Annals of R.S.C.B., ISSN: 1583-6258, Vol. 25, Issue 5, 2021, Pages. 5610 - 5615
Received 15 May 2021; Accepted 20 May 2021.

Federated Learning for Image Classification Using Federated Averaging Algorithm

Hrushi Patel[1*], Tapan Dandawala[2], R. Jeya[3]
[1,2, 3]SRM Institute of Science &Technology, Chennai, India
*ha2832@srmist.edu.in
*tr5462@srmist.edu.in
*jeya.r@ktr.srmuniv.ac.in

ABSTRACT

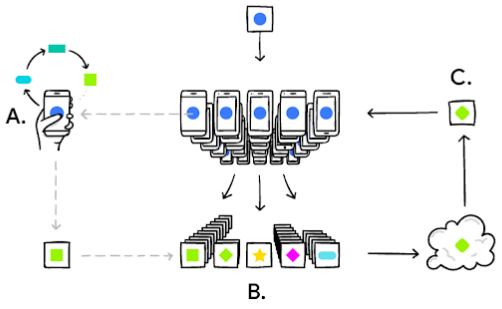
Image Classification, using traditional Machine Learning, is a very well-known technique but here in this paper we have used Federated Learning where the data of clients is not sent to the server and the model is trained itself on the user's device. Instead of sending data to the server we sent trained model to the server for further process. Federated Learning enables cell phones to work together to learn a common predictive model while storing all training data on the computer, effectively limiting machine learning of the need to store data in the cloud. This goes beyond using local models on mobile devices to make predictions from the model.
Training in the cloud. In our project we have used 70,000 dataset of fashion mist dataset for testing and training federated learning in 10 different categories. From the above dataset 60,000 dataset are used for training while other 10,000 are used for testing.
The 60,000-training data set is distributed among 5 users which act as a mobile device.

Introduction

The sensors, computing and communication technologies used in modern devices are getting more and more sophisticated in terms of efficiency and effectiveness.

Unlike traditional methods federated learning involves all the data storage and processing activities on the computer and eliminates the need for cloud storage services. This disintegration of machine learning from mobile cloud storage services allows the use of local models on mobile devices to make predictions by taking model training to the cloud.

Federated Learning (FL) in contrast, is a way to download the local model and integrate the updated model into the device itself (ala edge computing) using local data. These locally trained models are then uploaded from the devices back to the central server where they are integrated, which means the average weight, and then one integrated and improved updated model is sent back to the devices.



The Fashion MNIST Dataset contains 70,000 images which include 60,000 training images and 10,000 testing images. Each example is a 28x28 grayscale image that is associated with 10 different classes. This dataset is divided into 5 training batches and 1 test batch. The batch size is 12,000. There are 10 labels in the dataset i.e., T-shirt, Trouser, Dress, Pullover, Coat,Sandal, Shirt, Sneaker, Bag, Boot.

Annals of R.S.C.B., ISSN: 1583-6258, Vol. 25, Issue 5, 2021, Pages. 5610 - 5615
Received 15 May 2021; Accepted 20 May 2021.

Literature Review

IWei Yang, Bryan Lim, Nquyen Cong Luong, 2020, IEEE, Federated Learning in Mobile Edge Networks, A Comprehensive Survey.

It talks about introducing Federated Learning in mobile devices and also discuss the advantages and disadvantages of Federated Learning over traditional machine learning.
There are privacy and security issues and communication cost in traditional machine learning algorithms is higher.

IIKunal Chandiraman, Dhruv Garg, N Maheshwari, 2019, Elsevier, Performance Analysis of Distributed and Federated Learning Models on Private Data: -

The Federated learning model not only preserves privacy but is also fast and enables scale-based provisioning, even with mobile devices, with little computing effort.

III Li Li, YuxiFan, Mike Tse,Kuo-YiLin, Elsevier, A review of Applications in Federated Learning.

There are varieties of application were federated learning can be used and, in this paper, they have enlisted different application of it. As we know that privacy is becoming bigger concern now a days therefore Privacy Preserving Technology like this is required in order to overcome challenges of data loss and data sensibility.

IVViraaji Mothukuri, Reza M. Parizi, Seyedamin Pouriyeh, Yan Huang, Ali Dehghantanha, Gautam Srivastava, Elsevier," A Survey on Security and Privacy of Federated Learning"

In this paper they have examined the security vulnerabilities and threats in the federated learning environments.
But there are future challenges that we can counter like Security threats currently are communication bottlenecks, poisoning, and backdoor attacks.

V Nuria Rodríguez- Barrosoa, Goran Stipcich, Daniel Jiménez-López,2020, Elsevier, Federated Learning and Differential Privacy:
In this paper they have specifically focused on the privacy aspect of federated learning using the Sherpa.ai framework which uses specific guidelines in order to protect data privacy.

In this paper, it presents Sherpa.ai FL, which is unified framework for federated learning and differential privacy that is used to protect privacy of the users. It also has the same issue related to privacy that is generally breached by traditional models.

VITheodora S. Brisimi, Ruidi Chen, Theofanie Mela, Alex Olshevsky, 2018, Elsevier, "Federated learning of predictive models from federated Electronic Health Records": -

In this paper they have mentioned about using the electronic health records, it is possible to accurately predict heart-related hospitalizations. But data related to medical are generally not found.

VIINicola Rieke, Jonny Hancox, Wenqi Li, Fausto Milletarì, NPJ," The future of digital health with federated learning "

The paper analyzes on FL make it possible to gain knowledge in a collaborative manner. For example, in the form of a model agreement without moving patient information through the firewalls of the facilities in which they are located. There are many knowledge inconsistencies and also performance problems. Communication time is shortened as it is vital for medical purposes.

VIIIJakub Konečný, H. Brendan McMahan, Felix X. Yu, Peter Richtárik, Ananda Theertha Suresh, Dave Bacon, ArXiv, "Federated Learning: Strategies for Improving Communication Efficiency"

Annals of R.S.C.B., ISSN: 1583-6258, Vol. 25, Issue 5, 2021, Pages. 5610 - 5615
Received 15 May 2021; Accepted 20 May 2021.

The article describes different types of strategies for improving communication efficiency when dealing with a large amount of data. Due to the large number of clients, the highly unbalanced data available on each client, the relatively poor network connections and also the higher communication costs. These asymmetrical and unreliable connections represent a particular challenge for practical learning in a network.

IXLingjuan Lyu, Han Yu and Qiang Yang, ArXiv "Threats to Federated Learning: A Survey"

In this paper, in particular, they discussed the threats to federated learning and how it can be significantly more dangerous than traditional models. FL may not always provide adequate data protection safeguards because submitting model updates throughout the training process can still reveal sensitive information.

Proposed Work

In previous system the data from clients were sent to the server where the machine learning model was trained when that data was fed. In the proposed system we are using federated averaging algorithm which would just take the weights from distributed model and send it to the server which would take average of the weights and send it back to the heterogeneous devices and training on each device continues without transfer of data therefore increasing privacy and security.

Steps for the proposed system:

1. On the server, a generic (shared) model is trained and it sent to the selected devices.

2. On top of the generic model, a selection of clients is chosen for preparation. Here we have already divided dataset among 5 clients manually giving each of them 12,000 datasets each. There are thousands of devices available therefore devices are selected based on the performance of devices.

3. Based on an optimization algorithm like Adam's optimizer, the generic model is trained on the computers/devices itself, leveraging the users' private data.

4. The server receives a list of the model changes (i.e., the weights of the trained neural network). These weights are gathered from all different models.

5. To boost the shared model, the server collects weights from all devices and aggregates them. A new algorithm called the federated averaging algorithm is used for updating aggregation.

6. The method of sending a standardized model to mobile devices and updating them based on the received update is repeated. As the model are updated regularly, they again deployed to all the devices.

Benefits of Proposed System

1. Privacy

   It's not realistic to ask the user to upload vast quantities of data to the server in order to generate a generic model. The customer would incur extra costs as a result of this. Also, particularly for applications that require confidential user details, the user is likely to refuse uploading private data to help create a model. In comparison to centralized learning, federated learning is a good choice in cases where data is private or broad in size.

Annals of R.S.C.B., ISSN: 1583-6258, Vol. 25, Issue 5, 2021, Pages. 5610 - 5615
Received 15 May 2021; Accepted 20 May 2021.

As a result of the preceding issue, users' raw data does not need to be sent to the central cloud. This improves user privacy and decreases the likelihood of eavesdropping to some degree, assuming that FL participants and servers are not malicious.

Indeed, improved privacy would encourage more users to participate in shared model training, resulting in better coalition models that is combined by all local model.

2. Low communication time

FL permits ML models to be taught and modified in a constant manner. Meanwhile, real-time selections, which include event detection, may be taken locally. As model, no longersend any information to the server.

Consequently, now it'dno longer take time for the decisions like the traditional method where it would take lot of time.

This is important for time crucial applications which includes self-drivingvehiclein whichchoicesneed to be made in real-time otherwise lives might be at risk.

3. Personized model

As the model is trained locally it would be based on user's activity and more personalized to that particular user compared to the generic model where common model is deployed to all the user irrespective of their uses. Like in iPhone we have personized Siri suggestions which is based on our usage and it is trained on your device.

Methodology

- Data Preparation

The data is first divided into five clients, having 12,000 training images each.
The images are normalized and converted into greyscale image which would be useful for training the model. Thereafter we instantiated the client models. For every client, the test images are common (10,000) and 12,000 training dataset each which are manually divided.

- Model and Algorithm Used

For this we have used Adam optimizer and Sparse Categorical Cross Entropy as a loss function to calculate the loss and accuracy of the model. We use federated averaging algorithm to take average of the weights.

$$f(w) = \sum_{k=1}^{K} \frac{n_k}{n} F_k(w) \quad \text{where} \quad F_k(w) = \frac{1}{n_k} \sum_{i \in \mathcal{P}_k} f_i(w).$$

- Training the model

All the client are trained parallelly with unique dataset given to them. Next, we use the federated learning for training our client models for 50 communication rounds. Here we extracted the weights of each model and assigned the mean average of the weights to every model and train again in each communication round.

- Evaluate the model

Next, we train our client models and extract out the test accuracy for each client. Here, after training the model we record the accuracy.Thereafter we have trained model without using federated learning and record the results in order to find the difference between both models.

Annals of R.S.C.B., ISSN: 1583-6258, Vol. 25, Issue 5, 2021, Pages. 5610 - 5615
Received 15 May 2021; Accepted 20 May 2021.

- Make Predictions

With the model trained, you can use it to make predictions about some images.
Let's look at the ith image, predictions, and prediction array. Correct prediction labels are blue and incorrect prediction labels are red. The number gives the percentage (out of 100) for the predicted label.

Results

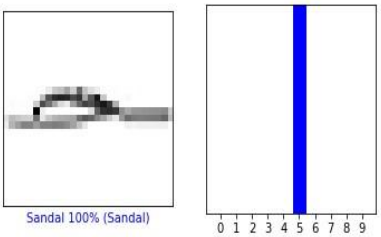
As we know that traditional machine learning algorithm are prone to security breaches and data leaks, we are trying to incorporate federated learning model which is faster and also provide nearly same accuracy by providing more security.

Below are results before updating the parameters:

Client	Training Accuracy on Individual Data (in %)	Testing Accuracy on Individual Data (in %)
Client-1	81.56	83
Client-2	83.12	84.67
Client-3	82.99	84.54
Client-4	81.53	84.29
Client-5	79.35	82.29

So, the accuracy of our model is 87.27 percent and the accuracy of traditional classification is around 85.4 percent. Therefore, federated learning not only provides privacy but also gives more accurate results in a fast manner. So, in near future the use of federated learning is going to be used widely as data leaks are becoming common this day

```
i = 8
plt.figure(figsize=(6,3))
plt.subplot(1,2,1)
plot_image(i, predictions[i], test_labels, test_images)
plt.subplot(1,2,2)
plot_value_array(i, predictions[i],  test_labels)
plt.show()
```



Annals of R.S.C.B., ISSN: 1583-6258, Vol. 25, Issue 5, 2021, Pages. 5610 - 5615
Received 15 May 2021; Accepted 20 May 2021.

Conclusion

Federated learning holds great promise as it can train models on a user's device without sharing the raw data, thereby maintaining privacy. As privacy becomes more important, the use of compound learning would increase.

It is important for us to find a workaround for the problems caused by the traditional ML model and there are problems such as communication costs, resource allocation and data security that FL can solve. Federated learning is the best privacy model while training accurate models on distributed devices. There are heterogeneous devices in which these models are implemented.

References

[1] Federated Learning for Image Classification,Tensor Flow-Tutorials

[2] Saheed Tejani,Federated Learning: A Step by Step Implementation in Tensorflow, Towards Data Science

[3] Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning," nature, vol. 521,no. 7553, p. 436, 2015.

[4] Wei Yang Bryan Lim, Nguyen Cong Luong, Dinh Thai Hoang, Yutao Jiao, Ying-Chang Liang, "Federated Learning in Mobile Edge Networks: A Comprehensive Survey", IEEE

[5] R. K. Ganti, F. Ye, and H. Lei, "Mobile crowdsensing: current state and future challenges," IEEE Communications Magazine, vol. 49, no. 11,pp. 32–39, 2011.

[6] Theodora S. Brisimi , Ruidi Chen, Theofanie Mela, Alex Olshevsky,2018,"Federated learning of predictive models from federated Electronic Health Records",Elsevier

[7] Jakub Konečný, H. Brendan McMahan, Felix X. Yu, Peter Richtárik, Ananda Theertha Suresh, Dave Bacon,

"Federated Learning: Strategies for Improving Communication Efficiency",ArXiv

[8] Nicola Rieke,Jonny Hancox, Wenqi Li , Fausto Milletarì,"The future of digital health with federated learning",NPJ

[9] Evolutionary optimization algorithms - A review
Jeya, R., Venkatakrishnan, G.R., Rengara, R., ...Bharath Raj, N., Ramanathan, G.Journal of Advanced Research in Dynamical and Control Systems, 2018, 10(10 Special Issue), pp. 1112–1122

[10] [Creating web server in android mobile and easy serving of information to clientsGummadidala, K.R., Jeya, R.Indian Journal of Science and Technology, 2016, 9(39), 102073

[11] Survey paper on hand gesture reconization based on surface EMG sensorsJagadeesan, S., Bajrachary, R.B., Bhusal, S., Jeya, R.AIP Conference Proceedings, 2019, 2112, 020172