1. Research question

Does adding a denoising step to DP-FL-GANs increase model accuracy while preserving privacy?

3. Results

Fed-Avg GAN
No Differential Privacy
No Denoising

Differential Privacy
No Denoising
DP-Fed-Avg GAN

Ours
Differential Privacy
Denoising

2. Why is it important?

Privacy-sensitive user data needs to stay on the device while still contributing to the global training of machine learning models without giving up the user's privacy and without a loss in accuracy

4. What went wrong?

Autoencoder trained at 20% noise. DP noise was arbitrary, causing blur.

5. Performance comparison

	GS-WGAN*	DP-Fed-Avg GAN	Ours
Frechet Inception Distance ↓	60	200	250
Generator loss ↓	?	-0.6	-0.5
Classifier accuracy ↑	?	60%	18%
Epsilon*** ↓	5.99 x 10^2	9.99 x 10^6 **	9.99 x 10^6 **

* Unverified results
** Ceiling value, actuals are lower
*** The impact of a single input to the output

Abbreviations:
DP = Differential Privacy
FL = Federated Learning GAN = Generative Adversarial Net

Responsible Professor:
Dr. Kaitai Liang
Kaitai.Liang@tudelft.nl

Supervisor:
Rui Wang
R.Wang-8@tudelft.nl

How to reach me:
Gregor Schram
g.schram@student.tudelft.nl

1. Research question

Does adding a denoising step to DP-FL-GANs increase model accuracy while preserving privacy?

Privacy-sensitive user data needs to stay on the device while still contributing to the global training of machine learning models without giving up the user's privacy and without a loss in accuracy

2. Why is it important?

3. Results

Fed-Avg GAN
No Differential
Privacy
No Denoising

Differential
Privacy
No Denoising
DP-Fed-Avg GAN

Ours
Differential
Privacy
Denoising

Autoencoder trained at 20% noise. DP noise was arbitrary, causing blur.

4. What went wrong?

New table

	GS-WGAN*	DP-Fed-Avg GAN	Ours
Frechet Inception Distance ↓	60	200	250
Generator loss ↓	?	-0.6	-0.5
Classifier accuracy ↑	?	60%	18%
Epsilon* ↓**	5.99 x 10^2	9.99 x 10^6 **	9.99 x 10^6 **

*** Unverified results**
**** Ceiling value, actuals are lower**
***** The impact of a single input to the output**

5. Performance comparison

1. Research question

Does adding a denoising step to DP-FL-GANs increase model accuracy while preserving privacy?

3. Results

Fed-Avg GAN
No Differential Privacy
No Denoising

Differential Privacy
No Denoising
DP-Fed-Avg GAN

Ours
Differential Privacy
Denoising

2. Why is it important?

Privacy-sensitive user data needs to stay on the device while still contributing to the global training of machine learning models without giving up the user's privacy and without a loss in accuracy

4. What went wrong?

Autoencoder trained at 20% noise. DP noise was arbitrary, causing blur.

5. Performance comparison

	GS-WGAN*	DP-Fed-Avg GAN	Ours
Frechet Inception Distance ↓	60	200	250
Generator loss ↓	?	-0.6	-0.5
Classifier accuracy ↑	?	60%	18%
Epsilon*** ↓	5.99 x 10^2	9.99 x 10^6 **	9.99 x 10^6 **

* Unverified results
** Ceiling value, actuals are lower
*** The impact of a single input to the output

Abbreviations:
DP = Differential Privacy
FL = Federated Learning GAN = Generative Adversarial Net

Responsible Professor:
Dr. Kaitai Liang
Kaitai.Liang@tudelft.nl

Supervisor:
Rui Wang
R.Wang-8@tudelft.nl

How to reach me:
Gregor Schram
g.schram@student.tudelft.nl