Design And Implementation of Multilayered Federated Learning: Enhancing Model Performance and Privacy

Mr. Vaibhav Ghubade[1], Ms. Nikki Gharde[2], Ms. Aastha Shewale[3], Mr. Pramay Dhone[4]

Department of Computer Science and Engineering

JD College Of Engineering and Management Nagpur

Abstract. One of the biggest technologies in the world is machine learning. In the field of artificial intelligence, it has different uses. The most important requirement in developing machine learning algorithms is the availability of data. In general, data are not stored in a single location and tend to be distributed across various points of view. Privacy concerns for the data owner are caused by the use of this data for machine learning algorithms. Federated Learning has been set up to deal with this issue.

In the field of machine learning, a new research topic is shared learning. In 2015, the interest in federated learning, particularly as a result of research on telecommunications, was higher. As you can see from the figure, Google's post of 2017 on AI was even more interesting. Perhaps the active topic for research will be federated learning. To meet the needs of advanced new learning process architectures in the field of machine learning, it is possible to expand the scope of the shared learning research.

By using machine learning algorithms to update the weights of local machines, and by aggregating them for our worldwide model, Federated Learning will ensure that data owners' privacy is protected. This provides a decentralized way to train machine learning models. This process is delivering good results, but it faces different challenges in its implementation. There is a loss of accuracy and efficiency if we attempt to increase the privacy of distributed learning algorithms. We are proposing to develop Multilayer Fusion Learning to tackle these issues. By adding an extra layer between the client and server nodes, we're introducing a new algorithm. Our objective is to improve the efficiency of a shared learning model while respecting data privacy. To test our model, we are using the MNIST database

Keywords: "privacy", "data", "machine learning", "distributed optimization", "communication", "model updates", "artificial intelligence", "deep learning".

Introduction

Federated learning is a distributed learning paradigm for machine learning training. A model from distributed and isolated data. In three main ways, FL differs from data center-based distributed training:

1. Statistical Heterogeneity
2. System constraints.
3. Trustworthiness.

Federated learning models work with a variety of machine learning techniques, but data types and contexts are important. Possible applications are mobile phone users, self-driving car learning activities, and predicting health risks from wearable devices.

Machine learning, training and reasoning are two steps in this process. In federated training, local machine learningML models are trained on different heterogeneous data sets. For example, if you use a machine learning application, it will detect errors in your machine learning application's predictions and correct them. These will generate a local training database on every user's device. These local data centers exchange model parameters on a regular basis. These parameters are locked before being exchanged in a large number of models. No sharing of local data samples is allowed. This will improve privacy and cyber security. We create a common global model. To integrate a global model with local ML models, Global Model properties are shared with the local data center.

Multi-layer federated learning faces several challenges that need to be addressed to ensure its successful implementation.

One of the main challenges is the heterogeneity of the data and devices involved in the learning process. The data may be non-iid, and the devices may have different hardware and software configurations, which can affect the performance of the learning process.

Another challenge is the privacy and security of the data, as the learning process involves sharing data across multiple devices. Ensuring data privacy and security is crucial to prevent data breaches and protect the data owner's rights.

Additionally, the communication overhead between the devices can be high, which can affect the efficiency of the learning process.

Model Convergence: Federated learning can be slow to converge, as each device works on its model. This can lead to a decrease in overall accuracy, as the models may not converge on the same solution.

Finally, the lack of a standardized framework for multi-layer federated learning can make it challenging to implement and compare different approaches. Addressing these challenges requires developing new algorithms and frameworks that can handle the heterogeneity of the data and devices, ensuring data privacy and security, reducing communication overhead, and standardizing the multi-layer federated learning process.

1. Cross-Silo Federated Learning

Federated learning is a distributed machine learning approach that enables training machine learning models using data from multiple devices without transferring the data to a central server. Cross-silo federated learning is an extension of federated learning that enables training machine learning models across multiple organizations or silos. Cross-silo federated learning can be used in various applications such as financial fraud detection, healthcare diagnosis, and autonomous driving. This report provides an overview of cross-silo federated learning, including its architecture, and there are various types of algorithms are there, and their applications.

Cross-silo federated learning consists of multiple organizations or silos, where each silo has its own data and machine learning model. The silos are connected through a secure communication channel, which enables the exchange of model parameters between silos.

In cross-silo federated learning, each silo has a different privacy requirement. therefore, each silo performs local computations using privacy-preserving techniques such as differential privacy, homomorphic encryption, and secure multiparty computation. The silos exchange model parameters using techniques such as secure aggregation, secure ensembling, and secure federated learning.

2. Cross-Device Federated Learning

Cross-device federated learning is a type of federated learning that involves training machine learning models across multiple edge devices, such as smartphones, wearables, vehicles, and IoT devices.

This approach enables learning at the edge, bringing model training to the data distributed on millions of devices, which can improve the efficiency and scalability of the learning process. Cross-device federated learning can be considered as model-centric and cross-device, where learning takes place on the device, and the model is updated and aggregated on the server. However, cross-device federated learning faces several challenges, such as the heterogeneity of the data and devices, the communication overhead between the devices, and the lack of a standardized framework for cross-device federated learning. To address these challenges, new algorithms and frameworks have been proposed, such as FedDCS, a distributed client selection framework for cross-device federated learning.

Cross-silo federated learning is another type of federated learning that involves training models across multiple organizations or silos, which can face additional challenges, such as data privacy and security.

Cross-device federated learning has several benefits that make it a promising approach for machine learning. One of the main benefits is the ability to train machine learning models on data distributed across millions of devices, which can improve the efficiency and scalability of the learning process.

Cross-device federated learning also enables learning at the edge, meaning it brings model training to the data distributed on millions of devices, which can improve the efficiency and scalability of the learning process.

Problem Statement

Models available today are mostly focused on efficiency or functionality, but very few are focused on privacy. One such model that gives enough privacy is cross-device federated learning which is not very efficient as compared to other models. We propose a model that uses the advantages of both cross-device and cross-silo federated learning to improve privacy and efficiency.

Literature Review

1. "Federated Learning: Strategies for Improving Communication Efficiency" by H. Brendan McMahan et al. (2016) - This paper introduced the concept of federated learning and discussed communication-efficient strategies for distributed training of deep neural networks.

2. "Federated Learning: Challenges, Methods, and Future Directions" by Yang Liu et al. (2019) - This survey paper provides an overview of federated learning and discusses various challenges, methods, and future research directions, including multilayer approaches.

3. "Secure Federated Transfer Learning" by Tian Li et al. (2019) - This paper explores secure transfer learning in a federated setting, which is relevant when dealing with multilayer models across multiple parties.

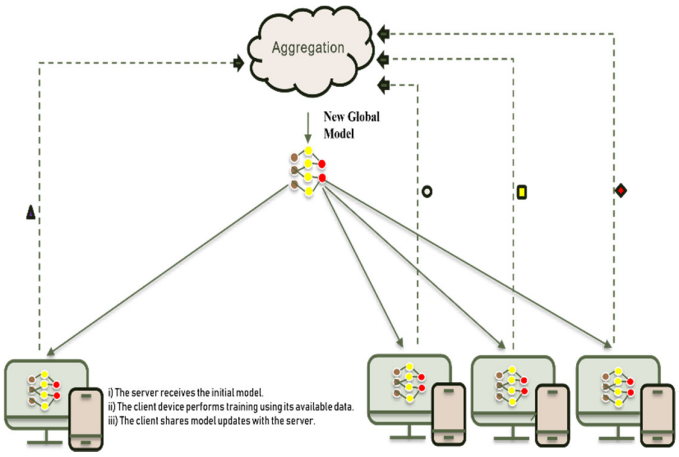
4. "Federated Multi-Task Learning" by Mehryar Mohri et al. (2019) - This paper addresses the problem of federated learning for multiple tasks, which can be applied in multilayer scenarios involving various subtasks.

5. "Efficient Deep Learning in Federated Edge Learning Systems" by Mingzhe Chen et al. (2020) - This work discusses efficient deep learning techniques in federated edge learning, which is relevant when applying multilayer models on edge devices.

6."Federated Meta-Learning for Recommendation" by Xinyi Wang et al. (2021) - This paper explores the application of federated meta-learning in recommendation systems, which can be extended to multilayer models for personalized recommendations.

7. "Secure Federated Multi-Task Learning with Application to Medical Imaging" by Kang Yang et al. (2021) - This research focuses on secure federated multi-task learning, particularly applied to medical imaging tasks, which often involve multilayer models.

Architecture



a. Client selection: The server chooses among the clients fitting the eligibility criteria. For example, client devices that are plugged into the charger and have good connection speed will be eligible for training our model.

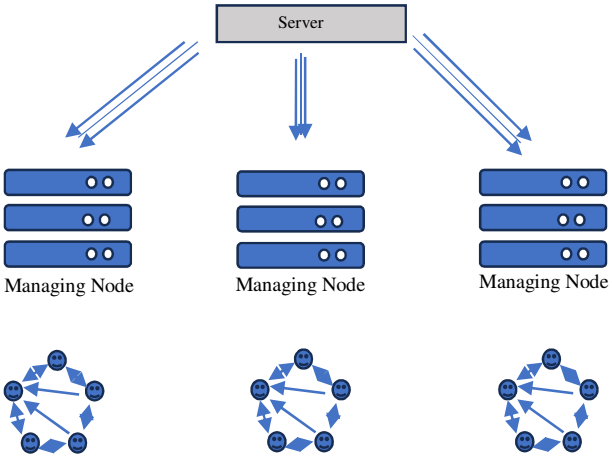
b. Broadcast: The clients then receive training models and weights from the server (e.g., TensorFlow graph).

c. Client computation: Clients then perform local computations and trains to update the model (e.g., SGD in Federated Averaging).

d. Aggregation: The server then aggregates the updates by clients. Various methods of aggregation like FedAvg, FedNova, etc. `can be applied for accuracy and encryption and differential privacy can be applied for increasing privacy.

e. Model update: The server locally updates the shared model based on the aggregated update computed from the clients that participated in the current round.

Our architecture comprises a management node between the client node and server:



Algorithm

1. Initialization: There are several clients in a network managed by managing nodes; the client k has local dataset D_k; each client's local model is initialized as W_o.

2. Managing nodes keeps track of clients using a decentralized model (Graph)

This model uses the advantages of both cross-device and cross-silo federated learning to improve privacy and efficiency. The global model is available with the server.

Result And Conclusion

Federated learning is a promising approach to machine learning that enables training models on decentralized data without the need to centralize or share that data. The main objectives of federated learning are to improve data privacy and security, reduce communication overhead, and enable learning at the edge.

Federated learning has several benefits, such as data privacy, scalability, and efficiency. However, it also faces several challenges, such as the heterogeneity of the data and devices, communication overhead, and lack of a standardized framework. To address these challenges, various algorithms and frameworks have been proposed, such as multi-layer federated learning, cross-device federated learning, and cross-silo federated learning.

These approaches aim to improve the efficiency, scalability, and privacy of the learning process. Federated learning has several potential applications, such as healthcare, finance, and IoT, where data privacy and security are critical. In conclusion, federated learning is a promising approach to machine learning that has the potential to revolutionize how we handle data and make decisions. However, there are still several open research questions and challenges that need to be addressed to realize the full potential of federated learning.

Acknowledgment

I would like to express my sincere gratitude to all those who have contributed to the completion of this research paper. Special thanks to Prof. Kiran Bode, for their invaluable guidance and support throughout this project. I am also thankful to Prof. Sujata More, for their assistance in data analysis. Additionally, I would like to acknowledge the support of Prof. Ashutosh Lanjewar Sir, for their feedback and encouragement. This research would not have been possible without the help of these individuals.

References

[1] He, Chaoyang, Songze Li, Jinhyun So, Xiao Zeng, Mi Zhang, Hongyi Wang, Xiaoyang Wang et al. "Fedml: A research library and benchmark for federated machine learning."arXiv preprint arXiv:2007.13518 (2020).

[2] H Brendan McMahan, Eider Moore, Daniel Ramage, Seth Hampson, and Blaise Agueray Arcas. Communication-efficient learning of deep networks from decentralized data. In Proceedings of the 20th International Conference on Artificial Intelligence and Statistics (original version on arxiv Feb. 2016).

[3] Bonawitz, Keith, Hubert Eichner, Wolfgang Grieskamp, Dzmitry Huba, Alex Ingerman, Vladimir Ivanov, Chloe Kiddon et al. "Towards federated learning at scale: System design." arXiv preprint arXiv:1902.01046 (2019).

[4] Li, Tian, Anit Kumar Sahu, Ameet Talwalkar, and Virginia Smith. "Federated learning: Challenges, methods, and future directions." IEEE Signal Processing Magazine 37.

[5] Koneˇcný, Jakub, H. Brendan McMahan, Felix X. Yu, Peter Richtárik, Ananda Theertha Suresh, and Dave Bacon. "Federated learning: Strategies for improving communication efficiency." arXiv preprint arXiv:1610.05492 (2016).