Evaluating the Potential of Federated Learning for Maize Leaf Disease Prediction

Thalita Mendonça Antico¹, Larissa F. Rodrigues Moreira², Rodrigo Moreira³

¹Institute of Exact and Technological Sciences (IEP)
Federal University of Viçosa (UFV), Rio Paranaíba, MG, Brazil

²Faculty of Computing (FACOM)
Federal University of Uberlândia (UFU), Uberlândia, MG, Brazil

{thalita.antico,rodrigo}@ufv.br, {larissarodrigues}@ufu.br

Abstract. The diagnosis of diseases in food crops based on machine learning seemed satisfactory and suitable for use on a large scale. The Convolutional Neural Networks (CNNs) perform accurately in the disease prediction considering the image capture of the crop leaf, being extensively enhanced in the literature. These machine learning techniques fall short in data privacy, as they require sharing the data in the training process with a central server, disregarding competitive or regulatory concerns. Thus, Federated Learning (FL) aims to support distributed training to address recognized gaps in centralized training. As far as we know, this paper inaugurates the use and evaluation of FL applied in maize leaf diseases. We evaluated the performance of five CNNs trained under the distributed paradigm and measured their training time compared to the classification performance. In addition, we consider the suitability of distributed training considering the volume of network traffic and the number of parameters of each CNN. Our results indicate that FL potentially enhances data privacy in heterogeneous domains.

1. Introduction

The rapid evolution of technologies in parallel with the increasingly sophisticated demands of users has generated unprecedented amounts of data. This large amount of data contains strategic information and knowledge whose extraction requires sophisticated computational methods. The extraction of dataset features can enable the construction of machine learning models to work in domains such as health, economics, and agriculture [Naeem et al. 2022].

Primarily, agriculture represents one of the main economic activities in the world, maize being the crop most produced in the world, leading Brazil to be the second largest exporter [Aragão and Contini 2021]. However, the maize crops are susceptible to certain leaf diseases, affecting production and reducing quality and productivity [Roese et al. 2020]. To overcome this limitation, Artificial Intelligence (AI) techniques allow building intelligent applications to support crop disease diagnosis [Ayoub Shaikh et al. 2022].

Machine learning paradigms, mainly supervised learning, require data to be centrally and locally available in the training phase. However, computing and storage resources are widely spread over multiple regions, and organizations require distributed training strategies to employ these resources [Li et al. 2020b].
However, heterogeneously distributed computing resources impose privacy and security challenges. Therefore, the Federated Learning (FL) paradigm emerges as a technique that exploits the potential of distributed resources by collaboratively training a machine pairing model [Liu et al. 2022]. The FL has already shown promise in recent applications in different fields such as medicine [Dayan and et al. 2021, Adnan et al. 2022], industrial engineering [Hu et al. 2018, Mowla et al. 2020], and mobile devices [Bochie et al. 2021].

This paper sheds light on the potential of FL as a suitable distributed machine learning approach for maize leaf diseases. As far as we know, this paper inaugurates the use and evaluation of FL applied in diagnosing diseases in maize leaves based on Convolutional Neural Networks (CNNs) and employing a centralized learning paradigm, where the data must be present in a central server to support the training phase. In the FL approach, the data could be spread over the training clients, which works distributed and asynchronously targeting to build a central model.

In a nutshell, our main contributions are: (1) a short state-of-the-art survey towards FL applied to agriculture challenge; (2) a numerical and practical evaluation of FL method for maize leaves disease; (3) a traffic volume evaluation of Convolutional Neural Network (CNN) distributed trained; (4) a performance and behavior evaluation CNNs distributed trained.

The remaining of the paper is organized as follows: Section 2 presents related work and highlights the contribution of our approach. Section 3 describes our proposed method. The performance evaluation is presented in the Section 4. In Section 5, we present and discuss the obtained results. Finally, Section 6 concludes the paper.

2. Related Work
Maize leaf disease identification based on the image is a research field with many approaches developed over the years [Sharma et al. 2021]. [DeChant et al. 2017] proposed the automatic identification of northern maize leaf blight using a pipeline of CNNs. [Lin et al. 2018] designed a multichannel CNN with cross-connection, pooling, and normalization schemes. They evaluated five types of images collected from maize planting in China.

[Zhang et al. 2018] enhanced the Cifar10 and GoogLeNet CNNs tuning parameters, modifying the pooling combinations, adding dropout operations, and rectified linear unit functions to speed the training step. [Alehegn 2019] proposed an approach based on color, texture, and morphological features to classify the Ethiopian maize diseases dataset using Support Vector Machine (SVM).

[Ahila Priyadharshini et al. 2019] proposed modifications in the LeNet architecture and applied a preprocessing step in the images using Principal Components Analysis (PCA) whitening. [Panigrahi et al. 2020] extracted color, shape, and textures features and evaluated several supervised classifiers to identify maize leaf disease, including Naive Bayes, Decision Tree, K-Nearest Neighbors (KNN), SVM, and Random Forest.

[Waheed et al. 2020] applied a hyperparameter tuning based on grid search to improve the classification performance of DenseNet. [da Rocha et al. 2020] proposed the hyperparameter optimization based on the Bayesian method and evaluated AlexNet,
ResNet50, and SqueezeNet CNNs trained with data augmentation and transfer learning. Similarly, [Subramanian et al. 2022a] and [Subramanian et al. 2022b] also applied Bayesian optimization and tested a dataset of images obtained from different sources.

[Haque et al. 2022] evaluated three CNN architecture inspired by InceptionV3 to identify maize leaf diseases in images collected in India. They used pre-trained models and applied data augmentation using rotation and brightness enhancement methods. [Amin et al. 2022] proposed a fusion of CNNs, considering EfficientB0 and DenseNet121 models to discover the complex feature of the infected maize leaf images.

[Moreira et al. 2022] proposed a low-cost and green-friendly architecture called AgroLens to support Smart Farm applications in environments with poor connectivity. They compared the classification performance of CNNs to handle maize leaf disease diagnosing supported by edge-compute devices.

In Table 1 we compared the recent contributions available in the literature in the scope of solutions to support maize leaf diagnosis based on images. The “Approach” column refers to the state-of-the-art proposals. The “Dataset” column indicates the dataset image considered. The “ML Algorithms” column indicates the algorithm utilized. The “Training Place” column characterizes if the solution was trained centralized or distributed. The “Evaluation Metric” indicates the classification performance considered. We observed in our short survey that all approaches considered accuracy evaluation metrics, and the accuracy obtained for each approach is indicated in the “Accuracy” column. Finally, the “Privacy Support” column characterizes the solution’s ability to support data privacy. Classification performance is the main strength of previous studies based on machine learning algorithms. However, these studies do not investigate distributed training. Thus, to overcome this gap, we propose an approach based on FL. Also, our method is more robust in addressing critical issues such as data privacy and security.

<table>
<thead>
<tr>
<th>Approach</th>
<th>Dataset</th>
<th>ML Algorithm</th>
<th>Training Place</th>
<th>Evaluation Metric</th>
<th>Accuracy (%)</th>
<th>Privacy Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>[DeChant et al. 2017]</td>
<td>Northern Leaf Blight 2016</td>
<td>CNN</td>
<td>Centralized</td>
<td>Accuracy, Precision, Recall, F1-Score</td>
<td>96.7</td>
<td>×</td>
</tr>
<tr>
<td>[Lin et al. 2018]</td>
<td>Own collected dataset</td>
<td>CNN Multichannel</td>
<td>Centralized</td>
<td>Accuracy</td>
<td>92.31</td>
<td>×</td>
</tr>
<tr>
<td>[Zhang et al. 2018]</td>
<td>PlantVillage and Google websites</td>
<td>CNN Cifar10 and GoogLeNet</td>
<td>Centralized</td>
<td>Accuracy</td>
<td>98.4</td>
<td>×</td>
</tr>
<tr>
<td>[Aghogho 2019]</td>
<td>Own collected dataset</td>
<td>SVM</td>
<td>Centralized</td>
<td>Accuracy</td>
<td>95.63</td>
<td>×</td>
</tr>
<tr>
<td>[Ahila Priyadharsini et al. 2019]</td>
<td>PlantVillage</td>
<td>CNN</td>
<td>Centralized</td>
<td>Accuracy</td>
<td>97.89</td>
<td>×</td>
</tr>
<tr>
<td>[Panigrahi et al. 2020]</td>
<td>PlantVillage</td>
<td>Naive Bayes, Decision Tree, KNN, SVM, Random Forest</td>
<td>Centralized</td>
<td>Accuracy</td>
<td>79.23</td>
<td>×</td>
</tr>
<tr>
<td>[Wahid et al. 2020]</td>
<td>Different sources</td>
<td>Dense CNN (DenseNet)</td>
<td>Centralized</td>
<td>Accuracy</td>
<td>98.06</td>
<td>×</td>
</tr>
<tr>
<td>[da Rocha et al. 2020]</td>
<td>PlantVillage</td>
<td>CNNs with Bayesian Optimization AlexNet, ResNet-50, SqueezeNet</td>
<td>Centralized</td>
<td>Accuracy, Precision, Recall, F1-Score</td>
<td>97</td>
<td>×</td>
</tr>
<tr>
<td>[Subramanian et al. 2022a]</td>
<td>PlantVillage, Kaggle, and Google websites</td>
<td>CNN VGG16</td>
<td>Centralized</td>
<td>Accuracy, Precision, Recall, F1-Score</td>
<td>99.21</td>
<td>×</td>
</tr>
<tr>
<td>[Subramanian et al. 2022b]</td>
<td>PlantVillage, Kaggle, and Google websites</td>
<td>CNNs VGG16, ResNet50, InceptionV3, Xception</td>
<td>Centralized</td>
<td>Accuracy, Precision, Recall, F1-Score</td>
<td>99</td>
<td>×</td>
</tr>
<tr>
<td>[Haque et al. 2021]</td>
<td>Own collected dataset</td>
<td>CNN InceptionV3</td>
<td>Centralized</td>
<td>Accuracy, Precision, Recall, F1-Score, Loss</td>
<td>95.99</td>
<td>×</td>
</tr>
<tr>
<td>[Amin et al. 2022]</td>
<td>PlantVillage</td>
<td>Fusion of CNNs EfficientNetB0, DenseNet</td>
<td>Centralized</td>
<td>Accuracy, Precision, Recall, F1-Score</td>
<td>98.56</td>
<td>×</td>
</tr>
<tr>
<td>[Moreira et al. 2022]</td>
<td>PlantVillage</td>
<td>Embedded CNNs AlexNet, DenseNet, SqueezeNet</td>
<td>Centralized</td>
<td>Accuracy, Precision, Recall, F1-Score</td>
<td>98.45</td>
<td>×</td>
</tr>
<tr>
<td>Our Approach (2022)</td>
<td>PlantVillage</td>
<td>CNNs with FL</td>
<td>Distributed</td>
<td>Accuracy, Precision, Recall, F1-Score</td>
<td>97.29</td>
<td>✓</td>
</tr>
</tbody>
</table>
3. Proposed Method

Traditional machine learning requires the dataset to be locally available to feed the model in the training process. Some datasets require access control and privacy, such as sensitive data from hospitals, governments, businesses, banks, and others [Mugunthan et al. 2020]. FL is a machine learning approach that does not require the data used in the supervised training process to be on the central server, leveraging data privacy as it can be processed locally [Truex et al. 2019, Zhang et al. 2021].

Figure 1 depicts the distribution of the training workload among clients that could join the hierarchy asynchronously. In this machine learning paradigm, the client locally trains the model with its data, protecting it in terms of privacy, and submits only the weights of the parameters of the used machine learning model to the central server. This learning paradigm supports heterogeneous client’s hardware capacity making FL a dynamic approach.

When receiving the weights from the trained machine learning model, the Server performs a mathematical merge operation on the weights of each model reported by the clients who trained locally on the dataset. Thus, the Server maintains a single machine learning model containing weights referring to local training, not requiring the Server to access specific data for each location, protecting the principles of privacy on sensitive data. There are several mathematical operations in the community to merge the weights that the central server can adopt, some known approaches are: FedAvg [McMahan et al. 2017], P-FedAvg [Zhong et al. 2021], FedProx [Li et al. 2020c], EdgeFed [Ye et al. 2020], SimFL [Li et al. 2020a] and others [Li et al. 2021].

This paper presents a performance evaluation of CNNs trained under the distributed paradigm. Thus, using FL we consider one (1) central server and \( K \) clients that connect to the server via the Institute of Electrical and Electronics Engineers (IEEE) 802.3 protocol [Brooks 2001]. Each customer receives a percentage proportional to the number of customers in the PlantVillage\(^1\) dataset, specifically from the maize culture, categorized into four classes included common rust (1192 images), gray leaf (513 images), northern leaf blight (985 images), and healthy leaves (1162 images) [Mohanty et al. 2016]. Thus, these clients using CNNs start the local training process, where each client trains CNN according to their learning rate, epochs, and others.

\(^1\)Available in: https://github.com/spMohanty/PlantVillage-Dataset
Figure 2 illustrates the method used in this paper, which consists of using FL as a distributed training paradigm. The maize leaf dataset feeds CNN, which runs locally on each client. When the client ends its training cycle, it uploads the weights to the central CNN model hosted by the central server.

![Proposed Method Diagram](image)

**Figure 2. Proposed Method.**

We onboarded the federated clients with five CNNs: AlexNet, SqueezeNet, ResNet-18, VGG-11, and ShuffleNet. These CNNs were chosen based on their success in previous classification tasks.

**AlexNet** [Krizhevsky et al. 2012] was the champion of the ImageNet Large Scale Visual Recognition Competition (ILSVRC) in 2012. It comprises five convolutional layers, three pooling layers, two fully connected layers, and a single Softmax output layer. Also, it uses dropout connections to reduce the overfitting and REctified Linear Unit (ReLU) activation function.

**SqueezeNet** [Iandola et al. 2016] is a lightweight CNN architecture with approximately 50 times fewer parameters than AlexNet. It comprises convolutional layers, pooling layers, and fire layers. The fire layers perform the functions of fully connected layers and dense layers, which are not present in SqueezeNet. In addition, SqueezeNet applies compression techniques to reduce the number of parameters.

**ResNet-18** [He et al. 2016] is a residual network designed to deal with vanishing gradient problems using identity connection. The identity connection provides a direct pathway for the gradient without a weight layer and does not change the value of the gradient. In addition, ResNet is composed of two dominant blocks: identity and convolutional. The identity block is the standard block used in ResNet and performs identity mapping. The convolutional block reduces the dimension of the activation. In our study, we considered a ResNet with 18 layers.

**VGG-11** [Simonyan and Zisserman 2014] is one of the CNNs belonging to the Visual Geometry Group (VGG) models designed to replace the larger filters with large sequences of convolutional filters of size $3 \times 3$. We considered VGG with 11 weight layers: eight convolutional layers and three fully connected layers.

Finally, **ShuffleNet** [Ma et al. 2018] is a lightweight CNN that applies grouped depthwise separable convolutions to generate feature maps. Also, this CNN included a shuffle operation that shuffles the channels within feature maps is introduced as the second stage of convolution.
We validated the performance of each CNN considering the set of tests divided according to the percentage of 80% images for training, 10% for validation, and 10% for testing. The process of merging the weights of the CNNs in this paper considered the FedAvg [McMahan et al. 2017]. The Algorithm 1 represents the steps of FedAvg divided into two different executions, the one executed by the Server and the one executed by the Client. In the Server execution, the model is initialized (line 2), and the highest value between the $C$ product is taken for each execution round, $K$, where $C$ is the participation ratio of the clients at each round and $K$ refers to the number of all clients (line 4).

Algorithm 1 Federated Averaging. $K$ clients are indexed by $k$; B is the size of the local minibach, $E$ is the local number of epochs, and $n$ is the learning rate

1: Server Runs  
2: Initializes the Model $W_0$  
3: for each round $t = 1, 2, ...$, do  
4: \hspace{1em} $m \leftarrow \max(C.K, 1)$  
5: \hspace{1em} $S_t \leftarrow$ (random set of $m$ clients)  
6: \hspace{1em} for each $K \in S_t$ in parallel do  
7: \hspace{2em} $w_{t+1}^k \leftarrow \text{UpdateClient}(k, w_t)$  
8: \hspace{1em} end for  
9: end for  
10: \hspace{1em} $\beta \leftarrow$ (divide $P_k$ in batches of size B)  
11: for each local epoch $i$ from 1 to $E$ do  
12: \hspace{1em} $w \leftarrow w - n\nabla l(w; b)$  
13: end for  
14: return $w$ to server

Thus, it chooses a random set of customers $S_t$ for training (line 5). The innermost loop (line 6) refers to the parallel execution of local, asynchronous, and distributed training that Clients trigger. As Clients train their models locally, they send their $w$ weights to the Server via UpdateClient (line 7), making the Server update the weights of the general model (line 8) by the arithmetic mean mathematical operation. From the Client’s perspective, the execution of ClientUpdate consists of dividing the dataset into mini-batches of size B (line 12) and interactively, the minibatch $\beta$ feeds the local model in the training process of each Client (line 13). When the training finishes, its weight $w$ will be sent to Server to improve the global model (line 16).

We used the dataset division in the Independent and Identically Distributed (IID) model in our federated learning approach to classifying diseases in maize leaves. In this division, each client runs the training on a dataset part distributed evenly across all of them.

4. Performance Evaluation

We built an experimental scenario to validate the suitability of FL training for different CNNs. The experimental scenario consists of a machine with a 3.00 GHz Intel Processor i5 processor, 32 GB of RAM, an NVIDIA GeForce GTX 1080 Ti GPU, and Ubuntu 16.04.7 LTS operating system. We used the PyTorch framework (version 1.6) for the deep learning modules and CUDA version 8.0 and cuDNN 6.0. The FL framework used in the performance evaluation was FedLab [Zeng et al. 2021].
On this machine, we run $k$ instances of Clients and 1 Server connected by changing the weights of CNN at each training stage via socket. The parameters of the experimental scenario are according to Table 2.

Table 2. Experimental Setup Parameters.

<table>
<thead>
<tr>
<th>World Size</th>
<th>Rank</th>
<th>Epoch</th>
<th>Learning Rate</th>
<th>Batch Size</th>
<th>Momentum</th>
<th>Classes</th>
<th>Workers</th>
<th>IP</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client</td>
<td>$k$</td>
<td>50</td>
<td>0.001</td>
<td>32</td>
<td>0.9</td>
<td>4</td>
<td>4</td>
<td>127.0.0.1</td>
<td>Any</td>
</tr>
<tr>
<td>Server</td>
<td>[3, 5]</td>
<td>1</td>
<td>50</td>
<td>-</td>
<td>-</td>
<td>4</td>
<td>4</td>
<td>127.0.0.1</td>
<td>3002</td>
</tr>
</tbody>
</table>

At the end of each run, according to the parameters in Table 2, FedLab generates performance metrics for each CNN. Accuracy, Precision, Recall, and F1-Score are used to assess the classification performance. These metrics considered the indices based on the number of true positives (TP), true negatives (TN), false positives (FP), and false-negative (FN) [Tan et al. 2018].

- **Accuracy**: is the hits of the classifier as whole (Eq. 1).
  
  \[
  \text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN}
  \] (1)

- **Precision**: is the hit rate per class for positive cases (Eq. 2).
  
  \[
  \text{Precision} = \frac{TP}{TP + FP}
  \] (2)

- **Recall**: is the rate of a relevant sample being classified correctly (Eq. 3).
  
  \[
  \text{Recall} = \frac{TP}{TP + FN}
  \] (3)

- **F1-Score**: is the harmonic mean of Recall and Precision (Eq. 4).
  
  \[
  F1-Score = 2 \times \frac{Recall \times Precision}{Recall + Precision}
  \] (4)

5. Results and Discussion

We carried out experiments validating the performance of each CNN trained with the FL paradigm. For each CNN, we run ten (10) executions with a random seed to assess the maximum performance that CNN can achieve. Thus, according to Table 3, we found that the CNNs with the highest accuracy were VGG-11 following AlexNet, with 97.29% and 96.87%, respectively. In addition, our results demonstrate that AlexNet was CNN that required the least time for training. Although the VGG-11 reached a high accuracy, this model demanded the most significant time in the training process, being unsuitable in FL scenarios where the training time is essential.

We measured the standard deviation of the ten (10) experiments for each CNN, recording it in Table 3 after the ± symbol. These experiments were run without seed locking to measure the variability of the results. We consider in our experiments the training time of CNNs considering the parameters of Table 2.

Our achieved accuracy is comparable to that found in the state of the art using the same parameters and dataset. Furthermore, our experiments suggest that ShuffleNet had the lowest accuracy when trained under the FL paradigm, about 75.65%.
Table 3. CNN Performance Comparison.

<table>
<thead>
<tr>
<th>CNN</th>
<th>Accuracy (%)</th>
<th>Precision (%)</th>
<th>Recall (%)</th>
<th>F1-Score (%)</th>
<th>Loss</th>
<th>Training Time (min)</th>
</tr>
</thead>
<tbody>
<tr>
<td>AlexNet</td>
<td>96.87 ± 0.34</td>
<td>94.75 ± 0.06</td>
<td>95.25 ± 0.05</td>
<td>94.75 ± 0.15</td>
<td>0.96</td>
<td>16.23</td>
</tr>
<tr>
<td>SqueezeNet</td>
<td>96.54 ± 0.83</td>
<td>92.5 ± 0.67</td>
<td>94.25 ± 0.72</td>
<td>95.25 ± 1.01</td>
<td>1.22</td>
<td>25.55</td>
</tr>
<tr>
<td>ResNet-18</td>
<td>94.86 ± 2.17</td>
<td>94.63 ± 0.18</td>
<td>94.80 ± 0.42</td>
<td>94.71 ± 0.29</td>
<td>2.84</td>
<td>27.95</td>
</tr>
<tr>
<td>VGG-11</td>
<td>97.29 ± 0.18</td>
<td>95.94 ± 0.21</td>
<td>96.59 ± 0.34</td>
<td>96.24 ± 0.27</td>
<td>6.45</td>
<td>78.78</td>
</tr>
<tr>
<td>ShuffleNet</td>
<td>75.65 ± 2.00</td>
<td>57.84 ± 0.61</td>
<td>64.27 ± 1.97</td>
<td>59.59 ± 1.96</td>
<td>16.25</td>
<td>19.99</td>
</tr>
</tbody>
</table>

To analyze the relationship between the accuracy achieved and the training time, we applied the statistical relationship test between the variables Training Time and Accuracy. Thus, through the Pearson correlation, we found that $r = -0.2$ leads us to infer that the relationship between training time and accuracy has a weak negative relationship. For our experiments, a weakly negative correlation means that the accuracy was high when training time was low, except for VGG-11. Also, the training time relates to the hyperparameters of each CNN, such as learning rate, batch size, and others. Our measurements bring the rate of training time.

In order to understand the accuracy of the models, we built confusion matrices to verify which classes of the dataset posed the most challenges in the training and generalization process of the model. We verified that for all CNNs the northern leaf blight class was correctly classified. On the other hand, the gray leaf and healthy classes proved to be more challenging. In Figure 3 we consolidate the confusion matrices generated from the CNNs.

Figure 3. Confusion matrices for each tested CNN.

Also, we evaluate the traffic volume used in the training process by the FL technique. This traffic volume relies on all data transferred between the federated clients in the training process. We summarize these results in Table 4, and it is worth noting that SqueezeNet, despite its classification performance, required less network traffic volume in the training process due to the number of CNN trainable parameters.

The results indicates that the traffic volume is related to the CNN structure. CNNs
with several layers and complex structures need to have the weights recorded in tensor data structures, generating large model sizes and, ultimately, high communication demands. In FL framework, we must define the round of training, which refers to the number of times of server requires from federated clients the training process.

<table>
<thead>
<tr>
<th>CNN</th>
<th>Traffic Volume (MB)</th>
<th>Number of Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>AlexNet</td>
<td>84.24</td>
<td>57,020,228</td>
</tr>
<tr>
<td>SqueezeNet</td>
<td>17.70</td>
<td>737,476</td>
</tr>
<tr>
<td>ResNet-18</td>
<td>34.14</td>
<td>11,178,564</td>
</tr>
<tr>
<td>VGG-11</td>
<td>90.92</td>
<td>128,788,228</td>
</tr>
<tr>
<td>ShuffleNet</td>
<td>30.18</td>
<td>1,257,704</td>
</tr>
</tbody>
</table>

The built federated learning rationale enhances data privacy trained where it is generated. In our carried experiments, we consider that training the maize leaf dataset in different and distributed clients makes it possible to assume that each one will only share the model weights and not the data each one has.

6. Concluding Remarks

Machine learning techniques have proved suitable for several tasks, such as disease prediction based on image of agricultural crops. In this paper, we evaluate the potential of FL to mitigate the data privacy gap that centralized machine learning techniques have. Thus, we evaluated the applicability of the FL method through five CNNs using maize leaf disease classification. For this, we built a short state-of-the-art survey. We found that the application of CNNs to predict diseases in maize leaves predominantly did not consider the distributed paradigm and, consequently, did not support privacy.

Our numerical results suggest that AlexNet, due to its structure, lower training time, and high accuracy, is suitable to operate in the FL model. Furthermore, it was worth noticing a weak negative correlation between accuracy and training time, leading us to conclude that for most of the models considered, in the distributed training approach, the training time is inversely proportional to the accuracy of the models. Also, through numerical results, we measured and concluded that the number of CNN parameters in the distributed learning paradigm strongly correlates with the volume of data exchanged in the training process.

Also, our numerical and practical evaluation indicated that FL could potentially enhance data privacy in heterogeneous domains. For future work, urges to evaluate alternatives weight aggregation techniques of CNNs in addition to verifying the impact of network failures on the model convergence time.

Acknowledgment

The authors acknowledge the financial support of the Federal University of Viçosa. Also, this study was financed in part by the Coordenação de Aperfeicoamento de Pessoal de Nível Superior – Brasil (CAPES) – Finance Code 001.

References


Iandola, F. N., Han, S., Moskewicz, M. W., Ashraf, K., Dally, W. J., and Keutzer, K. (2016). SqueezeNet: AlexNet-level accuracy with 50x fewer parameters and ¡0.5MB model size.


