
FEDERATED LEARNING FOR INTERNET OF THINGS: A FEDERATED LEARNING FRAMEWORK FOR ON-DEVICE ANOMALY DATA DETECTION

A PREPRINT

Tuo Zhang*, **Chaoyang He***, **Tianhao Ma**, **Lei Gao**, **Mark Ma**, **Salman Avestimehr**

Viterbi School of Engineering
University of Southern California
{tuozhang, chaoyang.he, tianhaom, leig, mzma, avestime}@usc.edu

October 19, 2021

ABSTRACT

Federated learning can be a promising solution for enabling IoT cybersecurity (i.e., anomaly detection in the IoT environment) while preserving data privacy and mitigating the high communication/storage overhead (e.g., high-frequency data from time-series sensors) of centralized over-the-cloud approaches. In this paper, to further push forward this direction with a comprehensive study in both algorithm and system design, we build FedIoT platform that contains FedDetect algorithm for on-device anomaly data detection and a system design for realistic evaluation of federated learning on IoT devices. Furthermore, the proposed FedDetect learning framework improves the performance by utilizing a local adaptive optimizer (e.g., Adam) and a cross-round learning rate scheduler. In a network of realistic IoT devices (Raspberry PI), we evaluate FedIoT platform and FedDetect algorithm in both model and system performance. Our results demonstrate the efficacy of federated learning in detecting a wider range of attack types occurred at multiple devices. The system efficiency analysis indicates that both end-to-end training time and memory cost are affordable and promising for resource-constrained IoT devices. The source code is publicly available at <https://github.com/FedML-AI/FedIoT>.

1 Introduction

Along with the faster Internet speed and more endpoints brought by the 5G, billions of IoT devices online will be deployed [Riad et al. \[2020\]](#). However, for the *data anomaly detection task* (e.g., DDoS attack detection), the centralized over-the-cloud approach [Meidan et al. \[2018\]](#) may not fit this trend due to data privacy and extremely high communication/storage overhead (e.g., high-frequency data from time-series sensors) centralizing data from numerous IoT devices. As such, researchers attempt to address these challenges using federated learning (FL), which is a trending paradigm that can train a global or personalized model without centralizing data from edge devices [Kairouz et al. \[2019\]](#). DIoT [Nguyen et al. \[2019\]](#) and IoTDefender [Fan et al. \[2020\]](#) employ FL for intrusion detection in IoT devices by collaboratively training isolated datasets for a global or even personalized model. [Liu et al. \[2021\]](#) further upgrades the model to a complex attention-based CNN-LSTM but mitigates the communication cost with Top- k gradient compression. Beyond detecting the abnormal data, [Rey et al. \[2021\]](#) even considers an adversarial setup where several malicious participants poison the federated model.

However, as the traffic volume of IoT-based DDoS attacks reaches unprecedented levels [Bertino and Islam \[2017\]](#), the efficacy of these works is unclear, mainly when the attacks spread to large-scale types and devices but training on the limited data from small-scale devices cannot obtain high accuracy. More significantly, our research community lacks an open, generic, and flexible FL-enabled IoT platform for advanced researches. Existing works only run simulations rather than perform experiments in real IoT platforms, or their specialized system design is not generalized enough for

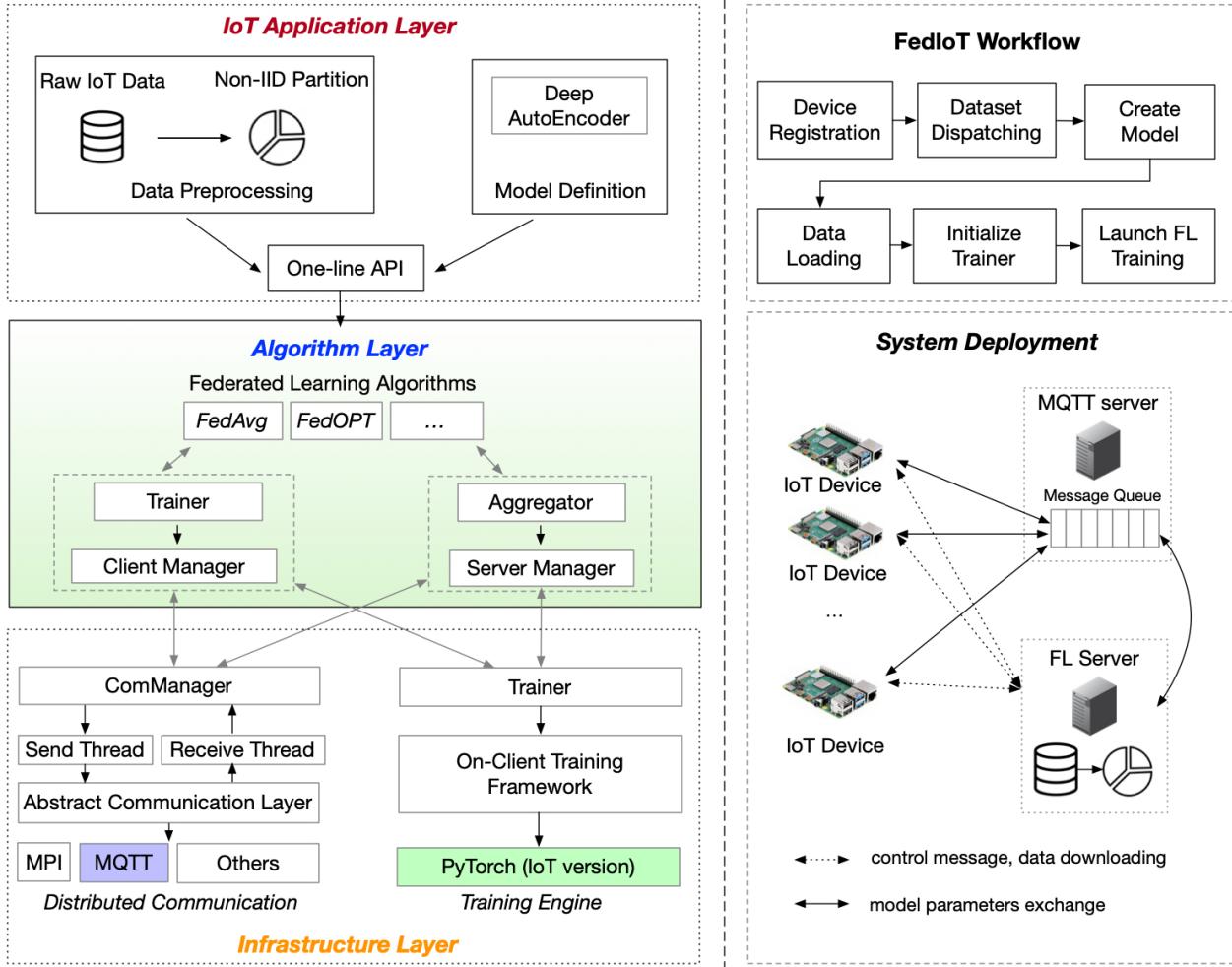


Figure 1: Overview of FedIoT Platform

future research. In addition, given that IoT devices are resource-constrained, system performance analysis is also an essential step. Unfortunately, none of these works provides such analysis towards practical deployment.

To further push forward the research in FL-based IoT cybersecurity, we build FedIoT platform with a simple but effective design philosophy that lays the foundation for future scientific research. The overall design spans dataset, model, algorithm, and system design. More specifically, we propose a federated learning algorithmic framework, FedDetect which utilizes adaptive optimizer (e.g., Adam) and cross-round learning rate scheduler, rather than naive FedAvg McMahan et al. [2016] for local training. In order to verify the effectiveness of FL for IoT security, we design a novel method to synthesize the testset from public dataset for FL-based IoT cybersecurity research. Its design aims to evaluate whether the global model obtained through FL training can recognize more attack types and has higher detection performance (the evaluation and test dataset cover all attack types on the entire IoT network). In addition, we build FedIoT platform for realistic IoT devices with a high degree of modularization and flexible APIs. As such, we can add new data, models, and algorithms with only lightweight modification. Most importantly, FedIoT supports both IoT edge training (e.g., Raspberry Pi) and CPU/GPU-based distributed training with the support of MQTT and MPI communication backend, respectively.

We evaluate FedIoT platform and FedDetect algorithm on N-BaIoT Meidan et al. [2018] dataset, and also analyze the system performance comprehensively (i.e., computational speed, communication cost, and memory cost). Our results demonstrate the efficacy of federated learning in detecting a large range of attack types. Our system efficiency analysis shows that the training time memory cost occupies only a small fraction of the entire host memory of the IoT platform (Raspberry Pi), and the end-to-end training time is feasible (less than 1 hour).

2 Algorithm and System Design

2.1 Overview

Federated learning (FL)-based IoT cybersecurity aims to detect network intrusion in IoT devices without centralizing a large amount of high frequent edge data. In this work, to analyze both algorithmic and system performance in real IoT devices, we build FedIoT platform with simple but effective design philosophy, as illustrated in Figure 1. The entire software architecture consists of three layers: the application layer, the algorithm layer, and the infrastructure layer. We make each layer and module perform its duty and have a high degree of modularization. In the application layer, FedIoT provides a one-line API (taking the Autoencoder model and data loader as inputs) to launch the federated training on IoT devices in a distributed computing manner. At the algorithm layer, FedIoT supports FedDetect and other algorithmic baselines such as FedAvg [McMahan et al. \[2017\]](#), FedOPT [Reddi et al. \[2020\]](#); at the infrastructure layer, FedIoT aims to support lightweight communication APIs with MQTT [Hunkeler et al. \[2008\]](#) (i.e., Message Queuing Telemetry Transport, a standard for IoT messaging), and IoT platform-customized PyTorch library [Paszke et al. \[2019\]](#) that can support on-device training for CPU or GPU-enabled IoT edge devices, such as Raspberry Pi and NVIDIA Jetson Nano.

We organize the remaining subsections as follows. Section 2.2 depicts an IoT scenario and threaten model with privacy requirements. Section 2.3 introduces how we synthesize a dataset to understand a larger attack type based on the N-BaIoT dataset. Section 2.4, Section 2.5 and Section 2.6 describe the AutoEncoder model, FedDetect algorithm, and the system design, respectively.

2.2 Threaten Model and Deployment

The primary goal for the FedDetect is to prevent the anomaly traffic from the malware, such as the DDoS attack, passing into the IoT devices. As a result, we design to deploy the FedDetect on the router, which makes the router as a security gateway to monitor IoT devices and perform anomaly detection to protect the cybersecurity. Figure 2 presents the deployment diagram. The incoming traffic will be filtered first by the security gateway before fed into the IoT devices. In this paper, we proposed the following assumptions for the discussion: *1. The IoT device may be vulnerable but not initially be compromised. 2. The Internet gateway (i.e. router) is not compromised.*

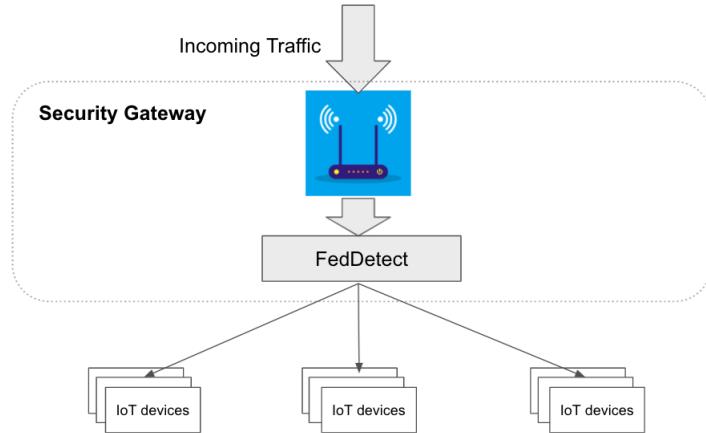


Figure 2: FedIoT deployment

2.3 Dataset and Preprocessing

We introduce a widely used public IoT dataset for anomaly detection and then synthesize a dataset for realistic evaluation on the FL-based method.

N-BaIoT dataset [Meidan et al. \[2018\]](#) is a widely used public dataset for research on anomaly detection of IoT data. N-BaIoT captures network traffic flow from 9 commercial IoT devices authentically attacked by network intrusions. Each IoT device has 2 subsets: one benign set containing normal network flow data only, and one attack data subset consisting of two common malware attacks, Mirai and BASHLITE, which each contain five different kinds of attack types.

In order to verify the effectiveness of FL for IoT security, different from previous works Nguyen et al. [2019], Fan et al. [2020], Ito et al. [2020], Liu et al. [2021], Rey et al. [2021], we hope to learn a detection model from benign data widely distributed in different types of devices that can identify a larger range of attacks. Specifically, we hope that the data design meets three characteristics: 1. *It contains training data of multiple device types (benign data);* 2. *Each device has no full set of all attack types;* 3. *The evaluation and test dataset should cover all attack types on the entire IoT network.* These requirements are based on several real-world assumptions:

- From the perspective of benign data, features of the network data flow among different types of devices are inconsistent. For example, a surveillance camera will record in real-time (24x7 hours), while the data generated by a doorbell is intermittent.
- The detection model should have the ability to identify multiple attack types, but the types of attacks encountered by a single device are likely to be only part of the full set. Only by learning with the feature of all attack types in the entire IoT network, the detection model on a single device can have the ability to detect unknown attacks in a wide range.
- Because of privacy (e.g., camera video) and extremely high communication/storage overhead (e.g., high-frequency data from time-series sensors), it is infeasible to centralize data on massive devices.

Therefore, we use N-BaIoT to synthesize the testset for FL-based IoT cybersecurity research. Our synthesized testset is generated by the following rules: 1. For each device, we assign 5000 samples of selected benign data as the training data and another 3000 samples of benign data as the evaluation dataset (i.e., calculating the anomaly threshold, see Section 2.4); 2. We enforce the global test dataset to compose all devices' benign data and all types of attack data. More specifically, for each device, we randomly select 500 malicious data samples from each type of the attack, and the same amount of benign data samples to synthesis the testset, making the testset perfectly balanced for binary classification.

2.4 Anomaly Detection with Deep Autoencoder

We apply a Deep Autoencoder Rumelhart et al. [1985] as the model for anomaly detection. Deep Autoencoder is simple but effective and does not lose the generality to evaluate FL algorithms and our FedIoT platform. Other advanced models (e.g., Variational Autoencoder, or attention-based CNN-LSTM Liu et al. [2021]) can also be applied into our framework without additional engineering efforts.

Model Definition Deep Autoencoder focuses on the reconstruction of the input data in an unsupervised learning manner. Essentially, Autoencoder splits the neural network into two segments, the encoder f_{θ_e} and the decoder f_{θ_d} . Encoder f_{θ_e} compresses the input \mathbf{x} to a latent space \mathbf{z} . Decoder f_{θ_d} then attempts to restore the original image after some generalized non-linear transformation. Mathematically, the loss function can be written as $\mathcal{L}(\mathbf{x}, \mathbf{x}') = \|\mathbf{x} - \mathbf{x}'\|^2 = \|\mathbf{x} - f_{\theta_d}(\mathbf{z})\|^2 = \|\mathbf{x} - f_{\theta_d}(f_{\theta_e}(\mathbf{x}))\|^2$. This loss is also called *reconstruction error* calculated by mean square error $MSE = \frac{1}{d} \sum_{i=1}^d (x_i - \hat{x}_i)^2$, where d is the dimension of the input. In essence, this loss function aims to encode the input to a latent representation \mathbf{z} such that it can be regenerated by the decoder. To minimize the loss, common deep learning optimizers such as Adam Kingma and Ba [2014] can be applied.

$$tr = \overline{MSE} + \alpha * \sigma(MSE) \quad (1)$$

Anomaly Detection In the application of anomaly detection, we train a deep Autoencoder with benign IoT traffic data to learn IoT devices' normal behavior, so that our Autoencoder could successfully extract and reconstruct features on benign samples but fails to do so on abnormal samples with unseen features. During detection phase, one input data sample that achieves a reconstruction error above a threshold will be detected as an abnormal data sample. In detail, after training Autoencoder on benign training dataset, we first calculate the reconstruction error (MSE) for each data sample from benign evaluation dataset, and then obtain the threshold by Equation 1, which computes the sum of the mean of MSE plus standard deviation of MSE over all evaluation samples. The value of threshold should be as large as possible to suppress the majority of benign samples while preventing abnormal samples from being classified into benign samples. Extensive experiments show that the overall performance is the best when α equals to 3.

2.5 FedDetect

We propose a federated learning algorithmic framework, FedDetect, for anomaly detection in distributed IoT devices. Distinguished from existing works on FL-based IoT anomaly detection, FedDetect utilizes adaptive optimizer (e.g., Adam) and cross-round learning rate scheduler, rather than naive FedAvg McMahan et al. [2016] for local training. FedDetect is summarized as Algorithm 1.

Algorithm 1: FedDetect

```

1: Initialization  $w_0$ 
2: for round  $t = 0, 1, \dots$  do
3:   Adjust cross-round learning rate (cosine scheduler)
4:   for client  $i = 0$  to  $K - 1$  do
5:      $w_{t+1}^i \leftarrow$  Local Training with Adam
6:     Upload  $w_{t+1}^i$  to Server
7:   end for
8:    $w_{t+1} = \frac{1}{K} \sum_{i=0}^{K-1} w_{t+1}^i$ 
9:   clients receive new model  $w_{t+1}$ 
10: end for
11: Globalized Threshold Algorithm
12:  $MSE_{Global} = [MSE^0, \dots, MSE^{K-1}]$ 
13:  $tr_{Global} = \overline{MSE_{Global}} + \alpha * \sigma(MSE_{Global})$ 

```

Local Adaptivity and Cross-round Learning Rate Scheduler The choice of Adam for local training and cross-round learning rate scheduler is based on our experimental observation. We empirically find that local Adam beats naive local SGD or SGD with momentum when applying a cross-round learning rate scheduler (e.g., cosine scheduler). The rationality of local adaptivity has been intensively verified its efficacy in CV and NLP tasks Wang et al. [2021], Reddi et al. [2020].

Global Threshold After achieving the global model via federated training, we propose a algorithmic module to calculate the anomaly threshold for each device, *Global Threshold*. More specially, in the Global Threshold algorithm, each device runs the global model locally to get the MSE sequence and then synchronizes it to the server, and the server uses MSE sequences from all devices to generate a unified global threshold for detection in each device.

Global Threshold algorithm objectively expresses the detection performance of the FL-trained global model on the entire IoT networks (i.e., detecting a larger range of attack types as introduced in Section 2.3). Experimental results demonstrate the efficacy of FL in diverse real-world scenarios (Section 3.4).

2.6 System Design

As illustrated in Figure 1, the entire software architecture of FedIoT platform consists of three layers: the application layer, the algorithm layer, and the infrastructure layer. FedIoT aims to provide an open, generic and flexible FL-enabled IoT platform for future research exploration.

In the application layer, APIs for data preprocessing described in Section 2.3 are provided. Combined with the model definition, we could launch the FL on IoT platforms using a one-line API. The figure also shows the workflow, which is a standard engineering practice that we suggest.

In the algorithm layer, beside the regular FedAvg and FedOPT FL aggregation functions, FedIoT supports customized local trainer, dataloader and FL aggregation functions. The FL client (IoT device) is maintained as an instance by the ClientManager, and the FL server is managed by ServerManager. They can exchange information with flexible APIs supported by the underlying abstract communication layer. By following this client-oriented programming design pattern, users can define their own client/server behavior when participating in training or coordination in the FL algorithm, so that FedIoT allows users to focus on algorithmic implementations instead of considering the low-level communication mechanism.

In the infrastructure layer, FedIoT supports AI-enabled IoT edge devices and the lightweight communication APIs for distributed system. With such testbeds built upon real-world hardware platforms, researchers can evaluate realistic system performance, such as training time, communication, and computation cost. Moreover, for FedIoT, researchers only need to program with Python to customize their research experiments without the need to learn new system frameworks or programming languages (e.g., Java, C/C++). MQTT Hunkeler et al. [2008] is supported for IoT setting. As such, we deploy two servers: the MQTT server for messaging passing and the FL server for federated aggregation. The model weight exchange is by MQTT messaging server, while control messages such as device registration and dataset distribution are transmitted through the FL server.

With these design, researchers can add new data, models, and algorithms with only lightweight modification.

3 Experiments

We evaluated FedIoT platform on two aspects: algorithmic performance in global model; a comprehensive analysis of the system efficiency, including computational speed, communication cost, and memory cost.

3.1 Setup

Implementation We implemented two computing paradigms of FedIoT platforms: (1) IoT edge training, and (2) CPU/GPU-based distributed training. For the IoT edge training, we choose 9 Raspberry Pi 4B as client devices and a GPU server that integrates both the FL server and the MQTT service. The local training will be implemented on the Raspberry Pi and the weight integration will be implemented on the GPU server.

Dataset and Model Definitions We evaluated FedIoT platform using the dataset described in Section 2.3. For the Autoencoder, we set the input with a dimension of 115, the same as the features of data. The encoder network has four hidden layers, as the dimension decreasing rate equals 75%, 50%, 33%, and 25%. The decoder has the same layer design as the encoder, but with an increasing sequence. The number of parameters for the Autoencoder is equal to 36628.

For the training dataset, we implement the min-max normalization, i.e. $x = \frac{x - x^{min}}{x^{max} - x^{min}}$, where x^{min} and x^{max} are the global minimum and maximum values over training samples of all devices. As for the evaluation and testing dataset, we use the same minimum and maximum values obtained from the training dataset to scale both benign and attack samples, which will make the testing data as the same distribution as benign training samples. This scaling will distort the original distribution for the malicious data, which decreases the restoration performance by the Autoencoder and assist the performance for the binary classification.

Hyper-parameters We searched for the learning rate on a range of {1, 0.1, 0.01, 0.001, 0.0001, 0.00001}, input batch size on a range of {8, 16, 32, 64, 128}, local training epoch on a range of {1, 50, 100, 120, 150, 200}, total training round on a range of {10, 30, 50, 100, 120, 150} and tested both *tanh* and *sigmoid* activation functions in Autoencoder. After hyper-parameter searching, we fixed the following hyper-parameters: the batch size for input is 64, the local training epoch in FL is 120, total training round is 30, and the activation function inside the Autoencoder is set as *tanh* function. More hyper-parameters can be found in our source code.

3.2 Baselines

To evaluate our proposed algorithm in Section 2.5 comprehensively, we design the following scenarios for the direct comparison:

- *CL-Single*: Each device trains a detection model with its own local dataset. This baseline can obtain the model performance when training a local model without the help of federated learning.
- *CL-Combined*: A detection model is trained with the merged data from nine devices. The result of this baseline serves as the upper bound performance for the centralized training. It may perform the best because it gathers all data samples from the entire IoT network.
- *FL-FedDect*: A detection model is trained via federated learning from nine devices with the FedDect algorithm. It may give similar performance as CL-Combined.

3.3 Metrics

Following the existing works, we use three metrics to evaluate the detection performance: accuracy (ACC), true positive rate (TPR), false positive rate (FPR), and true negative rate (TNR). The formulas and confusion matrix are shown below.

$$\begin{aligned} \bullet \quad ACC &= \frac{TP+TN}{TP+TN+FP+FN} & \bullet \quad TPR &= \frac{TP}{TP+FN} \\ \bullet \quad FPR &= \frac{FP}{TN+FP} & \bullet \quad TNR &= \frac{TN}{TN+FP} \end{aligned}$$

| | Predicted Benign | Predicted Malicious |
|------------------|---------------------|---------------------|
| Actual Benign | True Negative (TN) | False Positive (FP) |
| Actual Malicious | False Negative (FN) | True Positive (TP) |

Table 1: Performance of anomaly detection under both centralized training and federated training

| | Acc | FPR | TPR | TNR |
|--------------------|--------|--------|--------|--------|
| <i>CL-Single</i> | 73.82% | 37.50% | 86.56% | 62.50% |
| <i>CL-Combined</i> | 98.64% | 2.71% | 99.99% | 97.29% |
| <i>FL-FedDect</i> | 98.27% | 3.45% | 99.99% | 96.55% |

Table 2: CPU/GPU Training v.s. IoT Edge Training

| | Acc | FPR | TPR | TNR |
|---------------------|--------|-------|--------|--------|
| <i>Simulation</i> | 98.27% | 3.45% | 99.99% | 96.55% |
| <i>Raspberry Pi</i> | 97.47% | 4.78% | 99.99% | 95.22% |

3.4 Results of Learning Performance

Evaluation using the global threshold We first evaluated the performance of FedDect algorithm using the global threshold and compared its performance with three baselines. For the baseline CL-Single, we reported the average value of the nine devices’ model performances. The detailed results for the three scenarios are shown in the Table 1.

Understanding the result For the detection model, the more benign data the model can train on, the better performance it should have. Under the global evaluation, the baseline CL-Combined trains on all benign data. Consequently, it is the best performance among all models. Within the same amount of training samples, FL with distributed training achieves nearly the same performance compared to upper bound of centralized training, which demonstrates the efficiency of FedDect. The FedDect algorithm has much better performance than CL-Single, because the FedDect trains on more data among all devices collaboratively, thus it can capture more features. The FPR and TNR performance of FL is little worse than CL, because during ML optimization, the direction of gradient descent is shifted after the aggregation by averaging, leading to sub-optimal minimum, which may not be suitable for the local evaluation targets.

3.5 Analysis of System Efficiency

For the second part of the experiment, we evaluated the system performance of FedIoT with globalized threshold on the Raspberry Pi within N-BaIoT dataset.

We first verified that FedIoT on the real IoT device could achieve the same results as CPU/GPU distributed training. From Table 2, we could see that the results from the Raspberry Pi are nearly the same as the results from CPU/GPU simulation. The slight difference is due to different random initialization (i.e., different runs in different platforms).



Figure 3: Properties of Experiments on Raspberry Pi

We further tested the system efficiency on the Raspberry Pi platform. From Figure 3, we can see that the training time memory cost occupies only a small fraction of the entire host memory of Raspberry Pi (only 4G host memory). The training time per round is less than 1 minute. To understand the system cost more comprehensively, we analyzed the breakdown of the end-to-end training time when the bandwidth is 7.65MB/s (a reasonable bandwidth in 4G/5G wireless communication), and results are shown in Table 3. Overall, the end-to-end training time is an acceptable training time (less than 1 hour) for practical applications. We can also find that the ratio of communication almost costs half of the end-to-end training time, indicating that the communication compression technique Lin et al. [2017], Tang et al. [2018] is essential to improve the system performance in the IoT setting.

Table 3: Breakdown of the End-to-end Training Time

| Type | Value |
|--------------------------|---------------|
| end-to-end time | 2547 seconds |
| uplink latency | 0.167 seconds |
| communication time ratio | 42.2 % |
| computation time ratio | 57.8 % |
| bandwidth | 7.65 MB/s |

*Note: the communication time is measured by computing the interval between the timing when Raspberry Pi uploads local model to the server and the timing that Raspberry Pi receives the global model from the server. The experiment is implemented under the WiFi condition.

4 Related Works

Our work is related to the application of federated learning in IoT cybersecurity. DIoT [Nguyen et al. \[2019\]](#) is the first system to employ a federated learning approach to anomaly-detection-based intrusion detection in IoT devices. IoTDefender [Fan et al. \[2020\]](#) is another similar framework but obtains a personalized model by fine-tuning the global model trained with federated learning. [Ito et al. \[2020\]](#) evaluates FL-based anomaly detection framework with learning tasks such as aggressive driving detection and human activity recognition. [Liu et al. \[2021\]](#) further proposed an attention-based CNN-LSTM model to detect anomalies in an FL manner, and reduced the communication cost by using Top- k gradient compression. Recently, [Rey et al. \[2021\]](#) even evaluates the impact of malicious clients under the setting of FL-based anomaly detection. Compared to these existing works, our FedIoT platform is the first work that analyzes both algorithmic and system performance in a real IoT platform.

5 Conclusion

In this paper, to further push forward the research in FL-based IoT cybersecurity, we build FedIoT platform with a simple but effective design philosophy. We apply Deep Autoencoder [Rumelhart et al. \[1985\]](#) as the model for anomaly detection to evaluate FL algorithms and our FedIoT platform. Moreover, we propose FedDetect, a federated learning algorithmic framework that utilizes adaptive optimizer and cross-round learning rate scheduler, rather than naive FedAvg [McMahan et al. \[2016\]](#) for local training. FedIoT supports both IoT edge training and CPU/GPU-based distributed training with the support of MQTT and MPI communication backend, respectively. We evaluate FedIoT platform and FedDetect algorithm with global detection model, and also analyze the system performance comprehensively. Our results demonstrate the efficacy of federated learning in detecting a large range of attack types, and the system efficiency analysis shows that both end-to-end training time and memory cost is affordable and promising for resource-constrained IoT devices.

References

- Khaled Riad, Teng Huang, and Lishan Ke. A dynamic and hierarchical access control for iot in multi-authority cloud storage. *Journal of Network and Computer Applications*, 160:102633, 04 2020. doi:[10.1016/j.jnca.2020.102633](https://doi.org/10.1016/j.jnca.2020.102633).
- Yair Meidan, Michael Bohadana, Yael Mathov, Yisroel Mirsky, Asaf Shabtai, Dominik Breitenbacher, and Yuval Elovici. N-baiot—network-based detection of iot botnet attacks using deep autoencoders. *IEEE Pervasive Computing*, 17(3):12–22, 2018. doi:[10.1109/MPRV.2018.03367731](https://doi.org/10.1109/MPRV.2018.03367731).
- Peter Kairouz, H Brendan McMahan, Brendan Avent, Aurélien Bellet, Mehdi Bennis, Arjun Nitin Bhagoji, Keith Bonawitz, Zachary Charles, Graham Cormode, Rachel Cummings, et al. Advances and open problems in federated learning. *arXiv preprint arXiv:1912.04977*, 2019.
- Thien Nguyen, Samuel Marchal, Markus Miettinen, Hossein Fereidooni, N. Asokan, and Ahmad-Reza Sadeghi. Dİöt: A federated self-learning anomaly detection system for iot. pages 756–767, 07 2019. doi:[10.1109/ICDCS.2019.00080](https://doi.org/10.1109/ICDCS.2019.00080).
- Yulin Fan, Yang Li, Mengqi Zhan, Huajun Cui, and Yan Zhang. Iotdefender: A federated transfer learning intrusion detection framework for 5g iot. In *2020 IEEE 14th International Conference on Big Data Science and Engineering (BigDataSE)*, pages 88–95, 2020. doi:[10.1109/BigDataSE50710.2020.00020](https://doi.org/10.1109/BigDataSE50710.2020.00020).

- Yi Liu, Sahil Garg, Jiangtian Nie, Yang Zhang, Zehui Xiong, Jiawen Kang, and M. Shamim Hossain. Deep anomaly detection for time-series data in industrial iot: A communication-efficient on-device federated learning approach. *IEEE Internet of Things Journal*, 8(8):6348–6358, 2021. doi:[10.1109/JIOT.2020.3011726](https://doi.org/10.1109/JIOT.2020.3011726).
- Valerian Rey, Pedro Miguel Sánchez Sánchez, Alberto Huertas Celdrán, Gérôme Bovet, and Martin Jaggi. Federated learning for malware detection in iot devices. *arXiv preprint arXiv:2104.09994*, 2021.
- E. Bertino and N. Islam. Botnets and internet of things security. *Computer*, 50(02):76–79, feb 2017. ISSN 1558-0814. doi:[10.1109/MC.2017.62](https://doi.org/10.1109/MC.2017.62).
- H. Brendan McMahan, Eider Moore, Daniel Ramage, and Blaise Agüera y Arcas. Federated learning of deep networks using model averaging. *CoRR*, abs/1602.05629, 2016. URL <http://arxiv.org/abs/1602.05629>.
- Brendan McMahan, Eider Moore, Daniel Ramage, Seth Hampson, and Blaise Agüera y Arcas. Communication-efficient learning of deep networks from decentralized data. In Aarti Singh and Xiaoqin (Jerry) Zhu, editors, *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*, pages 1273–1282. PMLR, 2017. URL <http://proceedings.mlr.press/v54/mcmahan17a.html>.
- Sashank Reddi, Zachary Charles, Manzil Zaheer, Zachary Garrett, Keith Rush, Jakub Konečný, Sanjiv Kumar, and H Brendan McMahan. Adaptive federated optimization. *arXiv preprint arXiv:2003.00295*, 2020.
- Urs Hunkeler, Hong Linh Truong, and Andy Stanford-Clark. Mqtt-s—a publish/subscribe protocol for wireless sensor networks. In *2008 3rd International Conference on Communication Systems Software and Middleware and Workshops (COMSWARE'08)*, pages 791–798. IEEE, 2008.
- Adam Paszke, Sam Gross, Francisco Massa, Adam Lerer, James Bradbury, Gregory Chanan, Trevor Killeen, Zeming Lin, Natalia Gimelshein, Luca Antiga, et al. Pytorch: An imperative style, high-performance deep learning library. *arXiv preprint arXiv:1912.01703*, 2019.
- Rei Ito, Mineto Tsukada, and Hiroki Matsutani. An on-device federated learning approach for cooperative anomaly detection, 02 2020.
- David E Rumelhart, Geoffrey E Hinton, and Ronald J Williams. Learning internal representations by error propagation. Technical report, California Univ San Diego La Jolla Inst for Cognitive Science, 1985.
- Diederik P Kingma and Jimmy Ba. Adam: A method for stochastic optimization. *arXiv preprint arXiv:1412.6980*, 2014.
- Jianyu Wang, Zheng Xu, Zachary Garrett, Zachary B. Charles, Luyang Liu, and Gauri Joshi. Local adaptivity in federated learning: Convergence and consistency. 2021.
- Yujun Lin, Song Han, Huizi Mao, Yu Wang, and William J Dally. Deep gradient compression: Reducing the communication bandwidth for distributed training. *arXiv preprint arXiv:1712.01887*, 2017.
- Hanlin Tang, Shaoduo Gan, Ce Zhang, Tong Zhang, and Ji Liu. Communication compression for decentralized training. *arXiv preprint arXiv:1803.06443*, 2018.