
BACKDOOR DEFENSE IN FEDERATED LEARNING USING DIFFERENTIAL TESTING AND OUTLIER DETECTION

Yein Kim

University of California, San Diego
La Jolla, CA
y5kim@ucsd.edu

Huili Chen

University of California, San Diego
La Jolla, CA
huc044@ucsd.edu

Farinaz Koushanfar

University of California, San Diego
La Jolla, CA
farinaz@ucsd.edu

ABSTRACT

The goal of federated learning (FL) is to train one global model by aggregating model parameters updated independently on edge devices without accessing users' private data. However, FL is susceptible to *backdoor attacks* where a small fraction of malicious agents inject a targeted misclassification behavior in the global model by uploading polluted model updates to the server. In this work, we propose DiffFense, an automated defense framework to protect an FL system from backdoor attacks by leveraging *differential testing* and two-step MAD outlier detection, without requiring any previous knowledge of attack scenarios or direct access to local model parameters. We empirically show that our detection method prevents a various number of potential attackers while consistently achieving the convergence of the global model comparable to that trained under federated averaging (FedAvg). We further corroborate the effectiveness and generalizability of our method against prior defense techniques, such as Multi-Krum and coordinate-wise median aggregation. Our detection method reduces the average backdoor accuracy of the global model to below 4% and achieves a false negative rate of zero.

Keywords Federated learning · Backdoor attacks · Differential testing

1 Introduction

The widespread usage of computing devices, such as mobile phones and tablets, has increased the amount of proprietary user data. The wealth of data raises concerns about user privacy as well as providing opportunities to develop various machine learning (ML) models. To address this issue, a decentralized learning paradigm called *federated learning* (FL) has been proposed Yang et al. (2019). An FL system involves two parties: the cloud server, and multiple clients/agents. At each communication round, the server updates the global model based on the model updates from chosen local agents McMahan et al. (2017).

The FL paradigm avails the cloud server to learn an ML model without accessing users' private data. However, the lack of visibility to local training data and process exposes FL to *backdoor attacks* Bhagoji et al. (2019); Bagdasaryan et al. (2020). Malicious agents may inject a backdoor functionality into the global model, taking advantage of the lack of transparency. Existing FL backdoor attacks can be categorized into two types based on the backdoor injection mechanism: (*i*) *Data poisoning* attack crafts and injects poisoned inputs into the training set Bagdasaryan et al. (2020); Tolpegin et al. (2020). The backdoor is activated by the pre-defined pixel pattern or semantic triggers in the inputs. (*ii*) *Model poisoning* attack designs a regularized adversarial objective function to manipulate the model updates Bhagoji et al. (2019).

A variety of defense techniques have been proposed to mitigate backdoor attacks and hence, to enhance the security of federated learning systems. One line of research aims to distinguish and exclude malicious model updates from the server aggregation. Reject On Negative Impact (RONI) Barreno et al. (2010) empirically evaluates each local update and eliminates those with substantially negative impact on the global model's accuracy. AUROR Shen et al. (2016) clusters the local model updates into two groups based on the identified informative features and only uses the majority cluster to update the global model. Another line of research focuses on designing a robust aggregation rule for FL

systems. Krum Blanchard et al. (2017) has a Byzantine-resilient aggregation rule that only selects the local model update with the smallest pairwise distance from the closest local updates. FoolsGold Fung et al. (2018) assigns different learning rates to the selected agents based on the pairwise cosine similarity between the local model updates to mitigate the influence of backdoor adversaries.

Despite providing enhanced security against FL backdoor attacks, prior defense methods have the following two constraints: *(i) Limited generalizability and applicability.* They are not generalizable to different attack scenarios. Their threat models make assumptions about the ratio of adversaries or data distribution of local clients. FoolsGold Fung et al. (2018), for example, assumes that there are several colluding adversaries. Krum Blanchard et al. (2017) requires the knowledge of the number of adversaries. Krum is also designed for an FL setting where the training data are independent identically distributed (i.i.d.) across the local agents. Federated learning, however, is likely to have unbalanced and non-i.i.d data distribution McMahan et al. (2017). *(ii) High false alarm rates.* An ideal backdoor mitigation method preserves the final accuracy of the global model while reducing the success rate of backdoor attacks. Prior works such as RONI Barreno et al. (2010) and FoolsGold Fung et al. (2018) yield relatively high false alarm rates. Useful model updates from the benign clients may be discarded by the server, resulting in the degradation of the global model’s accuracy.

To address the above limitations, we propose DiffFense, the first automated FL defense framework that leverages *differential testing* and outlier detection as a filtering mechanism before FL aggregation is performed. To solve the generalization challenge, our threat model makes a minimal assumption on the attack scenario that benign clients are the majority among all local agents. We adapt the idea of differential testing to generate *differential inputs* that magnify the behavioral differences among models and compute “test statistics” based on local model predictions on those inputs. As such, our defense mechanism is applicable to the scenarios where local model parameters or weight updates cannot be accessed (e.g., when weights are encrypted Bonawitz et al. (2017)). We also modify *MAD-based outlier detection* and develop a variant, two-step MAD outlier detection. With the two-step outlier detection, DiffFense provisions a low false positive rate during backdoor detection, thus preserving the main task accuracy of the global model.

2 Problem Statement

2.1 Federate Learning

A federated learning system consists of a cloud server and N local agents. The i -th agent has training data D_i kept private from the server and other agents. The cloud server aims to train a global model G using information from the agents. To achieve this goal, the local agents perform model training on their own data and communicate the trained model with the server to share the knowledge of their private training set in a privacy-preserving manner.

To reduce the communication overhead, *communication-efficient* FL designs are proposed Konečný et al. (2016); Sattler et al. (2019) where local agents upload their weight updates (i.e., *increment*) instead of the model parameters. More specifically, at each round t , the server randomly selects a subset of local agents S_t . The number of models selected at each round is $K = |S_t| = \beta * N$ where β is the percentage of participating clients and N is the number of total clients. Each selected local agent $i \in S_t$ receives the current global model G^t and trains it with his local data using stochastic gradient descent (SGD), obtaining a locally updated model L_i^{t+1} . The agent sends its model update $\delta_i^{t+1} = L_i^{t+1} - G^t$ back to the server. The server then aggregates the model updates from the agents and adjust the global model with the learning rate η based on FedAvg:

$$G^{t+1} = G^t + \frac{\eta}{N} \sum_{i \in S_t} (L_i^{t+1} - G^t). \quad (1)$$

This ‘local training then global aggregation’ process repeats until the global model on the cloud server side converges.

2.2 Threat Model

DiffFense adheres to a realistic threat model described below. On the cloud server’s side, we make the following assumptions:

- The server has no access to each local agent’s training data or training process.
- The server has no direct access to local model parameters or updates (e.g., they are encrypted). However, they can feed inputs into local models and collect the corresponding outputs.

On the benign/malicious agents’ side, we assume that:

- The attacker has full control over his local training data and the training pipeline.

- The adversary can modify the weights of the local model before submitting it to the server.
- The adversary can change the local training method and configurations adaptively throughout the training process of the global model.

Furthermore, we assume that a majority of agents in the FL system are benign. The backdoor adversary has two goals: *(i) Stealthiness*. The malicious attackers need to ensure that their model parameters do not deviate too much from the benign models while achieving a high accuracy on clean data (to pass accuracy check). This is similar to evade the functional testing in traditional hardware Trojan detection Chakraborty et al. (2009); Saha et al. (2015). *(ii) Attack success*. To implement a successful attack, the adversary shall ensure that any input with the pre-defined trigger has a very high probability of being predicted as the target class.

Adversarial goal. Our work focuses on the standard backdoor attack setting in FL Bagdasaryan et al. (2020) and discuss how the attacker designs his objective function $\mathcal{L}_{\text{attacker}}$. First of all, to pass the accuracy check on clean validation data and remain unnoticeable, the adversary incorporates the empirical loss on the clean training data $\mathcal{L}_{\text{train}}$ in the objective function. Furthermore, the attacker penalizes his model for deviating from the ‘benign’ updates. This deviation is typically measured by a distance metric, such as L_p norm distance or cosine dissimilarity between the weight updates of two agents, resulting in the anomaly evasion loss \mathcal{L}_{ano} . Since the attacker cannot access other agents’ updates, \mathcal{L}_{ano} is substituted with the deviation of the adversary’s updated model parameters from the prior global model parameters. Finally, to inject the targeted backdoor behavior into the global model, the adversary designs an adversarial loss term $\mathcal{L}_{\text{target}}$ that performs the backdoor sub-task, i.e., misclassifying inputs with the trigger as the attack target class. To simplify, we merge the two classification loss terms on clean and backdoor data as $\mathcal{L}_{\text{class}} = \mathcal{L}_{\text{train}} + \mathcal{L}_{\text{target}}$. The total loss of the attacker is therefore formulated as:

$$\mathcal{L}_{\text{attacker}} = \alpha \mathcal{L}_{\text{class}} + (1 - \alpha) \mathcal{L}_{\text{ano}} \quad (2)$$

The hyper-parameters α control the trade-off between the attack stealthiness (\mathcal{L}_{ano}) and attack effectiveness ($\mathcal{L}_{\text{target}}$ term inside $\mathcal{L}_{\text{class}}$).

3 Methodology

3.1 Key Insight

First, we need to understand how a backdoor functionality can be implemented in a deep neural network (DNN). DNNs typically have a tremendous amount of parameters. The huge parameter space promotes the black box nature of a DNN Das & Rad (2020) while increasing its susceptibility to backdoor attacks. It is typically hard to distinguish a compromised DNN from benign ones solely based on its performance on test images - its generalization performance on original images is comparable to benign DNNs although it adopts an additional capability to classify certain images as the target label Bagdasaryan et al. (2020). This challenge arises a question - how can we differentiate models with benign and adversarial objectives without directly accessing and leveraging their parameters?

This is where *differential testing* comes into play. The goal of *differential testing* in deep learning is to generate *differential inputs* - corner-case inputs that induce divergent behaviors among models with supposedly similar functionalities McKeeman (1998); Pei et al. (2017). The cause underlying the networks’ prediction differences is the difference between their decision logic and boundaries. This discrepancy attributes to various factors such as training data distribution and configurations. We speculate that difference arising from data/model poisoning is more fundamental and profound than that from training data distribution and that suspected adversaries can be identified with these differential inputs. We also note that we only need to collect local model predictions on images without directly accessing model parameters. In our work, we group model predictions into two groups and try to enlarge the difference between the two instead of maximizing differences among all the models. This clustering simplifies our optimization setup.

Then the second question ensues: how can we identify potential adversaries out of the differential inputs? We formulate this problem as outlier detection and leverage hypothesis testing. Taking a conservative stance, our null hypothesis is the presence of adversaries - local agents in the minority cluster are adversarial. Roughly speaking, “test statistic” in the testing is the distance between the two prediction clusters. We note that “distantness” is a relative concept and take into account both the distance between the cluster centers and tightness of the majority cluster to decide how divergent the two clusters’ behaviors are.

3.2 Assumptions

In our method, we do not require direct access to local model parameters. However, we assume that we can feed inputs into each participating model and collect the corresponding predictions.

Furthermore, our method assumes that the server has a handful of validation images with a minimal requirement on the number and distribution. This requirement will be discussed in 4.3. The same set of validation images will be used to generate differential inputs at each global epoch.

3.3 Global Workflow

Our system consists of the following steps as in Figure 1:

1. Local training: Local agents are selected to download and train the current global model independently;
2. Selected agents submit their model updates to server;
3. Defense mechanism:
 - (a) Differential input generation: inputs validation images and outputs differential images and scores (to be defined in 3.5).
 - (b) Two-step MAD outlier detection: inputs scores and outputs a list of outliers
4. Server aggregation: exclude the outliers and update the global model by the average of inliers' updates

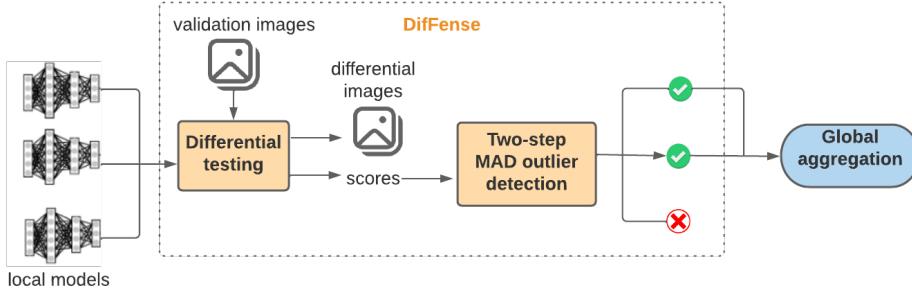


Figure 1: Global flow of DiffFense for detecting backdoor attacks in the federated learning system.

3.4 Differential Testing

Given validation images, we process differential inputs in batches and compute the score per class for efficiency. As the result, at the end of this stage, we have a batch of differential images and scores for local agents per image class.

Differential input generation. Given K agents and C image classes, we denote \mathbf{X} as a batch of images labeled as $c \in [C]$. We modify \mathbf{X} iteratively where each iteration consists for the following steps.

1. Each local model $i \in [K]$ outputs a prediction on each image $\mathbf{x} \in \mathbf{X}$ as $p^i(\mathbf{x}) \in \mathbb{R}^C$. In general, the prediction is a softmax function.
2. Take the average of the model's predictions over the batch to get a vector $\mathbf{p}^i \in \mathbb{R}^C$.
3. Optionally reduce the dimension of \mathbf{p}^i by PCA projection to get $\mathbf{q}^i \in \mathbb{R}^d$ where $d < C$. d can be determined by computing and thresholding the explained variance ratio. The purpose of this step is to reduce the dimensionality and hence, make the clustering easier in the next step.
4. Group the PCA projected model predictions into two clusters, G_1 and G_2 by running k-means clustering with 2 components. Without loss of generality, G_1 is the “majority cluster” where $|G_1| \geq |G_2|$.
5. Given the center vectors of the two clusters, μ_1 and μ_2 , run gradient ascent on the batch \mathbf{X} by taking the gradient of the objective function $\|\mu_1 - \mu_2\|_2$ with step size s .

Note that there are two hyperparameters, the step size in gradient ascent and the number of iterations. They can be tuned according to the dataset and the model architecture.

Score generation. We generate scores or “test statistics” used for hypothesis testing in the next stage. To help determining the confidence level of whether a local agent is adversary, we interpret score as the deviation from the majority cluster center. Instead of calculating a distinct score for each local model, we output two scores - one for the “majority” and the “minority” cluster respectively - per image class. This will make the process more scalable to the number of participant models. The goal is to understand the distance between the two clusters given these scores.

Models in the majority cluster will be assigned twice the norm of the majority cluster's standard deviation. Assuming normal distribution, 95% of points are within two standard deviations from the mean. It follows from this assumption that two standard deviation is a decent approximation of how far away a local model prediction is from the center for the majority cluster. On the other hand, models in the minority cluster will be assigned the norm of the distance between the two cluster centers. Therefore, the smaller the standard deviation norm of the majority cluster (the more concentrated the majority cluster is) and the greater the distance between the cluster centers are, the greater the difference between the two scores will be and the more likely the minority cluster will be detected as outliers in the ensuing hypothesis testing.

Complexity. We note that the computational complexity of this stage primarily depends on the number of distinct classes of validation images along with the number of images and the number of iterations.

Algorithm 1: Differential input and score generation

```

Input : seeds  $\leftarrow$  original test images
        dnns  $\leftarrow$  local DNNs
        classes  $\leftarrow$  image classes
        s  $\leftarrow$  step size in gradient ascent
        t  $\leftarrow$  number of iterations
        d  $\leftarrow$  number of PCA components
Output : gens  $\leftarrow$  generated differential images
          scores  $\leftarrow$  scores of local DNNs

gens := empty set
scores := empty dictionary
for  $c \in \text{classes}$  do
    // X is a batch of images belonging to class c
    X = seeds  $\in c$ 
    for  $i \leftarrow 1$  to t do
        pred := empty set
        for dnn  $\in \text{dnns}$  do
            // average of predictions on images of class c
            pred.add((dnn.predict(x) for x in X).mean)
        end
        predPca = PCA (preds, d)
        //  $G_1$  is the majority cluster ( $|G_1| \geq |G_2|$ )
         $G_1, G_2 = \text{KMeansCluster} (\text{predsPca}, 2)$ 
        obj =  $\|G_1.\text{mean} - G_2.\text{mean}\|$ 
        grad =  $\partial \text{obj} / \partial X$ 
        X = X + s  $\cdot$  grad
    end
    gens.add(X)
    for dnn  $\in G_1$  do
        // score of the majority cluster is twice its standard deviation norm
        scores[dnn].add( $2 * \|G_1.\text{std}\|$ )
    end
    for dnn  $\in G_2$  do
        // score of the minority cluster is clusters' mean difference norm
        scores[dnn].add( $\|G_1.\text{mean} - G_2.\text{mean}\|$ )
    end
end
return gens, scores

```

3.5 Two-step MAD Outlier Detection

Given a matrix of the scores concatenated across classes from 3.4, $\mathbf{P} \in \mathbb{R}^{C \times K}$, we run a statistical test to identify outliers, suspected adversaries.

First, we take the row-wise average of \mathbf{P} to get the mean score vector $\mathbf{p} \in \mathbb{R}^K$. This makes our score data one-dimensional. Median Absolute Deviation (MAD) outlier detection method Leys et al. (2013) makes a good candidate as a detection method whose measure of distance is robust to outliers in one-dimensional data.

As most models belong to the majority cluster and few in the minority have higher score values, we expect our data to be asymmetric with a long tail on the right side. This asymmetric distribution inspires us to use double MAD Rosenmai (2013) where two different MADs are used as separate denominators for points below and above the median.

We observe a few caveats in our problem. Especially when validation images are of only few classes, we expect more than 50% of data to have identical values, incurring “zero MAD case”. Furthermore, assuming that only a small fraction of adversaries participate in the server aggregation, there is a higher chance for models to be adversaries if there are fewer of them. For instance, models in the minority cluster are more likely to be adversaries if they take 10% of the total participants than 40% even with the same score. To sum up, we want a double MAD outlier detection method with the following properties:

- Tolerant of points whose deviations are smaller than the MAD;
- For points with deviations greater than the MAD, takes into account their ratio and absolute deviation value from the median;
- Robust to the zero MAD case.

To satisfy these properties, we propose a two-step MAD-based outlier detection using modified double MAD. In this method, we introduce the second MAD mad_2 besides the original MAD denoted mad_1 . Let $m_p = med(\mathbf{p})$, we compute the absolute deviation from the median vector as \mathbf{q} where $\mathbf{q}(i) = |\mathbf{p}(i) - m_p|$ for $i \in [K]$. Then the original MAD $mad_1 = med(\mathbf{q})$ is obtained. We compute the second MAD mad_2 as the weighted average of mad_1 and the median of absolute deviations greater than mad_1 :

$$mad_2 = \frac{|\{i|q_i \leq mad_1\}|}{K} mad_1 + \frac{|\{i|q_i > mad_1\}|}{K} med(\{q_i|q_i > mad_1\}).$$

where mad_1 is the denominator for points deviated less than mad_1 . Utilizing the conventional outlier cutoff value of 2 or 3, these points will all be determined as inliers. For points deviated more than mad_1 , we use mad_2 as the denominator. Hence $\mathbf{r} \in \mathbb{R}^K$ is defined for $i \in [K]$ as

$$\mathbf{r}(i) = \begin{cases} \frac{\mathbf{q}(i)}{mad_1} & \text{if } \mathbf{q}(i) \leq mad_1 \\ \frac{\mathbf{q}(i)}{mad_2} & \text{if } \mathbf{q}(i) > mad_1 \end{cases}$$

Finally, given a pre-defined cutoff threshold m (conventionally 2 or 3), we identify the set of outliers as $\{i|\mathbf{r}(i) > m\}$.

4 Experiments

FL aggregation rules. We evaluate the performance of DiffFense detection-based defense scheme and compare it against FL systems equipped with three different update rules. We assume that at global epoch t , K agents out of N total agents are selected for aggregation. We describe the FL aggregation rule of each method below.

■ **Federated averaging (FedAvg).** This is the conventional global model update rule without any defense, thus is used as the baseline in our experiments. The server updates the weights of the global model as:

$$G^{t+1} = G^t + \frac{\eta}{N} \sum_{i=1}^K (L_i^{t+1} - G^t), \quad (3)$$

where η is the global learning rate and L_i^{t+1} is the model parameter of the i -th participating local agent at the $(t+1)$ -th epoch. Throughout the experiments, the global learning rate is set to $\eta = \frac{1}{\beta}$ so that we take the average of only the participating models’ weight updates.

■ **Multi-Krum (Krum).** Assuming that there are b adversaries in the FL system, Krum requires the number of participants to satisfy $K \geq 2b + 3$ Blanchard et al. (2017). For the i -th local update $\delta_i^{t+1} = L_i^{t+1} - G^t$, Krum select a set of its $(K - b - 2)$ closest local updates N_i and add up the pairwise distances to obtain a score: $S(\delta_i^{t+1}) = \sum_{\delta \in N_i} \|\delta_i^{t+1} - \delta\|_p$. Krum chooses l local updates with the smallest distance scores $S(\delta_i^{t+1})$ as S_{t+1} (such that $|S_{t+1}| = l$ where $1 \leq l \leq K$) at each iteration and takes their average $\delta_{kru}^{t+1} = \text{avg}_{i \in S_{t+1}} \delta_i^{t+1}$ and uses it to update the global model:

$$G^{t+1} = G^t + \delta_{kru}^{t+1}. \quad (4)$$

Algorithm 2: Two-step MAD outlier detection

Input : $dnn \leftarrow$ local DNNs
 scores \leftarrow outlier scores of local DNNs
 $m \leftarrow$ threshold

Output : outliers \leftarrow local DNNs identified as outliers

```

meanScores := empty dictionary
diffs := empty dictionary
madDiffs := empty dictionary
outliers := empty set
for  $dnn \in dnn$  do
| meanScores[ $dnn$ ] = scores[ $dnn$ ].mean
end
med = meanScores.values.median
for  $dnn \in dnn$  do
| diff[ $dnn$ ] = |meanScores[ $dnn$ ] - med|
end
diffVals = diff.values
mad1 = diffVals.median
// ratio of models with difference greater than the median
mad2ratio = (diffVals > mad1).count/dnns.count
// mad2 is the weighted average of mad1 and the median of those greater than mad1
mad2 = mad2ratio * diffVals[diffVals > mad1].median + (1 - mad2ratio) * mad1
for  $dnn \in dnn$  do
| if diff[ $dnn$ ]  $\leq$  mad1 then
| | if mad1 = 0 then
| | | madDiffs[ $dnn$ ] = 0
| | end
| | else
| | | madDiffs[ $dnn$ ] = diff[ $dnn$ ]/mad1
| | end
| end
| else
| | madDiffs[ $dnn$ ] = diff[ $dnn$ ]/mad2
| end
| end
| end
| for  $dnn \in dnn$  do
| | if madDiffs[ $dnn$ ]  $>$  m then
| | | outliers.add( $dnn$ )
| | end
| end
| end
return outliers

```

In our experiment, we assume that Multi-Krum knows the number of adversaries, b in advance and chooses $l = K - b$ local updates for server aggregation.

■ **Coordinate-wise median (Coomed).** The paper Yin et al. (2018) shows that taking the coordinate-wise median can achieve the order-optimal statistical error rate in the case of a strongly convex loss function. The server updates the shared model's weights as:

$$G^{t+1} = G^t + \bar{\delta}^{t+1}, \quad (5)$$

where $\bar{\delta}^{t+1} := coomed(\delta_i^{t+1}|_{i=1,\dots,K})$ with the j^{th} coordinate $\bar{\delta}^{t+1}(j) = median(\delta_i^{t+1}(j)|_{i=1,\dots,K})$

Evaluation metrics. We use two evaluation metrics, global accuracy and backdoor accuracy throughout our experiments. Global accuracy is the accuracy of the shared model on the main task (i.e., the proportion of data examples that are correctly classified). Backdoor accuracy is the shared model's accuracy on the backdoor task, which is essentially the attack success rate. We measure the final global accuracy after convergence and the average backdoor accuracy during the global training process.

To assess DiffFense’s backdoor detection performance, we measure the false positive rates and false negative rates and report the average values over the entire training process.

When evaluating four aggregation methods, FedAvg, Krum, Coomed, and DiffFense, we identify the epoch that the global model starts converging and compare the maximum backdoor accuracy after that epoch.

Experimental setup. We detail the experimental setup and defense configurations of DiffFense below.

■ **Dataset and DNN models.** We conduct our experiments on two image datasets, Fashion MNIST and CIFAR10. Fashion MNIST Xiao et al. (2017) is a dataset of Zalando’s black and white article images. It includes 60,000 training images, 10,000 test images and 10 classes. We use a custom three-layer Convolutional Neural Network (CNN) that consists of 2 convolutional layers and a fully connected output layer. The CIFAR10 dataset Krizhevsky et al. (2009) includes RGB images of 10 classes. The training set contains 50,000 samples and the test set has 10,000 samples. We use a lightweight ResNet-18 CNN model He et al. (2016) with 2.7 million parameters as the model architecture.

■ **FL setting.** We assume that there are $N = 50$ local clients with the participation ratio of $\beta = 20\%$ (hence, at each global epoch, $m = 10$ number of agents will be selected for aggregation). The default number of adversaries in the FL system is set to 1 if not specified otherwise.

■ **Backdoor attack setting.** This attack variant includes both pixel-pattern and semantic backdoor attacks. In this scenario, we assume the server trains a global model for 150 iterations on Fashion MNIST and 300 iterations on CIFAR10 dataset. The training data is distributed to local agents in a *non-i.i.d* fashion based on a Dirichlet distribution with hyper-parameter 0.9 Minka (2000). The attackers use the objective function in Equation (2) with the hyperparameter $\alpha = 0.7$ to obtain malicious local updates while regularizing the deviation or the L_2 norm distance from the prior global model parameter. Both benign and adversarial models are trained locally for 3 epochs with a learning rate of 0.05, momentum of 0.9 and decay of 0.0005. The weight-scaling factor of the adversary is $\frac{N}{\eta} = 10$ where N is the number of total participants and η is the global learning rate. When there are $b > 1$ adversaries at an epoch, we assume that they “collude” by evenly distributing the scaling factor by b . Reducing the scaling factor may help the adversaries avoid being detected by the server.

We detail the configuration of each attack below:

- *Pixel-pattern backdoors* require the modification of inputs in a special way during training and testing. In the training stage, we use a white square sticker of size 4 on the bottom-right corner as the trigger and add it to 20 images of each data batch of size 64. Following the paper Bagdasaryan et al. (2020), we add the Gaussian noise of standard deviation $\sigma = 0.01$ to each backdoor image to facilitate model generalization. For testing, backdoor images are generated in the same way.
- *Semantic backdoors* induce the model to mis-predict unmodified inputs with certain features. As suggested in the paper Bagdasaryan et al. (2020), we select images with three features from CIFAR10 dataset as semantic triggers - green cars, cars with racing stripes and cars with vertically striped walls in the background. These chosen images are mislabeled as “airplane”. As in pixel-pattern attacks, we add the Gaussian noise of standard deviation $\sigma = 0.01$ to each backdoor image. We split the training data so that only adversaries have access to the backdoor images. Out of total 63 backdoor images, 48 images are used for training, and 15 are held out for the test phase. An attacker trains his local model with a batch size of 64 and each batch includes 20 backdoor images. Backdoor test images, generated by randomly flipping and cropping the held-out images, are used to compute the backdoor accuracy of the global model.

To sum up, we experiment with three attack scenarios: (*i*) pixel-pattern attack on Fashion-MNIST, (*ii*) pixel-pattern attack on CIFAR10 and (*iii*) semantic attack on CIFAR10.

■ **DiffFense configuration.** The workflow of DiffFense is described in Algorithm 1, 2. We set the step size in gradient descent $s = 0.5$, the number of iterations $t = 20$ and the number of PCA components $d = 2$ when generating differential inputs. The cutoff threshold in the two-step MAD outlier detection is set to $m = 3$.

In 4.3, we analyze DiffFense’s performance against the number and distribution of differential images. In other experiments, we generate 20 differential images chosen randomly with the uniform distribution from 10 classes.

4.1 Results

We compare the performance between FedAvg (baseline) and DiffFense under pixel-pattern attack in Table 1 and semantic attack in Table 3, given one adversary. We can observe that DiffFense’s global model accuracy is comparable to FedAvg’s. Regardless of the trigger pattern, DiffFense is more robust to attacks with the average backdoor accuracy

of below 2%. DiffFense’s strong FL performance is attributed to its low false positive rate of below 7% and zero false negative rate as shown in Table 2, 4.

We further observe that differential testing is effective for distinguishing adversaries from benign agents. In Figure 2, adversaries’ PCA-projected predictions on a differential image are clearly segregated from the benign models’ regardless of the number of participant attackers. In particular, as shown in figure 3, the average prediction distribution of an adversary on differential inputs stands out, outputting an abnormally high value on the targeted class.

Table 1: Performance comparison between the FedAvg and DiffFense against **pixel-pattern** attacks on **Fashion-MNIST** after 150 global epochs and **CIFAR10** after 300 global epochs.

	F-MNIST		CIFAR10	
	FEDAVG	DIFFENSE	FEDAVG	DIFFENSE
FINAL GA (%)	82.1	84.3	89.62	88.87
MEAN BA (%)	6.15	0.68	7.71	0.25

Table 2: Average of false positive rate and false negative rate of DiffFense against **pixel-pattern** attacks on **Fashion-MNIST** and **CIFAR10**.

	F-MNIST	CIFAR10
MEAN FPR (%)	5	5
MEAN FNR (%)	0	0

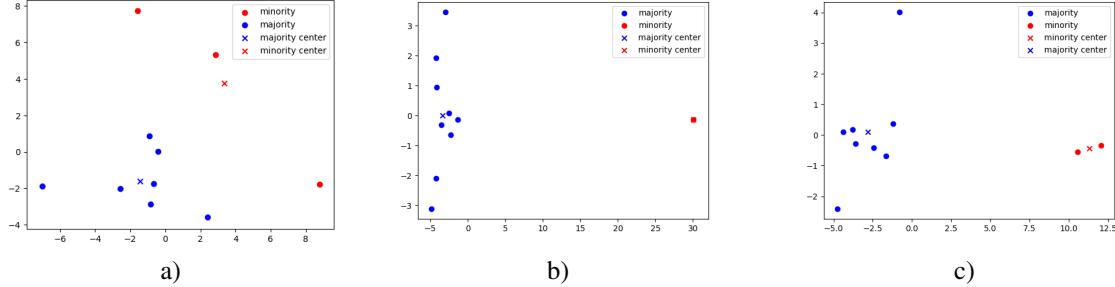


Figure 2: Distribution of PCA-projected predictions by two clusters a) without, b) with an adversary and c) with two adversaries

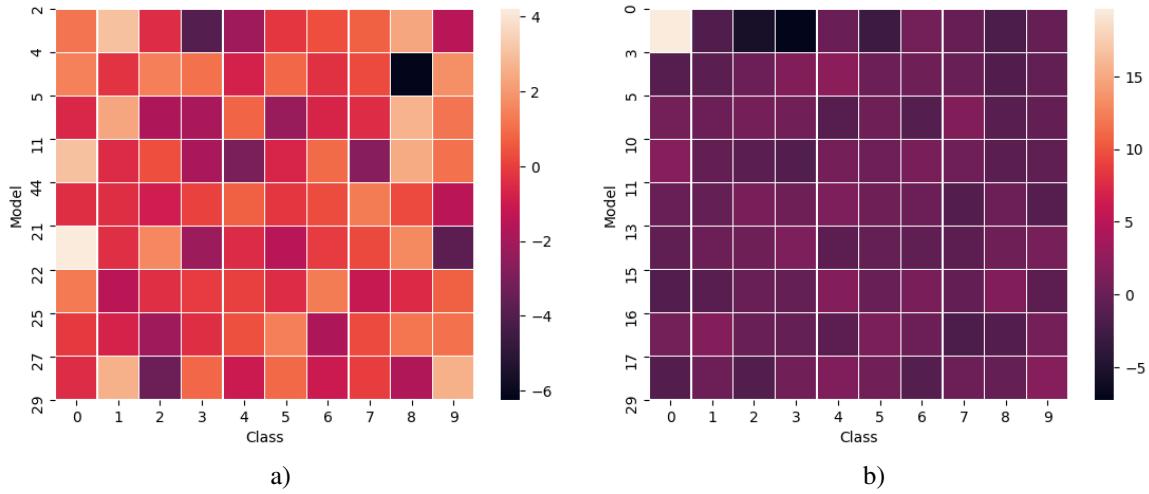


Figure 3: Average prediction score distribution on differential inputs of ten models at an epoch a) without and b) with an adversary who targets the label of backdoor images at “0”

Table 3: Performance comparison between FedAvg, Multi-Krum (denoted as Krum), CooMedian and DiffFense against **semantic** attack on **CIFAR10** dataset with a different number of adversaries.

NUMBER OF ADVERSARIES	1				2				3			
	FEDAVG	KRUM	COOMED	DIFFENSE	FEDAVG	KRUM	COOMED	DIFFENSE	FEDAVG	KRUM	COOMED	DIFFENSE
FINAL GA	89.06	90.04	85.91	89.41	89.7	89.87	88.82	84.1	89.18	87.94	88.89	89.77
MAX BA	100	34.8	45.9	10.5	99.9	96.8	94.5	11.9	100	98.8	96.8	15.5
MEAN BA	14.85	2.84	4.4	0.41	17.86	2.07	9.69	1.15	24.8	3.6	4.29	1.94

4.2 Comparative Analysis against Multiple Adversaries

We evaluate the performance of DiffFense against FedAvg and other defense mechanisms, Multi-Krum and CooMed, given multiple adversaries ranging from 1 to 3. We run experiments on CIFAR10 dataset under semantic attack. The higher the number of adversaries is, the more frequently an adversary may be chosen for the server aggregation. Even when all the three adversaries are selected at an epoch, $K \geq 2b + 3$ with the number of participant models, $K = 10$ and the number of adversaries, $b = 3$. Hence, our attack setting satisfies the Krum's requirement.

We can observe in Table 3, 4 that DiffFense obtains a lower average backdoor accuracy than other methods with consistently zero false negative rate while achieving a global accuracy comparable to the baseline with below 7% of false positive rate. Compared to Multi-Krum, DiffFense successfully detects all the adversaries while yielding a lower false positive rate, regardless of the number of adversaries.

We also compute the maximum backdoor accuracy of each method after the global model reaches the test accuracy of 85% in Table 3. DiffFense' backdoor accuracy is consistently lower than 16% while other methods' reach 95% with multiple adversaries. To sum up, DiffFense steadily presents a stronger performance than FedAvg, Multi-Krum and CooMed given a various number of adversaries.

Table 4: Mean false positive rate and false negative rate of DiffFense and Multi-Krum over 300 rounds given different numbers of adversaries under **semantic** attack on **CIFAR10** dataset.

NUMBER OF ADVERSARIES	1		2		3	
	KRUM	DIFFENSE	KRUM	DIFFENSE	KRUM	DIFFENSE
MEAN FPR	8.23	6.7	16	4.16	27.17	3.54
MEAN FNR	0	0	0.8	0	0.48	0

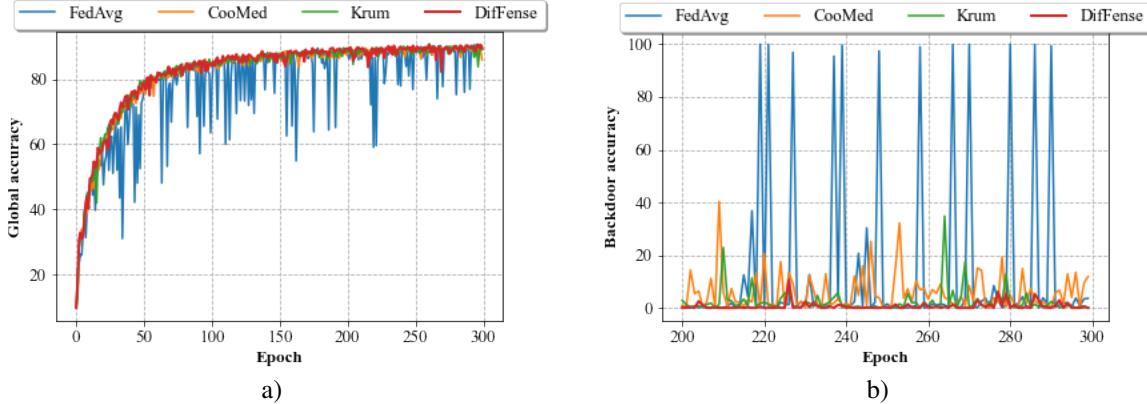


Figure 4: Progression plot of a) the global accuracy throughout the entire training process and b) the backdoor accuracy during the last 100 epochs under semantic attack on CIFAR10 given 1 adversary

4.3 Ablation Study

Number of differential images. We run a sensitivity analysis to investigate whether DiffFense's effectiveness is correlated with the number of generated differential images. We can observe that the final global accuracy is consistently around 89% while the average backdoor accuracy is below 4%. The average false positive rate is also comparable, ranging from 5% to 8% and the average false negative rate is zero.

Distribution of differential images. Fixing the number of differential images as 20, we differentiate the number of distinct classes that the images belong to. We assume that differential images are *i.i.d* distributed across the given classes. We can observe that the average false positive rate decreases as more classes are used while false negative rate is flat zero. However, even with one class, DiffFense achieves a false positive rate of below 9% and the final global accuracy comparable to the one whose differential images are from all the classes. This alleviates the burden of securing

Table 5: Performance analysis of DiffFense with respect to the number of differential images generated with 300 epochs of global training on **CIFAR10** dataset under **semantic** attack.

# DIFFERENTIAL INPUTS	20	50	100
FINAL GA	89.41	89.93	89.15
MEAN BA	0.41	2.49	3.14
MEAN FPR	6.7	7.73	5.47
MEAN FNR	0	0	0

Table 6: Performance analysis of the DiffFense with respect to the number of distinct classes that 20 differential images belong to, generated with 300 epochs of global training on **CIFAR10** dataset under **semantic** attack.

# DIFFERENTIAL INPUT CLASSES	1	2	5	10
FINAL GA	89.71	89.86	89.51	89.54
MEAN BA	2.34	3.03	3.23	5.34
MEAN FPR	8.87	8.93	7.37	4.43
MEAN FNR	0	0	0	0

validation images distributed across a number of classes. Also, using images from only few classes can reduce the runtime as the computational complexity of Algorithm 1 is affected by the number of image classes.

Two-step MAD outlier detection. We corroborate the effectiveness of two-step MAD outlier detection compared to the original single and double MAD variants. Single MAD suffers from a high false positive rate while double MAD from a high false negative rate (100%). Two-step MAD outlier detection achieves the zero false negative rate while suppressing the false positive rate to below 7%.

Table 7: DifFense’s performance based on different MAD outlier detection methods on **CIFAR10** dataset under **semantic** attack.

OUTLIER DETECTION	TWO-STEP MAD	DOUBLE MAD	SINGLE MAD
FINAL GA	89.41	89.21	88.31
MEAN BA	0.41	14.34	6.09
MEAN FPR	6.7	1.17	23.17
MEAN FNR	0	100	0

5 Conclusion

In this work, we design and experiment DiffFense, an automated defense framework in FL based on differential testing and two-step MAD outlier detection. Our method addresses limitations of the prior defense mechanisms by requiring minimal knowledge of the attack setting. We also empirically show that DiffFense yields a backdoor accuracy lower than other aggregation methods while achieving a global accuracy comparable to the baseline, FedAvg. DiffFense successfully detects and excludes any number of adversaries while suppressing a false positive rate below 10%. The performance of DiffFense is steadily strong regardless of the number and distribution of differential images.

References

- Bagdasaryan, E., Veit, A., Hua, Y., Estrin, D., and Shmatikov, V. How to backdoor federated learning. In Chiappa, S. and Calandra, R. (eds.), *Proceedings of the Twenty Third International Conference on Artificial Intelligence and Statistics*, volume 108 of *Proceedings of Machine Learning Research*, pp. 2938–2948. PMLR, 26–28 Aug 2020.
- Barreno, M., Nelson, B., Joseph, A. D., and Tygar, J. D. The security of machine learning. *Mach. Learn.*, 81(2): 121–148, November 2010. ISSN 0885-6125.
- Bhagoji, A. N., Chakraborty, S., Mittal, P., and Calo, S. Analyzing federated learning through an adversarial lens. In Chaudhuri, K. and Salakhutdinov, R. (eds.), *Proceedings of the 36th International Conference on Machine Learning*, volume 97 of *Proceedings of Machine Learning Research*, pp. 634–643, Long Beach, California, USA, 09–15 Jun 2019. PMLR.
- Blanchard, P., El Mhamdi, E. M., Guerraoui, R., and Stainer, J. Machine learning with adversaries: Byzantine tolerant gradient descent. In Guyon, I., Luxburg, U. V., Bengio, S., Wallach, H., Fergus, R., Vishwanathan, S., and Garnett, R. (eds.), *Advances in Neural Information Processing Systems 30*, pp. 119–129. Curran Associates, Inc., 2017.

- Bonawitz, K., Ivanov, V., Kreuter, B., Marcedone, A., McMahan, H. B., Patel, S., Ramage, D., Segal, A., and Seth, K. Practical secure aggregation for privacy-preserving machine learning. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, CCS '17, pp. 1175–1191, New York, NY, USA, 2017. Association for Computing Machinery. ISBN 9781450349468. doi:10.1145/3133956.3133982. URL <https://doi.org/10.1145/3133956.3133982>.
- Chakraborty, R. S., Wolff, F., Paul, S., Papachristou, C., and Bhunia, S. Mero: A statistical approach for hardware trojan detection. In *International Workshop on Cryptographic Hardware and Embedded Systems*, pp. 396–410. Springer, 2009.
- Das, A. and Rad, P. Opportunities and challenges in explainable artificial intelligence (xai): A survey. *ArXiv*, abs/2006.11371, 2020.
- Fung, C., Yoon, C. J. M., and Beschastnikh, I. Mitigating sybils in federated learning poisoning, 2018.
- He, K., Zhang, X., Ren, S., and Sun, J. Deep residual learning for image recognition. In *2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, pp. 770–778, 2016. doi:10.1109/CVPR.2016.90.
- Konečný, J., McMahan, H. B., Yu, F. X., Richtárik, P., Suresh, A. T., and Bacon, D. Federated learning: Strategies for improving communication efficiency. *arXiv preprint arXiv:1610.05492*, 2016.
- Krizhevsky, A., Nair, V., and Hinton., G. *The CIFAR-10 dataset.*, 2009. URL <https://www.cs.toronto.edu/~kriz/cifar.html>.
- Leys, C., Ley, C., Klein, O., Bernard, P., and Licata, L. Detecting outliers: Do not use standard deviation around the mean, use absolute deviation around the median. *Journal of Experimental Social Psychology*, 49:764–766, 07 2013.
- McKeeman, W. M. Differential testing for software. *DIGITAL TECHNICAL JOURNAL*, 10(1):100–107, 1998.
- McMahan, B., Moore, E., Ramage, D., Hampson, S., and y Arcas, B. A. Communication-efficient learning of deep networks from decentralized data. In Singh, A. and Zhu, X. J. (eds.), *Proceedings of the 20th International Conference on Artificial Intelligence and Statistics, AISTATS 2017, 20-22 April 2017, Fort Lauderdale, FL, USA*, volume 54 of *Proceedings of Machine Learning Research*, pp. 1273–1282. PMLR, 2017.
- Minka, T. P. Estimating a dirichlet distribution. Technical report, 2000.
- Pei, K., Cao, Y., Yang, J., and Jana, S. Deepxplore: Automated whitebox testing of deep learning systems. In *Proceedings of the 26th Symposium on Operating Systems Principles*, SOSP '17, pp. 1–18, New York, NY, USA, 2017. Association for Computing Machinery. ISBN 9781450350853. doi:10.1145/3132747.3132785. URL <https://doi.org/10.1145/3132747.3132785>.
- Rosenmai, P. Using the median absolute deviation to find outliers. <http://eurekastatistics.com/using-the-median-absolute-deviation-to-find-outliers/>, Nov 2013.
- Saha, S., Chakraborty, R. S., Nuthakki, S. S., Mukhopadhyay, D., et al. Improved test pattern generation for hardware trojan detection using genetic algorithm and boolean satisfiability. In *International Workshop on Cryptographic Hardware and Embedded Systems*, pp. 577–596. Springer, 2015.
- Sattler, F., Wiedemann, S., Müller, K.-R., and Samek, W. Robust and communication-efficient federated learning from non-iid data. *IEEE transactions on neural networks and learning systems*, 2019.
- Shen, S., Tople, S., and Saxena, P. Auror: Defending against poisoning attacks in collaborative deep learning systems. In *Proceedings of the 32nd Annual Conference on Computer Security Applications*, ACSAC '16, pp. 508–519, New York, NY, USA, 2016. Association for Computing Machinery.
- Tolpegin, V., Truex, S., Gursoy, M. E., and Liu, L. Data poisoning attacks against federated learning systems. In Chen, L., Li, N., Liang, K., and Schneider, S. (eds.), *Computer Security – ESORICS 2020*, pp. 480–501, Cham, 2020. Springer International Publishing. ISBN 978-3-030-58951-6.
- Xiao, H., Rasul, K., and Vollgraf, R. Fashion-mnist: a novel image dataset for benchmarking machine learning algorithms, 2017.
- Yang, Q., Liu, Y., Chen, T., and Tong, Y. Federated machine learning: Concept and applications. *ACM Transactions on Intelligent Systems and Technology (TIST)*, 10(2):1–19, 2019.
- Yin, D., Chen, Y., Ramchandran, K., and Bartlett, P. Byzantine-robust distributed learning: Towards optimal statistical rates. *arXiv preprint arXiv:1803.01498*, 2018.