Property Inference: Results

Labeled Faces In the Wild (LFW) dataset

61

#Participants	No Defense	LDP (ϵ = 10.7)	CDP (ϵ = 4.7)	CDP (ϵ = 8.1)
5	90%	83%	59%	85%
10	89%	81%	57%	83%
15	88%	80%	54%	82%
20	87%	78%	53%	79%
25	85%	70%	53%	77%
30	81%	68%	51%	73%

#Participants	No Defense	LDP (ϵ = 10.7)	CDP (ϵ = 8.1)
5	0.97	0.95	0.94
10	0.87	0.86	0.85
15	0.76	0.75	0.76
20	0.70	0.70	0.68
25	0.54	0.52	0.50
30	0.48	0.47	0.45

Main Task (Gender Classification) Accuracy

AUC of the Property Inference Attack

Property Inference: Results

Labeled Faces In the Wild (LFW) dataset

#Participants	No Defense	LDP (ϵ = 10.7)	CDP (ϵ = 4.7)	CDP (ϵ = 8.1)
5	90%	83%	59%	85%
10	89%	81%	57%	83%
15	88%	80%	54%	82%
20	87%	78%	53%	79%
25	85%	70%	53%	77%
30	81%	68%	51%	73%

Main Task (Gender Classification) Accuracy

#Participants	No Defense	LDP (ϵ = 10.7)	CDP (ϵ = 8.1)
5	0.97	0.95	0.94
10	0.87	0.86	0.85
15	0.76	0.75	0.76
20	0.70	0.70	0.68
25	0.54	0.52	0.50
30	0.48	0.47	0.45

AUC of the Property Inference Attack

Take-Aways

LDP and CDP can defend against white-box membership inference attacks in FL without destroying utility

Neither LDP nor CDP successfully defend against the property inference attack with the experimented privacy budgets