiang, J., 2025. Fm2 learning: Llm-based federated multi-task multi-domain learning for consumer electronics and iot enhancement. *IEEE Transactions on Consumer Electronics*.

Chen, G., Wang, Q., Feng, Y. and Rekik, I., 2025. Metadata-driven federated learning of connectional brain templates in non-IID multi-domain scenarios. *IEEE Transactions on Medical Imaging*.

Liu, J., Du, L., Li, Y., Liu, R.P., Li, Y., Teng, F. and Hou, F.Y., 2025. Adaptive Federated Learning to Optimize Integrated Flows in Cyber-Physical Data Centers. *arXiv preprint arXiv:2511.00623*.

Mannaperumal, M. and Venkatesan, D., 2026. Improving Multi-Domain Autonomous Driving Data Classification Using Federated Learning-Based Yolo With Adaptive Dilated Residual Attention Network. *International Journal of Adaptive Control and Signal Processing*, *40*(2), pp.254-274.

Iqbal, S., Zhong, X., Khan, M.A., Wu, Z., AlHammadi, D.A., Liu, W. and Choudhry, I.A., 2025. Hierarchical continual learning for domain-knowledge retention in healthcare federated learning. *IEEE Transactions on Consumer Electronics*.

Hou, S., Li, S. and Buyukates, B., 2025. Privacy-preserving prompt personalization in federated learning for multimodal large language models. *arXiv preprint arXiv:2505.22447*.

Zhao, J., 2023. Privacy-preserving fine-tuning of artificial intelligence (ai) foundation models with federated learning, differential privacy, offsite tuning, and parameter-efficient fine-tuning (peft). *Authorea Preprints*.

Zheng, Y., Yeung, P.H., Xia, J., Ju, T., Tang, P., Qiu, W. and Rajapakse, J.C., 2025, October. FedDEAP: Adaptive Dual-Prompt Tuning for Multi-Domain Federated Learning. In *Proceedings of the 33rd ACM International Conference on Multimedia* (pp. 5375-5384).

Sun, B., Huo, H., Yang, Y. and Bai, B., 2021. Partialfed: Cross-domain personalized federated learning via partial initialization. *Advances in Neural Information Processing Systems*, *34*, pp.23309-23320.

Wu, M., Wang, K., Xu, H., Yao, X. and Zhang, P., 2025, September. FMER: A Federated Learning Approach for Privacy-Preserving Micro-Expression Recognition. In *2025 IEEE International Conference on Unmanned Systems (ICUS)* (pp. 1617-1622). IEEE.