Rishabh Gupta

Department of Computer Science and Engineering
The University of Aizu
Aizuwakamatsu, Japan

Federated Learning with Differential Privacy based Data Protection Model for Enhancing Utility and Convergence

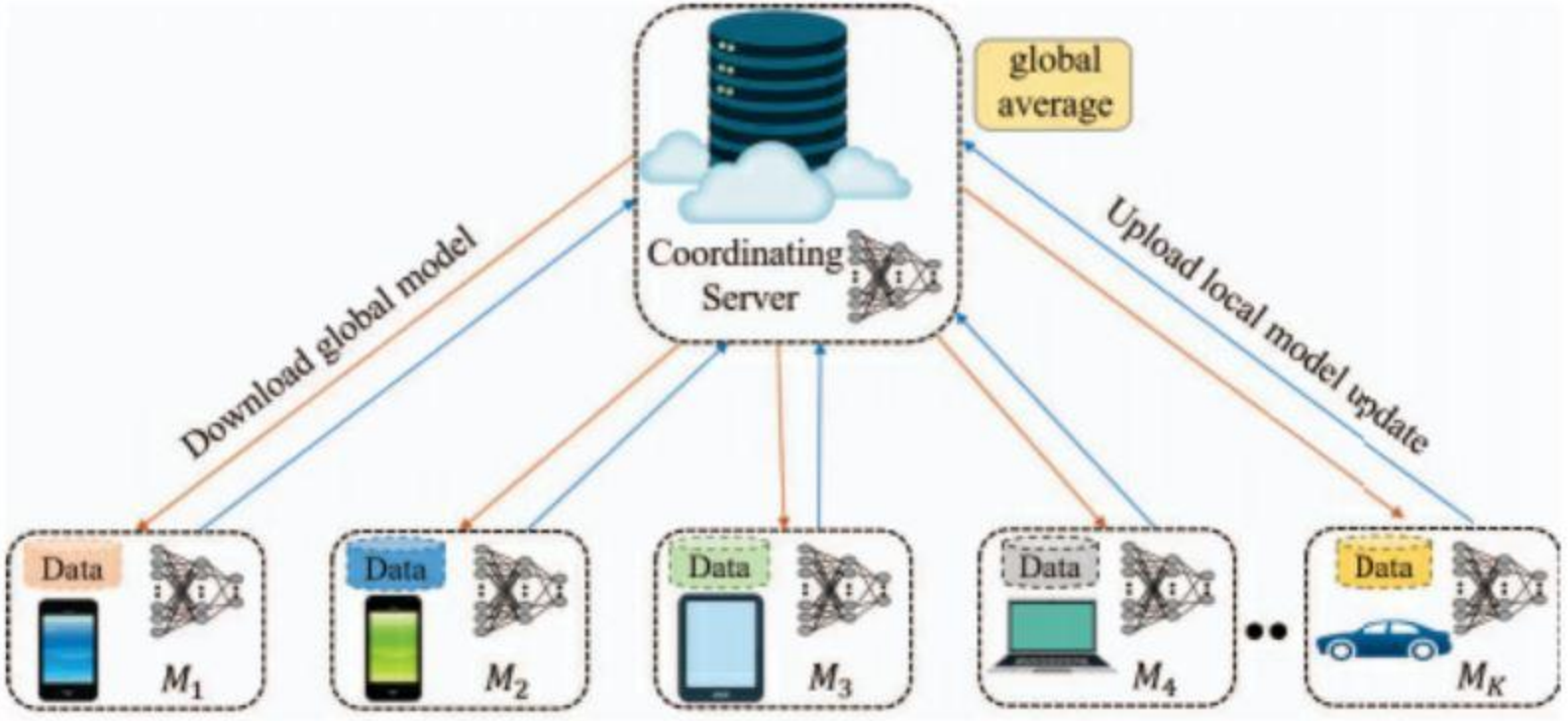
Outline

Outline

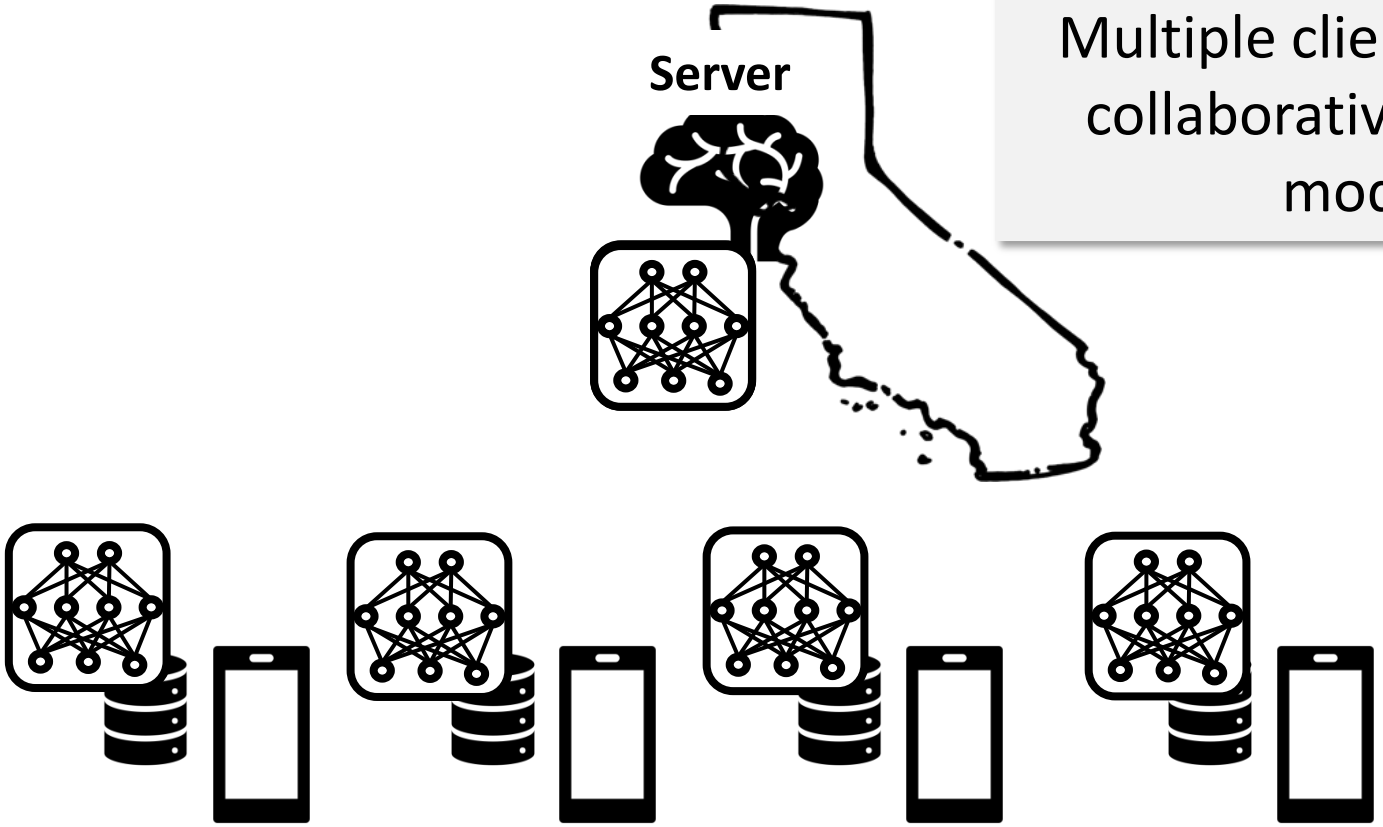
- Introduction and Motivation
  - ✓ Challenges of conventional Machine Learning
- Novel Work
  - ✓ Proposed Model
  - ✓ Experimental parameters and Results
- Summary

Federated Learning

A machine learning technique that trains an algorithm via multiple independent sessions, each using its own dataset



Federated Learning

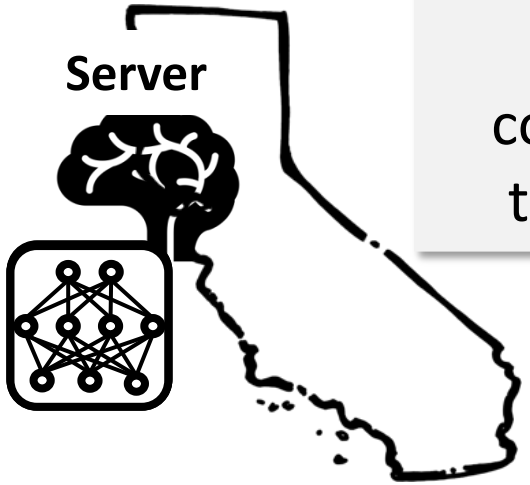


Multiple clients want to collaboratively train a model

Federated Learning

In each iteration

Download global model from server



Multiple clients want to collaboratively train a model

Federated Learning

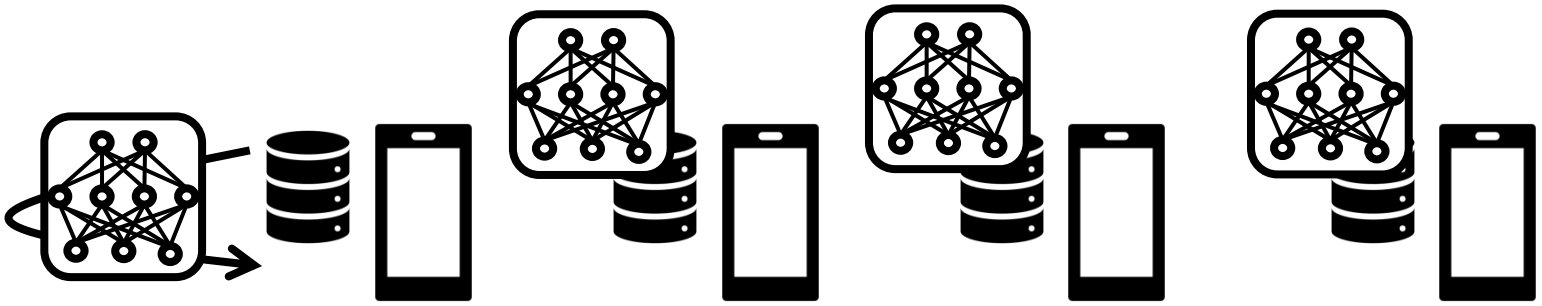
Multiple clients want to collaboratively train a model

In each iteration

Share model updates

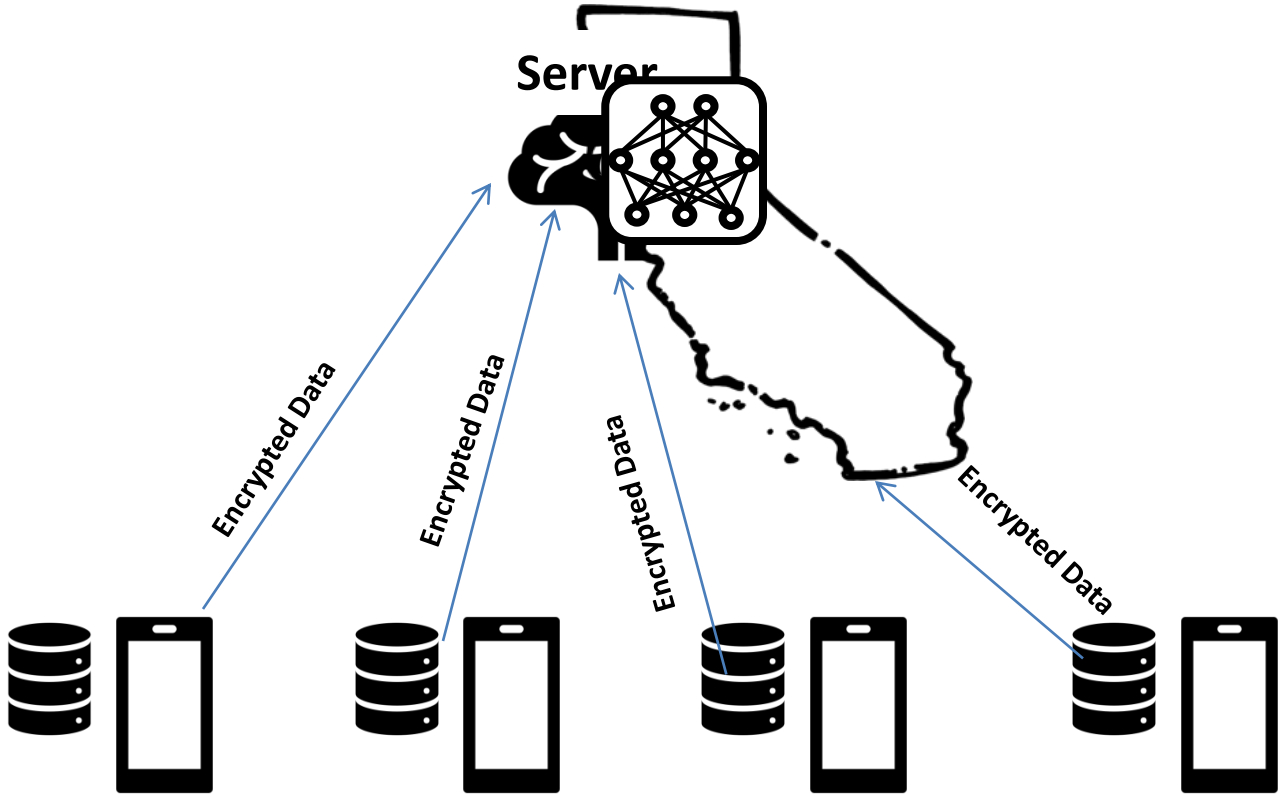
Server

Sharing updates rather than data... **how much privacy gained?**



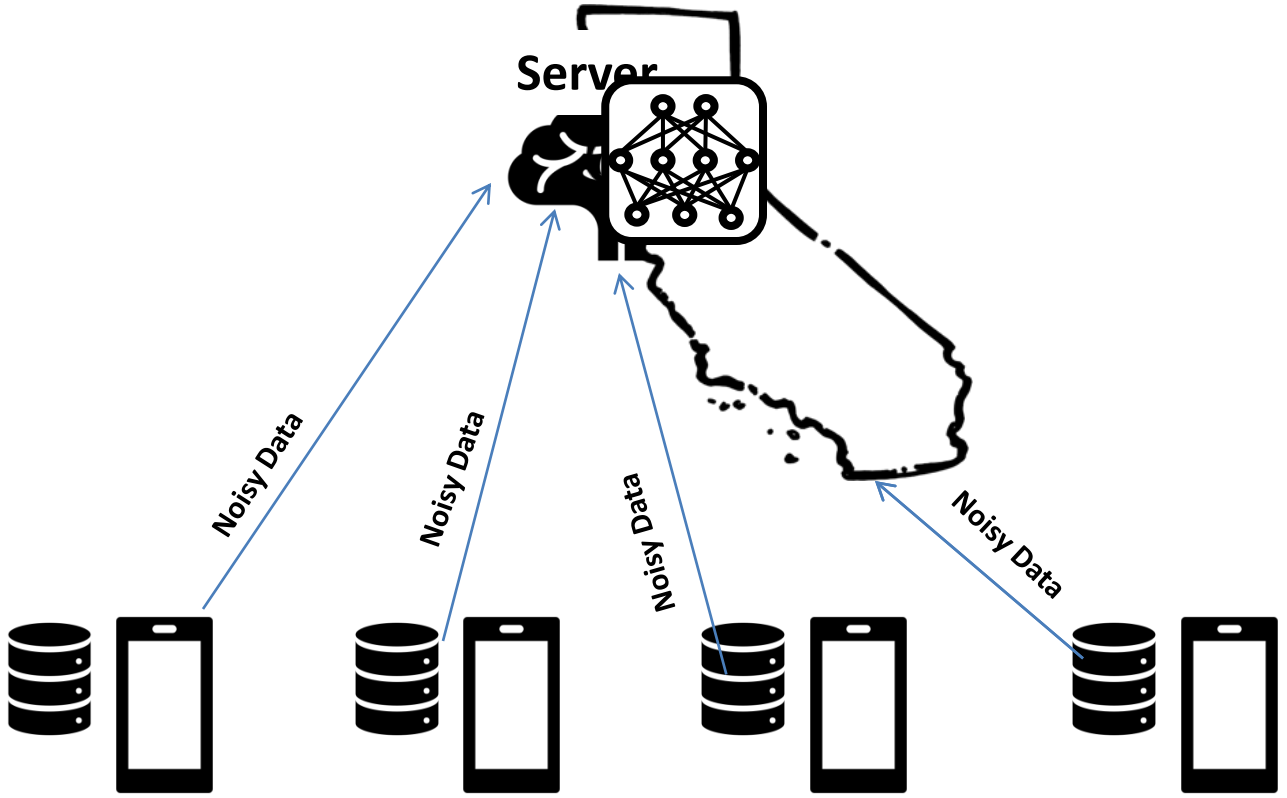
Train on a batch

Motivation



[1] Liang, J., Qin, Z., Xue, L., Lin, X. and Shen, X., 2021. Verifiable and secure svm classification for cloud-based health monitoring services. *IEEE Internet of Things Journal*, *8*(23), pp.17029-17042.
[2] Prabhakaran, V. and Kulandasamy, A., 2021. Hybrid semantic deep learning architecture and optimal advanced encryption standard key management scheme for secure cloud storage. *Neural Computing and Applications*, *33*(21), pp.14459-14479.
[3] Qiu, H., Qiu, M. and Lu, Z., 2020. Selective encryption on ECG data in body sensor network based on supervised machine learning. *Information Fusion*, *55*, pp.59-67.

Motivation



[1] Wu, X., Zhang, Y., Shi, M., Li, P., Li, R. and Xiong, N.N., 2022. An adaptive federated learning scheme with differential privacy preserving. *Future Generation Computer Systems*, *127*, pp.362-372.
[2] Zhao, Y., Zhao, J., Yang, M., Wang, T., Wang, N., Lyu, L., Niyato, D. and Lam, K.Y., 2020. Local differential privacy-based federated learning for internet of things. *IEEE Internet of Things Journal*, *8*(11), pp.8836-8853.
[3] Arachchige, P.C.M., Bertok, P., Khalil, I., Liu, D., Camtepe, S. and Atiquzzaman, M., 2019. Local differential privacy for deep learning. *IEEE Internet of Things Journal*, *7*(7), pp.5827-5842.
[4] Zhang, T., Zhu, T., Xiong, P., Huo, H., Tari, Z. and Zhou, W., 2019. Correlated differential privacy: Feature selection in machine learning. IEEE Transactions on Industrial Informatics, 16(3), pp.2115-2124.

Challenges in Federated learning

Challenges:

- **Size of data:** Each users has very limited data
- **Privacy Concerns:** Sensitive information can still be revealed to third party or central server during the communication.
- **Expensive Communication:** communication in the network can be slower than local computation by many orders of magnitude.

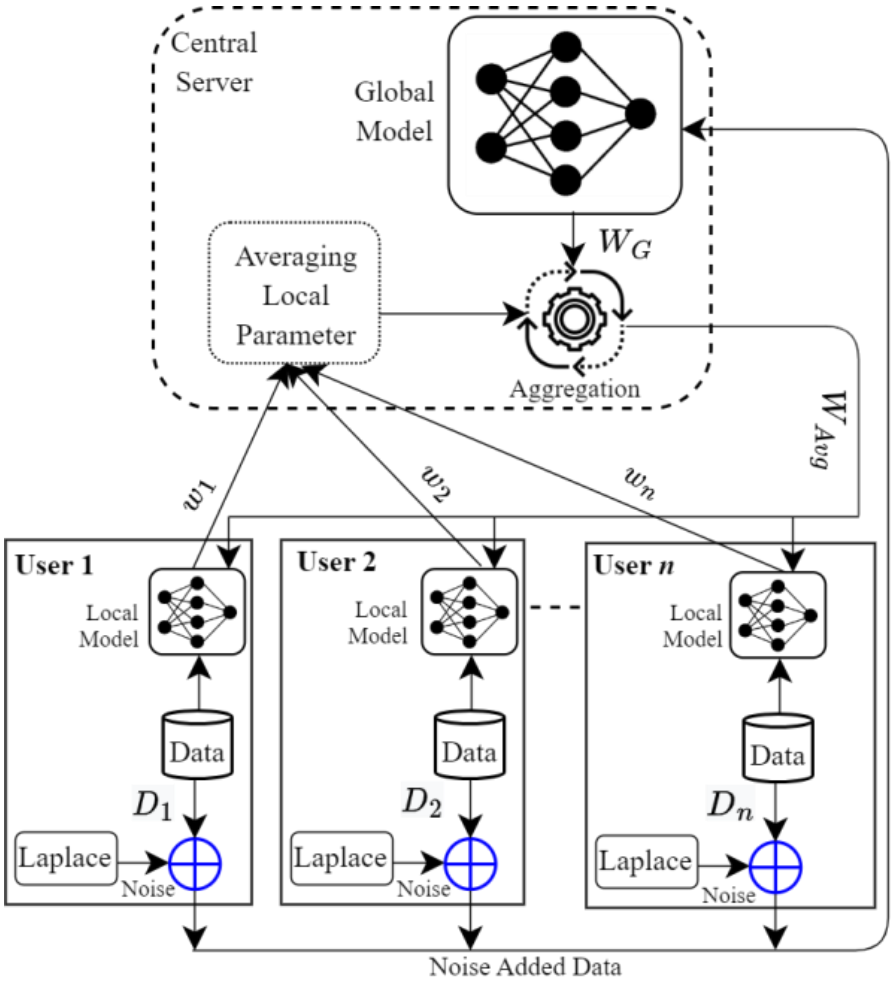
Alazab, M., RM, S.P., Parimala, M., Maddikunta, P.K.R., Gadekallu, T.R. and Pham, Q.V., 2021. Federated learning for cybersecurity: concepts, challenges, and future directions. IEEE Transactions on Industrial Informatics, 18(5), pp.3501-3509.)

Challenges in Federated learning

Table: Comparison of performance parameter over MNIST dataset with iterations = 2 and number of users = 10

Each user has images	Iteration	Model		
		FedAvg-ANN	FedAvg-MLP	FedAvg-CNN
		Accuracy (%)	Accuracy (%)	Accuracy (%)
4	2	41.66	41.66	50.00
8	2	68.00	64.00	74.00
39	2	82.50	85.00	85.83

Proposed Model



Experiments

(a) idea

Train the Global Model with noisy data
Train the Local Models with raw data

(b) dataset

MNIST dataset with 60000 samples

(c) result

Accuracy, Precision, F-Score
Loss

Summary

- Previous proposed model don't consider the case when each user has small amount of data which practically are the real world scenario
- Both raw and noisy data were used to examine the performance of federated method, which is better than previous works.
- The newly proposed model improve securely sharing the data to the central server, while maintaining utility and reducing convergence time.


Thank you