Archives available at journals.mriindia.com

International Journal on Advanced Computer Engineering and Communication Technology

ISSN: 2278-5140

Volume 15 Issue 01, 2026

Federated Learning for Privacy-Preserving Optimization in Multi-Domain Optical Networks: A Comprehensive Review

[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: 08 March 2026

Revision: 26 March 2026

Acceptance: 05 April 2026

Keywords

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

Abstract

Further sophistication of optical communication systems, coupled with increased speed of data traffic has necessitated the requirement of smart and scalable network management optimization techniques. Multi-domain optical networks are those networks in which various administrative domains are connected and work together, which bring various challenges in terms of privacy, data sharing, interoperability and resource optimization. Traditional centralized machine learning approaches are not going to be useful in such configurations since they need to aggregate the data, which can be a communication and privacy and security burden. The new paradigm of Federated Learning (FL) has emerged as a promising prospect to enable the joint training of models without accessing raw data. In this review paper, the idea of federated learning is discussed in detail in the context of multi-domain optical networks with a focus on how it could be used to implement privacy-preserving optimization. The paper discusses the fundamentals, structure, key algorithms, use case, issues, and future studies. It will equip the researcher and practitioners with an in-depth concept of how federated learning is able to revolutionize next-generation optical networking systems.

Introduction

The optical networks constitute the foundation of the international communication infrastructure and enable the transmission of high data rates and volumes at a high speed over the continents. There has been an increase in multi-domain optical networks as a network architecture has developed. Such networks are made up of different interconnected domains, which are administratively controlled. But even though this kind of structure provides a higher level of scalability and flexibility, it also presents coordination, data sharing and optimization problems.

The use of traditional optimization methods in optical networks usually assumes the use of central data collection and processing. However in a multi-domain environment, the domains are usually unwilling or unable to share the raw data due to privacy concerns, regulatory requirements and market competition. This is a disadvantage of centralized machine learning approaches.

To address these challenges, Federated Learning is a problem solving tool that can be employed to train decentralized models. One paradigm model is trained on domain-specific data, and only model updates are sent to a central aggregator. This will facilitate learning together and ensure privacy of data. Multi-domain optical networks with federated learning has been of great interest since this may be used to improve the network

performance without compromising on confidentiality.

Basics of Federated Learning.

1. Concept and Principles

Federated Learning (FL) is a distributed machine learning paradigm that aims to overcome the drawbacks of conventional centralized learning systems, especially in areas where data confidentiality, ownership, and security are crucial issues. Unlike the conventional approaches of integrating the information of different sources into a centralized server to be trained, in federated learning, two or more clients or entities can jointly train a common global model, without their data being stored in a central location. This radical change in the learning paradigm makes sure that sensitive data does not leave its original place and, therefore, the chances of data breaches are significantly low, which guarantees compliance with privacy laws as well.

Each client in federation learning, e.g. a domain controller in a multi-domain optical network, possesses its local data and trains a local model on its own. The client sends model updates to a central aggregation server, upon a round of local training, e.g. gradients or weights. These updates are then added together by the server of all the participating clients to come up with a better global model. This combination is typically performed by algorithms like Federated Averaging, computed by taking a weighted average of the local model parameters, based on the size of the dataset of each client. The new world model is then re-shared to everyone and the cycle repeats itself until everyone is converged.

This collaborative optimization process is captured by the mathematical formulation of federated learning. The global objective function is given as:

F(w)=k=1∑KnnkFk(w)and F k (w)

is the local loss of the k th client and n k is the amount of data samples in the client and n is the amount of data samples in all clients. It is this formulation that underlines the fact that the global objective is simply a weighted summation of the local objectives, with the client with more datasets having a proportionately more influence on the global model. This design in particular is appropriate in the heterogeneous environment where the distribution of data among the participants is very diverse.

One of the values of federated learning is the data locality, which ensures that raw data remains within the local domain. This is especially true in multi-domain optical networks where each domain may harbor sensitive information about its operations such as traffic patterns, routing policies and performance metrics. The other concept is collaborative intelligence, where various parties have the option of joining into the learning process without necessarily sharing their data, therefore, coming up with more robust and generalized models. Further, federated learning centers its attention on the concept of refinements, whereby the model gets improved with each round of local training and global aggregation.

2. Key Characteristics

The features that make federated learning a particular method which may be particularly relevant in distributed and privacy-sensitive environments include a set of features. One of the most salient features is decentralization since the training process is decentralized among a number of clients, and is not confined to a central server. Such a decentralization not only gives a larger capacity to scale, but also minimizes single point of failure, which makes the system less robust.

Another attribute is privacy preservation. The nature of federated learning will automatically minimize the chances of sensitive data leaking as the raw data will not be transferred outside local domain. This is necessary in the circumstances where share data is restricted due to law, regulation or competition. It could be further enhanced with the help of such techniques as secure aggregation or differential privacy that are able to make even the model updates shared insensitive.

Another important aspect of federated learning is its efficiency in communication. Though the implementation would mean periodic communication between the clients and the central server, it saves a lot of data as opposed to centralized implementation. Instead of transferring data of large size, model parameters or gradients are transferred that tend to be much smaller. This renders federated learning more practical in a bandwidth-limited scenario.

The other interesting characteristic is that it can be applied in handling heterogeneous data distributions. In reality, especially in multi-domain optical networks, data across multiple domains are not non-independent and non-identically distributed (non-IID). Federated learning is supposed to be capable of operating under such conditions, which, however, can only be done with the assistance of certain algorithms and optimization strategies that will ensure the stable convergence.

Lastly, federated learning enhances scalability and flexibility whereby new clients can enter or exit the training process on-the-fly. Such

flexibility is especially useful in large-scale networks in which the number of domains involved might vary over time.

3. Federated Learning Workflow

Federated learning has a workflow made up of a sequence of coordinated actions that allow the training of models in a collaborative fashion without compromising the privacy of data. It starts with the creation of a global model in a central server. This model can be randomly initialized or pre-trained with the publicly available data.

After being initiated, the global model is shared with all the participating clients. The clients then locally train on their own dataset and update the model parameters based on their local objective function. This local training can be done with several repetitions or epochs based on the implementation and system needs.

After local training, each client sends its new model parameters to the central server. It is notable that no raw data are exchanged in the process. These updates are then aggregated by the server with a relevant aggregation algorithm, like weighted averaging. The outcome is a more global model, which takes into consideration knowledge of all customers involved.

New global model is then provided to the clients substituting their past local models. When a communication round is over, this happens. It is repeated in a number of rounds until a stable solution of the model is attained or the desired level of performance is achieved.

This is a workflow of continuous improvement that is employed to make sure that the model is enhanced and that the privacy of data is highly ensured. It also allows the system to be adaptive to the changing data patterns and network conditions and therefore, it is highly flexible in a dynamic environment such as the optical networks.

Overview of Multi-Domain Optical Networks

1. Architecture and Characteristics

Multi-domain optical networks consist of several network domains which are related and managed by various administrative entities. These industries work together to provide end to end communication services to the state of the art and still manage their internal operations. Scalability and flexibility of this decentralized design are essential, but coordination and optimization are complex.

Multi-domain optical network architecture typically contains domain controllers, optical switches and inter-domain communication channels. Control plane and control policy of each domain can vary greatly with control plane and control policy of other domains. Regardless of such differences, domains should collaborate to provide effective routing, resource assignment and service delivery.

The primary peculiarities of such networks are heterogeneity of infrastructure and protocols, decentralized control system and low level of data exchange. The heterogeneity is brought about by the fact that there are differences in hardware, software and operational policies across fields. Distributed control also ensures that each domain can operate independently and data sharing is possible in most instances to save sensitive information and competitive advantages.

2. Challenges in Multi-Domain Environments

Multi-domain optical networks have a number of issues that make the process of efficient optimization and management difficult. Lack of global visibility is one of the major challenges. Since each domain only has access to its data, it becomes difficult to make globally optimal decisions in terms of routing, resource allocation and fault management.

This is also an addition to the privacy issue whereby domains are not easily prepared to divulge information on how they work to other individuals. This limits the use of the classical optimization techniques which rely on the overall network knowledge. The other outstanding challenge is interoperability since differences in protocols and technologies in different fields can lead to lack of smooth communication and coordination.

Numerous coordination mechanisms are needed to make sure that various domains can collaborate successfully. This entails creating trust, establishing standard interfaces and implementing effective communication protocols. Additionally, there is the dynamism of the network traffic and topology, another dimension of complexity which must be dealt with by adaptive and intelligent solutions.

These barriers indicate that new approaches such as federated learning that are capable of attaining collaborative optimization without imposing any effects on data privacy and domain autonomy are needed.

Motivation for Federated Learning in Optical Networks

1. Privacy Concerns

In the contemporary optical networks especially those in the multi-domain setting, the data is not only technical but it is normally very sensitive and strategic. Traffic patterns, bandwidth usage, routing policies, user behavior, and failure logs are types of information that might provide

important insights into the infrastructure and operational strategies of a network operator. These data disclosure in fields may result in the exposure of vulnerability, loss of competitive advantage and even violation of regulatory frameworks in terms of data protection and confidentiality.

One such example is that traffic patterns will indicate the peak times of usage, the distribution of customers and demand of services, which is helpful to the competitors. On the same note, logs of failures and maintenance can be used to identify vulnerabilities of infrastructure that can be used maliciously. One of the biggest impediments to efficient global optimization will be the reluctance to exchange such sensitive information in multi-domain optical networks where administrative entities will need to collaborate.

The restrictions on the sharing of operational data are also likely to be imposed by regulatory provisions such as the data protection laws and industry compliance regulations. As a result, the traditional approaches, which rely on the centralized data collection, are no longer possible. These privacy concerns can be addressed with Federated Learning, where the information is not transferred out of its own domain. Only model updates are shared in the data that is shared and this significantly reduces the risk of sensitive information being leaked whilst still being able to collaboratively share intelligence.

2. Limitations of Centralized Learning

The traditional use of centralized machine learning models to optimize networks has some severe limitations to using on multi-domain optical networks. One of the primary issues is scalability. The more domains and the amount of data, the harder it becomes to effectively process and manage the data using centralized systems. The need to transfer the big data to the central server leads to bottlenecks and delays making the optimization in real-time difficult.

Communication overhead is another major issue at hand. The data generated by the optical networks is huge and to convey it to a central location, a lot of resources and bandwidth are needed. Not only does this add to the cost of operation, but also causes latency which might adversely affect time sensitive services like dynamic routing and fault detection.

Single points of failure are also susceptible to centralized systems. The entire learning and optimization process can be stopped due to the breakage of the central server or its violation. This is of particular concern to the truly critical infrastructure like optical networks where reliability is of primary concern.

In addition, centralized learning presupposes that data in various domains is easily integrated, which is not always so. The dissimilarity of the data heterogeneity, the dissimilarity of format and the dissimilarity of network policy make the process of aggregation also complex. This type of restrictions shows that a more decentralized and flexible approach is needed, which federated learning can provide effectively.

3. Advantages of Federated Learning

Federated Learning has a number of benefits that allow it to be highly optimized in multi-domain optical networks. One of the most significant benefits of it is privacy preservation. Federated learning can reduce the risk of data leakage and guarantee the adherence to privacy regulations by localizing data and sharing solely model updates.

Another significant benefit is less cost of communication. Rather than pass bulk quantities of raw data, model parameters or gradients are shared among domains and the aggregation server. This eliminates the need to use much bandwidth and enhances effective learning process.

Collaborative optimization is also possible with federated learning. They can train a global model in different ways, so that the system can be able to use different sources of data without endangering confidentiality. This leads to superior and robust models as compared to those trained on single datasets.

In addition, distributed decision-making is facilitated by federated learning. Each of the disciplines has the local model and is able to make decisions regarding local and global knowledge. This becomes especially crucial in dynamic systems such as optical networks, with which one needs to adapt quickly to the changing conditions.

Moreover, federated learning also increases the resistance to failure of systems because they do not rely on a single centralized system. Even though some of the domains do not participate in a particular round, the system will be capable of functioning and updating the world model. Such strength renders federated learning to be a viable and dependable solution to optimizing networks at scale.

Federated Learning Architectures in Optical Networks

1. Centralized Federated Architecture

The centralized federated architecture is the most common architecture in federated learning system. A central server coordinates the training

process and combines model updates across all domains in this model. All domains train a local model and submit its updates to the central server which then integrates the updates to create a global model.
Such architecture is relatively simple to implement, and it allows coordinating the process of learning. It also gives predictability in model updating where all the domains receive the same global model upon completion of each round of aggregation. However, the scalability may be an issue when the domains that are used in such an approach are centralized.
In addition, the central server may be a bottleneck especially in case of a large network whereby the number of communication rounds is high. Nevertheless, centralized federated architecture is still extensively utilized because it is easy and efficient in systems of medium size.

2. Hierarchical Federated Learning
Hierarchical federated learning is based on the centralized model and introduces a series of levels of aggregation between them. Instead of the direct communication of all the domains with a central server, they are arranged into clusters, each cluster possessing a local aggregator. These local aggregators combine update information of their respective domains and send the aggregated information to a higher level server.
This multi-level architecture can provide more scalability and reduce the load of the central server. It also decreases latency, as local aggregation can be performed more quickly within clusters. The hierarchical federated learning is especially applicable in large optical networks where the domains are geographically separated.
The other advantage of this approach is that it has a greater control of the heterogeneity. The domains overlap in the same cluster and could be trained to produce a local model and further aggregate it. This leads to a better convergence and system performance.

3. Decentralized Federated Learning
The concept of federated learning (decentralized) does not involve having a central server at all. In this architecture domains are interrelated with each other to share model updates. Aggregation is done by use of peer-to-peer communication protocols.
This approach aids in enhancing resilience since the single point of failure that is associated with centralized systems is removed. It also enhances privacy in that there is no central body that receives all changes in the model. Decentralized federated learning is a particularly suitable concept in the setting where the level of trust towards a central authority is low.
However, this architecture introduces new challenges such as increased complexity in regards to coordination and synchronization. Ensuring consistency in the global model becomes more difficult and because of the need to conduct multiple peer-to-peer interactions, the overhead of the communication can be larger. However, one of the promising trends is the decentralized federated learning that moves towards the full optimization of a network.

Algorithms and Techniques
1. Federated Averaging (FedAvg)
Federated Averaging (FedAvg) is the most popular federated learning algorithm. It works by averaging the updates of the models sent by the participating clients in a weighted manner. The weights are often proportional to the size of the dataset of each client, with the larger datasets having a larger impact on the global model.
FedAvg is easy, effective, and efficient in most of the situations. It minimizes the convergence communication round and is able to tolerate partial client participation. Its performance however, may be bad in a situation where there is high heterogeneity of the environment where the data distributions vary highly across domains.

2. Federated Reinforcement Learning
Federated reinforcement learning is a type of reinforcement learning that introduces the principle of federated learning, which allows making the decision-making process dynamic and adaptive. This model has domains that act as agents and learn the optimum policies in their local environment and share knowledge with other agents through federated updates.
The technique applies particularly in optical networks in routing, spectrum allocation and traffic management. Under federated reinforcement learning, domains are able to collaborate in order to learn strategies that optimize the overall network performance and dynamically adapt to new situations.

3. Secure Aggregation Techniques
The secure aggregation techniques will be aimed at safeguarding the privacy of the model updates during aggregation. These approaches make sure that individual updates are not available or can be deduced by other players or the central server.
All techniques typically used to achieve secure aggregation are cryptographic masking, homomorphic encryption, and multi-party computation. The methods enhance the privacy and security of federated learning systems and

consequently, can be applied more to sensitive applications on optical networks.

4. Differential Privacy

Another technique that is significant in federated learning to safeguard sensitive information is referred to as differential privacy. It involves the addition of noise, which is properly calibrated, to the model updates before they are propagated, in such a way that the impact of each single data point cannot be ascertained.

This method has good privacy assurances and does not compromise the overall utility of the model. When applied in the context of optical networks, it is possible to ensure the protection of sensitive operational data and at the same time provide the opportunity to collaborate effectively across domains using the concept of differential privacy.

Applications in Multi-Domain Optical Networks

1. Traffic Prediction

Traffic prediction is one of the most critical roles in optical networks since it directly affects resource allocation, congestion management, as well as quality of service. The multi-domain optical network traffic patterns are extremely dynamic and may be highly dissimilar in various domains due to the differences in the behavior of users, user distribution, and service demand. Conventional traffic prediction models, use centralized data that in most cases is not complete or is not available in a multi-domain scenario owing to privacy and administration restrictions.

Federated learning is a viable solution since each of the domains can learn local prediction models using their traffic data and contribute to a shared global model. This system enables the system to record the local and global traffic pattern without having to exchange raw data. Due to this, domains are able to enjoy the benefits of collective intelligence without compromising the privacy of their internal information.

Federated learning can predict both short time and long time variations in traffic in real world applications. Short term projections will help in real time traffic management, whereby the networks real time rearrange the routing paths and assign resources to avoid overloading of the networks. Long-term predictions are used to support capacity planning and infrastructure development since the trends of growth and peak demand time are known.

The other major advantage of federated traffic prediction is that it can cope with heterogeneity of data. Since the dynamics of the traffic of each domain may be different, the federated model can be trained to a more generalized model capable of working in a wide range of conditions. The resultant effect is that it is more accurate in prediction when compared to independent dataset trained models. Furthermore, federated strategies are capable of changing over time variations in the traffic flow by updating the global model through a series of learning rounds.

2. Resource Allocation

Resource (bandwidth, spectrum, routing) allocation efficiency is a natural problem in multi-domain optical networks, where resources (bandwidth, spectrum, routing) must be allocated across multiple administrative domains. It seeks to accomplish maximum utilization of the network and minimization of the latency, congestion, and service disruptions. However, it becomes difficult to optimal distribution of resources due to the lack of information about other spheres and unreliable network conditions.

It is possible to optimize the allocation of resources jointly through federated learning without the availability of all data. Both spheres may be trained on their local data to make estimates on resource demand and optimization of allocation strategies. Such local models are added to a global model that represents a wider network behavior to make more informed decisions.

Federated learning can be applied in routing and spectrum assignment problems as an example, though the aim in both is to find optimal paths and allocate frequency bands to transmit data. Using federated models, domains can predict network congestion and change strategies on resource allocation. This gives an enhanced load balance and reduced blocking probability.

Federated reinforcement learning can also be used to enhance resource allocation as domains can be trained to adopt the best policies by interacting with the network environment. Every sphere is a local learner, which learns and shares knowledge with other individuals. This process of collaborative learning enables the system to adjust to new situations and to use resources optimally on-the-fly.

Also, federated learning helps to optimize two or more performance objectives, in which performance metrics including latency, throughput, and energy consumption should be optimized together. Federated models are able to detect trade-offs and create balanced solutions by combining the information in two or more domains to enhance the overall performance of the network.

3. Fault Detection

Key features of optical network management are fault detection and reliability of the network. Outages in optical networks may cause severe service interruptions, loss of money and decrease in customer satisfaction. Multi-domain environments are particularly difficult to detect and diagnose faults due to lack of visibility and cross-domain sharing of data.

Federated learning is also a very strong concept in collaborative fault detection since the domains are able to share knowledge without sensitive information. Local models may be trained domain-by-domain, based on the operational data of the domain, e.g. signal quality measures, error rates and performance records. These local models are used to get a global model which can discover patterns and correlations across domains.

This cooperative method enhances correct fault detection and promptness. To take just one example, not all types of faults will manifest themselves consistently across domains, and that a federated model may be better aware of such disparities than a single-domain model. Early detection of anomalies will enable network operators to make timely decisions to reduce the duration of failure, as well as increase reliability.

Root cause analysis can also be implemented with the help of federated learning, the aim of which is to determine the root cause of a failure. The system will be in a better position to comprehend the complex interaction and dependencies within the network by integrating the knowledge in various domains. This results in quick and precise diagnosis of problems.

Moreover, the federated techniques offer resiliency by way of distributed monitoring and detection. Communication is still possible in the other domains, though some of them fail or have communication issues, the rest of the system can continue functioning and detecting anomalies with the rest of the participants. Federated learning is particularly suitable to large-scale and mission-critical networks due to its distributed nature.

4. Service Provisioning

Multi-domain optical networks Service provisioning is about the establishment of end-to-end connections that satisfy certain quality of service (QoS) requirements. This encompasses bandwidth, latency, reliability and availability parameters. Such applications as cloud computing, video streaming and real-time communication have to be supported by efficient service provisioning.

The advantage of federated learning is that it enhances the quality of service provisioning since it enables the making of intelligent and adaptive decisions across the domains. Using the assistance of information presented by a number of sources, federated models are able to predict the demand of services, evaluate the performance of networks and refine provisioning policies. This results in better QoS and minimal disruption of services.

One of the most significant is the benefit of federated learning in service provisioning, which is the diminishing likelihood of blocking. Blocking is one of the situations in which the network is unable to connect a requested network due to poor resources. Federated models can greatly decrease the chances of blocking by forecasting demand and maximizing resource allocation, enhancing user experience.

Dynamic service provisioning of federated learning is also achievable, in which connections are established and reconfigured in dynamic fashion based on the changing conditions in the network. This is particularly useful in such surroundings where the variations in the traffic patterns are very high. Federated learning helps the network to adapt fast and efficiently, by continually updating the global model.

In addition, federated methods enable cross-domain coordination, enabling different domains to collaborate effectively to deliver end-to-end services. It is done without the need to share data in detail and maintains the autonomy and privacy of each domain.

Privacy and Security Considerations

1. Threat Models

Although federated learning is much more privacy-protective, in that raw data is confined to local areas, it does not completely remove security threats. In fact, decentralization and collaboration of federated learning introduces new attack surfaces, particularly in the context of multi-domain optical networks in which parties may not necessarily be fully trusted of one another.

One of the most critical threats is model poisoning. In this type of attack, an attacker actively corrupts the local model updates and sends them to the aggregation server. Since the global model is constructed out of these updates, it takes only a few compromised clients to make any significant impact on the performance or add backdoors. These attacks can result in incorrect traffic predictions, inefficiency in routing choices in optical networks, or even deliberate network instability.

Another significant issue is inference attacks. The raw data is not exchanged, but the adversary may analyze the changes in the model or the final worldwide model to infer exploitable details on

the underlying datasets. An attacker could also be interested in re-creating traffic patterns or identifying specific usage patterns in a domain, as an example. It poses a particular problem in the multi-domain optical networks where the operational data is highly sensitive, and is typically linked with the business strategies.

Threats that are based on communication are also present and this complicates the security environment. During model exchange, attackers may steal or alter the information that is exchanged in the process of updating models by using techniques such as eavesdropping or man-in-the-middle attacks. These threats can compromise confidentiality and integrity of federated learning process. When such transmissions are large, like in large optical networks, the security of these transmissions is even more challenging because communication pathways cross multiple domains and infrastructures.

Free-riding is another emerging threat as some of the participants enjoy the global model without making any significant update. This not only decreases the efficiency of the entire system, but also brings about questions of fairness. Also, sybil attacks, in which a single attacker has several fake clients, can increase the effectiveness of malicious actions and interfere with the learning process.

All these threat models point to the fact that on the one hand, federated learning enhances privacy at the data level, but it is necessary to implement effective security measures to secure the learning process itself.

2. Mitigation Strategies

To address the threats mentioned above, a broad spectrum of mitigation measures has been created, with an aim to not only increase privacy but also security in federated learning systems.

Secure federated learning is based on encryption-based methods. Secure aggregation protocols make sure that individual model updates are encrypted prior to their transmission and can only be decrypted in aggregate form. This does not allow the central server or any other player to see individual contributions. Homomorphic encryption can further enhance this by enabling the computation to be done on encrypted data which guarantees end to end confidentiality.

Another commonly used method to improve the resistance to inference attacks is differential privacy. Differential privacy provides the guarantee that the contribution of a single data point is not identifiable by adding noise to model updates carefully calibrated. This offers great mathematical privacy assurances with a reasonable model performance.

Anomaly detection mechanisms are important to protect against model poisoning attacks. These methods examine new model updates to detect suspicious or conflicting behavior. Any updates that do not align with the pattern can be indicated or dropped and this way the integrity of the global model is maintained. Advanced mechanisms can be based on machine learning itself to identify malicious activities in real time.

Authentication and access control: It is guaranteed that the participants who are allowed to participate in the federated learning process are the authorized ones. This will deter intrusion and minimize the susceptibility to sybil attacks. To deliver tamper-proof and decentralized authentication, identity management systems based on blockchain are also being investigated.

Moreover, strong aggregation methods like the median-based or trimmed mean aggregation can minimize the impact of the outliers and malicious updates. These techniques work especially well in the settings where a group of participants can be compromised.

All these mitigation strategies are used to establish a multi-layered defense system that improves the security, reliability, and trustworthiness of federated learning in multi-domain optical networks.

Challenges and Limitations

1. Data Heterogeneity

One of the most basic issues of federated learning is its data heterogeneity. Multi domain optical networks have different conditions in the various domains, resulting in variations in data distributions. Traffic patterns, network configurations, user behavior, and operational policies might vary considerably across domains. This non-independent non-identically distributed (non-IID) data is very challenging to model training. Federated learning algorithms like FedAvg rely on the assumption that there is certain similarity in datasets, and when this assumption is not met, the global model can slow down in convergence, or may not reach optimal performance at all.

Additionally, the heterogeneity may result in biased models, which may be efficient to specific domains, yet inadequate to others. To solve this problem, sophisticated algorithms have to be created, which should be able to adapt to different distributions of data and provide fairness among the participants.

2. Communication Overhead

Despite the fact that federated learning will not require the transmission of raw data, model updates in both directions between clients and the aggregation server will be frequent. In large

scale optical networks where there are many domains, this communication may pose a major bottleneck.
In every round of federated learning, model parameters are to be exchanged, and their size can be huge, depending on the complexity of the model. The cumulative communication cost may cause the network resources to be overstretched and the latency to rise as more participants are involved.
To alleviate this challenge, efficient communication schemes including model compression, update sparsification and asynchronous communication are necessary. Nevertheless, these methodologies can create trade-offs between model accuracy and efficiency of communication.

3. Scalability Issues
Another important constraint of federated learning in the multi-domain optical network is scalability. The more domains are involved, the more complex the process of coordination of the training process is.
Such difficulties as scheduling communication, its synchronization and half-baked attendance of clients are to be addressed. Aggregation servers can be centralized which can cause delays and a decrease in system performance. Solutions may be found in hierarchical and decentralized architectures, but these bring extra complexity during the system design and implementation.
To achieve scalability, efficiency, and reliability is an open research question in federated learning.

4. Trust and Governance
Federated learning requires a critical element of trust in order to collaborate effectively. Multi-domain optical networks might contain domains that are in conflict of interest and may not be willing to engage in a common learning.
The questions of data ownership, fairness in models, and incentives schemes should be discussed very attentively. Participants must be assured that their inputs will be important and that the global model will serve all the areas fairly. Rules, responsibilities and accountability mechanisms must be established through governance structures.
Active participation can be incentivized through incentive systems (e.g., reward-based participation or weighting based on contributions). Yet, the construction of the decent and efficient incentive systems is a complicated process and both technical and economic aspects have to be taken into account.

Performance Evaluation Metrics
The effectiveness of federated learning in multi-domain optical networks can only be evaluated using a complex range of performance indicators. These measures can give information about the efficiency, accuracy and feasibility of the system.
One of the most common metrics is accuracy, which quantifies the accuracy with which the model is able to cope with tasks, i.e. predicting traffic, detecting faults, allocating resources, etc. High accuracy means that the model has managed to extract appropriate patterns using distributed data.
Another key metric is the convergence speed, which is the speed at which the model converges to a stable solution. The system is more efficient with a faster convergence which reduces training time and communication overhead.
Communication efficiency measures the quantity of data shared in the training process. This metric is particularly important in optical networks, where bandwidth is a valuable resource.
Scalability is the capacity of the system to support a growing number of participants and perform at a reasonable level without serious performance declines. Privacy preservation evaluates the performance of the methods of securing sensitive information.
Other metrics can be such as robustness which is the ability of the system to endure attacks or failure and fairness which is the ability of all the participants to gain out of the global model. Collectively, these metrics can give a comprehensive picture of the system performance and inform the development of more efficient federated learning solutions.

Future Research Directions
1. Integration with SDN and AI
Combining federated learning with Software-Defined Networking (SDN) and artificial intelligence is one of the promising ways of research in the future. SDN offers programmability and centralized control, which allows dynamically configuring network resources. It can be used together with federated learning to enable more efficient coordination and optimization across domains.
Artificial intelligence methods can also be used to improve the decision-making process by providing predictive analytics, automated fault identification, and automated resource management. Such integration can result in more adaptive and resilient optical networks.

2. Blockchain Integration
The blockchain technology provides decentralized and safe system of controlling federated learning procedures. Blockchain can

contribute to trust and transparency by giving an immutable list of transaction and model updates, which can increase the trust of the participants.
Smart contracts can also be employed to automate activities like authentication of participants, the distribution of incentives, and model validation. This minimizes the requirement of a central authority and enhances system reliability.

3. Adaptive Learning Models

The adaptive federated learning models need to be developed to manage the dynamic character of optical networks. These models must be in a position to adapt to the evolving traffic pattern, network conditions, and data distributions real-time.
Other methods that could be investigated to improve adaptability include meta-learning, transfer learning, and online learning. The highly dynamic environment can be enhanced by such models to improve performance and stability.

4. Energy Efficiency

Large-scale network systems are becoming energy-efficient. Computational and communication costs associated with federated learning are high and may result in high energy consumption.
It should conduct research to create lightweight models, effective training algorithms, and energy-conscious communication protocols. Such developments can ensure that federated learning is more sustainable and can be deployed in the real world in optical networks.

Conclusion

Federated learning has become an effective technique that assists in privacy-preserving optimization in multi-domain optical networks. It solves key problems related to centralized learning, such as privacy concerns, communication costs, and scalability. Federated learning allows collaboration on intelligence without sharing data, which means that it opens new opportunities in the network management and optimization areas.
In spite of the benefits, there are still a number of challenges such as heterogeneity in data, security vulnerabilities and complexities in coordination. The future research directions should be towards creating powerful, scalable and secure federated learning models that can fit the special needs of optical networks. With the ongoing technological advancement, federated learning is likely to be the key in the development of the next generation of intelligent and privacy-conscious communication systems.

Reference

Zhang, X., Gu, R., Dong, J., Chen, J., Sang, W. and She, C., 2023, November. Field trial of privacy-preserving resource allocation in multi-domain optical networks based on federated reinforcement learning. In *2023 Asia Communications and Photonics Conference/2023 International Photonics and Optoelectronics Meetings (ACP/POEM)* (pp. 01-04). IEEE.

Tian, C., Xie, Y., Chen, X., Li, Y. and Zhao, X., 2024. Privacy-preserving cross-domain recommendation with federated graph learning. *ACM Transactions on Information Systems*, *42*(5), pp.1-29.

Nampalli, R.C.R., 2025. Federated Learning for Multi-Domain Transportation Networks. *Available at SSRN 5867702*.

Xiong, R., Zheng, H. and Xiao, D., 2025, June. CSPFed: Compressed Sensing-Enhanced Privacy-Preserving Federated Learning for Efficient Multi-Domain Scenarios. In *ICC 2025-IEEE International Conference on Communications* (pp. 392-397). IEEE.

Chen, G., Zhang, X., Su, Y., Lai, Y., Xiang, J., Zhang, J. and Zheng, Y., 2023, June. Win-win: a privacy-preserving federated framework for dual-target cross-domain recommendation. In *Proceedings of the AAAI Conference on Artificial Intelligence* (Vol. 37, No. 4, pp. 4149-4156).

Chen, G., Zhang, X., Su, Y., Lai, Y., Xiang, J., Zhang, J. and Zheng, Y., 2023, June. Win-win: a privacy-preserving federated framework for dual-target cross-domain recommendation. In *Proceedings of the AAAI Conference on Artificial Intelligence* (Vol. 37, No. 4, pp. 4149-4156).

Wang, L., Wang, S., Zhang, Q., Wu, Q. and Xu, M., 2025. Federated user preference modeling for privacy-preserving cross-domain recommendation. *IEEE Transactions on Multimedia*.

Ghazal, T.M., Hasan, M.K., Hussein, A.H., Pandey, B.K., Ahmad, M., Safie, N. and Cascone, L., 2025. Federated learning with small and large models with privacy-preserving data space for holographic Internet of Things in consumer electronics. *IEEE Transactions on Consumer Electronics*.

Wang, Z., Goudarzi, M., Gong, M. and Buyya, R., 2026. A Knowledge Distillation-empowered Adaptive Federated Reinforcement Learning Framework for Multi-Domain IoT Applications

Scheduling. *IEEE Transactions on Mobile Computing*.

Oreoluwa, O., 2024. Federated Learning and Trust Fabric for Cross-Domain Network Resilience. *Available at SSRN 5976334*.

DIBBO, S.V., YOSHIMURA, H. and VHADURI, S., 2025. Challenges and Opportunities of Federated Learning In the Age of IoT: A Multi-Domain Comprehensive Survey.

Zhang, J., Duan, Y., Niu, S., Cao, Y. and Lim, W.Y.B., 2024. Enhancing federated domain adaptation with multi-domain prototype-based federated fine-tuning. *arXiv preprint arXiv:2410.07738*.

Haripriya, R., Khare, N. and Pandey, M., 2025. Privacy-preserving federated learning for collaborative medical data mining in multi-institutional settings. *Scientific Reports*, *15*(1), p.12482.

Feng, Y., Yuan, J., Liu, J., Lu, Y. and Wu, H., 2026. Cross-Domain Collaborative Federated Intelligence for Wireless Computing Power Networks. *Journal of Intelligent Computing and Networking*, *2*(1), pp.22-34.

Anaedevha, R. N., Trofimov, A. G., & Borodachev, Y. V. (2026). Differentially Private Optimal Transport for Multi-Cloud Intrusion Detection: A Privacy-Preserving Federated Domain Adaptation Framework. *Authorea Preprints*.

Anaedevha, R.N., Trofimov, A.G. and Borodachev, Y.V., 2026. Differentially Private Optimal Transport for Multi-Cloud Intrusion Detection: A Privacy-Preserving Federated Domain Adaptation Framework. *Authorea Preprints*.

Khan, J., 2025. Federated ETL Architectures for Multi-Domain Data Integration: Balancing Decentralization, Privacy, and Analytical Performance in Distributed Data Ecosystems.

Ibrahimi, M., Temiz, F., Musumeci, F. and Tornatore, M., 2024, July. Vertical federated learning for failure localization in partially disaggregated optical networks. In *2024 IEEE 25th International Conference on High Performance Switching and Routing (HPSR)* (pp. 1-6). IEEE.

Esmat, H.H. and Lorenzo, B., 2026. Federated network slicing in multi-domain, multi-technology, and multi-provider networks. *IEEE Transactions on Networking*.

Cai, J., Zhou, Z., Huang, Z., Dai, W. and Yu, F.R., 2023. Privacy-preserving deployment mechanism for service function chains across multiple domains. *IEEE Transactions on Network and Service Management*, *21*(1), pp.1241-1256.

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.

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.

Israel, O., 2025. Cross-Domain Privacy Challenges in Cloud-Telecom AI Systems: From Data Minimization to Secure Sharing.

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.

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.