

Reza Shokri

List of Publications by Year in descending order

Source: <https://exaly.com/author-pdf/2306273/publications.pdf>

Version: 2024-02-01

26
papers

5,085
citations

1307594

7
h-index

1720034

7
g-index

26
all docs

26
docs citations

26
times ranked

2925
citing authors

#	ARTICLE	IF	CITATIONS
1	Membership Inference Attacks Against Machine Learning Models. , 2017, , .		1,550
2	Privacy-Preserving Deep Learning. , 2015, , .		879
3	Comprehensive Privacy Analysis of Deep Learning: Passive and Active White-box Inference Attacks against Centralized and Federated Learning. , 2019, , .		626
4	Quantifying Location Privacy. , 2011, , .		462
5	Protecting location privacy. , 2012, , .		263
6	Machine Learning with Membership Privacy using Adversarial Regularization. , 2018, , .		202
7	Synthesizing Plausible Privacy-Preserving Location Traces. , 2016, , .		119
8	On the Optimal Placement of Mix Zones. Lecture Notes in Computer Science, 2009, , 216-234.	1.3	118
9	Privacy-preserving deep learning. , 2015, , .		115
10	Privacy Risks of Securing Machine Learning Models against Adversarial Examples. , 2019, , .		103
11	Privacy Games: Optimal User-Centric Data Obfuscation. Proceedings on Privacy Enhancing Technologies, 2015, 2015, 299-315.	2.8	80
12	Plausible deniability for privacy-preserving data synthesis. Proceedings of the VLDB Endowment, 2017, 10, 481-492.	3.8	80
13	Evaluating the Privacy Risk of Location-Based Services. Lecture Notes in Computer Science, 2012, , 31-46.	1.3	71
14	Quantifying Interdependent Privacy Risks with Location Data. IEEE Transactions on Mobile Computing, 2017, 16, 829-842.	5.8	62
15	A distortion-based metric for location privacy. , 2009, , .		58
16	A Non-Parametric Generative Model for Human Trajectories. , 2018, , .		50
17	Privacy Games Along Location Traces. ACM Transactions on Privacy and Security, 2017, 19, 1-31.	3.0	45
18	Membership Inference Attacks Against Adversarially Robust Deep Learning Models. , 2019, , .		39

#	ARTICLE	IF	CITATIONS
19	On the Privacy Risks of Model Explanations. , 2021, , .		32
20	Predicting Users' Motivations behind Location Check-Ins and Utility Implications of Privacy Protection Mechanisms. , 2015, , .		30
21	A Predictive Model for User Motivation and Utility Implications of Privacy-Protection Mechanisms in Location Check-Ins. IEEE Transactions on Mobile Computing, 2018, 17, 760-774.	5.8	28
22	Bypassing Backdoor Detection Algorithms in Deep Learning. , 2020, , .		27
23	On the Privacy Risks of Algorithmic Fairness. , 2021, , .		24
24	What Does it Mean for a Language Model to Preserve Privacy?. , 2022, , .		18
25	Model Explanations with Differential Privacy. , 2022, , .		3
26	Membership Encoding for Deep Learning. , 2020, , .		1