

Dopamine: Differentially Private Secure Federated Learning on Medical Data

Mohammad Malekzadeh, Burak Hasircioglu, Nitish Mital, Kunal Katarya,
Mehmet Emre Ozfatura, Deniz Gündüz

Department of Electrical and Electronic Engineering, Imperial College London.
{m.malekzadeh, b.hasircioglu18, n.mital, kunal.katarya15, m.ozfatura, d.gunduz}@imperial.ac.uk

Abstract

While rich medical datasets are hosted in hospitals distributed across countries, concerns on patients’ privacy is a barrier against utilizing such data to train deep neural networks (DNNs) for medical diagnostics. We propose *Dopamine*, a system to train DNNs on distributed medical data, which employs federated learning (FL) with differentially-private stochastic gradient descent (DPSGD), and, in combination with secure multi-party aggregation, can establish a better privacy-utility trade-off than the existing approaches. Results on a diabetic retinopathy (DR) task show that *Dopamine* provides a privacy guarantee close to the centralized training counterpart, while achieving a better classification accuracy than FL with parallel differential privacy where DPSGD is applied without coordination. Code is available at <https://github.com/ipc-lab/private-ml-for-health>.

1 Introduction

Deep neural networks (DNNs) facilitate disease recognition from medical data, particularly for patients who do not have immediate access to doctors. Medical images are processed with DNNs for faster diagnosis of skin disease (Esteve et al. 2017), lung cancer (Dunnmon et al. 2019), or diabetic retinopathy (DR) (Gulshan et al. 2016). However, the memorization capacity of DNNs can be exploited by adversaries for reconstruction of a patient’s data (Carlini et al. 2019), or the inference of a patient’s participation in the training dataset (Shokri et al. 2017; Dwork et al. 2017). Due to such privacy risks and legal restrictions, medical data can rarely be found in one centralized dataset; thus, there has been a surge of interest in *privacy* and *utility* preserving training on distributed medical datasets (Kaissis et al. 2020).

Federated learning (FL) (McMahan et al. 2017) trains a DNN where hospitals collaborate with a central server in training a global model on their local datasets. At each round, the server sends the current model to each hospital, then hospitals update the model on their private datasets and send the model back to the server. The hospitals’ updates are susceptible to information leakage about the patients’ data due to model over-fitting to training data (Carlini et al. 2019). *Differential privacy* (DP) (Dwork and Roth 2014) limits an adversary’s certainty in inferring a patient’s presence in the training dataset. Before optimizing the DNN, Gaussian random noise is added to the computed gradi-

ents on the patients’ data to achieve differentially-private stochastic gradient descent (DPSGD) (Abadi et al. 2016).

We propose *Dopamine*, a customization of DPSGD for FL, which, in combination with secure aggregation by homomorphic encryption, can establish a better privacy-utility trade-off than the existing approaches, as elaborated in Section 3. Experimental results on the DR dataset (Choi et al. 2017), using SqueezeNet (Iandola et al. 2016) as a benchmark DNN, show that *Dopamine* can achieve a DP bound close to the centralized training counterpart, while achieving better classification accuracy than FL with parallel DP where each hospitals apply typical DPSGD on their side without any specific coordination. We provide theoretical analysis for the guaranteed privacy by *Dopamine*, and discuss the differences between *Dopamine* and the seminal work proposed by (Truex et al. 2019): our solution allows to properly keep track of the privacy loss at each round as well as taking advantage of the *momentum* in FL-based DPSGD (Qian 1999) which improves the DNN’s accuracy.

The main contribution of this paper is the design and implementation of FL on medical images while satisfying patient-level DP. While previous works on medical datasets (as discussed in Appendix, Section B) either do not guarantee a formal notion of privacy, *e.g.* (Li et al. 2020), or apply weaker notion of DP, *e.g.* parameter-level DP (Li et al. 2019), to the best of our knowledge, *Dopamine* is the first system that implements FL-based DPSGD that guarantees patient-level DP for a dataset of medical images. Finally, we publish a simulation environment to facilitate further research on privacy-preserving training on distributed medical image datasets.

2 Dopamine’s Methodology

Problem Formulation¹ Let each hospital $k \in \{1, \dots, K\}$ own a dataset, \mathbb{D}_k , with an unknown number of patients, where each patient i participates with one labeled data (\mathbf{x}_i, y_i) . The global server owns a (small) validation dataset \mathbb{D}_G , and we consider a DNN’s *utility* as its predic-

¹As notation, we use lower-case *italic*, *e.g.* x , for variable scalars; upper-case *italic*, *e.g.* X , for constant scalars; bold font, *e.g.* \mathbf{X} , for vectors, matrices, and tensors; blackboard font, *e.g.* \mathbb{X} , for sets; and calligraphic font, *e.g.* \mathcal{X} , for functions and algorithms.

tion accuracy on \mathbb{D}_G . The goal is to collaboratively train a DNN while satisfying the patient-level DP.

We assume a *threat model* where patients only trust their local hospital, and hospitals are honest and non-colluding. The global server is honest but curious. Finally, hospitals and the server do not trust any other third parties.

We assume the patient's *privacy*, defined by (ϵ, δ) , is a bound on the patient-level DP loss. The hospitals aim to ensure their patients a computational DP against the server during training, and an information-theoretical DP against the server and any other third parties after training. It is called computational DP as a cryptosystem is only robust against computationally-bounded adversaries. *Dopamine* assumes that adversaries are computationally bounded during training, which is a typical assumption, but after training they can be computationally unbounded.

Dopamine's Training

The training procedure is given in Algorithm 1, where we perform distributed SGD among K hospitals². At each round t , each hospital k samples a batch of samples from its local dataset, $\mathbb{D}_k^t \in \mathbb{D}_k$, where each local sample is chosen independently and with probability q . Due to independent sampling, the batch size is not fixed, and is a binomial random variable with parameters q and $|\mathbb{D}_k|$. Let $|\mathbb{D}_k^t|$ and γ denote the batch size and the learning rate, respectively. Let C denote the maximum value of the L_2 -norm of per-sample gradients. If a per-sample gradient has a norm greater than this, then its norm is clipped according to the procedure defined in (Abadi et al. 2016).

As we assume that the hospitals do not trust the server, a potential solution is, for each hospital, to add a large amount of noise to the model updates, \mathbf{w}_k^t , to keep them differentially private from the server. However, adding a large amount of noise has the undesirable effect of decreasing the accuracy of the trained model. A better solution is to employ secure aggregation of the model updates, which prevents the server from discovering the hospital's model updates. Since the model updates are now hidden from the server, the hospitals can add less amount of noise to keep their model updates differentially private from the server, thus increasing the accuracy of the trained model.

Lemma 1. *If each hospital adds Gaussian noise sampled from $\mathcal{N}(\mu = 0, \sigma^2 = \frac{2 \ln(1.25/\delta)C^2}{\epsilon^2 |\mathbb{D}_k^t|^2 K})$ to its local model update before sending it to the server, then the average of the model update revealed to the server and other hospitals is (ϵ, δ) -DP.*

Proof. Let us consider the effect of one patient in hospital k . Let \mathbf{w} be the DNN's parameters, and $\mathbf{w}_k^t - \mathbf{w}_G^{t-1}$ be the (noiseless) model update of the hospital k at round t . Due to secure aggregation, the server and other hospitals receive (unencrypted) $\mathbf{w}_G^t - \mathbf{w}_G^{t-1}$ as

$$\frac{1}{K} \sum_{k=1}^K (\mathbf{w}_k^t - \mathbf{w}_G^{t-1}).$$

²A background on *federated learning*, *differential privacy*, and *secure aggregation* is provided in Appendix, Section B

Algorithm 1 Dopamine's Training

```

1: Input:  $K$ : number of hospitals,  $\mathbb{D}$ : distributed dataset,
    $\mathbf{w}$ : model's trainable parameters,  $\mathcal{L}(\cdot, \cdot)$ : loss function,
    $q$ : sampling probability,  $\sigma$ : noise scale,  $C$ : gradient norm
   bound,  $\eta$ : learning rate,  $\beta$ : momentum,  $T$ : number of
   rounds,  $(\epsilon, \delta)$ : bounds on the patient-level differential
   privacy loss.
2: Output:  $\mathbf{w}$ : final parameters.
3:  $\mathbf{w}_G^0$  = random initialization.
4:  $\hat{\epsilon} = 0$ 
5: for  $t : 1, \dots, T$  do
6:   for  $k : 1, \dots, K$  do
7:      $\mathbf{w}_k^t = \mathbf{w}_G^{t-1}$ 
8:      $\mathbb{D}_k^t = \text{Sampling}(\mathbb{D}_k)$  //by uniformly sampling
       each item in  $\mathbb{D}_k$  independently with probability  $q$ .
9:     for  $\mathbf{x}_i \in \mathbb{D}_k^t$  do
10:       $\mathbf{g}^t(\mathbf{x}_i) = \nabla_{\mathbf{w}} \mathcal{L}(\mathbf{w}_k^t, \mathbf{x}_i)$ 
11:       $\bar{\mathbf{g}}^t(\mathbf{x}_i) = \mathbf{g}^t(\mathbf{x}_i) / \max(1, \frac{\|\mathbf{g}^t(\mathbf{x}_i)\|_2}{C})$ 
12:    end for
13:     $\tilde{\mathbf{g}}_k^t = \frac{1}{|\mathbb{D}_k^t|} (\sum_i \bar{\mathbf{g}}^t(\mathbf{x}_i) + \mathcal{N}(0, \frac{\sigma^2 \cdot C^2 \cdot \mathbf{I}}{K}))$ 
14:     $\hat{\mathbf{g}}_k^t = \tilde{\mathbf{g}}_k^t + \beta \hat{\mathbf{g}}_k^{t-1}$  //  $\hat{\mathbf{g}}_k^0 = 0$ 
15:     $\mathbf{w}_k^t = \mathbf{w}_k^t - \eta \hat{\mathbf{g}}_k^t$ 
16:  end for
17:   $\hat{\epsilon} = \text{CalculatePrivacyLoss}(\delta, q, \sigma, t)$  // by Mo-
    ments Accountant (Abadi et al. 2016)
18:  if  $\hat{\epsilon} > \epsilon$  then
19:    return  $\mathbf{w}_G^{t-1}$ 
20:  end if
21:   $\mathbf{w}_G^t = \frac{1}{K} (\text{SecureAggregation}(\sum_k \mathbf{w}_k^t))$ 
22: end for

```

Since each per-sample gradient is bounded by C and the hospital samples $|\mathbb{D}_k^t|$ data points, $\|\mathbf{w}_k^t - \mathbf{w}_G^{t-1}\|_2 \leq \frac{C}{|\mathbb{D}_k^t|}$, $\forall k \in [K]$. Note that changing one sample in any of the hospitals can only change the gradients at that hospital. Combining these with the triangle inequality, we have

$$\|\mathbf{w}_G^t - \mathbf{w}_G^{t-1}\|_2 \leq \frac{C}{|\mathbb{D}_k^t| K}.$$

Thus, to guarantee a patient-level (ϵ, δ) -DP at each round, the effective noise added to each model update must have a variance of

$$\sigma_{\text{effective}}^2 = \frac{2 \ln(1.25/\delta) C^2}{\epsilon^2 K^2 |\mathbb{D}_k^t|^2}.$$

Since n_k s are independent and identically distributed (iid), then $\text{Var}(\frac{1}{K} \sum_{k=1}^K n_k) = \frac{\sigma^2}{K}$. Thus, every hospital k adds noise $n_k \sim \mathcal{N}(\mu = 0, \sigma^2)$ to its local update, and the effective noise added to the global model update, $\mathbf{w}_G^t - \mathbf{w}_G^{t-1}$, is $\frac{1}{K} \sum_{k=1}^K n_k$. With the σ^2 given in Lemma 1, the variance of the effective noise is $\frac{2 \ln(1.25/\delta) C^2}{\epsilon^2 |\mathbb{D}_k^t|^2 K^2}$, which is what is needed for a patient-level (ϵ, δ) -DP among all hospitals. \square

The Issue with Multiple Local Updates

An approach similar to our Algorithm 1 is proposed by (Truex et al. 2019) (Section 5.2), where they allow each

party to carry out multiple local SGD steps before sharing the updated model with the server. We argue that this approach has an important drawback: it may violate the critical assumption in the *moments accountant* (MA) procedure (Abadi et al. 2016) for tracking the privacy loss at each round, and for the same reason, it does not allow using momentum for SGD (line 14 in our Algorithm 1), which helps to improve the model’s accuracy.

The MA is introduced by (Abadi et al. 2016) for keeping track of a bound on the moments of the *privacy loss random variable*, in the sense of DP, that depends on the random noise added to the algorithm’s output. In the proof provided by (Abadi et al. 2016), the MA is updated by sequentially applying DP mechanism \mathcal{M} . Particularly, (Abadi et al. 2016) model the system by letting the mechanism at round t , \mathcal{M}^t , to have access to the output of all the previous mechanisms $\mathcal{M}^{t-1}, \mathcal{M}^{t-2}, \dots, \mathcal{M}^1$, as the auxiliary input. Hence, to properly calculate the privacy loss at round t , one needs to make sure that the amount of privacy loss in the previous $t - 1$ rounds are properly bounded by adding the proper amount of noise.

In Algorithm 1, we allow each hospital to add a Gaussian noise of variance σ^2/K , at each round, and then share the updated model to securely perform FedAvg (McMahan et al. 2017). Thus, before running any other computation on the DNN, we add the correct amount of effective noise that is needed by MA to calculate the privacy loss (see Lemma 1). However, (Truex et al. 2019) allow the local model to be updated for multiple (e.g. 100) local iterations while at each iteration the DNN model that is used as the input is the output of the previous iterations with a less amount of noise added to the model than what is needed to effectively be added to the model. Therefore, the effect of a sample data point on the model parameters can become larger and larger, as at each local iteration less amount of noise is added to hide the effect of that point; and consequently the sequential property of the proof in MA may be violated.

Fixing this issue, our algorithm allows to take advantage of both privacy loss tracking with the MA and using SGD with momentums. We emphasize that although our Algorithm needs more communications due to sharing model updates after every iteration, this cost can be tolerated considering the importance of the other two aspects in medical data processing: model accuracy and privacy guarantee.

3 Evaluation

Dataset

Diabetic retinopathy is an eye condition that can cause vision loss in diabetic patients. It is diagnosed by examining scans of the blood vessels of a patient’s retina - thereby making this an image classification task. A DR dataset (Choi et al. 2017), available at <https://www.kaggle.com/c/aptos2019-blindness-detection/data>, exists to solve this task. The problem is to classify the images of patients’ retina into five categories: *No DR*, *Mild DR*, *Moderate DR*, *Severe DR*, and *Proliferative DR*. The dataset consists of 2931 variable-sized images for training, and 731 images for testing. To deal with the variation in image dimensions, all

images were resized into the same dimensions of 224×224 during pre-processing.

DNN Architecture

We use SqueezeNet (Iandola et al. 2016): a convolutional neural network architecture that has 50x fewer parameters than the famous AlexNet, but is shown to achieve the same level of accuracy on the ImageNet dataset. The size of the model is a very important factor for both training and inference, which is one of the main motivations for using SqueezeNet. Moreover, SqueezeNet can achieve a classification accuracy of about 80% on the DR dataset while the current best accuracy reported on the Kaggle’s competition³ on this dataset is about 83% using a much larger DNN, EfficientNet-B3, that has 18x more parameters than SqueezeNet⁴.

Baselines

There are several approaches for training a DNN that provide us different trade-offs between utility, privacy, and complexity. We compare *Dopamine* against the following well-known approaches:

Non-Private Centralized Training (C). Every hospital shares their data with the server, such that a centralized dataset \mathbb{D} is available for training. In this method the problem is reduced to architecture search and optimization procedure for training a DNN on \mathbb{D} . This method provides the best utility, a moderate complexity, but no privacy. It results in a single point of failure in the case of data breach. Moreover, in situations where patients are from different countries or private organizations, it is almost impossible reaching an agreement on a single trusted curator.

Centralized Training with DP (CDP). When a trusted curator is available, one can trade some utility in the method C to guarantee central DP for the patients by using a differentially private training mechanism such as DPSGD (Abadi et al. 2016). The complexity of CDP is similar to C, except for the fact that existing DP mechanisms make the training of DNNs slower and less accurate, as they require performing additional tasks such as per-sample gradient clipping and noise addition.

Non-Private FL (F). Considering that a trusted curator is not realistic in many scenarios due to legal, security, and business constraints, hospitals can collaborate via a FL instead of directly sharing their patients’ sensitive data. In F, every hospital has its own dataset that may differ in size and quality. We assume the server runs FedAvg (McMahan et al. 2017). While F introduces some serious communication complexities, it removes the need for trusted curator and enables an important layer of privacy protection. Basically, after sharing the data in the methods C and CDP, hospitals

³<https://www.kaggle.com/c/aptos2019-blindness-detection/notebooks>

⁴We use the Pytorch implementation of SqueezeNet available at https://pytorch.org/docs/stable/_modules/torchvision/models/squeezenet.html

have no more control on the type and amount of information that can be extracted from their patients’ data. However, in F , hospitals do not share the original data, but some aggregated statistics or the results of a computation over the dataset. Even more, hospitals can decide to stop releasing information at any time, thus having more control over the type and amount of information sharing. Although it seems that the utility of F might be lower than that of C , there are many studies showing that with a more sophisticated algorithms, one can achieve the same utility as C .

FL with Parallel DP (FPDP). Similar to CDP, one can apply a DP mechanism to the local training procedure at the hospital side. Thus, every hospital locally provides a central DP guarantee. Notice that this is different from a local DP guarantee (Dwork and Roth 2014), as each hospital is a trusted curator. In FPDP, a much better privacy can be provided than the previous methods. However, as the size of each local dataset \mathbb{D}^i is much smaller than the size of the whole dataset \mathbb{D} , more noise should be added to achieve the same level of privacy, which results in a utility loss.

Results

Dopamine proposes FL with a Central DP guarantee that is similar to F , except the hospitals add noise to their gradients before running a secure aggregation procedure to aggregate the models at the server. *Dopamine* is similar to FPDP in the sense that the hospitals add noise to their gradients, but thanks to secure aggregation, the variance of the noise hospitals add is less than FPDP by an order of K .

Figure 1 compares the classification accuracy (top plot) and DP bound (bottom plot) of all the introduced methods for SqueezeNet trained on the DR dataset. We show the mean and standard deviation of these 5 runs for each method. To be fair, for each method we tuned the hyper-parameters to achieve the best accuracy of that method. For FL scenarios, we have divided the dataset equally among 10 hospitals ($K = 10$) in an iid manner, thus each hospital owns 293 images. For F and FPDP we perform FedAvg (McMahan et al. 2017) where each hospital performs 5 local epochs in between each global epoch, and at each round half of the hospitals are randomly chosen to participate. The details of the hyper-parameters used and the source code to reproduce the results are provided at https://github.com/ipc-lab/private-ml-for-health/tree/main/private_training/

We see that *Dopamine*’s bound is very close to that of the centralized training counterpart CDP, and even better than CDP at early epochs. *Dopamine* achieves a better classification accuracy than FPDP and more importantly much better patient-level privacy guarantee. Notice that, in FPDP, one needs to add noise with a variance K times larger to get the same privacy level of CDP which, in our experiments, we found that this amount of noise makes learning impossible. Finally, we see that F , compared to C , has a competitive performance but there still is a considerable accuracy gap between F and *Dopamine* which is due to privacy protection provided. Such a gap can be mitigated if we could get access to a larger dataset and proportionally reduce the amount of

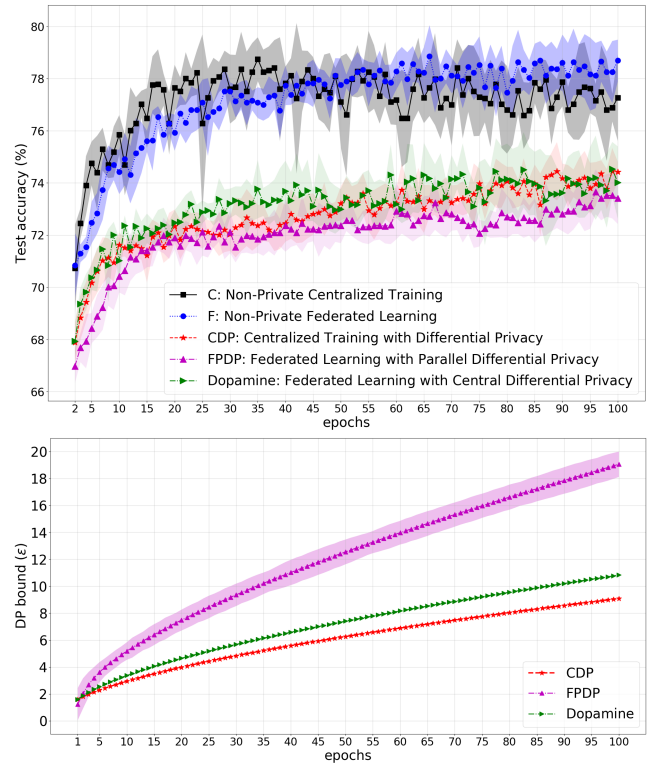


Figure 1: Comparison of (top) classification accuracy vs. (bottom) DP bound on DR dataset. *Dopamine* achieves a very close DP bound, of the centralized training counterpart, while it also get better classification accuracy than federated learning with parallel DP. For all DP methods, $\delta = 10^{-4}$.

noise without weakening privacy protection.

4 Conclusion and Future Work

In this paper, we proposed *Dopamine*, a novel scheme to collaboratively train DNNs on private datasets of medical images distributed across several hospitals. Experiments on a benchmark dataset of DR images show that *Dopamine* can outperform existing baselines by providing a better utility-privacy trade-off.

There are some important directions to follow as future work: (i) we aim to combine the proposed secure aggregation functionality (discussed in Appendix C) to the *Dopamine*’s training pipeline. (ii) Current privacy-analysis only allows us to have one local iteration. We observed that allowing local hospitals to perform more than one iteration can improve the accuracy by about 3%. We will carry out the privacy analysis for this case in the future. (iii) Existing DP libraries do not allow using arbitrary DNN architectures. They are either not compatible with more recent architectures, like EfficientNet, or they need too much resources. Making DP training faster is still an open area of research and engineering. (iv) Finally, we aim to evaluate *Dopamine* on other medical datasets, and investigate novel method for accuracy improvement while retaining the privacy protection provided.

References

- Abadi, M.; Chu, A.; Goodfellow, I.; McMahan, H. B.; Mironov, I.; Talwar, K.; and Zhang, L. 2016. Deep learning with differential privacy. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, 308–318.
- Bittau, A.; Erlingsson, U.; Maniatis, P.; Mironov, I.; Raghunathan, A.; Lie, D.; Rudominer, M.; Kode, U.; Tinnes, J.; and Seefeld, B. 2017. Prochlo: Strong privacy for analytics in the crowd. In *Proceedings of the 26th Symposium on Operating Systems Principles*, 441–459. ACM.
- Bonawitz, K.; Eichner, H.; Grieskamp, W.; Huba, D.; Ingerman, A.; Ivanov, V.; Kiddon, C.; Konecny, J.; Mazzocchi, S.; McMahan, H. B.; Van Overveldt, T.; Petrou, D.; Ramage, D.; and Roselander, J. 2019. Towards federated learning at scale: System design. In *Proceedings of the 2nd SysML Conference, Palo Alto, CA, USA*.
- Carlini, N.; Liu, C.; Erlingsson, Ú.; Kos, J.; and Song, D. 2019. The secret sharer: Evaluating and testing unintended memorization in neural networks. In *28th USENIX Security Symposium (USENIX Security 19)*, 267–284.
- Choi, J. Y.; Yoo, T. K.; Seo, J. G.; Kwak, J.; Um, T. T.; and Rim, T. H. 2017. Multi-categorical deep learning neural network to classify retinal images: A pilot study employing small database. *PLOS ONE* 12: 1–16.
- Choudhury, O.; Gkoulalas-Divanis, A.; Salonidis, T.; Sylla, I.; Park, Y.; Hsu, G.; and Das, A. 2020. Anonymizing Data for Privacy-Preserving Federated Learning. *arXiv preprint arXiv:2002.09096*.
- Cormode, G.; Jha, S.; Kulkarni, T.; Li, N.; Srivastava, D.; and Wang, T. 2018. Privacy at scale: Local differential privacy in practice. In *Proceedings of the 2018 International Conference on Management of Data*, 1655–1658.
- Ding, B.; Kulkarni, J.; and Yekhanin, S. 2017. Collecting telemetry data privately. In *Advances in Neural Information Processing Systems*, 3571–3580.
- Doröz, Y.; Çetin, G. S.; and Sunar, B. 2016. On-the-fly Homomorphic Batching/Unbatching. In *Financial Cryptography Workshops*.
- Dunmon, J. A.; Yi, D.; Langlotz, C. P.; Ré, C.; Rubin, D. L.; and Lungren, M. P. 2019. Assessment of convolutional neural networks for automated classification of chest radiographs. *Radiology* 290(2): 537–544.
- Dwork, C.; McSherry, F.; Nissim, K.; and Smith, A. 2006. Calibrating noise to sensitivity in private data analysis. In *Theory of cryptography conference*, 265–284. Springer.
- Dwork, C.; and Roth, A. 2014. The algorithmic foundations of differential privacy. *Foundations and Trends in Theoretical Computer Science* 9(3-4): 211–407.
- Dwork, C.; Smith, A.; Steinke, T.; and Ullman, J. 2017. Exposed! a survey of attacks on private data.
- Erlingsson, Ú.; Feldman, V.; Mironov, I.; Raghunathan, A.; Talwar, K.; and Thakurta, A. 2019. Amplification by shuffling: From local to central differential privacy via anonymity. In *Proceedings of the Thirtieth Annual ACM-SIAM Symposium on Discrete Algorithms*, 2468–2479. SIAM.
- Erlingsson, Ú.; Pihur, V.; and Korolova, A. 2014. Rappor: Randomized aggregatable privacy-preserving ordinal response. In *Proceedings of the 2014 ACM SIGSAC conference on computer and communications security*, 1054–1067.
- Esteva, A.; Kuprel, B.; Novoa, R. A.; Ko, J.; Swetter, S. M.; Blau, H. M.; and Thrun, S. 2017. Dermatologist-level classification of skin cancer with deep neural networks. *nature* 542(7639): 115–118.
- Fan, J.; and Vercauteren, F. 2012. Somewhat Practical Fully Homomorphic Encryption. *Cryptology ePrint Archive*, Report 2012/144.
- Gao, D.; Ju, C.; Wei, X.; Liu, Y.; Chen, T.; and Yang, Q. 2019. HHHFL: Hierarchical Heterogeneous Horizontal Federated Learning for Electroencephalography. *arXiv preprint arXiv:1909.05784*.
- Gentry, C. 2009. *A Fully Homomorphic Encryption Scheme*. Ph.D. thesis, Stanford, CA, USA.
- Gulshan, V.; Peng, L.; Coram, M.; Stumpe, M. C.; Wu, D.; Narayanaswamy, A.; Venugopalan, S.; Widner, K.; Madams, T.; Cuadros, J.; Kim, R.; Raman, R.; Nelson, P. C.; Mega, J. L.; and Webster, D. R. 2016. Development and Validation of a Deep Learning Algorithm for Detection of Diabetic Retinopathy in Retinal Fundus Photographs. *JAMA* 316(22): 2402–2410.
- 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 0.5 MB model size. *arXiv preprint arXiv:1602.07360*.
- Kaissis, G. A.; Makowski, M. R.; Rückert, D.; and Braren, R. F. 2020. Secure, privacy-preserving and federated machine learning in medical imaging. *Nature Machine Intelligence* 1–7.
- Kifer, D.; Messing, S.; Roth, A.; Thakurta, A.; and Zhang, D. 2020. Guidelines for Implementing and Auditing Differentially Private Systems. *arXiv preprint arXiv:2002.04049*.
- Li, W.; Milletari, F.; Xu, D.; Rieke, N.; Hancox, J.; Zhu, W.; Baust, M.; Cheng, Y.; Ourselin, S.; Cardoso, M. J.; et al. 2019. Privacy-preserving federated brain tumour segmentation. In *International Workshop on Machine Learning in Medical Imaging*, 133–141. Springer.
- Li, X.; Gu, Y.; Dvornek, N.; Staib, L.; Ventola, P.; and Duncan, J. S. 2020. Multi-site fmri analysis using privacy-preserving federated learning and domain adaptation: Abide results. *arXiv preprint arXiv:2001.05647*.
- Lyubashevsky, V.; Peikert, C.; and Regev, O. 2013. On Ideal Lattices and Learning with Errors over Rings. *J. ACM* 60(6). ISSN 0004-5411.
- McMahan, B.; Moore, E.; Ramage, D.; Hampson, S.; and y Arcas, B. A. 2017. Communication-efficient learning of

deep networks from decentralized data. In *Artificial Intelligence and Statistics*, 1273–1282. PMLR.

Pfohl, S. R.; Dai, A. M.; and Heller, K. 2019. Federated and Differentially Private Learning for Electronic Health Records. *arXiv preprint arXiv:1911.05861*.

Qian, N. 1999. On the momentum term in gradient descent learning algorithms. *Neural networks* 12(1): 145–151.

Regev, O. 2009. On Lattices, Learning with Errors, Random Linear Codes, and Cryptography. *J. ACM* 56(6). ISSN 0004-5411.

SEAL. 2020. Microsoft SEAL (release 3.5). <https://github.com/Microsoft/SEAL>. Microsoft Research, Redmond, WA.

Sheller, M. J.; Reina, G. A.; Edwards, B.; Martin, J.; and Bakas, S. 2018. Multi-institutional deep learning modeling without sharing patient data: A feasibility study on brain tumor segmentation. In *International MICCAI Brainlesion Workshop*, 92–104. Springer.

Shokri, R.; Stronati, M.; Song, C.; and Shmatikov, V. 2017. Membership inference attacks against machine learning models. In *2017 IEEE Symposium on Security and Privacy (SP)*, 3–18. IEEE.

Titus, A. J.; Kishore, S.; Stavish, T.; Rogers, S. M.; and Ni, K. 2018. PySEAL: A Python wrapper implementation of the SEAL homomorphic encryption library.

Truex, S.; Baracaldo, N.; Anwar, A.; Steinke, T.; Ludwig, H.; Zhang, R.; and Zhou, Y. 2019. A Hybrid Approach to Privacy-Preserving Federated Learning. In *Proceedings of the 12th ACM Workshop on Artificial Intelligence and Security, AISec’19*, 1–11. New York, NY, USA: Association for Computing Machinery. ISBN 9781450368339.

Wang, T.; Blocki, J.; Li, N.; and Jha, S. 2017. Locally differentially private protocols for frequency estimation. In *26th USENIX Security Symposium (USENIX Security 17)*, 729–745.

A Related Work

(Sheller et al. 2018) apply FL, without any privacy guarantee, for the segmentation of brain tumor images using a deep convolutional neural network, known as U-Net. They compare FL with a baseline collaborative learning scenario where hospitals iteratively train a shared model in turn, and show that FL outperforms such baseline. (Pfohl, Dai, and Heller 2019) employ FL with FedAvg and DPSGD algorithms to train logistic regression and feedforward networks with one hidden layer for in-hospital mortality and prolonged length of stay prediction using the patients electronic health records. Comparing FL with a centralized approach, when DP is used in both cases, their experimental results show that while centralized training can achieve a good DP bound with $\epsilon \approx 1$, but FL with DP performs poorly in terms of both accuracy and ϵ . Considering the differences in type of the device, number of sensors, and the placement of the sensors that is used in each hospital for collecting Electroencephalography (EEG) data, (Gao et al. 2019) propose an application of a FL for training a classifier over heterogeneous

data; however they do not consider any formal privacy guarantee. (Li et al. 2020) use FL among hospitals for training an fMRI image classification and add some noise to the trained parameters before sharing them with the server which does not follow the requirement of a valid differentially private mechanism, thus it does not provide a formal privacy guarantee. (Choudhury et al. 2020) offer a k-anonymity based privacy guarantee to generate a syntactic tabular dataset, instead of the original dataset, and use it for participating in a FL. (Li et al. 2019) proposes an FL system for brain tumour segmentation in a method where each hospital owns a dataset of MRI scans. However, their implementation does not satisfy patient-level DP, but parameter-level DP, which for neural networks is not a meaningful privacy protraction.

B Background

Differential Privacy

When we want to publish the results of a computation $\mathcal{F}(\mathbb{D})$, over a private dataset \mathbb{D} , differential privacy (DP) helps us to bound the ability of an adversary in distinguishing whether any specific sample data was included in the dataset \mathbb{D} or not. DP has a worst-case threat model, assuming that all-but-one can collude and adversaries can have access to any source of side-channel information.

Definition 1 (Differential Privacy). Given $\epsilon, \delta \geq 0$, a mechanism (i.e. algorithm) \mathcal{M} satisfies (ϵ, δ) -differential privacy if for all pairs of neighboring datasets \mathbb{D} and \mathbb{D}' differing in only one sample, and for all $\mathbb{Y} \subset \text{Range}(\mathcal{M})$, we have

$$\Pr(\mathcal{M}(\mathbb{D}) \in \mathbb{Y}) \leq e^\epsilon \Pr(\mathcal{M}(\mathbb{D}') \in \mathbb{Y}) + \delta, \quad (1)$$

where ϵ is the parameter that specifies the privacy loss (i.e. e^ϵ), δ is the probability of failure in assuring the upper-bound on the privacy loss, and the probability distribution \Pr is over the internal randomness of the mechanism \mathcal{M} , holding the dataset fixed (Dwork et al. 2006; Dwork and Roth 2014). When $\delta = 0$, it is called pure DP, which is a stronger but less flexible in terms of the mechanism design.

For approximating a deterministic function \mathcal{F} , such as the mean or sum, a typical example of \mathcal{M} in Equation (1) is a zero-mean Laplacian or Gaussian noise addition mechanism (Dwork and Roth 2014), where the variance is chosen according to the sensitivity of \mathcal{F} that is the maximum of the absolute distance $|\mathcal{F}(\mathbb{D}) - \mathcal{F}(\mathbb{D}')|$ among all pairs of neighboring datasets \mathbb{D} and \mathbb{D}' (Dwork et al. 2006). In general, to be able to calculate the sensitivity of \mathcal{F} , we need to know, or to bound, the $\text{Range}(\mathcal{F})$; otherwise we cannot design a reliable DP mechanism.

Definition 2 (Gaussian Mechanism). Gaussian mechanism adds a Gaussian noise to a function $\mathcal{F}(x)$ so that the response to be released is (ϵ, δ) -differentially private. It is defined as

$$\mathcal{M}(x) = \mathcal{F}(x) + \mathcal{N}(\mu = 0, \sigma^2 = \frac{2 \ln(1.25/\delta)(\Delta_2 f)^2}{\epsilon^2}),$$

where $\Delta_2(\mathcal{F})$ is the L_2 sensitivity of $\mathcal{F}(x)$ to the neighboring datasets (Dwork and Roth 2014).

DP mechanisms are in two types: central DP and local DP. In central DP, we consider a model where there is a trusted server, thus the patients original data is shared with that server. The trusted server then run \mathcal{M} on the collected data before sharing the result with other parties. In local DP, every patient randomly transforms data at the patient's side without needing to trust the server or other parties (Erlingsson, Pihur, and Korolova 2014; Wang et al. 2017; Erlingsson et al. 2019). Thus, in terms of privacy guarantee, local DP ensures that the probability of discovering the true value of the user's shared data is limited to a mathematically defined upper-bound. However, central DP gives such an upper-bound for the probability of discovering whether a specific user has shared their data or not.

DP mechanisms are mostly used for computing aggregated statistics, such as the sum, mode, mean, most frequent, or histogram of the dataset (Bittau et al. 2017; Ding, Kulkarini, and Yekhanin 2017; Cormode et al. 2018). DP mechanisms can also be used for training machine learning models on sensitive datasets while providing differential privacy guarantees for the people that are included in the training dataset (Abadi et al. 2016; Bonawitz et al. 2019; Kifer et al. 2020).

Federated Learning

Many parameterized machine learning problems can be modeled as a *stochastic optimization problem*

$$\min_{\mathbf{w} \in \mathbb{R}^d} := \mathbb{E}_{\mathbb{D} \sim \mathcal{D}} \mathcal{L}(\mathbf{w}, \mathbb{D}), \quad (2)$$

where \mathbf{w} denotes the model parameters, \mathbb{D} is a random dataset sampled from the true, but unknown, data distribution \mathcal{D} , and \mathcal{L} is a task-specific empirical loss function.

The core idea of the federated learning strategy is to solve the stochastic optimization problem, Equation (2), in a distributed manner such that participating users do not share their local data set with each other but the model parameters to seek a consensus. Accordingly, the objective of K users that collaborate to solve Equation (2) is reformulated as the sum of K loss functions that defined over different sample datasets, where each corresponds to a different user:

$$\min_{\mathbf{w}} \mathcal{L}(\mathbf{w}) = \frac{1}{K} \sum_{k=1}^K \mathbb{E}_{\mathbb{D}_k \sim \mathcal{D}_k} \mathcal{L}(\mathbf{w}, \mathbb{D}_k) \quad (3)$$

where \mathcal{D}_k denotes the portion of the dataset allocated to the user k . Stochastic Gradient Decent (SGD) is a common approach to solve machine learning problems that are represented in the form of Equation (2). Hence, FL considers the problem that written according to the distributed scenario in Equation (3) and aim to solve it using SGD method in a decentralized way.

Homomorphic Encryption

Fully Homomorphic Encryption (FHE) allows computation of arbitrary functions \mathcal{F} on encrypted data, thus enabling a plethora of applications like private computation offloading. Gentry (Gentry 2009) was the first to show that FHE is possible with a method that includes the following steps:

(i) to construct a somewhat homomorphic encryption (SHE) scheme that can evaluate functions of low degree, (ii) to simplify the decryption circuit, (iii) to evaluate the decryption circuit on the encrypted ciphertexts homomorphically to obtain new ciphertexts with a reduced inherent noise. The third step is called bootstrapping, and this allows computations of functions of arbitrary degree. Here, the degree of a function is the number of operations that must be performed in sequence to compute the function. For example, to compute x^2 , one multiplication is necessary, therefore its degree is 1, while to compute x^3 , 2 multiplications ($x * x$ and $x * x^2$) are necessary, and therefore its degree is 2.

The security of homomorphic encryption schemes is based on the Learning With Errors (LWE) problem (Regev 2009), or its ring variant called Ring Learning With Errors (RLWE) (Lyubashevsky, Peikert, and Regev 2013), the hardness of which can be shown to be equivalent to that of classical hard problems on ideal lattices, which are the basis for a lot of post-quantum cryptography. All FHE schemes add a *small noise* component during encryption of a message with a *public key*, which makes the decryption very hard unless one has access to a *secret key*. The decrypted message obtained consists of the message corrupted by a small additive noise, which can be removed if the noise is "small enough". Each computation on ciphertexts increases the noise, which ultimately grows large enough to fail the decryption. The bootstrapping approach is used to lower the noise in the ciphertext to a fixed level. Addition of ciphertexts increases the noise level very slowly, while multiplication of ciphertexts increases the noise very fast. When FHE is only used for aggregation, the bootstrapping step, which is a computationally expensive procedure, is not usually necessary since the noise never grows to a large enough size.

While machine learning models compute on floating point parameters, encryption schemes work only on fixed point parameters, or equivalently, integer parameters, which can be obtained by appropriately scaling and rounding fixed point values. Given an integer u to encode and an integer base b , a base- b expansion of u is computed, and represented as a polynomial with the same coefficients. The expansion uses a 'balanced' representation of integers modulo b as the coefficients, that is, when b is odd, the coefficients are chosen to lie in the range $\left[-\frac{(b-1)}{2}, \frac{(b-1)}{2}\right]$, and when b is even, the coefficients are chosen to lie in the range $\left[-\frac{b}{2}, \frac{(b-1)}{2}\right]$, except if b is two, when the coefficients are chosen to lie in the set $\{0, 1\}$. For example, if $b = 2$, the integer $26 = 2^4 + 2^3 + 2^1$ is encoded as the polynomial $x^4 + x^3 + x$. If $b = 3$, $26 = 3^3 - 3^0$ is encoded as the polynomial $x^3 - 1$. Decoding is done by computing the polynomial representation at $x = b$. To map an integer to a polynomial ring $R = \mathbb{Z}[x]/f(x)$, where $f(x)$ is a monic polynomial of degree d , the polynomial representation of the integer is viewed as being a plaintext polynomial in R . The base b is called the *plaintext modulus*. The most popular choice of $f(x)$ is $x^d + 1$, with $d = 2^n$ called the *polynomial modulus*. Let $q > 1$ be a positive integer, then we denote the set of integers $[-\frac{q}{2}, \frac{q}{2}]$ by \mathbb{Z}_q , and the set of polynomials in

R with coefficients in \mathbb{Z}_q by R_q . The integer q is called the *coefficient modulus*, and is usually set much larger than the plaintext modulus.

For multi-dimensional vectors, the Single-Instruction-Multiple-Data (SIMD) technique, also known as *batching* (Doröz, Çetin, and Sunar 2016), encodes a given array of multiple integers into a single plaintext polynomial in R_q . A single computation instruction on such a plaintext polynomial is equivalent to simultaneously executing that instruction on all the integers in that array, thus speeding up the computation by many orders of magnitude. The plaintext modulus is assumed to be larger than any integer in the given array. The length of the array is assumed to be equal to the degree of the polynomial modulus d , and in case that its size is less than d , then it is padded with zeros to make its length equal to d . Lagrange interpolation is performed over the array of integers to obtain a polynomial of degree $d - 1$, thus obtaining the plaintext polynomial in R_q encoding d integers.

C Secure Aggregation

Secure aggregation helps in providing a computational DP guarantee, even during the training procedure, so that the hospitals do not need to trust the server. We use the Brakerski-Fan-Vercauteren (BFV) scheme (Fan and Vercauteren 2012) for homomorphic encryption. For security parameter λ , random element $s \in R_q$, $\Delta = \lfloor \frac{q}{b} \rfloor$, and a discrete probability distribution $\chi = \chi(\lambda)$, the BFV scheme is implemented as follows:

- **SecretKeyGen** (1^λ): sample $s \leftarrow \chi$, and output $sk = s$.
- **PublicKeyGen** (sk): sample $a \leftarrow R_q$, $e \leftarrow \chi$, and output

$$pk = \left([-(as + e)]_q, a \right). \quad (4)$$

- **Encrypt**(pk, m): To encrypt a message $m \in R_b$, let $p_0 = pk[0]$ and $p_1 = pk[1]$, and sample $u, e_1, e_2 \leftarrow \chi$, and output

$$ct = \left([p_0 u + e_1 + \Delta \cdot m]_q, [p_1 u + e_2]_q \right). \quad (5)$$

- **Decrypt**(sk, ct): Set $s = sk$, $c_0 = ct[0]$, and $c_1 = ct[1]$, and compute

$$\left[\left[\frac{b \cdot [c_0 + c_1 s]_q}{q} \right] \right]_b. \quad (6)$$

We use the open source PySEAL library (Titus et al. 2018), which provides a python wrapper API for the original SEAL library published by Microsoft (SEAL). We simulate the federated learning environment over the message passing interface (MPI), with the rank 0 process modeling the server, and the rank $1, \dots, K$ processes modeling hospitals that participate in the training. The plaintext modulus b is chosen to be 40961, while the polynomial modulus d is chosen to be $x^{4096} + 1$. Therefore, each ciphertext can pack $d = 4096$ integers with magnitude less than 40961 for SIMD operations, thus speeding up the communication and computation on encrypted data by 4096 times. The methodology is as follows:

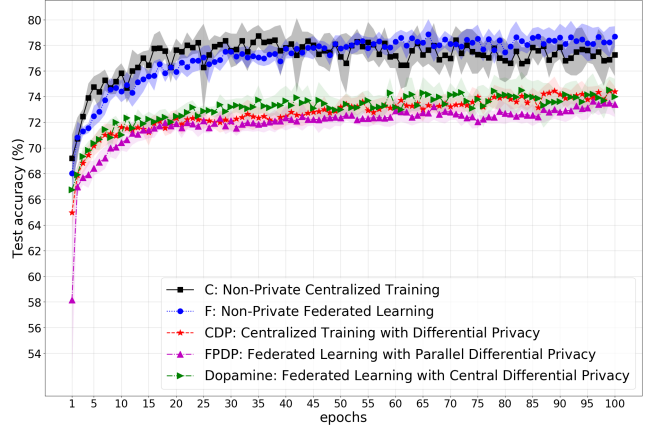


Figure 2: The top plot in Figure 1, but starting from epoch 1.

1. **Key generation and distribution:** A public key and secret key are generated by the rank 1 process (hospital 1). The public key is broadcasted to all involved parties, while the secret key is shared with the hospitals but not the server.
2. The server initializes the model to be trained, and sends the model to the hospitals in the first round.
3. Each hospital performs an iteration on its local model based on Algorithm 1, at the end of which each hospital has the updated model.
4. Each active hospital:
 - flattens the tensor of model parameters into a 1D array w ,
 - converts the floating point values in the array to 3 digit integers by multiplying each value by 10^3 , and then rounding it to the nearest integer.
 - partitions the array w into chunks of $d = 4096$ parameters, denoted by w_1, \dots, w_l , where $l = \lceil \frac{\text{length}(w)}{4096} \rceil$,
 - encrypts the chunks w_1, \dots, w_l , with the public key, into ciphertexts ct_1, \dots, ct_l , respectively, using the batching technique, and sends the list of ciphertexts to the server.
5. The server adds the received encrypted updates and sends the encrypted aggregated model to the hospitals for the next round.
6. The hospitals decrypt the received aggregate array w , scale and convert each integer value to a floating point value of correct precision, divide each value by the number of hospitals that were active in the previous round, and finally reshape w back to the structure of the original model.
7. Go to step 3.

At the end of the above procedure the hospitals send the final unencrypted updated models to the server, who aggregates them and updates the global model for the final time to obtain the final trained model.