Effect of Homomorphic Encryption on the Performance of Training Federated Learning Generative Adversarial Networks

Ignjat Pejic[@], Kaitai Liang, Rui Wang

[@]i.pejic@tudelft.nl

Background Information

General Adversarial Network (GAN): Generative Machine learning(ML) model where two neural networks compete with each other in order to generate new realistic fake data [1].

Federated Learning (FL): ML training technique where ML model is trained in a distribtuted decentralized setting. Therefore, data never leaves the local edge devices [2].

Homomorphic Encryption (HE): Encryption technique that allows computations to be performed on the cipher texts. There are three main types, listed below:

- Partial Homomorphic Encryption (PHE)
- Somewhat Homomorphic Encryption (SHE)
- Fully Homomorphic Encryption (FHE)

Multi Party Computation (MPC): a cryptography technique with homomorphic properties.

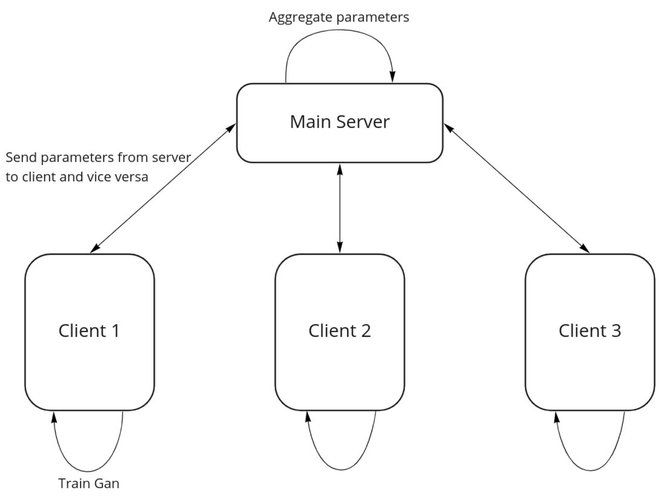

Figure 1: Visualization of FL-GAN

Research Topic

Implement a Federated Learning Generative Adversarial Network with Homomorphic Encryption, and study the effect of HE on the performance (and accuracy) of training the model. We also decided to add MPC for comparison.

System Model and Methodology

Our model will consist of three clients, a main centralized server, and a key generator where necessary. Our clients and server will be honest-but-curious, meaning that they will follow the algorithm specified but try to learn as much as possible from received information.

The algorithm used will be the following. Our server will partition the dataset and send each partition to the appropriate client. Each client will then train the data, before sending the encrypted model parameters to the main server. The main server will then aggregate the parameters of all clients before sending them back to each client. The clients will then decrypt the received parameters, before updating the model and continuing the training process for desired number of epochs. Where possible, our key generator will generate the keys and send them to each client, trying to leave the server out of the loop.

We have 3 clients and our FL is set to 50 epochs. Each client has 24 Pytorch Tensors and 6342272 parameters.

Results

- All our experiments were performed on a machine with a Intel(R) Core (TM) i7-8750H processor with 2.20GHz
- Base case FL-GAN took 16 hours to run

Figure 2: BCELoss for FL-GAN

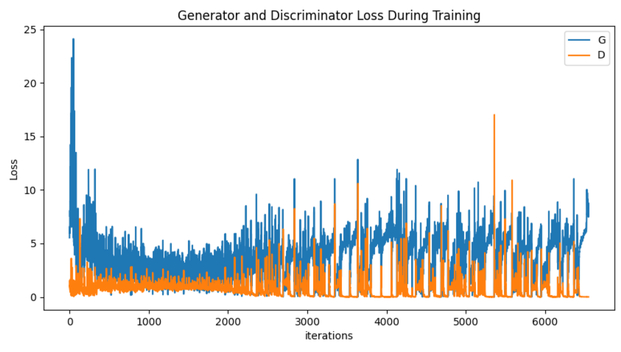

Table 1: Results for Paillier Cryptosystem for 3 clients and 50 epochs

K.S. [a]	T.F.O.E. (s) [b]	T.F.O.D. (s) [c]	T.A.T.P.C.P.E. (s) [d]	T.A.T.T. (s) [e]
64	0.000105	1.612e-5	771	115650
128	0.0005040	0.00018	4311	646650
256	0.00134	0.00058	12177	1826574
512	0.00671	0.00023	44015	6602305

[a] Key Size
[b] Time for one encryption
[c] Time for one decryption
[d] Total additional time per client per epoch
[e] Total additional time taken (3 clients,50 epoch)

Table 2: Results Comparison

Method	Total Extra Time (s)	Time Complexity
PHE	646650 (180h)	$\mathcal{O}(p)$
SHE-1[a]	4848408 (1346h)	$\mathcal{O}(p)$
SHE-2[b]	2137 (36m)	$\mathcal{O}(t)$
MPC	55.2	$\mathcal{O}(t)$

[a] Encryption per parameter
[b] Encryption per tensor

Conclusion

Overall, we see that the stronger the level of encryption, the higher the performance loss was, as initially believed. It is a difficult but crucial issue to balance the performance loss and privacy increase.

In the future, it would be important to test different implementations of the FL-GAN, as different tools have different encryption optimizations. Moreover, testing a real world scenario would provide more accurate results.

[1] A. Creswell, T. White, V. Dumoulin, K. Arulkumaran, B. Sengupta, and A. A. Bharath, "Generative adversarial networks: Anoverview," IEEE Signal Processing Magazine,vol. 35, no. 1, pp. 53–65, Jan. 2018, issn: 1558-0792. doi: 10.1109/MSP.2017.2765202.
[2] P. Kairouz, H. B. McMahan, B. Avent, et al.,Advances and open problems in federated learning, 2019. doi: 10.48550/ARXIV.1912.04977. [Online]. Available: https://arxiv.org/abs/1912.04977.

TU Delft Delft University of Technology