COMPARATIVE ANALYSIS OF FEDERATED MACHINE LEARNING ALGORITHMS

Abstract: In this paper, the authors propose a new machine learning paradigm, federated machine learning. This method produces accurate predictions without revealing private data. It requires less network traffic, reduces communication costs and enables private learning from device to device. Federated machine learning helps to build models and further the models are moved to the device. Applications are particularly prevalent in healthcare, finance, retail, etc., as regulations make it difficult to share sensitive information. Note that this method creates an opportunity to build models with huge amounts of data by combining multiple databases and devices. There are many algorithms available in this area of machine learning and new ones are constantly being created. Our paper presents a comparative analysis of algorithms: FedAdam, FedYogi and FedSparse. But we need to keep in mind that FedAvg is at the core of many federated machine learning algorithms. Data testing was conducted using the Flower and Kaggle platforms with the above algorithms.

Federated machine learning technology is usable in smartphones and other devices where it can create accurate predictions without revealing raw personal data. In organizations, it can reduce network load and enable private learning between devices. Federated machine learning can help develop models for the Internet of Things that adapt to changes in the system while protecting user privacy. And it is also used to develop an AI model to meet the risk requirements of leaking client's personal data. The main aspects to consider are privacy and security of the data, the choice of the client to whom the algorithm itself will be directed to process the data, communication costs as well as its quality, and the platform for model aggregation.

Keywords: federated learning; FedAvg; FedAdam; FedYogi; FedSparse; loss; accuracy.

Introduction

The usage of federated Learning helps clients to train a global model without sharing their data. It is a new machine learning paradigm that works with decentralized data from multiple clients to train a global model [1]. These days, “big” data is collected by distributed networks made up of gadgets, cars, and cellphones. Local data storage is getting more and more appealing due to the devices is rising processing capability and worries about the transmission of sensitive information. Clients in federated learning independently gather local data according to their own device [2].
The main idea is sending the model to the device and the data stays on the device. This method guarantees that the learning process of the model works right on the end devices. So, you can train the model on datasets located in different places without having to interact with the actual data, to make the universal global model with no necessity to centralize the local data. Individualized data stays localized, minimizing the potential risk of client data exposure [3].

Put differently, the training of a machine learning model through federated learning doesn’t necessitate the data to be situated on a central server. Instead, federated learning employs decentralized approaches to train models that are centrally located. The training process in federated learning is iterative, involving multiple rounds of training. This iterative nature ensures ongoing learning and the exchange of knowledge [4].

The description of the working process is:
1. to select a model that has either already been trained or is not yet trained at all, and then transfer the global model to local devices or local servers;
2. to train local models on local datasets;
3. to learn a shared prediction model until all the training data stays on the device [5].

The cloud is for transferring the values of the local model, Figure 1. The aggregate data are used by the global models to calculate optimal performance. To incorporate the global model into the local model, the attributes of the global model are then moved to local data centers [6].

The term “federated” started to appear in academic articles in 2015 year. I looked through platforms such as IEEE, Google Scholar, etc. I present the results of my research. In the past 2015 year [7] and 2016 year [8], the first publications on federated averaging in telecommunication systems have appeared. Another important aspect for active research is to solve the problem of how to reduce the communication load in federated learning. Publications in 2017 year [9] and 2018 year [10] focused on developing strategies for resource allocation, especially for reducing the communication costs between nodes with algorithms and models, and on characterizing robustness to differential privacy attacks. The diagram below shows «The use of the term “federated learning” by year», Figure 2.
**Literature review**

In work [11] you can see definition of federated learning trains algorithms on decentralized edge devices, guaranteeing congeniality and data sharing among participants. It has applications in privacy-sensitive areas like medicine, banking, and manufacturing. There are three different forms of federated learning: horizontal, vertical and transfer. In federated learning have existed many ready algorithms, some of them in paper [12], including FedAvg (averaging algorithm), FedMA (matched averaging algorithm), FedProx, FedAmp (attentive message passing algorithm), MOON (model-contrastive learning algorithm) and FedLab [13].

In this paper [14] you can find summary of FL methodologies and illustrates how they can be applied in a number of IoT, including smart cities, medicine and industrialization. It also covered research opportunities of FL in IoT. The architecture of FL divided in different categories based on scale of federation, data partitioning and communication architecture. Also, during our research we used framework Flower. The description of it is in work [15]. Flower (FL) is another open-source framework for federated learning. Flower provides an abstraction for federated learning and allows developers to create and manage federated models easily. Flower supports several different algorithms for optimizing model training. In paper [16] are the applications of federated learning: Gboard, medicine, smart retail, finance, autonomous vehicles, smart grids, agriculture, industrialization. Looking through the paper [17], we see various uses of federated learning. The application of federated learning in smart devices and the Internet of Things is now beginning to take off. The researcher [18] concentrated only on examining the AI methodologies used by researchers for device protection and data security aspects, notably for Industrial IoT systems (IIOT) with decentralized design, which create enormous amounts of data and are security crucial.

The authors of [19] discuss the vulnerability of poisoning attacks considering the distributed nature of FL. Byzantine and backdoor attacks are variants of poisoning attacks. Currently, there is interest in federated learning algorithms, that are resistant to poisoning attacks. Defense strategies are anomaly detection, robust aggregation, and perturbation mechanism. In [20], the authors proposed to use fuzzy logic with a strategy to allocate different weights among clients. As a conclusion it was found that Federated Averaging algorithm shows worse results than the above-mentioned method.

**Problem statement**

The analysis of algorithms of federated learning has shown, that the first main algorithm is FedAvg, and now is the basis of many algorithms, but Per-FedAvg built the concept of indi-
visualized federated learning. Each newly created algorithm corrects weaknesses of previous algorithms by expanding upon robustness [21].

The base of the algorithm FedAvg-DWA is FedAvg. The idea of sampling weights is used in this technique to train the logistic regression model. You can give each sample a weight during the client-side local training phase. This method’s main idea is to make the model more sensitive to the loss of minority class samples during training, which will cause the model to concentrate more on correctly predicting positive class samples when the loss function is being optimized [22].

Here, FedVar, which improves data processing on the central server by utilizing the dispersion of weights. By calculating the weight’s norm tensors to calculate the mean and variance, and by calculating an advanced weight average including weights within the calculated scale of the standard deviation, a special data distribution is excluded, and a universal model is completed. As a result, the model performs better overall. By contrasting it with the current algorithms FedAvg, the suggested algorithm’s performance is confirmed [23]. After comparing FedProx, FedAvg, and Scaffold with alternative local updating approaches, we find that FedProx is consistently slow-going. FedAvg always moves more slowly than FedProx and more quickly than Scaffold [24].

Materials and methods
At first, the datasets needed to be specified before the experiments could be conducted. We have assessed the methods by looking at several federated learning algorithms. We want to identify the dataset; we utilize for algorithm development when designing platforms and algorithms. Our decision is to be utilizing the CIFAR-10 which was assembled by Alex Krizhevsky [25]. Color pictures (60,000 32x32) split into 10 groups, with 6,000 photos in every group. Totally are 10,000 test photos and 50,000 training photos.

10000 photos make up each of the 5 training group and one test package that comprise the dataset. There are precisely 1000 unsystematically chosen photos from every group in the test packages. The last photos are split up randomly across the training package; however, certain training packages could include more photos from one group than another. Every training package has just 5000 photos from all the groups combined.

The next step is about data testing platforms:
1. Flower.
2. Kaggle.

Flower is a federated learning system that works with single-node or multi-node compute clusters as well as actual edge devices to enable training and evaluation in huge cohorts. This makes it possible to explore techniques in a scalable manner in real-world settings, such the constrained computing resources seen in most federated learning workloads. Flower is also fully extensible and can incorporate new algorithms, training strategies and communication protocols. With Flower, you can make experiments that use both algorithmic and system aspects of federated learning in five machine learning processes with up to 15 million clients [26].

At second, Kaggle is a platform service for in machine learning was founded in 2010. Companies and its specialists provide the dataset and themes for competitions, and users propose, for example, analysis models. A system where the companies and institutions providing the challenges purchase outstanding analytical models in exchange for prize money. In addition, the method for analyzing the data sets provided not only by the competition function but also by the kernel function will be published. A kernel is an environment that can run the data input, analysis process, output, etc. on a browser in notebook format, which is the smallest unit of an analysis project on Kaggle. A user can simply run the code in the browser without having to create an analysis environment on their own computer [27].
Results and Discussion

In this section, we have presented the definition of algorithms of federated learning that used in our experiments. But before we move on to the dependence of the algorithms of FedAvg, FedOpt, FedAdam, FedYogi, FedSparse, you can see on the Figure 3.

![Figure 3. The algorithms of federated learning](image)

Definition:

1. **Algorithm FedAvg**

McMahan was the first, who introduce FedAvg he took notice of minimizing communication costs. The specific workflow of the algorithm is as follows [28]:

1. The K clients are indexed by $k$; $B$ is the local minibatch size, $E$ is the number of local epochs, and $\mu$ is the learning rate.
2. **Server executes:**
   - initialize $\omega_0$
   3. **for each round** $t = 1, 2, \ldots$ **do**
   4. $m \leftarrow \max(C \cdot K, 1)$
   5. $S_t \leftarrow \text{(random set of } m \text{ clients)}$
   6. **for each client** $k \in S_t$ **in parallel do**
   7. $\omega_{t+1} \leftarrow \text{ClientUpdate} (k, \omega_t)$
   8. $m_t = \sum_{k \in S_t} n_k$
   9. $\omega_{t+1} = \sum_{k \in S_t} \frac{n_k}{m_t} \omega_{t+1}^k$
10. **ClientUpdate** $(k, \omega)$:
   11. $B \leftarrow \text{(split } P_k \text{ into batches of size } B)$
   12. **for** each local epoch $i$ from 1 to $E$ **do**
   13. **for** batch $b \in B$ **do**
   14. $\omega \leftarrow \omega - \mu \nabla l(\omega; b)$
   15. return to server

An optimization problem of federated learning in algorithm FedAvg you can see in this formula [29]:

$$
\min_{x \in \mathbb{R}^d} f(x) = \frac{1}{m} \sum_{i=1}^{m} F_i(x),
$$

where, $F_i(x) = E_{x \sim D_i}[f_i(x, z)]$ – loss function of i-th client, $z \in Z$

$D_i$ – data distribution of i-th client

FedAvg is a method for training algorithms in which the data is distributed across many different servers or devices. It ensures data privacy and security and maintains the locality of the data so that models can be trained without sharing raw data.
2. Algorithm FedOpt
Algorithm FedOpt is based on FedAvg [30].

1: Input: \( x_0, \text{ClientOpt}, \text{ServerOpt} \)
2: for \( t = 0, \ldots, T - 1 \) do
3: \hspace{1em} Sample a subset \( S \) of clients
4: \hspace{1em} \( x_{t,0}^i = x_t \)
5: \hspace{1em} for each client \( i \in S \) in parallel do
6: \hspace{2em} for \( k = 0, \ldots, K - 1 \) do
7: \hspace{3em} Compute an unbiased estimate \( g_{i,k}^t \) of \( \nabla F_i(x_{i,k}^t) \)
8: \hspace{3em} \( x_{i,k+1}^t = \text{ClientOpt}(x_{i,k}^t, g_{i,k}^t, \mu_t, t) \)
9: \hspace{3em} \( \Delta_t^i = x_{i,K}^t - x_t \)
10: \hspace{3em} \( \Delta_t = \frac{1}{|S|} \sum_{i \in S} \Delta_t^i \)
11: \hspace{3em} \( x_{t+1} = \text{ServerOpt}(x_t - \Delta_{t,\mu_t}) \)

ServerOpt is one of Adagrad, Yogi, or Adam’s adaptive optimization techniques. FedOpt apply adaptive techniques on the server and clients; it is a cross-device algorithm with the equivalent communication expenses as FedAvg.

3. Algorithm FedAdam
Before proceeding to the description of the FedAdam algorithm, we should clarify that this algorithm is based on the FedOpt, which algorithm we described above.

1: Initialization: \( x_0, \theta_{-1} \geq \tau^2 \), decay parameters \( \beta_1, \beta_2 \in [0,1) \)
2: for \( t = 0, \ldots, T - 1 \) do
3: \hspace{1em} Sample a subset \( S \) of clients
4: \hspace{1em} \( x_{t,0}^i = x_t \)
5: \hspace{1em} for each client \( i \in S \) in parallel do
6: \hspace{2em} for \( k = 0, \ldots, K - 1 \) do
7: \hspace{3em} Compute an unbiased estimate \( g_{i,k}^t \) of \( \nabla F_i(x_{i,k}^t) \)
8: \hspace{3em} \( x_{i,k+1}^t = x_{i,K}^t - \mu \theta_t \Delta_t^i \)
9: \hspace{3em} \( \Delta_t^i = x_{i,K}^t - x_t \)
10: \hspace{3em} \( \Delta_t = \frac{1}{|S|} \sum_{i \in S} \Delta_t^i \)
11: \hspace{3em} \( m_t = \beta_1 m_{t-1} + (1 - \beta_1) \Delta_t \)
12: \hspace{3em} \( \theta_t = \beta_2 \theta_{t-1} + (1 - \beta_2) \Delta_t^2 \)
13: \hspace{3em} \( x_{t+1} = x_t + \mu \frac{m_t}{\sqrt{\theta_t + \tau}} \)

4. Algorithm FedYogi

1: Initialization: \( x_0, \theta_{-1} \geq \tau^2 \), decay parameters \( \beta_1, \beta_2 \in [0,1) \)
2: for \( t = 0, \ldots, T - 1 \) do
3: \hspace{1em} Sample a subset \( S \) of clients
4: \hspace{1em} \( x_{t,0}^i = x_t \)
5: \hspace{1em} for each client \( i \in S \) in parallel do
6: \hspace{2em} for \( k = 0, \ldots, K - 1 \) do
Our goal was to see the results of federated learning algorithms on the Flower and Kaggle platform to practically see the actions and results of federated learning algorithms in practice, to further determine the direction of our research work to create a new federated learning algorithm. For this purpose, we have chosen FedAdam, FedYogi, FedSparse algorithms to compare their results and see the pros and cons of these existing algorithms.

Description of our experiment. To train the models we used algorithms with the ready-made Cifar10 dataset, in the base of the Flower and Kaggle platforms.

After training, we obtain losses (distributed), losses (centralized) and values of accuracy. The values and the average of last 10 evaluations, you can see in the Table 1 and Figures 4-6.

<table>
<thead>
<tr>
<th>Method</th>
<th>Rounds</th>
<th>Clients</th>
<th>Cifar10</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>Losses (distributed)</td>
</tr>
<tr>
<td>FedAdam</td>
<td>100</td>
<td>10</td>
<td>3,57</td>
</tr>
<tr>
<td>FedYogi</td>
<td>100</td>
<td>10</td>
<td>3,77</td>
</tr>
<tr>
<td>FedSparse</td>
<td>100</td>
<td>10</td>
<td>3,78</td>
</tr>
</tbody>
</table>
Figure 4. The values of accuracy

Figure 5. The values of loss (centralized)
Figure 6. The values of loss (distributed)

We found out experientially, the accuracy of FedAdam - 63.06, FedYogi - 59.62, the accuracy of FedSparse – 64.04, we can conclude that the algorithm FedSparse gives more accurate values of accuracy. Also, regarding losses (distributed and centralized), FedSparse has better results than FedAdam and FedYogi.

It was a good experience to train models in Flower, because on this platform you can connect a desirable number of clients and choose number of rounds. It’s a very convenient framework to work with federated learning.

Conclusion

Federated machine learning has advantages over traditional machine learning methods, including data security, data diversity, continuous real-time learning, and hardware efficiency. However, there are key challenges such as communication efficiency, managing multiple systems in one network, handling statistical data heterogeneity, as well as issues related to privacy and confidentiality.

As a result of our research, federated machine learning algorithms, namely FedAdam, FedYogi, and FedSparse, were analyzed and tested. Conducted tests allowed us to identify the advantages and disadvantages of these algorithms using data from various datasets. In our research, the FedAdam algorithm demonstrated the best performance, and we decided to use it in further studies.

Literature review has shown that most researchers in the field of federated learning use the FedAvg algorithm. However, the FedAdam algorithm, based on the FedAvg algorithm, proved to be more effective in our research. Additionally, machine learning methods and neural networks, including fuzzy neural networks, were applied in the study to solve high-dimensional tasks [32].
Federated learning technology has broad practical applications. For instance, it is beneficial in smartphones, where it allows for accurate predictions without disclosing original data. In organizations, federated learning can reduce network load and provide private learning between devices. It also aids in developing models for the Internet of Things that adapt to system changes while safeguarding user privacy. Federated learning is also applied in healthcare, where restrictions prevent easy exchange of protected medical information. Furthermore, it is used for developing artificial intelligence models in compliance with regulatory requirements, utilizing vast amounts of data from multiple databases and devices.

References


