Differentially Private Empirical Risk Minimization

Journal of Machine Learning Research
12, 1069-1109

Citation Report

#	Article	IF	Citations
1	Protecting count queries in study design. Journal of the American Medical Informatics Association: JAMIA, 2012, 19, 750-757.	2.2	22
2	iDASH: integrating data for analysis, anonymization, and sharing. Journal of the American Medical Informatics Association: JAMIA, 2012, 19, 196-201.	2.2	130
3	Differential privacy based on importance weighting. Machine Learning, 2013, 93, 163-183.	3.4	17
4	Toward practicing privacy. Journal of the American Medical Informatics Association: JAMIA, 2013, 20, 102-108.	2.2	44
5	Signal Processing and Machine Learning with Differential Privacy: Algorithms and Challenges for Continuous Data. IEEE Signal Processing Magazine, 2013, 30, 86-94.	4.6	128
6	Privacy and Data-Based Research. SSRN Electronic Journal, 0, , .	0.4	1
7	Sharing privacy-sensitive access to neuroimaging and genetics data: a review and preliminary validation. Frontiers in Neuroinformatics, 2014, 8, 35.	1.3	51
8	Privacy Preserving RBF Kernel Support Vector Machine. BioMed Research International, 2014, 2014, 1-10.	0.9	22
9	Model Aggregation for Distributed Content Anomaly Detection. , 2014, , .		8
10	Scalable privacy-preserving data sharing methodology for genome-wide association studies. Journal of Biomedical Informatics, 2014, 50, 133-141.	2.5	90
11	Bounds on the sample complexity for private learning and private data release. Machine Learning, 2014, 94, 401-437.	3.4	34
14	Kernel Association for Classification and Prediction: A Survey. IEEE Transactions on Neural Networks and Learning Systems, 2015, 26, 208-223.	7.2	40
15	A spectrum of sharing: maximization of information content for brain imaging data. GigaScience, 2015, 4, 2.	3.3	13
16	COINSTAC: A Privacy Enabled Model and Prototype for Leveraging and Processing Decentralized Brain Imaging Data. Frontiers in Neuroscience, 2016, 10, 365.	1.4	73
17	Differentially-private learning of low dimensional manifolds. Theoretical Computer Science, 2016, 620, 91-104.	0.5	2
18	A differential privacy framework for matrix factorization recommender systems. User Modeling and User-Adapted Interaction, 2016, 26, 425-458.	2.9	68
19	On reconstructability of quadratic utility functions from the iterations in gradient methods. Automatica, 2016, 66, 254-261.	3.0	4
20	Distributed Differentially Private Stochastic Gradient Descent: An Empirical Study. , 2016, , .		6

#	Article	IF	Citations
21	Local learning-based feature weighting with privacy preservation. Neurocomputing, 2016, 174, 1107-1115.	3.5	11
22	Single subject prediction of brain disorders in neuroimaging: Promises and pitfalls. NeuroImage, 2017, 145, 137-165.	2.1	688
23	Perturbed robust linear estimating equations for confidentiality protection in remote analysis. Statistics and Computing, 2017, 27, 775-787.	0.8	1
24	Partitioning-Based Mechanisms Under Personalized Differential Privacy. Lecture Notes in Computer Science, 2017, 10234, 615-627.	1.0	16
25	Crowd-ML: A library for privacy-preserving machine learning on smart devices. , 2017, , .		0
26	Differentially Private Data Analysis. Advances in Information Security, 2017, , 49-65.	0.9	0
27	Private classification with limited labeled data. Knowledge-Based Systems, 2017, 133, 197-207.	4.0	8
28	Perturbation of convex risk minimization and its application in differential private learning algorithms. Journal of Inequalities and Applications, 2017, 2017, 9.	0.5	2
29	Privacy calculus and its utility for personalization services in e-commerce: An analysis of consumer decision-making. Information and Management, 2017, 54, 427-437.	3.6	62
30	New Collaborative Filtering Algorithms Based on SVD++ and Differential Privacy. Mathematical Problems in Engineering, 2017, 2017, 1-14.	0.6	20
31	PrivPfC: differentially private data publication for classification. VLDB Journal, 2018, 27, 201-223.	2.7	12
32	Randomized learning: Generalization performance of old and new theoretically grounded algorithms. Neurocomputing, 2018, 298, 21-33.	3.5	5
33	Distributed Privacy-Preserving Collaborative Intrusion Detection Systems for VANETs. IEEE Transactions on Signal and Information Processing Over Networks, 2018, 4, 148-161.	1.6	116
34	Differentially Private Distributed Online Learning. IEEE Transactions on Knowledge and Data Engineering, 2018, 30, 1440-1453.	4.0	70
35	Deep learning for healthcare: review, opportunities and challenges. Briefings in Bioinformatics, 2018, 19, 1236-1246.	3.2	1,459
36	Minimax Optimal Procedures for Locally Private Estimation. Journal of the American Statistical Association, 2018, 113, 182-201.	1.8	167
37	Differentially Private Model Selection with Penalized and Constrained Likelihood. Journal of the Royal Statistical Society Series A: Statistics in Society, 2018, 181, 609-633.	0.6	6
38	Differentially private classification with decision tree ensemble. Applied Soft Computing Journal, 2018, 62, 807-816.	4.1	33

#	Article	IF	Citations
40	Algorithms that remember: model inversion attacks and data protection law. Philosophical Transactions Series A, Mathematical, Physical, and Engineering Sciences, 2018, 376, 20180083.	1.6	82
41	A Review of Privacy-Preserving Machine Learning Classification. Lecture Notes in Computer Science, 2018, , 671-682.	1.0	2
42	Understanding mean-field effects of large-population user data obfuscation in machine learning. , 2018, , .		0
43	SoK: Security and Privacy in Machine Learning. , 2018, , .		238
44	Towards privacy preserving social recommendation under personalized privacy settings. World Wide Web, 2019, 22, 2853-2881.	2.7	16
45	Model averaging with privacy-preserving. Communications in Statistics Part B: Simulation and Computation, 2019, , 1-14.	0.6	0
46	On the Compatibility of Privacy and Fairness. , 2019, , .		44
47	Semi-supervised learning with summary statistics. Analysis and Applications, 2019, 17, 837-851.	1.2	1
48	Privacy Preserving Synthetic Data Release Using Deep Learning. Lecture Notes in Computer Science, 2019, , 510-526.	1.0	33
49	Efficient and Secure Decision Tree Classification for Cloud-Assisted Online Diagnosis Services. IEEE Transactions on Dependable and Secure Computing, 2021, 18, 1632-1644.	3.7	96
50	Making Machine Learning Forget. Lecture Notes in Computer Science, 2019, , 72-83.	1.0	5
51	Differentially Private Significance Tests for Regression Coefficients. Journal of Computational and Graphical Statistics, 2019, 28, 440-453.	0.9	14
52	Differentially Private Image Classification Using Support Vector Machine and Differential Privacy. Machine Learning and Knowledge Extraction, 2019, 1, 483-491.	3.2	25
53	Differentially Private Hypothesis Transfer Learning. Lecture Notes in Computer Science, 2019, , 811-826.	1.0	37
54	Supervised Joint Nonlinear Transform Learning with Discriminative-Ambiguous Prior for Generic Privacy-Preserved Features. , 2019, , .		0
55	Elliptical modeling and pattern analysis for perturbation models and classification. International Journal of Data Science and Analytics, 2019, 7, 103-113.	2.4	0
56	DP-ADMM: ADMM-Based Distributed Learning With Differential Privacy. IEEE Transactions on Information Forensics and Security, 2020, 15, 1002-1012.	4.5	92
57	Differential privacy for sparse classification learning. Neurocomputing, 2020, 375, 91-101.	3.5	12

#	Article	IF	Citations
58	A survey of local differential privacy for securing internet of vehicles. Journal of Supercomputing, 2020, 76, 8391-8412.	2.4	29
59	Protecting patient privacy in survival analyses. Journal of the American Medical Informatics Association: JAMIA, 2020, 27, 366-375.	2.2	14
60	Differentially Private Actor and Its Eligibility Trace. Electronics (Switzerland), 2020, 9, 1486.	1.8	3
61	Differentially Private Optimal Power Flow for Distribution Grids. IEEE Transactions on Power Systems, 2021, 36, 2186-2196.	4.6	20
62	Correlated data in differential privacy: Definition and analysis. Concurrency Computation Practice and Experience, 2022, 34, e6015.	1.4	7
63	Differentially Private Precision Matrix Estimation. Acta Mathematica Sinica, English Series, 2020, 36, 1107-1124.	0.2	3
64	Robust Transparency Against Model Inversion Attacks. IEEE Transactions on Dependable and Secure Computing, 2020, 18, 1-1.	3.7	5
65	Model-Protected Multi-Task Learning. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2022, 44, 1002-1019.	9.7	6
66	Differentially private 1R classification algorithm using artificial bee colony and differential evolution. Engineering Applications of Artificial Intelligence, 2020, 94, 103813.	4.3	12
67	Practical and Secure SVM Classification for Cloud-Based Remote Clinical Decision Services. IEEE Transactions on Computers, 2021, 70, 1612-1625.	2.4	20
68	Privacy-Preserving Blockchain-Based Nonlinear SVM Classifier Training for Social Networks. Security and Communication Networks, 2020, 2020, 1-10.	1.0	9
69	A Comprehensive Survey on Local Differential Privacy toward Data Statistics and Analysis. Sensors, 2020, 20, 7030.	2.1	43
70	ICAIL Doctoral Consortium, Montreal 2019. Artificial Intelligence and Law, 2020, 28, 267-280.	3.0	0
71	Selective Feature Anonymization for Privacy-Preserving Image Data Publishing. Electronics (Switzerland), 2020, 9, 874.	1.8	12
72	Privacy-Preserving Stochastic Gradual Learning. IEEE Transactions on Knowledge and Data Engineering, 2021, 33, 3129-3140.	4.0	3
73	A Privacy-Preserving Multi-Task Learning Framework for Face Detection, Landmark Localization, Pose Estimation, and Gender Recognition. Frontiers in Neurorobotics, 2019, 13, 112.	1.6	12
74	Bounded privacy-utility monotonicity indicating bounded tradeoff of differential privacy mechanisms. Theoretical Computer Science, 2020, 816, 195-220.	0.5	5
75	Community Detection in Online Social Networks: A Differentially Private and Parsimonious Approach. IEEE Transactions on Computational Social Systems, 2020, 7, 151-163.	3.2	18

#	Article	IF	Citations
78	Instance-Based Transfer Learning. , 2020, , 23-33.		0
79	Feature-Based Transfer Learning. , 2020, , 34-44.		0
80	Model-Based Transfer Learning. , 2020, , 45-57.		0
81	Relation-Based Transfer Learning. , 2020, , 58-67.		1
82	Heterogeneous Transfer Learning. , 2020, , 68-92.		0
83	Adversarial Transfer Learning. , 2020, , 93-104.		0
84	Transfer Learning in Reinforcement Learning. , 2020, , 105-125.		0
85	Multi-task Learning. , 2020, , 126-140.		0
86	Transfer Learning Theory. , 2020, , 141-150.		1
87	Few-Shot Learning. , 2020, , 177-195.		1
88	Lifelong Machine Learning. , 2020, , 196-208.		0
89	Privacy-Preserving Transfer Learning. , 2020, , 211-220.		1
90	Transfer Learning in Natural Language Processing. , 2020, , 234-256.		3
91	Transfer Learning in Dialogue Systems. , 2020, , 257-278.		0
92	Transfer Learning in Bioinformatics. , 2020, , 293-306.		0
93	Transfer Learning in Activity Recognition. , 2020, , 307-323.		0
94	Transfer Learning in Urban Computing. , 2020, , 324-333.		0
97	Transitive Transfer Learning. , 2020, , 151-167.		0

#	Article	IF	Citations
98	AutoTL: Learning to Transfer Automatically. , 2020, , 168-176.		0
99	Transfer Learning in Computer Vision. , 2020, , 221-233.		2
100	Transfer Learning in Recommender Systems. , 2020, , 279-292.		1
101	Private Empirical Risk Minimization With Analytic Gaussian Mechanism for Healthcare System. IEEE Transactions on Big Data, 2022, 8, 1107-1117.	4.4	6
102	Structure and Sensitivity in Differential Privacy: Comparing K-Norm Mechanisms. Journal of the American Statistical Association, 2021, 116, 935-954.	1.8	11
103	Major advancements in kernel function approximation. Artificial Intelligence Review, 2021, 54, 843-876.	9.7	11
104	A Survey of Differentially Private Regression for Clinical and Epidemiological Research. International Statistical Review, 2021, 89, 132-147.	1.1	4
105	Differentially Private Tensor Deep Computation for Cyberâ€“Physicalâ€“Social Systems. IEEE Transactions on Computational Social Systems, 2021, 8, 236-245.	3.2	0
106	Clustering-Learning-Based Long-Term Predictive Localization in 5G-Envisioned Internet of Connected Vehicles. IEEE Transactions on Intelligent Transportation Systems, 2021, 22, 5232-5246.	4.7	17
107	Privacy attacks against deep learning models and their countermeasures. Journal of Systems Architecture, 2021, 114, 101940.	2.5	7
108	Effects of differential privacy techniques: Considerations for end users. Research in Social and Administrative Pharmacy, 2021, 17, 930-941.	1.5	0
109	Local Differential Privacy for data collection and analysis. Neurocomputing, 2021, 426, 114-133.	3.5	11
110	Latent Dirichlet Allocation Model Training With Differential Privacy. IEEE Transactions on Information Forensics and Security, 2021, 16, 1290-1305.	4.5	16
111	More Than Privacy: Applying Differential Privacy in Key Areas of Artificial Intelligence. IEEE Transactions on Knowledge and Data Engineering, 2021, , 1-1.	4.0	42
112	Learning Privately with Labeled and Unlabeled Examples. Algorithmica, 2021, 83, 177-215.	1.0	1
113	Privacy-Preserving Parametric Inference: A Case for Robust Statistics. Journal of the American Statistical Association, 2021, 116, 969-983.	1.8	9
114	Privacy Preserving Text Representation Learning Using BERT. Lecture Notes in Computer Science, 2021, , 91-100.	1.0	1
115	Differentially Private ADMM Algorithms for Machine Learning. IEEE Transactions on Information Forensics and Security, 2021, 16, 4733-4745.	4.5	8

#	Article	IF	Citations
116	Adaptive Privacy Preserving Deep Learning Algorithms for Medical Data. , 2021, , .		14
117	Stochastic Gradient Method with Barzilaiâ€“Borwein Step for Unconstrained Nonlinear Optimization. Journal of Computer and Systems Sciences International, 2021, 60, 75-86.	0.2	2
118	Quantifying Membership Privacy via Information Leakage. IEEE Transactions on Information Forensics and Security, 2021, 16, 3096-3108.	4.5	15
119	A Systematic Review of Challenges and Techniques of Privacy-Preserving Machine Learning. Lecture Notes in Networks and Systems, 2021, , 19-41.	0.5	1
120	Differentially Private Linear Regression Analysis via Truncating Technique. Lecture Notes in Computer Science, 2021, , 249-260.	1.0	2
121	Monitoring-Based Differential Privacy Mechanism Against Query Flooding-Based Model Extraction Attack. IEEE Transactions on Dependable and Secure Computing, 2022, 19, 2680-2694.	3.7	12
122	Differential Privacy for Tensor-Valued Queries. IEEE Transactions on Information Forensics and Security, 2022, 17, 152-164.	4.5	6
123	Shuffled Model of Federated Learning: Privacy, Accuracy and Communication Trade-Offs. IEEE Journal on Selected Areas in Information Theory, 2021, 2, 464-478.	1.9	23
124	Three Variants of Differential Privacy: Lossless Conversion and Applications. IEEE Journal on Selected Areas in Information Theory, 2021, 2, 208-222.	1.9	16
125	Adversarial Privacy-Preserving Graph Embedding Against Inference Attack. IEEE Internet of Things Journal, 2021, 8, 6904-6915.	5.5	36
126	Machine Unlearning. , 2021, , .		113
127	ABCDP: Approximate Bayesian Computation with Differential Privacy. Entropy, 2021, 23, 961.	1.1	2
128	Differentially Private Federated Learning: An Information-Theoretic Perspective. , 2021, , .		7
129	Privacy-Preserving Convex Factorization Machine. , 2021, , .		0
130	Research on an Adaptive Neural Network K-Pixel Adversarial Example Generation Algorithm. Journal of Circuits, Systems and Computers, 0, , 2250007.	1.0	1
131	Differentially Private Distance Learning in Categorical Data. Data Mining and Knowledge Discovery, 2021, 35, 2050-2088.	2.4	0
132	Regularized Loss Minimizers with Local Data Perturbation: Consistency and Data Irrecoverability. , 2021, , .		0
134	Preserving Geo-Indistinguishability of the Emergency Scene to Predict Ambulance Response Time. Mathematical and Computational Applications, 2021, 26, 56.	0.7	6

#	Article	IF	Citations
135	Resisting membership inference attacks through knowledge distillation. Neurocomputing, 2021, 452, 114-126.	3.5	17
136	Prescriptive analytics with differential privacy. International Journal of Data Science and Analytics, 2022, 13, 123-138.	2.4	2
137	Differentially private SGD with non-smooth losses. Applied and Computational Harmonic Analysis, 2022, 56, 306-336.	1.1	7
138	Escaping Saddle Points of Empirical Risk Privately and Scalably via DP-Trust Region Method. Lecture Notes in Computer Science, 2021, , 90-106.	1.0	1
139	Privacy-Aware Load Ensemble Control: A Linearly-Solvable MDP Approach. IEEE Transactions on Smart Grid, 2022, 13, 255-267.	6.2	6
140	Differential Privacy with Variant-Noise for Gaussian Processes Classification. Lecture Notes in Computer Science, 2019, , 107-119.	1.0	5
142	Security Evaluation of Support Vector Machines in Adversarial Environments. , 2014, , 105-153.		62
143	Robust and Private Bayesian Inference. Lecture Notes in Computer Science, 2014, , 291-305.	1.0	36
144	Achieving Accuracy Guarantee for Answering Batch Queries with Differential Privacy. Lecture Notes in Computer Science, 2015, , 305-316.	1.0	1
145	Differentially Private Multi-task Learning. Lecture Notes in Computer Science, 2016, , 101-113.	1.0	12
146	Processing Text for Privacy: An Information Flow Perspective. Lecture Notes in Computer Science, 2018, , 3-21.	1.0	3
147	Privately Solving Linear Programs. Lecture Notes in Computer Science, 2014, , 612-624.	1.0	10
149	Federated Tensor Factorization for Computational Phenotyping. , 2017, 2017, 887-895.		62
150	Deep Learning with Gaussian Differential Privacy. , 2020, 2020, .		46
151	Free gap information from the differentially private sparse vector and noisy max mechanisms. Proceedings of the VLDB Endowment, 2019, 13, 293-306.	2.1	7
152	Artificial intelligence for COVID-19: battling the pandemic with computational intelligence. Intelligent Medicine, 2022, 2, 13-29.	1.6	18
153	Analysis of Application Examples of Differential Privacy in Deep Learning. Computational Intelligence and Neuroscience, 2021, 2021, 1-15.	1.1	6
154	Privacy Background. Springer Theses, 2013, , 19-45.	0.0	0

#	Article	IF	Citations
155	Differentially-Private Learning of Low Dimensional Manifolds. Lecture Notes in Computer Science, 2013, , 249-263.	1.0	0
156	Differentially Private Empirical Risk Minimization with Input Perturbation. Lecture Notes in Computer Science, 2017, , 82-90.	1.0	10
157	Gaussian Mixture Models for Classification and Hypothesis Tests Under Differential Privacy. Lecture Notes in Computer Science, 2017, , 123-141.	1.0	3
159	DPNE: Differentially Private Network Embedding. Lecture Notes in Computer Science, 2018, , 235-246.	1.0	9
160	A Differential Privacy Workflow for Inference of Parameters in the Rasch Model. Lecture Notes in Computer Science, 2019, , 113-124.	1.0	0
161	A Survey on Deep Learning Techniques for Privacy-Preserving. Lecture Notes in Computer Science, 2019, , 29-46.	1.0	23
162	Differentially Private Non-parametric Machine Learning as a Service. Lecture Notes in Computer Science, 2019, , 189-204.	1.0	2
163	Data Anonymization for Privacy Aware Machine Learning. Lecture Notes in Computer Science, 2019, , 725-737.	1.0	6
164	Medical Text and Image Processing: Applications, Issues and Challenges. Learning and Analytics in Intelligent Systems, 2020, , 237-262.	0.5	12
165	Privacy-Preserving Nonlinear SVM Classifier Training Based on Blockchain. Communications in Computer and Information Science, 2020, , 278-288.	0.4	2
166	Forgetting Outside the Box: Scrubbing Deep Networks of Information Accessible from Input-Output Observations. Lecture Notes in Computer Science, 2020, , 383-398.	1.0	33
167	Mixed-Privacy Forgetting in Deep Networks. , 2021, , .		31
168	On the Privacy Risks of Algorithmic Fairness. , 2021, , .		24
169	A differential privacy-based classification system for edge computing in IoT. Computer Communications, 2022, 182, 117-128.	3.1	9
170	Privacy preserving classification over differentially private data. Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 2021, 11, e1399.	4.6	4
171	Differential Privacy at Risk: Bridging Randomness and Privacy Budget. Proceedings on Privacy Enhancing Technologies, 2021, 2021, 64-84.	2.3	3
172	Scaling up Differentially Private Deep Learning with Fast Per-Example Gradient Clipping. Proceedings on Privacy Enhancing Technologies, 2021, 2021, 128-144.	2.3	6
173	Sample Complexity Bounds for Differentially Private Learning. JMLR Workshop and Conference Proceedings, 2011, 2011, 155-186.	1.4	1

#	Article	IF	Citations
174	Convergence Rates for Differentially Private Statistical Estimation. , 2012, 2012, 1327-1334.		2
175	Privacy-Preserving Data Sharing for Genome-Wide Association Studies. Journal of Privacy and Confidentiality, 2013, 5, 137-166.	1.1	32
176	Learning from Data with Heterogeneous Noise using SGD. JMLR Workshop and Conference Proceedings, 2015, 2015, 894-902.	1.4	2
177	Privacy-Preserving Methods for Vertically Partitioned Incomplete Data. AMIA ... Annual Symposium proceedings, 2020, 2020, 348-357.	0.2	1
178	p-Power Exponential Mechanisms for Differentially Private Machine Learning. IEEE Access, 2021, 9, 155018-155034.	2.6	1
179	Image Anonymization using Deep Convolutional Generative Adversarial Network. Journal of Physics: Conference Series, 2021, 2089, 012012.	0.3	1
180	DPWSS: differentially private working set selection for training support vector machines. PeerJ Computer Science, 2021, 7, e799.	2.7	2
181	Gradient Leakage Attack Resilient Deep Learning. IEEE Transactions on Information Forensics and Security, 2022, 17, 303-316.	4.5	15
182	A Correlated Noise-Assisted Decentralized Differentially Private Estimation Protocol, and its Application to fMRI Source Separation. IEEE Transactions on Signal Processing, 2021, 69, 6355-6370.	3.2	5
183	Data desensitization mechanism of Android application based on differential privacy. , 2021, , .		2
184	A Decentralized Machine Learning Scheme with Input Perturbation-Based Differential Privacy. , 2022, , .		0
185	Private Cross-Silo Federated Learning for Extracting Vaccine Adverse Event Mentions. Communications in Computer and Information Science, 2021, , 490-505.	0.4	2
186	Privacy-Preserving Federated Learning Model for Healthcare Data. , 2022, , .		14
187	Free gap estimates from the exponential mechanism, sparse vector, noisy max and related algorithms. VLDB Journal, 2023, 32, 23-48.	2.7	1
188	Achieving Private and Fair Truth Discovery in Crowdsourcing Systems. Security and Communication Networks, 2022, 2022, 1-15.	1.0	5
189	Differentially Private Singular Value Decomposition for Training Support Vector Machines. Computational Intelligence and Neuroscience, 2022, 2022, 1-11.	1.1	4
190	Differentially Private Simple Linear Regression. Proceedings on Privacy Enhancing Technologies, 2022, 2022, 184-204.	2.3	1
191	Secure tumor classification by shallow neural network using homomorphic encryption. BMC Genomics, 2022, 23, 284.	1.2	6

#	Article	IF	Citations
192	Handling data heterogeneity with generative replay in collaborative learning for medical imaging. Medical Image Analysis, 2022, 78, 102424.	7.0	8
193	Adaptive Clipping Bound of Deep Learning with Differential Privacy. , 2021, , .		2
194	Just Keep Your Concerns Private: Guaranteeing Heterogeneous Privacy and Achieving High Availability for ERM Algorithms. , 2021, , .		0
195	Achieving Differential Privacy in Vertically Partitioned Multiparty Learning. , 2021, , .		6
196	Interval Privacy: A Framework for Privacy-Preserving Data Collection. IEEE Transactions on Signal Processing, 2022, 70, 2443-2459.	3.2	4
197	Laplacian Smoothing Stochastic ADMMs With Differential Privacy Guarantees. IEEE Transactions on Information Forensics and Security, 2022, 17, 1814-1826.	4.5	1
198	Lessons from the AdKDDâ€™21 Privacy-Preserving ML Challenge. , 2022, , .		0
199	Data pricing in machine learning pipelines. Knowledge and Information Systems, 2022, 64, 1417-1455.	2.1	9
200	Differentially Private Accelerated Optimization Algorithms. SIAM Journal on Optimization, 2022, 32, 795-821.	1.2	3
201	Perturbed M-Estimation: A Further Investigation of Robust Statistics for Differential Privacy. Springer Series in the Data Sciences, 2022, , 337-361.	0.1	1
202	Responsible and Regulatory Conform Machine Learning for Medicine: A Survey of Challenges and Solutions. IEEE Access, 2022, 10, 58375-58418.	2.6	7
203	Differentially private multivariate time series forecasting of aggregated human mobility with deep learning: Input or gradient perturbation?. Neural Computing and Applications, 0, , .	3.2	2
204	Privacy-Preserving Outsourcing Scheme for SVM on Vertically Partitioned Data. Security and Communication Networks, 2022, 2022, 1-19.	1.0	1
205	Noise-Augmented Privacy-Preserving Empirical Risk Minimization withÂDual-Purpose Regularizer andÂPrivacy Budget Retrieval andÂRecycling. Lecture Notes in Networks and Systems, 2022, , 660-681.	0.5	0
206	Membership Inference Attacks on Machine Learning Model. International Journal of Scientific Research in Computer Science Engineering and Information Technology, 2022, , 31-38.	0.2	0
207	Collaborative Private Classifiers Construction. Advanced Sciences and Technologies for Security Applications, 2023, , 15-45.	0.4	1
208	Mechanism and Recent Trends of Federated Learning as a Privacy Technology. Ieice Ess Fundamentals Review, 2023, 16, 196-204.	0.1	0
209	A Stochastic Gradient Descent Algorithm Based onÂAdaptive Differential Privacy. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, 2022, , 133-152.	0.2	0

#	Article	IF	Citations
210	Iterative Shrink Threshold Differential Privacy Algorithm Based on Gradient Perturbation and BB Step Size. Advances in Applied Mathematics, 2023, 12, 183-202.	0.0	0
211	FedAUXfdp: Differentially Private One-Shot Federated Distillation. Lecture Notes in Computer Science, 2023, , 100-114.	1.0	0
212	Optimal algorithms for differentially private stochastic monotone variational inequalities and saddle-point problems. Mathematical Programming, 2024, 204, 255-297.	1.6	0