Imperial College London

Dopamine: Differentially Private Federated Learning on Medical Data

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

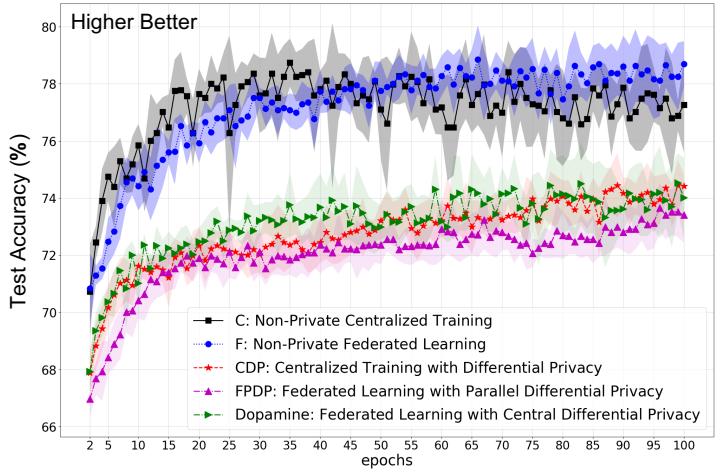
Problem: K **hospitals** each owns a private dataset of **medical images:** $(\mathbf{X}, \mathbf{y})$
A server orchestrates training of a **Deep Neural Net** while preserving privacy.

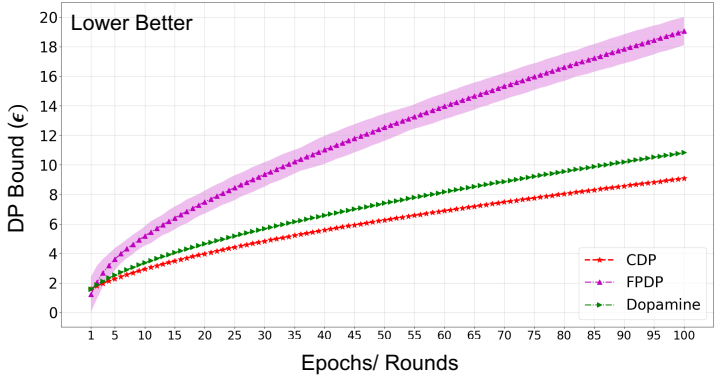
Idea: Using **DP-SGD**, with a noise scaled to the number of participating hospitals, and performing a **secure federated DPSGD** at each round.

Our Solution (Dopamine) compared to other **baselines**:

1) Centralized Learning without Privacy
2) Federated Learning without Privacy
3) Centralized Learning with Differential Privacy
4) Federated Learning with Parallel Differential Privacy

- **(1)** & **(3)** are not achievable in practice (e.g. due to law)
- **(2)** & **(4)** does not provide any (meaningful) privacy
- **Dopamine** achieves the best **utility-privacy trade-off.**





Code:
https://github.com/ipc-lab/private-ml-for-health

Model: SqueezeNet
Input Size :224 x 224
(Iandola, F. N., et al. 2016)

Dataset: (5 classes)
Diabetic Retinopathy
(Choi, J. Y.; et. al. . 2017)