L-diversity: privacy beyond k-anonymity

DOI: 10.1109/icde.2006.1
, 2006, , .

#	Paper	IF	Citations
1234	Injecting utility into anonymized datasets. **2006**,		122
1233	Secure Anonymization for Incremental Datasets. **2006**, 48-63		84
1232	Personalized privacy preservation. **2006**,		324
1231	Towards Balancing Data Usefulness and Privacy Protection in K-Anonymisation. **2006**,		1
1230	Workload-aware anonymization. **2006**,		105
1229	(␣k)-anonymity. **2006**,		114
1228	On the efficiency of checking perfect privacy. **2006**,		22
1227	From statistical knowledge bases to degrees of belief. **2006**,		1
1226	Anonymizing sequential releases. **2006**,		123
1225	Probabilistic privacy analysis of published views. **2006**,		3
1224	Privacy via pseudorandom sketches. **2006**,		31
1223	Achieving anonymity via clustering. **2006**,		116
1222	Towards the Diversity of Sensitive Attributes in k-Anonymity. **2006**,		
1221	Privacy in the Electronic Society. **2006**, 1-21		1
1220	Approximate algorithms for K-anonymity. **2007**,		63
1219	Privacy, accuracy, and consistency too. **2007**,		220
1218	Spatial generalisation algorithms for LBS privacy preservation. **2007**, 1, 179-207		20

1217 Capturing data usefulness and privacy protection in K-anonymisation. **2007**, 44

1216 GhostDB. **2007**, 20

1215 Hiding the presence of individuals from shared databases. **2007**, 134

1214 Private web search. **2007**, 32

1213 Tuning anonymity level for assuring high data quality: an empirical study.. **2007**, 2

1212 PRIVE. **2007**, 233

1211 MultiRelational k-Anonymity. **2007**, 33

1210 Realizing Privacy-Preserving Features in Hippocratic Databases. **2007**, 3

1209 Privacy Protection on Multiple Sensitive Attributes. **2007**, 141-152 6

1208 M-invariance. **2007**, 246

1207 Anonymity. **2007**, 323-353 83

1206 L -diversity. **2007**, 1, 3 1449

1205 Anonymizing Classification Data for Privacy Preservation. **2007**, 19, 711-725 192

1204 Study on K-anonymity Models of Sharing Medical Information. **2007**, 4

1203 Hiding in the Crowd: Privacy Preservation on Evolving Streams through Correlation Tracking. **2007**, 34

1202 Aggregate Query Answering on Anonymized Tables. **2007**, 127

1201 An entropy based method for measuring anonymity. **2007**, 11

1200 k-Anonymization Without Q-S Associations. **2007**, 753-764

1199	Privacy protection on sliding window of data streams. **2007**,	14
1198	Information disclosure under realistic assumptions. **2007**,	37
1197	K-anonymization incremental maintenance and optimization techniques. **2007**,	23
1196	Preventing Location-Based Identity Inference in Anonymous Spatial Queries. **2007**, 19, 1719-1733	406
1195	Exploratory mining in cube space. **2007**, 15, 29-54	14
1194	Handicapping attacker's confidence: an alternative to k-anonymization. **2007**, 11, 345-368	87
1193	Thoughts on k-anonymization. **2007**, 63, 622-645	72
1192	A recursive search algorithm for statistical disclosure assessment. **2008**, 16, 165-196	18
1191	A framework for condensation-based anonymization of string data. **2008**, 16, 251-275	14
1190	An Efficient Clustering Algorithm for k-Anonymisation. **2008**, 23, 188-202	10
1189	Anonymity preserving pattern discovery. **2008**, 17, 703-727	60
1188	Providing k-anonymity in data mining. **2008**, 17, 789-804	55
1187	Towards optimal k-anonymization. **2008**, 65, 22-39	27
1186	A privacy preserving technique for distance-based classification with worst case privacy guarantees. **2008**, 66, 264-288	13
1185	e-inclusion: privacy preserving re-publication of dynamic datasets. **2008**, 9, 1124-1133	3
1184	Preserving Privacy in Social Networks Against Neighborhood Attacks. **2008**,	371
1183	Managing and Querying Encrypted Data. **2008**, 163-190	8
1182	Private Data Analysis via Output Perturbation. **2008**, 383-414	3

1181 On Unifying Privacy and Uncertain Data Models. **2008**, 35

1180 Supporting anonymous location queries in mobile environments with privacygrid. **2008**, 206

1179 A survey of state-of-the-art in anonymity metrics. **2008**, 17

1178 Inference Analysis in Privacy-Preserving Data Re-publishing. **2008**, 10

1177 Towards trajectory anonymization. **2008**, 98

1176 Privacy-Preserving Data Publishing Based on De-clustering. **2008**, 2

1175 Preservation of Privacy in Publishing Social Network Data. **2008**, 6

1174 Injector: Mining Background Knowledge for Data Anonymization. **2008**, 36

1173 A Personalized (a,k)-Anonymity Model. **2008**, 7

1172 Robust De-anonymization of Large Sparse Datasets. **2008**, 849

1171 Privacy Preservation in the Publication of Trajectories. **2008**, 163

1170 Butterfly: Protecting Output Privacy in Stream Mining. **2008**, 8

1169 A Complete (alpha,k)-Anonymity Model for Sensitive Values Individuation Preservation. **2008**, 3

1168 PLUS: Synthesizing privacy, lineage, uncertainty and security. **2008**, 7

1167 An improved l-diversity model for numerical sensitive attributes. **2008**, 1

1166 k-Anonymization Revisited. **2008**, 44

1165 On Anti-Corruption Privacy Preserving Publication. **2008**, 29

1164 HIDE: An Integrated System for Health Information DE-identification. **2008**, 31

1163	Publishing Sensitive Transactions for Itemset Utility. **2008**,	27
1162	Set-Expression Based Method for Effective Privacy Preservation. **2008**,	1
1161	(□,□)-Uniqueness: Anonymity Management for Data Publication. **2008**,	3
1160	A Data Sanitization Method for Privacy Preserving Data Re-publication. **2008**,	2
1159	Reference models for network data anonymization. **2008**,	3
1158	An Improved V-MDAV Algorithm for l-Diversity. **2008**,	8
1157	A brief survey on anonymization techniques for privacy preserving publishing of social network data. **2008**, 10, 12-22	211
1156	The cost of privacy. **2008**,	145
1155	An l-MDAV microaggregation algorithm for sensitive attribute l-diversity. **2008**,	1
1154	Anonymizing transaction databases for publication. **2008**,	94
1153	Privacy preserving serial data publishing by role composition. **2008**, 1, 845-856	46
1152	Anonymity for continuous data publishing. **2008**,	45
1151	Privacy-preserving anonymization of set-valued data. **2008**, 1, 115-125	151
1150	Data utility and privacy protection trade-off in k-anonymisation. **2008**,	18
1149	Workload-aware anonymization techniques for large-scale datasets. **2008**, 33, 1-47	57
1148	Differential Privacy: A Survey of Results. **2008**, 1-19	1056
1147	Resisting structural re-identification in anonymized social networks. **2008**, 1, 102-114	293
1146	On static and dynamic methods for condensation-based privacy-preserving data mining. **2008**, 33, 1-39	23

1145 Zerber. **2008**, 24

1144 An efficient clustering method for k-anonymization. **2008**, 43

1143 Protecting privacy in recorded conversations. **2008**, 3

1142 Privacy. **2008**, 6

1141 Virtual trip lines for distributed privacy-preserving traffic monitoring. **2008**, 214

1140 Anonymizing bipartite graph data using safe groupings. **2008**, 1, 833-844 83

1139 InstantDB: Enforcing Timely Degradation of Sensitive Data. **2008**, 5

1138 A Critique of k-Anonymity and Some of Its Enhancements. **2008**, 64

1137 Towards a Privacy Diagnosis Centre: Measuring k-Anonymity. **2008**, 2

1136 Privacy-safe network trace sharing via secure queries. **2008**, 15

1135 Does enforcing anonymity mean decreasing data usefulness?. **2008**, 1

1134 Relationship privacy. **2009**, 62

1133 Distributed Anonymization: Achieving Privacy for Both Data Subjects and Data Providers. **2009**, 191-207 26

1132 Privacy-Aware Collaborative Spam Filtering. **2009**, 20, 725-739 20

1131 Human Behavior and Challenges of Anonymizing WLAN Traces. **2009**, 5

1130 Privacy preservation for attribute order sensitive workload in medical data publishing. **2009**, 2

1129 An Improved Method for Privacy Preserving Data Mining. **2009**, 10

1128 TIAMAT. **2009**, 2, 1618-1621 13

1127	Personalized-Granular k-Anonymity. **2009**,	1
1126	Towards Preference-Constrained k-Anonymisation. **2009**, 231-245	11
1125	Preserving FDs in K-Anonymization by K-MSDs and Association Generalization. **2009**,	
1124	A Lattice-Based Privacy Aware Access Control Model. **2009**,	13
1123	An efficient online auditing approach to limit private data disclosure. **2009**,	3
1122	The union-split algorithm and cluster-based anonymization of social networks. **2009**,	39
1121	Anonymization-based attacks in privacy-preserving data publishing. **2009**, 34, 1-46	10
1120	Injecting purpose and trust into data anonymisation. **2009**,	6
1119	k-automorphism. **2009**, 2, 946-957	219
1118	On the comparison of microdata disclosure control algorithms. **2009**,	3
1117	A Privacy Enhancing Approach for Identity Inference Protection in Location-Based Services. **2009**,	1
1116	(□□k)-anonymity: An effective privacy preserving model for databases. **2009**,	
1115	Privacy Preserving k-Anonymity for Re-publication of Incremental Datasets. **2009**,	1
1114	Privately querying location-based services with SybilQuery. **2009**,	71
1113	Privacy aware data sharing. **2009**,	9
1112	Detecting privacy violations in database publishing using disjoint queries. **2009**,	2
1111	A tree-based approach to preserve the privacy of software engineering data and predictive models. **2009**,	2
1110	Anonymizing location-based RFID data. **2009**,	0

1109 ANGEL: Enhancing the Utility of Generalization for Privacy Preserving Publication. **2009**, 21, 1073-1087 41

1108 Multirelational k-Anonymity. **2009**, 21, 1104-1117 52

1107 Class-based graph anonymization for social network data. **2009**, 2, 766-777 107

1106 Optimal random perturbation at multiple privacy levels. **2009**, 2, 814-825 30

1105 Anonymization of set-valued data via top-down, local generalization. **2009**, 2, 934-945 99

1104 Distribution based microdata anonymization. **2009**, 2, 958-969 6

1103 HIDE. **2009**, 6

1102 Confidentiality-preserving distributed proofs of conjunctive queries. **2009**, 3

1101 Anonymizing moving objects. **2009**, 82

1100 Continuous privacy preserving publishing of data streams. **2009**, 36

1099 Privacy protection for RFID data. **2009**, 17

1098 Anonymized data. **2009**, 28

1097 On the tradeoff between privacy and utility in data publishing. **2009**, 124

1096 Privacy integrated queries. **2009**, 510

1095 Adversarial-knowledge dimensions in data privacy. **2009**, 18, 429-467 2

1094 Genetic algorithm-based clustering approach for k-anonymization. **2009**, 36, 9784-9792 17

1093 (日k)-anonymous data publishing. **2009**, 33, 209-234 28

1092 Revelation on demand. **2009**, 25, 5-28 1

1091	Query Evaluation on a Database Given by a Random Graph. **2009**, 44, 503-532	1
1090	Disclosure Control of Business Microdata: A Density-Based Approach. **2009**, 77, 196-211	2
1089	An integrated framework for de-identifying unstructured medical data. **2009**, 68, 1441-1451	41
1088	k-Anonymous data collection. **2009**, 179, 2948-2963	22
1087	Task Independent Privacy Preserving Data Mining on Medical Dataset. **2009**,	6
1086	. **2009**,	40
1085	Hiding distinguished ones into crowd. **2009**,	5
1084	Preserving Anonymity of Recurrent Location-Based Queries. **2009**,	16
1083	Data publishing against realistic adversaries. **2009**, 2, 790-801	29
1082	Privacy of Value-Added Context-Aware Service Cloud. **2009**, 547-552	4
1081	. **2009**,	4
1080	Using Anonymized Data for Classification. **2009**,	40
1079	Preventing Unwanted Social Inferences with Classification Tree Analysis. **2009**,	4
1078	Secure kNN computation on encrypted databases. **2009**,	465
1077	A New Grid-Based Cloaking Algorithm for Privacy Protection in Location-Based Services. **2009**,	6
1076	Deriving Private Information from Association Rule Mining Results. **2009**,	10
1075	A local distributed peer-to-peer algorithm using multi-party optimization based privacy preservation for data mining primitive computation. **2009**,	
1074	Security considerations in the design and peering of RFID Discovery Services. **2009**,	6

1073 Efficient Anonymizations with Enhanced Utility. **2009**, 4

1072 Twins (1): Extending SQL to Support Corporation Privacy Policies in Social Networks. **2009**, 2

1071 Simple data transformation method for privacy preserving data re-publication. **2009**,

1070 Modeling and Integrating Background Knowledge in Data Anonymization. **2009**, 33

1069 A Model for Privacy Policy Visualization. **2009**, 20

1068 SQL Privacy Model for Social Networks. **2009**, 4

1067 Fine-Grain Perturbation for Privacy Preserving Data Publishing. **2009**, 2

1066 . **2009**, 16

1065 An Attack on the Privacy of Sanitized Data that Fuses the Outputs of Multiple Data Miners. **2009**, 5

1064 A framework for efficient data anonymization under privacy and accuracy constraints. **2009**, 34, 1-47 49

1063 Caching as Privacy Enhancing Mechanism in Location-Based Services. **2009**, 2

1062 Extending l-Diversity for Better Data Anonymization. **2009**,

1061 Energy Efficient Privacy Preserved Data Gathering in Wireless Sensor Networks Having Multiple Sinks. **2009**, 2

1060 Engineering Privacy. **2009**, 35, 67-82 247

1059 A novel privacy preserving approach for database security. **2009**,

1058 The Challenges of Effectively Anonymizing Network Data. **2009**, 17

1057 Against Classification Attacks: A Decision Tree Pruning Approach to Privacy Protection in Data Mining. **2009**, 57, 1496-1509 17

1056 Verification of the Security against Inference Attacks on XML Databases. **2009**, E92-D, 1022-1032 3

1055	Protecting location privacy against spatial inferences. **2009**,	17
1054	Minimizing minimality and maximizing utility. **2010**, 3, 1045-1056	22
1053	Classifying data from protected statistical datasets. **2010**, 29, 875-890	28
1052	On the use of economic price theory to find the optimum levels of privacy and information utility in non-perturbative microdata anonymisation. **2010**, 69, 399-423	4
1051	Anonymizing bipartite graph data using safe groupings. **2010**, 19, 115-139	38
1050	Enabling search services on outsourced private spatial data. **2010**, 19, 363-384	77
1049	Suppressing microdata to prevent classification based inference. **2010**, 19, 385-410	2
1048	Resisting structural re-identification in anonymized social networks. **2010**, 19, 797-823	61
1047	A local asynchronous distributed privacy preserving feature selection algorithm for large peer-to-peer networks. **2010**, 24, 341-367	29
1046	Privacy-Preserving Data Sharing in Cloud Computing. **2010**, 25, 401-414	33
1045	Mining non-redundant diverse patterns: an information theoretic perspective. **2010**, 4, 89-99	
1044	Online Anonymity Protection in Computer-Mediated Communication. **2010**, 5, 570-580	5
1043	Anonymization of moving objects databases by clustering and perturbation. **2010**, 35, 884-910	117
1042	Preserving privacy in participatory sensing systems. **2010**, 33, 1266-1280	84
1041	Small domain randomization. **2010**, 3, 608-618	14
1040	A New Privacy Preserving Approach Used in Cloud Computing. **2010**, 439-440, 1318-1323	0
1039	A Novel Privacy Preserving Model for Datasets Re-Publication. **2010**, 108-111, 1433-1438	
1038	Non-homogeneous generalization in privacy preserving data publishing. **2010**,	38

1037 Privacy-aware location data publishing. **2010**, 35, 1-42 39

1036 Preserving privacy in social networks against subgraph attacks. **2010**,

1035 Unified Metric for Measuring Anonymity and Privacy with Application to Online Social Network. **2010**,

1034 On Attribute Disclosure in Randomization Based Privacy Preserving Data Publishing. **2010**, 4

1033 A Distributed Query Protocol for Continuous Privacy Preserving in Wireless Sensor Networks. **2010**, 1

1032 Anonymization of electronic medical records for validating genome-wide association studies. **2010**, 107, 7898-903 98

1031 . **2010**, 22, 943-956 105

1030 From t-Closeness-Like Privacy to Postrandomization via Information Theory. **2010**, 22, 1623-1636 102

1029 Privacy-preserving similarity-based text retrieval. **2010**, 10, 1-39 31

1028 Information Integration for Terrorist or Criminal Social Networks. **2010**, 41-57 1

1027 Presence without Complete World Knowledge. **2010**, 22, 868-883 23

1026 Achieving anonymity via clustering. **2010**, 6, 1-19 51

1025 Towards publishing recommendation data with predictive anonymization. **2010**, 10

1024 A practice-oriented framework for measuring privacy and utility in data sanitization systems. **2010**, 11

1023 Anonymizing data with quasi-sensitive attribute values. **2010**, 9

1022 k-Anonymity in the Presence of External Databases. **2010**, 22, 392-403 18

1021 A privacy data set release method for balancing privacy protection and usability. **2010**, 1

1020 GSSK: A Generalization Step Safe Algorithm in Anonymizing Data. **2010**, 1

1019	B-CASTLE: An Efficient Publishing Algorithm for K-Anonymizing Data Streams. **2010**,	11
1018	Fragments and loose associations. **2010**, 3, 1370-1381	28
1017	KIDS:K-anonymization data stream base on sliding window. **2010**,	4
1016	Versatile publishing for privacy preservation. **2010**,	15
1015	Privacy-preserving data publishing. **2010**,	2
1014	Search-log anonymization and advertisement. **2010**,	1
1013	Relationships and data sanitization. **2010**,	13
1012	Beyond Safe Harbor: Automatic Discovery of Health Information De-identification Policy Alternatives. **2010**, 2010, 163-172	12
1011	Expressing privacy metrics as one-symbol information. **2010**,	5
1010	Restoring compromised privacy in micro-data disclosure. **2010**,	
1009	Towards an axiomatization of statistical privacy and utility. **2010**,	54
1008	Performance study of active tracking in a cellular network using a modular signaling platform. **2010** ,	6
1007	Inference control to protect sensitive information in text documents. **2010**,	3
1006	Towards a Risk-Driven Methodology for Privacy Metrics Development. **2010**,	9
1005	Toward Identity Anonymization in Social Networks. **2010**, 359-385	8
1004	Generalizing terrorist social networks with K-nearest neighbor and edge betweeness for social network integration and privacy preservation. **2010**,	3
1003	An Efficient Method for Knowledge Hiding Through Database Extension. **2010**,	
1002	Query m-Invariance: Preventing Query Disclosures in Continuous Location-Based Services. **2010**,	31

1001	Towards wider cloud service applicability by security, privacy and trust measurements. **2010**,	6
1000	Differentially private aggregation of distributed time-series with transformation and encryption. **2010**,	266
999	A Survey of Privacy-Preservation of Graphs and Social Networks. **2010**, 421-453	63
998	Privacy-preserving data publishing. **2010**, 42, 1-53	867
997	Research on Privacy Protection Based on K-Anonymity. **2010**,	1
996	A Privacy Data Release Method Based on Game Theory. **2010**,	1
995	Preserving privacy in semantic-rich trajectories of human mobility. **2010**,	8
994	A Brief Survey on De-anonymization Attacks in Online Social Networks. **2010**,	23
993	Correlation hiding by independence masking. **2010**,	5
992	Privacy preservation in transaction databases based on anatomy technique. **2010**,	0
991	Towards a Common Notion of Privacy Leakage on Public Database. **2010**,	2
990	Mobile systems location privacy: MobiPriv a robust k anonymous system. **2010**,	6
989	Ontology-Enhanced Interactive Anonymization in Domain-Driven Data Mining Outsourcing. **2010**,	1
988	Probabilistic Inference Protection on Anonymized Data. **2010**,	2
987	. **2010**,	7
986	Global privacy guarantee in serial data publishing. **2010**,	9
985	A new perspective of privacy protection: Unique distinct l-SR diversity. **2010**,	
984	Research on Diversity of Sensitive Attribute of K-Anonymity. **2010**,	0

983	K-isomorphism. **2010**,	160
982	Secure and effective anonymization against re-publication of dynamic datasets. **2010**,	
981	New Approach to Quantification of Privacy on Social Network Sites. **2010**,	13
980	Anonymizing Temporal Data. **2010**,	6
979	A New Approach to Manage Security against Neighborhood Attacks in Social Networks. **2010**,	23
978	Privacy Preservation Naïve Bayes Classification for a Vertically Distribution Scenario Using Trusted Third Party. **2010**,	3
977	Privacy Frost: A User-Oriented Data Anonymization Tool. **2011**,	3
976	Rating: Privacy Preservation for Multiple Attributes with Different Sensitivity Requirements. **2011**,	13
975	Separating the baby from the bathwater: Toward a generic and practical framework for anonymization. **2011**,	2
974	A model for privacy policy agreement in online services. **2011**,	
973	Towards a Safe Realization of Privacy-Preserving Data Publishing Mechanisms. **2011**,	0
972	Safe realization of the Generalization privacy mechanism. **2011**,	
971	Decision Support for Patient Consent Management. **2011**,	1
970	A Privacy Reinforcement Approach against De-identified Dataset. **2011**,	1
969	A fast p-sensitive l-diversity Anonymisation algorithm. **2011**,	8
968	CASTLE: Continuously Anonymizing Data Streams. **2011**, 8, 337-352	70
967	Privacy in Social Networks: A Survey. **2011**, 277-306	46
966	Spatial Data Management. **2011**, 3, 1-149	10

965 A Graph Enrichment Based Clustering over Vertically Partitioned Data. **2011**, 42-54

964 Adaptive, secure, and scalable distributed data outsourcing. **2011**, 6

963 Protection of query privacy for continuous location based services. **2011**, 78

962 On the (f)utility of untrusted data sanitization. **2011**, 1

961 Trusted Framework for Health Information Exchange. **2011**, 3

960 On the Design and Analysis of the Privacy-Preserving SVM Classifier. **2011**, 23, 1704-1717 95

959 Privacy-Preserving Data Mining from Outsourced Databases. **2011**, 411-426 5

958 Utilizing IHE-based Electronic Health Record systems for secondary use. **2011**, 50, 319-25 9

957 Empirical Comparisons of Attack and Protection Algorithms for Online Social Networks. **2011**, 5, 705-712

956 . **2011**, 62, 2755-2769 2

955 Publishing anonymous survey rating data. **2011**, 23, 379-406 26

954 SABRE: a Sensitive Attribute Bucketization and REdistribution framework for t-closeness. **2011**, 20, 59-81 42

953 Local and global recoding methods for anonymizing set-valued data. **2011**, 20, 83-106 68

952 A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements. **2011**, 16, 3-32 241

951 The k-anonymity and l-diversity approaches for privacy preservation in social networks against neighborhood attacks. **2011**, 28, 47-77 148

950 COAT: COnstraint-based anonymization of transactions. **2011**, 28, 251-282 35

949 Efficient systematic clustering method for k-anonymization. **2011**, 48, 51-66 52

948 Preventing range disclosure in k-anonymised data. **2011**, 38, 4559-4574 12

947	A family of enhanced -diversity models for privacy preserving data publishing. **2011**, 27, 348-356	31
946	Multi-objective optimization based privacy preserving distributed data mining in Peer-to-Peer networks. **2011**, 4, 192-209	5
945	Mixture of gaussian models and bayes error under differential privacy. **2011**,	1
944	Can the Utility of Anonymized Data be Used for Privacy Breaches?. **2011**, 5, 1-24	36
943	Provenance views for module privacy. **2011**,	24
942	Differentially private data cubes. **2011**,	73
941	Personal privacy vs population privacy. **2011**,	45
940	Privacy-aware mobile location-based systems. **2011**,	0
939	Utility-driven anonymization in data publishing. **2011**,	3
938	Preserving privacy of moving objects via temporal clustering of spatio-temporal data streams. **2011** ,	4
937	Identity obfuscation in graphs through the information theoretic lens. **2011**,	31
936	Privacy preservation in the dissemination of location data. **2011**, 13, 6-18	24
935	Query-Aware Anonymization in Location-Based Service. **2011**,	3
934	BM (Break-Merge): An Elegant Approach for Privacy Preserving Data Publishing. **2011**,	
933	A Privacy-Aware Bayesian Approach for Combining Classifier and Cluster Ensembles. **2011**,	
932	Issues in the Development of Location Privacy Theory. **2011**,	2
931	Increment Update Algorithms Basing on Semantic Similarity Degree for K-Anonymized Dataset. **2011**, 267, 328-333	
930	Anonoymizing Methods against Republication of Incremental Numerical Sensitive Data. **2011**, 267, 499-503	

929	State-of-the-art in distributed privacy preserving data mining. **2011**,	5
928	k-Anonymization in the Presence of Publisher Preferences. **2011**, 23, 1678-1690	4
927	Instant anonymization. **2011**, 36, 1-33	11
926	Anonymous Publication of Sensitive Transactional Data. **2011**, 23, 161-174	44
925	Protecting Privacy Against Record Linkage Disclosure: A Bounded Swapping Approach for Numeric Data. **2011**, 22, 774-789	19
924	Output privacy in data mining. **2011**, 36, 1-34	59
923	An analytical solution for consent management in patient privacy preservation. **2012**,	7
922	Recursive partitioning and summarization. **2012**,	9
921	Answering vertex aggregate queries using anonymized social network data. **2012**,	
920	Differential privacy in data publication and analysis. **2012**,	30
919	GUPT. **2012**,	109
918	Privacy preservation by disassociation. **2012**, 5, 944-955	41
917	Obfuscation of sensitive data in network flows. **2012**,	13
916	Privacy and utility for defect prediction: Experiments with MORPH. **2012**,	32
915	Hardware acceleration and data-utility improvement for low-latency privacy preserving mechanism. **2012**,	2
914	Location l-Diversity against Multifarious Inference Attacks. **2012**,	1
913	Privacy Issues in Social Networks: A Brief Survey. **2012**, 509-518	4
912	Hiding trajectory on the fly. **2012**,	2

911	N-SA K-anonymity Model: A Model Exclusive of Tuple Suppression Technique. **2012**,	3
910	Design and Evaluation of SensorSafe: A Framework for Achieving Behavioral Privacy in Sharing Personal Sensory Information. **2012**,	3
909	. **2012**,	1
908	A decentralized Location-Query-Sensitive Cloaking algorithm for LBS. **2012**,	3
907	An algorithm to achieve k-anonymity and l-diversity anonymisation in social networks. **2012**,	9
906	Decidability of the Security against Inference Attacks Using a Functional Dependency on XML Databases. **2012**, E95.D, 1365-1374	1
905	MHD: A New Method towards Privacy Protecting Datasets Published. **2012**, 214, 792-798	
904	Slicing: A New Approach for Privacy Preserving Data Publishing. **2012**, 24, 561-574	139
903	Efficient microaggregation techniques for large numerical data volumes. **2012**, 11, 253-267	20
902	A Coalitional Game Theoretic Mechanism for Privacy Preserving Publishing Based on k-Anonymity. **2012**, 6, 889-896	4
901	Secure distributed computation of anonymized views of shared databases. **2012**, 37, 1-43	12
900	An efficient method to implement data private protection for dynamic numerical sensitive attributes. **2012**,	1
899	Message Passing Based Privacy Preserve in Social Networks. **2012**,	0
898	A Semantics-Based Privacy-Aware Approach for Fragmenting Business Processes. **2012**,	0
897	Applicability of existing anonymization methods to large location history data in urban travel. **2012**,	3
896	A trusted information sharing skeleton for privacy preservation. **2012**,	1
895	Enhancing Privacy and Accuracy in Probe Vehicle-Based Traffic Monitoring via Virtual Trip Lines. **2012**, 11, 849-864	64
894	An efficient approach for data privacy in distributed environment using Nearest Neighbor Search Anonymization. **2012**,	

893	Reconstructing Profiles from Information Disseminated on the Internet. **2012**,	5
892	A Hybrid Approach to Private Record Matching. **2012**, 9, 684-698	8
891	PShare: Position sharing for location privacy based on multi-secret sharing. **2012**,	17
890	A survey of transaction dada anonymous publication. **2012**,	1
889	Risk-based modelling for managing privacy protection. **2012**,	0
888	Reducing Amount of Information Loss in k-Anonymization for Secondary Use of Collected Personal Information. **2012**,	1
887	A Study on the Impact of Data Anonymization on Anti-discrimination. **2012**,	6
886	Obfuscating the Topical Intention in Enterprise Text Search. **2012**,	14
885	Differentially Private Spatial Decompositions. **2012**,	197
884	A planetary nervous system for social mining and collective awareness. **2012**, 214, 49-75	48
883	A Look-Ahead Approach to Secure Multiparty Protocols. **2012**, 24, 1170-1185	7
882	A Model for Quantifying Information Leakage. **2012**, 25-44	5
881	Location Privacy and Attacker Knowledge: Who Are We Fighting against?. **2012**, 96-115	7
880	Anonymisation of Social Networks and Rough Set Approach. **2012**, 269-309	3
879	Sensitive Label Privacy Protection on Social Network Data. **2012**, 562-571	14
878	Enabling Multilevel Trust in Privacy Preserving Data Mining. **2012**, 24, 1598-1612	35
877	Demonstration of Damson: Differential Privacy for Analysis of Large Data. **2012**,	4
876	A new model for privacy preserving sensitive Data Mining. **2012**,	8

875	Privacy in mobile technology for personal healthcare. **2012**, 45, 1-54	118
874	Privacy Enhancing Framework on PaaS. **2012**,	6
873	A Randomized Response Model For Privacy Preserving Smart Metering. **2012**, 3, 1317-1324	52
872	On the identity anonymization of high-dimensional rating data. **2012**, 24, 1108-1122	3
871	More than modelling and hiding: towards a comprehensive view of Web mining and privacy. **2012**, 24, 697-737	13
870	Publishing Set-Valued Data Against Realistic Adversaries. **2012**, 27, 24-36	7
869	Secure multidimensional range queries over outsourced data. **2012**, 21, 333-358	133
868	Biometric Security and Privacy Using Smart Identity Management and Interoperability: Validation and Vulnerabilities of Various Techniques. **2012**, 29, 63-89	2
867	Privacy aware publishing of successive location information in sensor networks. **2012**, 28, 913-922	5
866	Kd-trees and the real disclosure risks of large statistical databases. **2012**, 13, 260-273	10
865	Limiting disclosure of sensitive data in sequential releases of databases. **2012**, 191, 98-127	30
864	An approximate microaggregation approach for microdata protection. **2012**, 39, 2211-2219	12
863	Hiding co-occurring prioritized sensitive patterns over distributed progressive sequential data streams. **2012**, 35, 1116-1129	2
862	. **2012**, 61, 101-117	14
861	On learning cluster coefficient of private networks. **2013**, 3, 925-938	10
860	Toward a taxonomy of communications security models. **2013**, 3, 181-195	1
859	Anonymization technique through record elimination to preserve privacy of published data. **2013**,	12
858	Semantic trajectories modeling and analysis. **2013**, 45, 1-32	304

857 Re-identification of Smart Meter data. **2013**, 17, 653-662 34

856 Toward Efficient Filter Privacy-Aware Content-Based Pub/Sub Systems. **2013**, 25, 2644-2657 18

855 Efficient and flexible anonymization of transaction data. **2013**, 36, 153-210 37

854 Empirical privacy and empirical utility of anonymized data. **2013**, 19

853 A K-anonymity model with strongly identifiable attributes. **2013**,

852 The Costs of Privacy in Local Energy Markets. **2013**, 13

851 Anonymizing Face Images by Using Similarity-Based Metric. **2013**, 3

850 Privacy Measurement for Social Network Actor Model. **2013**, 10

849 Achieving Probabilistic Anonymity Against One-to-Multiple Linkage Attacks. **2013**, 1

848 HALT: Hybrid anonymization of longitudinal transactions. **2013**, 2

847 Privacy-preserving computation for location-based information survey via mobile cloud computing. **2013**,

846 Privacy-Preserving Kernel k-Means Outsourcing with Randomized Kernels. **2013**, 6

845 (K, G)-anonymity model based on grey relational analysis. **2013**, 1

844 SONET: A SOcial NETwork Model for Privacy Monitoring and Ranking. **2013**, 10

843 GASNA. **2013**, 2

842 A modification of the Lloyd algorithm for k-anonymous quantization. **2013**, 222, 185-202 19

841 Privacy protection method for fine-grained urban traffic modeling using mobile sensors. **2013**, 56, 50-69 32

840 Supporting Pattern-Preserving Anonymization for Time-Series Data. **2013**, 25, 877-892 13

839	Class Restricted Clustering and Micro-Perturbation for Data Privacy. **2013**, 59,	19
838	. **2013**,	20
837	An anonymized method for classification with weighted attributes. **2013**,	1
836	On the measurement of privacy as an attacker's estimation error. **2013**, 12, 129-149	24
835	An Iterative Algorithm for Differentially Private Histogram Publication. **2013**,	
834	Data anonymization and integrity checking in cloud computing. **2013**,	4
833	EPS: Encounter-Based Privacy-Preserving Scheme for Location-Based Services. **2013**,	12
832	The Scourge of Internet Personal Data Collection. **2013**,	4
831	MobiCache: When k-anonymity meets cache. **2013**,	4
830	SplitX. **2013**,	13
829	A propagation model for provenance views of public/private workflows. **2013**,	4
828	Efficient and accurate strategies for differentially-private sliding window queries. **2013**,	14
827	Utility-maximizing event stream suppression. **2013**,	11
826	Incorporating Privacy into the Undergraduate Curriculum. **2013**,	1
825	de-linkability. **2013**,	2
824	Privacy for Location-based Services. **2013**, 4, 1-85	36
823	Lightweight privacy-preserving peer-to-peer data integration. **2013**, 6, 157-168	3
822	Efficient Time-Stamped Event Sequence Anonymization. **2013**, 8, 1-53	5

821 A Multi-phase k-anonymity Algorithm Based on Clustering Techniques. **2013**, 365-372 1

820 Privacy by design. **2013**, 19

819 Privacy-Preserving Data Publishing Based on Utility Specification. **2013**, 0

818 ANGELMS: A privacy preserving data publishing framework for microdata with multiple sensitive attributes. **2013**,

817 (k, ℓ)-Anonymity: An anonymity model for thwarting similarity attack. **2013**, 1

816 Perturbed Gibbs Samplers for Generating Large-Scale Privacy-Safe Synthetic Health Data. **2013**, 5

815 An enhanced l-diversity privacy preservation. **2013**, 1

814 A novel algorithm of personalized-granular k-anonymity. **2013**,

813 SplitX. **2013**, 43, 315-326 6

812 openPDS: protecting the privacy of metadata through SafeAnswers. **2014**, 9, e98790 120

811 A Semantic Approach for Semi-Automatic Detection of Sensitive Data. **2014**, 27, 23-44 2

810 Smart Grid Data Anonymization for Smart Grid Privacy. **2014**, 89-96 2

809 Improving the Utility of Differential Privacy via Univariate Microaggregation. **2014**, 130-142 6

808 Agent-Based Privacy Aware Feedback System. **2014**, 725-738 1

807 Privacy-aware filter-based feature selection. **2014**, 3

806 How to Find an Appropriate K for K-Anonymization. **2014**, 2

805 A Generalized Approach for Social Network Integration and Analysis with Privacy Preservation. **2014**, 259-280 0

804 PRECISE:PRivacy-prEserving Cloud-assisted quality Improvement Service in hEalthcare. **2014**, 2014, 176-183 11

803	Aroma. **2014**,	7
802	. **2014**,	0
801	Anonymization on refining partition: Same privacy, more utility. **2014**,	
800	K-concealment based Distributed Anonymization for the Cloud. **2014**,	
799	Differential privacy with □eighbourhood for spatial and dynamic datasets. **2014**,	6
798	POLA: A privacy-preserving protocol for location-based real-time advertising. **2014**,	2
797	Privacy-Preserving Queries over Outsourced Data with Access Pattern Protection. **2014**,	5
796	Toward inference attacks for k-anonymity. **2014**, 18, 1871-1880	11
795	Achieving k-anonymity in privacy-aware location-based services. **2014**,	208
794	Preserving privacy for sensitive values of individuals in data publishing based on a new additive noise approach. **2014**,	5
793	Obtaining K -obfuscation for profile privacy in social networks. **2014**, 7, 1384-1398	
792	Resisting label-neighborhood attacks in outsourced social networks. **2014**,	3
791	Comparison of ID3 and CART-ANFIS approach for play-tennis data. **2014**,	0
790	. **2014**,	3
789	Sensitive attribute based non-homogeneous anonymization for privacy preserving data mining. **2014**,	2
788	Effects of External Information on Anonymity and Role of Transparency with Example of Social Network De-anonymisation. **2014**,	2
787	Mining Standardized Semantic Interoperable Electronic Healthcare Records. **2014**, 179-193	4
786	Identity obfuscation in graphs through the information theoretic lens. **2014**, 275, 232-256	20

785 Optimizing the design parameters of threshold pool mixes for anonymity and delay. **2014**, 67, 180-200 8

784 A data recipient centered de-identification method to retain statistical attributes. **2014**, 50, 32-45 14

783 MAGE: A semantics retaining K-anonymization method for mixed data. **2014**, 55, 75-86 9

782 Effective mix-zone anonymization techniques for mobile travelers. **2014**, 18, 135-164 10

781 Ensuring location diversity in privacy-preserving spatio-temporal data publishing. **2014**, 23, 609-625 34

780 Measuring the privacy of user profiles in personalized information systems. **2014**, 33, 53-63 37

779 Enhancing data utility in differential privacy via microaggregation-based (k)-anonymity. **2014**, 23, 771-794 100

778 . **2014**, 26, 1591-1601 19

777 Identity Protection in Sequential Releases of Dynamic Networks. **2014**, 26, 635-651 14

776 K-anonymity for social networks containing rich structural and textual information. **2014**, 4, 1 6

775 Protecting the primary users' operational privacy in spectrum sharing. **2014**, 50

774 Loki: A privacy-conscious platform for crowdsourced surveys. **2014**, 7

773 Specification and Deployment of Integrated Security Policies for Outsourced Data. **2014**, 17-32 2

772 m-cloud -- Distributed Statistical Computation Using Multiple Cloud Computers. **2014**, 6

771 . **2014**, 9, 709-718 6

770 Publishing data from electronic health records while preserving privacy: a survey of algorithms. **2014**, 50, 4-19 115

769 Protecting Location Privacy with Clustering Anonymization in vehicular networks. **2014**, 14

768 A data anonymous method based on overlapping slicing. **2014**, 4

767	Quantifying the costs and benefits of privacy-preserving health data publishing. **2014**, 50, 107-21	24
766	Small sum privacy and large sum utility in data publishing. **2014**, 50, 20-31	5
765	dependency for privacy-preserving XML data publishing. **2014**, 50, 77-94	5
764	. **2014**, 102, 270-281	51
763	Disassociation for electronic health record privacy. **2014**, 50, 46-61	33
762	Improving accuracy of classification models induced from anonymized datasets. **2014**, 256, 138-161	14
761	m -Privacy for Collaborative Data Publishing. **2014**, 26, 2520-2533	26
760	A framework for a privacy-aware feature selection evaluation measure. **2015**,	3
759	Mitigating Storage Side Channels Using Statistical Privacy Mechanisms. **2015**,	21
758	K-anonymity against neighborhood attacks in weighted social networks. **2015**, 8, 3864-3882	7
757	. **2015**, 9, 1256-1269	53
756	An approach for prevention of privacy breach and information leakage in sensitive data mining. **2015**, 45, 134-140	23
755	Differentially Private Frequent Sequence Mining via Sampling-based Candidate Pruning. **2015**, 2015, 1035-1046	11
754	Dataless Data Mining: Association Rules-Based Distributed Privacy-Preserving Data Mining. **2015**,	4
753	Graded medical data publishing based on clustering. **2015**,	
752	An Efficient Generalized Clustering Method for Achieving K-Anonymization. **2015**,	5
751	SECRETA: A Tool for Anonymizing Relational, Transaction and RT-Datasets. **2015**, 83-109	4
750	Aligning the Conflicting Needs of Privacy, Malware Detection and Network Protection. **2015**,	2

749 Utility-Constrained Electronic Health Record Data Publishing Through Generalization and Disassociation. **2015**, 149-177 2

748 Privacy impact assessment for online social networks. **2015**, 3

747 Location privacy preserving techniques for location based services over road networks. **2015**, 13

746 Privacy-Preserving Detection of Anomalous Phenomena in Crowdsourced Environmental Sensing. **2015**, 313-332 4

745 Aspern smart ICT: Data analytics and privacy challenges in a smart city. **2015**, 12

744 Dissemination of anonymized streaming data. **2015**, 1

743 A personalized two-tier cloaking scheme for privacy-aware location-based services. **2015**, 17

742 Anonymizing transactional datasets. **2015**, 23, 89-106 2

741 Risk-Aware Information Disclosure. **2015**, 266-276 8

740 Privacy by diversity in sequential releases of databases. **2015**, 298, 344-372 23

739 A survey on privacy preserving data mining. **2015**, 13

738 A privacy mechanism for mobile-based urban traffic monitoring. **2015**, 20, 1-12 8

737 Statistical Database Auditing Without Query Denial Threat. **2015**, 27, 20-34 4

736 Obfuscation of Sensitive Data for Incremental Release of Network Flows. **2015**, 23, 672-686 6

735 An Adaptive Learning Model for k-Anonymity Location Privacy Protection. **2015**, 7

734 Systematic Literature Review on the Anonymization of High Dimensional Streaming Datasets for Health Data Sharing. **2015**, 63, 348-355 12

733 Database Privacy. **2015**, 9-35 3

732 Policy-Carrying Data. **2015**, 7

731	On Information-theoretic Measures for Quantifying Privacy Protection of Time-series Data. **2015**,	7
730	Privacy-preserving strategies in service quality aware Location-Based Services. **2015**,	1
729	A robust privacy preserving model for data publishing. **2015**,	3
728	Differential privacy in telco big data platform. **2015**, 8, 1692-1703	34
727	Privacy-Preserving Data Publishing in the Cloud: A Multi-level Utility Controlled Approach. **2015**,	4
726	Towards Privacy Preservation in Strategy-Proof Spectrum Auction Mechanisms for Noncooperative Wireless Networks. **2015**, 23, 1271-1285	25
725	Database Fragmentation with Confidentiality Constraints. **2015**,	12
724	Differentially-Private Mining of Moderately-Frequent High-Confidence Association Rules. **2015**,	2
723	A Survey of Anonymization Algorithms for Electronic Health Records. **2015**, 17-34	4
722	On the anonymizability of graphs. **2015**, 45, 571-588	0
721	Secure support vector machines outsourcing with random linear transformation. **2015**, 44, 147-176	8
720	Publishing histograms with outliers under data differential privacy. **2016**, 9, 2313-2322	8
719	Differentially private frequent itemset mining via transaction splitting. **2016**,	3
718	Big data privacy: a technological perspective and review. **2016**, 3,	123
717	Semantic-based graph data anonymization for big data analysis. **2016**,	0
716	Overview of research center for information technology innovation in Taiwan Academia Sinica. **2016**,	
715	Model for Hiding Data Relationships Based on Chunk-Confusion in Cloud Computing. **2016**,	
714	An efficient private FIM on hadoop MapReduce. **2016**,	1

713 Data privacy protection based on sensitive attributes dynamic update. **2016**, 4

712 Two-phase entropy based approach to big data anonymization. **2016**, 2

711 Differential-Privacy-Based Citizen Privacy Preservation in E-Government Applications. **2016**,

710 . **2016**, 4

709 Data Protection Issues of Integrated Electronic Health Records (EHR). **2016**, 787-790 3

708 Social Network Integration and Analysis with Privacy Preservation. **2016**, 459-475

707 Preserving prosumer privacy in a district level smart grid. **2016**, 1

706 Privacy-Aware Big Data Warehouse Architecture. **2016**, 3

705 Time obfuscation-based privacy-preserving scheme for Location-Based Services. **2016**, 1

704 Time obfuscation-based privacy-preserving scheme for location-based services. **2016**, 5

703 Anatomisation with slicing: a new privacy preservation approach for multiple sensitive attributes. **2016**, 5, 964 27

702 IMR based Anonymization for Privacy Preservation in Data Mining. **2016**, 1

701 Privacy preserving data mining on published data in healthcare: A survey. **2016**, 2

700 Differentially private multi-party high-dimensional data publishing. **2016**, 19

699 Differentially Private Frequent Subgraph Mining. **2016**, 2016, 229-240 16

698 Evaluating applicability of perturbation techniques for privacy preserving data mining by descriptive statistics. **2016**, 3

697 Survey of Big Data Information Security. **2016**, 3

696 Differential Privacy: From Theory to Practice. **2016**, 8, 1-138 41

695	An Attribtue-Based Statistic Model for Privacy Impact Assessment. **2016**,	1
694	Achieving Probabilistic Anonymity in a Linear and Hybrid Randomization Model. **2016**, 11, 2187-2202	7
693	Anonymizing multimedia documents. **2016**, 19, 135-155	1
692	Quantification of private information leakage from phenotype-genotype data: linking attacks. **2016**, 13, 251-6	48
691	Privacy-preserving kernel k-means clustering outsourcing with random transformation. **2016**, 49, 885-908	15
690	Preventing sensitive relationships disclosure for better social media preservation. **2016**, 15, 173-194	
689	On Efficient and Robust Anonymization for Privacy Protection on Massive Streaming Categorical Information. **2017**, 14, 507-520	30
688	Location Anonymization With Considering Errors and Existence Probability. **2017**, 47, 3207-3218	4
687	Anonymizing and Sharing Medical Text Records. **2017**, 28, 332-352	29
686	Evaluating the Risk of Data Disclosure Using Noise Estimation for Differential Privacy. **2017**,	2
685	Data-Driven Approach for Evaluating Risk of Disclosure and Utility in Differentially Private Data Release. **2017**,	2
684	Utility Cost of Formal Privacy for Releasing National Employer-Employee Statistics. **2017**,	25
683	Big data security and privacy in healthcare: A Review. **2017**, 113, 73-80	87
682	Machine Learning and Knowledge Extraction in Digital Pathology Needs an Integrative Approach. **2017**, 13-50	14
681	Tutorial on Information Theoretic Metrics Quantifying Privacy in Cyber-Physical Systems. **2017**, 57-76	
680	A level-cut heuristic-based clustering approach for social graph anonymization. **2017**, 7, 1	1
679	Privacy Preservation Strategy in Time-Sensitive LBSs. **2017**,	0
678	DPLK-Means: A Novel Differential Privacy K-Means Mechanism. **2017**,	12

677 Identity vs. Attribute Disclosure Risks for Users with Multiple Social Profiles. **2017**, 6

676 A framework for adaptive differential privacy. **2017**, 1, 1-29 20

675 A New Approach to Utility-Based Privacy Preserving in Data Publishing. **2017**, 2

674 An Anonymization Method to Improve Data Utility for Classification. **2017**, 57-71 6

673 Hierarchical PSO Clustering on MapReduce for Scalable Privacy Preservation in Big Data. **2017**, 36-44 3

672 Efficient privacy-preserving content recommendation for online social communities. **2017**, 219, 440-454 30

671 A Survey of Big Data Security and Privacy Preserving. **2017**, 34, 544-560 24

670 Privacy preserving big data publishing: a scalable k-anonymization approach using MapReduce. **2017**, 11, 271-276 20

669 A scheme of privacy protection based on genetic algorithm for behavior pattern of social media users. **2017**,

668 A journey on privacy protection strategies in big data. **2017**, 1

667 Privacy-Preserving Big Data Stream Mining: Opportunities, Challenges, Directions. **2017**, 6

666 Implementing privacy using modified tree and map technique. **2017**, 3

665 An anonymization method combining anatomy and permutation for protecting privacy in microdata with multiple sensitive attributes. **2017**, 7

664 An Improved (k,p,l)-Anonymity Method for Privacy Preserving Collaborative Filtering. **2017**,

663 Research on K anonymity algorithm based on association analysis of data utility. **2017**, 1

662 A novel approach for securely processing information on dew sites (Dew computing) in collaboration with cloud computing: An approach toward latest research trends on Dew computing. **2017**, 2

661 Research on privacy preserving method based on T-closeness model. **2017**, 3

660 Enhanced additive noise approach for privacy-preserving tabular data publishing. **2017**, 1

659	Research and implementation of the algorithm for data de-identification for Internet of Things. **2017**,	0
658	A Relative Privacy Model for Effective Privacy Preservation in Transactional Data. **2017**,	2
657	How to Cooperate Locally to Improve Global Privacy in Social Networks? On Amplification of Privacy Preserving Data Aggregation. **2017**,	1
656	Group privacy-aware disclosure of association graph data. **2017**,	3
655	Differential privacy-based data de-identification protection and risk evaluation system. **2017**,	1
654	. **2017**,	2
653	The innovative secrecy measure for data broadcasting. **2017**,	0
652	Privacy-preserving Chi-squared testing for genome SNP databases. **2017**, 2017, 3884-3889	3
651	Large dataset summarization with automatic parameter optimization and parallel processing for outlier detection. **2017**,	
650	Attribute based diversity model for privacy preservation. **2017**,	
649	. **2017**,	
648	Canvas White Paper 4 Technological Challenges in Cybersecurity. **2017**,	2
647	Towards Privacy Preserving Publishing of Set-Valued Data on Hybrid Cloud. **2018**, 6, 316-329	20
646	Privacy-Preserving Publishing of Multilevel Utility-Controlled Graph Datasets. **2018**, 18, 1-21	9
645	The Privacy Implications of Cyber Security Systems. **2018**, 51, 1-27	28
644	Secure partial encryption with adversarial functional dependency constraints in the database-as-a-service model. **2018**, 116, 1-20	
643	A Research on the IOT Perception Environment Security and Privacy Protection Technology. **2018**, 104-115	1
642	Challenges and techniques in Big data security and privacy: A review. **2018**, 1, e13	7

641 Large dataset summarization with automatic parameter optimization and parallel processing for local outlier detection. **2018**, 30, e4466 5

640 Differential privacy: its technological prescriptive using big data. **2018**, 5, 15

639 Leveraging Spatial Diversity for Privacy-Aware Location-Based Services in Mobile Networks. **2018**, 13, 1524-1534 20

638 Privacy Characterization and Quantification in Data Publishing. **2018**, 30, 1756-1769 9

637 Big healthcare data: preserving security and privacy. **2018**, 5, 188

636 Hermes: A Privacy-Preserving Approximate Search Framework for Big Data. **2018**, 6, 20009-20020 4

635 Resisting re-identification mining on social graph data. **2018**, 21, 1759-1771 9

634 A Two-Phase Algorithm for Differentially Private Frequent Subgraph Mining. **2018**, 30, 1411-1425 16

633 Mutual Correlation-based Optimal Slicing for Preserving Privacy in Data Publishing. **2018**, 593-601

632 Virtualization Model for Processing of the Sensitive Mobile Data. **2018**, 121-133 1

631 Cross-Bucket Generalization for Information and Privacy Preservation. **2018**, 30, 449-459 8

630 From location to location pattern privacy in location-based services. **2018**, 56, 533-557 7

629 Anatomization through generalization (AG): A hybrid privacy-preserving approach to prevent membership, identity and semantic similarity disclosure attacks. **2018**, 9

628 Two Privacy-Preserving Approaches for Publishing Transactional Data Streams. **2018**, 6, 23648-23658 14

627 Encyclopedia of Big Data Technologies. **2018**, 1-9

626 Collaborative ensemble learning under differential privacy. **2018**, 16, 73-87 8

625 Privacy in Control and Dynamical Systems. **2018**, 1, 309-332 12

624 Blind Filtering at Third Parties: An Efficient Privacy-Preserving Framework for Location-Based Services. **2018**, 17, 2524-2535 46

623	A Survey on Privacy Preserving Dynamic Data Publishing. **2018**, 8, 1-20	2
622	AQ-DP: A New Differential Privacy Scheme Based on Quasi-Identifier Classifying in Big Data. **2018**,	2
621	A Novel (K, X)-isomorphism Method for Protecting Privacy in Weighted social Network. **2018**,	
620	Preserving Privacy for Hubs and Links in Social Networks. **2018**,	1
619	A Survey of Privacy Concerns in Wearable Devices. **2018**,	5
618	Autonomous, Decentralized and Privacy-Enabled Data Preparation for Evidence-Based Medicine with Brain Aneurysm as a Phenotype. **2018**, E101.B, 1787-1797	2
617	Graph-Based Data-Collection Policies for the Internet of Things. **2018**,	1
616	Privacy Preserving on Trajectories Created by Wi-Fi Connections in a University Campus. **2018**,	1
615	A Distributional Model of Sensitive Values on p-Sensitive in Multiple Sensitive Attributes. **2018**,	3
614	Efficient k-Anonymization through Constrained Collaborative Clustering. **2018**,	3
613	Privacy Issues and Data Protection in Big Data: A Case Study Analysis under GDPR. **2018**,	26
612	Privacy Preserving Big Data Publishing. **2018**,	8
611	Assessing Data Usefulness for Failure Analysis in Anonymized System Logs. **2018**,	3
610	Location privacy protection with a semi-honest anonymizer in information centric networking. **2018** ,	4
609	Adaptive Anonymization of Data using b-Edge Cover. **2018**,	3
608	An Efficient Way of Anonymization Without Subjecting to Attacks Using Secure Matrix Method. **2018**,	1
607	Secure Medical Data Collection via Local Differential Privacy. **2018**,	2
606	Privacy-Enhancing Technologies. **2018**, 9-33	

605	You Are Where You App: An Assessment on Location Privacy of Social Applications. **2018**,	2
604	Privacy-Preserving Algorithms for Multiple Sensitive Attributes Satisfying t-Closeness. **2018**, 33, 1231-1242	23
603	An information-aware visualization for privacy-preserving accelerometer data sharing. **2018**, 8,	11
602	Toward Scalable Anonymization for Privacy-Preserving Big Data Publishing. **2018**, 297-304	2
601	Privacy Policy and Technology in Biomedical Data Science. **2018**, 1, 115-129	11
600	Towards an anonymous incident communication channel for electric smart grids. **2018**,	3
599	Protecting Infrastructure Data via Enhanced Access Control, Blockchain and Differential Privacy. **2018**, 113-125	8
598	Incremental k -Anonymous Microaggregation in Large-Scale Electronic Surveys With Optimized Scheduling. **2018**, 6, 60016-60044	4
597	Precision Driven Privacy-Preserving Anonymization for Social Data Using Segmentation. **2018**,	0
596	Enhancing E-Healthcare Privacy Preservation Framework through L-Diversity. **2018**,	2
595	Users' Privacy Protection Scheme in Location Based Services. **2018**,	
594	HMC. **2018**, 2, 1-25	4
593	Anatomy of a Privacy-Safe Large-Scale Information Extraction System Over Email. **2018**,	4
592	Privacy-Preserving Triangle Counting in Large Graphs. **2018**,	11
591	Linking Differential Identifiability with Differential Privacy. **2018**, 232-247	4
590	Privacy Protection in Location-Based Services: A Survey. **2018**, 73-96	6
589	Achieve Efficient and Privacy-Preserving Medical Primary Diagnosis Based on kNN. **2018**,	3
588	An Information-Theoretic Approach to Time-Series Data Privacy. **2018**,	3

587	Risks of Sharing Cyber Incident Information. **2018**,	4
586	Privacy-preserving Anonymization with Restricted Search (PARS) on Social Network Data for Criminal Investigations. **2018**,	1
585	A Module for Protecting Data Location Privacy on Mobile Devices. **2018**,	
584	. **2018**, 6, 26543-26557	9
583	Contract-Based Private Data Collecting. **2018**, 59-88	
582	Obfuscation At-Source. **2018**, 2, 1-24	14
581	An efficient algorithm for minimal edit cost of graph degree anonymity. **2018**,	1
580	. **2018**,	1
579	Data Privacy in Hadoop Using Anonymization and T-Closeness. **2018**, 459-468	
578	The Case for Personalized Anonymization of Database Query Results. **2018**, 261-285	
577	Privacy Preservation Using Various Anonymity Models. **2018**, 119-130	1
576	Differentially private histogram publishing through Fractal dimension for dynamic datasets. **2018**,	2
575	Personalised anonymity for microdata release. **2018**, 12, 341-347	5
574	Design of an Anonymity-Preserving Group Formation Based Authentication Protocol in Global Mobility Networks. **2018**, 6, 20673-20693	41
573	Replacement AutoEncoder: A Privacy-Preserving Algorithm for Sensory Data Analysis. **2018**,	14
572	Does k -Anonymous Microaggregation Affect Machine-Learned Macrotrends?. **2018**, 6, 28258-28277	9
571	Dynamic Modeling of Location Privacy Protection Mechanisms. **2018**, 26-39	
570	Enhancing Privacy and Availability for Data Clustering in Intelligent Electrical Service of IoT. **2019**, 6, 1530-1540	100

569	Privacy in Internet of Things: From Principles to Technologies. **2019**, 6, 488-505	44
568	Two privacy-preserving approaches for data publishing with identity reservation. **2019**, 60, 1039-1080	8
567	Scalable non-deterministic clustering-based k-anonymization for rich networks. **2019**, 18, 219-238	10
566	Differentially Private Mechanisms for Budget Limited Mobile Crowdsourcing. **2019**, 18, 934-946	9
565	Security Services Using Blockchains: A State of the Art Survey. **2019**, 21, 858-880	182
564	A Study on Privacy-Preserving Approaches in Online Social Network for Data Publishing. **2019**, 99-115	3
563	DP-LTOD: Differential Privacy Latent Trajectory Community Discovering Services over Location-Based Social Networks. **2019**, 1-1	14
562	Enhance PATE on Complex Tasks With Knowledge Transferred From Non-Private Data. **2019**, 7, 50081-50094	4
561	Highly Efficient Privacy Preserving Location-Based Services with Enhanced One-Round Blind Filter. **2019**, 1-1	25
560	Sanitizing and measuring privacy of large sparse datasets for recommender systems. **2019**, 1	8
559	Privacy vs. Utility: An Enhanced K-coRated. **2019**, 566-578	
558	. **2019**,	
557	Trajectory Anonymization: Balancing Usefulness about Position Information and Timestamp. **2019**,	1
556	Differential Privacy-Preserving Density Peaks Clustering Based on Shared Near Neighbors Similarity. **2019**, 7, 89427-89440	5
555	The Automatic Detection of Sensitive Data in Smart Homes. **2019**, 404-416	0
554	Studying L-Diversity and K-Anonymity Over Datasets with Sensitive Fields. **2019**, 63-73	
553	Anonymization in Online Social Networks Based on Enhanced Equi-Cardinal Clustering. **2019**, 6, 809-820	16
552	Test-Driven Anonymization for Artificial Intelligence. **2019**,	0

551 Introduction. **2019**, 1-8

550 Matching Games. **2019**, 11-37

549 Contract Theory. **2019**, 38-107

548 Stochastic Games. **2019**, 108-111

547 Games with Bounded Rationality. **2019**, 112-122

546 Learning in Games. **2019**, 123-143

545 Equilibrium Programming with Equilibrium Constraints. **2019**, 144-167

544 Miscellaneous Games. **2019**, 168-192

543 Applications of Game Theory in the Internet of Things. **2019**, 195-257

542 Applications of Game Theory in Network Virtualization. **2019**, 258-269

541 Applications of Game Theory in Cloud Networking. **2019**, 270-314

540 Applications of Game Theory in Context-Aware Networks and Mobile Services. **2019**, 315-346

539 Applications of Game Theory for Green Communication Networks. **2019**, 347-376

538 4G, 5G, and Beyond. **2019**, 377-424

537 Security. **2019**, 425-458

536 Index. **2019**, 494-496

535 UHRP: Uncertainty-Based Pruning Method for Anonymized Data Linear Regression. **2019**, 19-33

534 A New Weight and Sensitivity Based Variable Maximum Distance to Average Vector Algorithm for Wearable Sensor Data Privacy Protection. **2019**, 7, 104045-104056 3

533	Challenges of Privacy-Preserving Machine Learning in IoT. **2019**,	7
532	Cover-up: a probabilistic privacy-preserving graph database model. **2019**, 1	2
531	Interchange-Based Privacy Protection for Publishing Trajectories. **2019**, 7, 138299-138314	3
530	Pseudonymization risk analysis in distributed systems. **2019**, 10,	9
529	Anonymizing building data for data analytics in cross-organizational settings. **2019**,	5
528	Privacy Preserving of IP Address through Truncation Method in Network-based Intrusion Detection System. **2019**,	0
527	Sensitive and Private Data Analysis. **2019**,	2
526	De-anonymizing Scale-Free Social Networks by Using Spectrum Partitioning Method. **2019**, 147, 441-445	0
525	A K-anonymous clustering algorithm based on the analytic hierarchy process. **2019**, 59, 76-83	8
524	The CO.R.E. Project. An Integrated Security Approach to Self-Monitoring and Medical Record Keeping. **2019**, 4, 1-8	
523	tau -Safe (l,k)-Diversity Privacy Model for Sequential Publication With High Utility. **2019**, 7, 687-701	8
522	Privacy Protection for Context-Aware Services: A Two-Layer Three-Party Game Model. **2019**, 124-136	
521	Enhanced Secured Map Reduce layer for Big Data privacy and security. **2019**, 6,	13
520	Safer Program Behavior Sharing Through Trace Wringing. **2019**,	0
519	Privacy Preservation in Publishing Electronic Health Records Based on Perturbation. **2019**, 125-140	0
518	Quantifying privacy vulnerability of individual mobility traces: A case study of license plate recognition data. **2019**, 104, 78-94	9
517	. **2019**, 7, 45773-45782	14
516	An Algorithm for l-diversity Clustering of a Point-Set. **2019**,	1

515	Privacy-Preserving Distributed Data Fusion Based on Attribute Protection. **2019**, 15, 5765-5777	9
514	Differential Privacy Preservation in Deep Learning: Challenges, Opportunities and Solutions. **2019**, 7, 48901-48911	38
513	PrivSem: Protecting location privacy using semantic and differential privacy. **2019**, 22, 2407-2436	5
512	A Survey of Spatial Crowdsourcing. **2019**, 44, 1-46	30
511	Privacy preserving publication of relational and transaction data: Survey on the anonymization of patient data. **2019**, 32, 45-61	11
510	Privacy-preserving Cross-domain Location Recommendation. **2019**, 3, 1-21	11
509	Enabling Differentially Private in Big Data Machine Learning. **2019**,	0
508	Local privacy protection classification based on human-centric computing. **2019**, 9,	15
507	Differentially Private Geo-Social Ranking. **2019**,	
506	Data Privacy Quantification and De-identification Model Based on Information Theory. **2019**,	0
505	Cluster-Based Anonymization of Directed Graphs. **2019**,	1
504	Self-Emerging Data Infrastructures. **2019**,	1
503	Preserving Privacy in Personal Data Processing. **2019**,	2
502	AnonymousNet: Natural Face De-Identification With Measurable Privacy. **2019**,	24
501	GDAGAN: An Anonymization Method for Graph Data Publishing Using Generative Adversarial Network. **2019**,	1
500	An Efficient Location Privacy Preserving Model based on Geohash. **2019**,	5
499	EVChain: A Blockchain-based Credit Sharing in Electric Vehicles Charging. **2019**,	8
498	Enabling Privacy Policies for mHealth Studies. **2019**,	0

497	Non-Stochastic Hypothesis Testing with Application to Privacy Against Hypothesis-Testing Adversaries. **2019**,	5
496	An Improved Differential Privacy Algorithm Using Frequent Pattern Mining. **2019**,	0
495	A novel utility metric to measure information loss for generalization and suppression techniques in Privacy Preserving Data publishing. **2019**,	1
494	MR-Anonymization: A Relationship-based Privacy Model. **2019**,	
493	Personalized Privacy Protection with Spatio-Temporal Features in Social Networks. **2019**,	1
492	Improving Privacy in Graphs Through Node Addition. **2019**,	
491	K-Anonymity without the Prior Value of the Threshold k: Revisited. **2019**,	
490	Privacy-Preserving Statistical Analysis of Health Data Using Paillier Homomorphic Encryption and Permissioned Blockchain. **2019**,	4
489	A Mondrian-based Utility Optimization Model for Anonymization. **2019**,	1
488	A Practical Differentially Private Support Vector Machine. **2019**,	
487	Embracing Opportunities of Livestock Big Data Integration with Privacy Constraints. **2019**,	1
486	. **2019**, 16, 1054-1069	3
485	Subspace-based aggregation for enhancing utility, information measures, and cluster identification in privacy preserved data mining on high-dimensional continuous data. **2019**, 1-10	2
484	Accuracy-Aware Service Recommendation with Privacy. **2019**,	
483	An Approach for Distributing Sensitive Values in k-Anonymity. **2019**,	1
482	Practical Access Pattern Privacy by Combining PIR and Oblivious Shuffle. **2019**,	4
481	Differentially Privacy-preserving Social IoT. **2019**,	1
480	A Framework for Privacy Quantification: Measuring the Impact of Privacy Techniques Through Mutual Information, Distance Mapping, and Machine Learning. **2019**, 11, 241-261	0

479	A relative privacy model for effective privacy preservation in transactional data. **2019**, 31, e4923	3
478	A privacy preserving location service for cloud-of-things system. **2019**, 123, 215-222	22
477	Against Signed Graph Deanonymization Attacks on Social Networks. **2019**, 47, 725-739	8
476	Efficient subgraph search on large anonymized graphs. **2019**, 31, e4511	0
475	Big Data Privacy in Biomedical Research. **2020**, 6, 296-308	11
474	Towards an Automatic Detection of Sensitive Information in Mongo Database. **2020**, 138-146	
473	An efficient method for privacy-preserving trajectory data publishing based on data partitioning. **2020**, 76, 5276-5300	5
472	Multi-Party High-Dimensional Data Publishing Under Differential Privacy. **2020**, 32, 1557-1571	11
471	A utility based approach for data stream anonymization. **2020**, 54, 605-631	3
470	Blockchain and Federated Learning for Privacy-Preserved Data Sharing in Industrial IoT. **2020**, 16, 4177-4186	282
469	A Unified Framework for Clustering Constrained Data Without Locality Property. **2020**, 82, 808-852	2
468	Multi-platform data collection for public service with Pay-by-Data. **2020**, 79, 33503-33518	
467	. **2020**, 15, 895-910	5
466	Low-cohesion differential privacy protection for industrial Internet. **2020**, 76, 8450-8472	14
465	$X-BAND$: Expiration Band for Anonymizing Varied Data Streams. **2020**, 7, 1438-1450	0
464	Privacy as a Service: Anonymisation of NetFlow Traces. **2020**, 561-571	
463	Ensuring Privacy-Aware Data Release: An Analysis of Applicability of Privacy Enhancing Techniques to Real-world Datasets. **2020**,	0
462	When Machine Learning Meets Privacy in 6G: A Survey. **2020**, 22, 2694-2724	56

461	Supercomputing and Secure Cloud Infrastructures in Biology and Medicine. **2020**, 3, 391-410	1
460	Perturbation-Hidden: Enhancement of Vehicular Privacy for Location-Based Services in Internet of Vehicles. **2020**, 1-1	2
459	A Survey of Game Theoretical Privacy Preservation for Data Sharing and Publishing. **2020**, 205-216	1
458	Every Anonymization Begins with k: A Game-Theoretic Approach for Optimized k Selection in k-Anonymization. **2020**,	3
457	DPARM: Differentially Private Association Rules Mining. **2020**, 8, 142131-142147	0
456	Generative adversarial networks enhanced location privacy in 5G networks. **2020**, 63, 1	8
455	Non-cryptographic Approaches for Collaborative Social Network Data Publishing - A Survey. **2020**,	0
454	Differential Privacy for Evolving Network Based on GHRG. **2020**, 2020, 1-12	
453	Privacy-Preserving Data Visualization: Reflections on the State of the Art and Research Opportunities. **2020**, 39, 675-692	9
452	A Data Desensitization Algorithm for Privacy Protection Electric Power Industry. **2020**, 768, 052059	
451	GeoSecure-R: Secure Computation of Geographical Distance using Region-anonymized GPS Data. **2020**,	1
450	A Survey on Differentially Private Machine Learning [Review Article]. **2020**, 15, 49-64	33
449	Towards formalizing the GDPR's notion of singling out. **2020**, 117, 8344-8352	10
448	Design of Privacy-Preserving Dynamic Controllers. **2020**, 65, 3863-3878	6
447	A Differentially Private Big Data Nonparametric Bayesian Clustering Algorithm in Smart Grid. **2020**, 7, 2631-2641	9
446	. **2020**, 8, 112515-112529	2
445	Sensitive k-Anonymity: An Anonymization Model for IoT based Electronic Health Records. **2020**, 9, 716	13
444	. **2020**, 1-1	2

443	UDPP: Blockchain based Open Platform as a Privacy Enabler. **2020**,	
442	Enhanced anonymous models for microdata release based on sensitive levels partition. **2020**, 155, 9-23	3
441	Collaborative Trajectory Mining in Smart-Homes to Support Early Diagnosis of Cognitive Decline. **2020**, 1-1	7
440	Attribute susceptibility and entropy based data anonymization to improve users community privacy and utility in publishing data. **2020**, 50, 2555-2574	6
439	New Blind Filter Protocol: An Improved Privacy-Preserving Scheme for Location-Based Services. **2020**, 63, 1886-1903	2
438	Gaussian Privacy Protector for Online Data Communication in a Public World. **2020**,	0
437	Impact of prior knowledge on privacy leakage in trajectory data publishing. **2020**, 23, 1291-1300	2
436	Preserving empirical data utility in k-anonymous microaggregation via linear discriminant analysis. **2020**, 94, 103787	3
435	A Privacy-Preserving Multi-Task Learning Framework for Face Detection, Landmark Localization, Pose Estimation, and Gender Recognition. **2019**, 13, 112	3
434	A low cost and un-cancelled laplace noise based differential privacy algorithm for spatial decompositions. **2020**, 23, 549-572	4
433	Effective Removal of Privacy Breaches in Disassociated Transactional Datasets. **2020**, 45, 3257-3272	4
432	Amplified locality-sensitive hashing-based recommender systems with privacy protection. **2020**, e5681	41
431	Protecting survey data on a consumer level. **2020**, 8, 3-17	0
430	Privacy-Preserving Public Release of Datasets for Support Vector Machine Classification. **2020**, 1-1	3
429	DP-FL: a novel differentially private federated learning framework for the unbalanced data. **2020**, 23, 2529-2545	11
428	Flexible data anonymization using ARX□urrent status and challenges ahead. **2020**, 50, 1277-1304	13
427	Subspace based noise addition for privacy preserved data mining on high dimensional continuous data. **2020**, 1	2
426	Toward a new way of minimizing the loss of information quality in the dynamic anonymization. **2020**,	

425	On Safeguarding Privacy and Security in the Framework of Federated Learning. **2020**, 34, 242-248	71
424	Secured segmentation for ICD datasets. **2021**, 12, 5309-5324	9
423	Privacy-preserving point-of-interest recommendation based on geographical and social influence. **2021**, 543, 202-218	7
422	Privacy preserving big data analytics: A critical analysis of state-of-the-art. **2021**, 11,	2
421	Remodeling: improved privacy preserving data mining (PPDM). **2021**, 13, 131-137	
420	Parking recommender system privacy preservation through anonymization and differential privacy. **2021**, 3, e12297	2
419	A new location-based privacy protection algorithm with deep learning. **2021**, 4, e139	0
418	Can driving patterns predict identity and gender?. **2021**, 12, 151-166	1
417	Heterogeneous differential privacy for vertically partitioned databases. **2021**, 33, e5607	2
416	Standardization of Big Data and Its Policies. **2021**, 79-107	
415	A Study on Challenges of Big Data and Their Approaches in Present Environment. **2021**, 483-495	2
414	Distributed Semi-Private Image Classification Based on Information-Bottleneck Principle. **2021**,	
413	Privacy-preserving healthcare informatics: a review. **2021**, 36, 04005	5
412	Distributed L-diversity using spark-based algorithm for large resource description frameworks data. **2021**, 77, 7270-7286	
411	Towards Privacy Protection Composition Framework on Internet of Vehicles. **2021**, 1-1	3
410	A Survey on Privacy Preserving Dynamic Data Publishing. **2021**, 1635-1657	
409	Encyclopedia of Cryptography, Security and Privacy. **2021**, 1-4	
408	Encyclopedia of Cryptography, Security and Privacy. **2021**, 1-3	

407	An Overview on Protecting User Private-Attribute Information on Social Networks. **2021**, 102-117	1
406	Incremental Anonymous Privacy-Protecting Data Mining Method Based on Feature Correlation Algorithm. **2021**, 204-214	
405	Security Protection Technology of Electrical Power System Based on Edge Computing. **2021**,	0
404	Trace Me If You Can: An Unlinkability Approach for Privacy-Preserving in Social Networks. **2021**, 1-1	0
403	L-RDFDiversity: Distributed De-Identification for Large RDF Data with Spark. **2021**, 243-249	
402	Ameliorating the Privacy on Large Scale Aviation Dataset by Implementing MapReduce Multidimensional Hybrid k-Anonymization. **2021**, 683-714	
401	An efficient clustering-based anonymization scheme for privacy-preserving data collection in IoT based healthcare services. **2021**, 14, 1629-1649	19
400	A User-Centric Mechanism for Sequentially Releasing Graph Datasets under Blowfish Privacy. **2021**, 21, 1-25	1
399	Differential identifiability clustering algorithms for big data analysis. **2021**, 64, 1	2
398	PREFER. **2021**, 5, 1-25	1
397	Scalable Distributed Data Anonymization. **2021**,	0
396	. **2021**,	1
395	An Efficient and Secure Blockchain-Based SVM Classification for a COVID-19 Healthcare System. **2021**,	0
394	P3GM: Private High-Dimensional Data Release via Privacy Preserving Phased Generative Model. **2021**,	1
393	Location Privacy-preserving Mechanisms in Location-based Services. **2021**, 54, 1-36	15
392	Improved privacy preserving method for periodical SRS publishing. **2021**, 16, e0250457	1
391	Data Anonymization for Pervasive Health Care: Systematic Literature Mapping Study. **2021**, 9, e29871	2
390	Anonymization of Daily Activity Data by Using □diversity Privacy Model. **2021**, 12, 1-21	2

389 Evaluation of the Privacy Risks of Personal Health Identifiers and Quasi-Identifiers in a Distributed Research Network: Development and Validation Study. **2021**, 9, e24940

388 Differentially Private Decision Tree Based on Pearson□ Correlation Coefficient. **2021**, 0

387 Anonymous location sharing in urban area mobility. **2021**, 63, 1849 1

386 Y□ge Verisi Yay□lamada Mahremiyet Duyarl□ Yeni Bir Model □erisi ve Uygulamas□

385 Anonymization Techniques for Privacy Preservation in Social Networks: A Review. **2021**, 14-21

384 An Anatomization Model for Farmer Data Collections. **2021**, 2, 1

383 Privacy-preserving data collection for 1: M dataset. **2021**, 80, 31335-31356

382 On Optimizing the Trade-off between Privacy and Utility in Data Provenance. **2021**, 4

381 Privacy Preservation Techniques for Sequential Data Releasing. **2021**,

380 Differential Privacy-Preserving User Linkage across Online Social Networks. **2021**,

379 Healthcare Cram□ Generative Adversarial Network (HCGAN). 1 0

378 Secondary Use of Clinical Data in Data-Gathering, Non-Interventional Research or Learning Activities: Definition, Types, and a Framework for Risk Assessment. **2021**, 23, e26631 2

377 A Privacy Preservation Model for RFID Data-Collections is Highly Secure and More Efficient than LKC-Privacy. **2021**, 1

376 Security Protection of Information Utilizing Halfway Speculation. **2021**, 1964, 042097

375 Privacy Preserving Data Mining.

374 Differentially Private Attributed Network Releasing Based on Early Fusion. **2021**, 2021, 1-13 2

373 Quasi-Identifier Recognition Algorithm for Privacy Preservation of Cloud Data Based on Risk Reidentification. **2021**, 2021, 1-13 2

372 Set-Based Adaptive Distributed Differential Evolution for Anonymity-Driven Database Fragmentation. **2021**, 6, 380 6

371	Differentially Private Web Browsing Trajectory over Infinite Streams. **2021**, 2021, 1-14	
370	Exposing safe correlations in transactional datasets. 1	
369	Face Image Publication Based on Differential Privacy. **2021**, 2021, 1-20	2
368	A Novel Privacy Preservation Mechanism for Wireless Medical Sensor Networks. **2021**, 173-182	1
367	A Review of Privacy-Preserving Federated Learning for the Internet-of-Things. **2021**, 21-50	7
366	Weak k-Anonymity: A Low-Distortion Model for Protecting Privacy. **2006**, 60-71	10
365	k-Anonymous Decision Tree Induction. **2006**, 151-162	16
364	Balancing Smartness and Privacy for the Ambient Intelligence. **2006**, 255-258	4
363	Protecting Location Privacy through Semantics-aware Obfuscation Techniques. **2008**, 231-245	13
362	Privacy in Data Mining. **2009**, 687-716	9
361	Privacy-Preserving Data Mining: A Survey. **2008**, 431-460	14
360	A Survey of Multiplicative Perturbation for Privacy-Preserving Data Mining. **2008**, 157-181	15
359	From Data Privacy to Location Privacy. **2009**, 217-246	5
358	Avoiding Attribute Disclosure with the (Extended) p-Sensitive k-Anonymity Model. **2010**, 353-373	3
357	Private Location-Based Information Retrieval via k-Anonymous Clustering. **2010**, 421-430	1
356	Practical Distributed Privacy-Preserving Data Analysis at Large Scale. **2014**, 219-252	0
355	A Differentially Private and Truthful Incentive Mechanism for Traffic Offload to Public Transportation. **2018**, 366-385	1
354	Secure and Efficient Multi-Party Directory Publication for Privacy-Preserving Data Sharing. **2018**, 71-94	1

353	Sharing Cyber Threat Intelligence Under the General Data Protection Regulation. **2019**, 28-41	5
352	Security and Privacy in Social Networks: Data and Structural Anonymity. **2020**, 265-293	3
351	A Data Utility-Driven Benchmark for De-identification Methods. **2019**, 63-77	4
350	Privacy and Policy in Polystores: A Data Management Research Agenda. **2019**, 68-81	4
349	Density Peak Clustering Algorithm Based on Differential Privacy Preserving. **2019**, 20-32	2
348	Lightweight Outsourced Privacy-Preserving Heart Failure Prediction Based on GRU. **2020**, 521-536	1
347	Ontology-Based Modeling of Privacy Vulnerabilities for Data Sharing. **2020**, 109-125	1
346	Blockchain Applications in Healthcare A Review and Future Perspective. **2020**, 198-218	3
345	Distributed Differential Evolution for Anonymity-Driven Vertical Fragmentation in Outsourced Data Storage. **2020**, 213-226	8
344	A Semantic Model for Personal Consent Management. **2013**, 146-151	4
343	A Model of Privacy and Security for Electronic Health Records. **2014**, 202-213	3
342	P3RN:Personalized Privacy Protection Using Query Semantics over Road Networks. **2014**, 323-335	2
341	Privacy in Crowdsourced Platforms. **2015**, 57-84	5
340	k-degree Closeness Anonymity: A Centrality Measure Based Approach for Network Anonymization. **2015**, 299-310	3
339	Formal Verification of Privacy Properties in Electric Vehicle Charging. **2015**, 17-33	5
338	Secure Similarity Queries: Enabling Precision Medicine with Privacy. **2016**, 61-70	1
337	Data Anonymization as a Vector Quantization Problem: Control Over Privacy for Health Data. **2016**, 193-203	2
336	Towards Flexible K-Anonymity. **2016**, 288-297	1

335	Privacy Models and Disclosure Risk Measures. **2017**, 111-189	3
334	Utility Aware Clustering for Publishing Transactional Data. **2017**, 481-494	6
333	Privacy-Utility Tradeoff for Applications Using Energy Disaggregation of Smart-Meter Data. **2017**, 214-234	2
332	Reversible Data Perturbation Techniques for Multi-level Privacy-Preserving Data Publication. **2018**, 26-42	2
331	Privacy-Preserving Publication of User Locations in the Proximity of Sensitive Sites. **2008**, 95-113	5
330	Exclusive Strategy for Generalization Algorithms in Micro-data Disclosure. **2008**, 190-204	3
329	Protecting the Publishing Identity in Multiple Tuples. **2008**, 205-218	5
328	Quality Aware Privacy Protection for Location-Based Services. **2007**, 434-446	11
327	(₽k)-anonymity Based Privacy Preservation by Lossy Join. **2007**, 733-744	3
326	Speeding Up Clustering-Based k-Anonymisation Algorithms with Pre-partitioning. **2007**, 203-214	2
325	MobiHide: A Mobilea Peer-to-Peer System for Anonymous Location-Based Queries. **2007**, 221-238	69
324	Clustering-Based K-Anonymisation Algorithms. **2007**, 761-771	6
323	Generating Microdata with P-Sensitive K-Anonymity Property. **2007**, 124-141	11
322	An Ad Omnia Approach to Defining and Achieving Private Data Analysis. **2007**, 1-13	15
321	Probabilistic Anonymity. **2007**, 56-79	10
320	Privacy-Preserving Data Mining through Knowledge Model Sharing. **2007**, 97-115	6
319	Preserving the Privacy of Sensitive Relationships in Graph Data. **2007**, 153-171	111
318	An Anonymity Model Achievable Via Microaggregation. **2008**, 209-218	6

317	ARUBA: A Risk-Utility-Based Algorithm for Data Disclosure. **2008**, 32-49	4
316	Generalization-Based Privacy-Preserving Data Collection. **2008**, 115-124	4
315	From t-Closeness to PRAM and Noise Addition Via Information Theory. **2008**, 100-112	12
314	Disclosure Analysis and Control in Statistical Databases. **2008**, 146-160	1
313	Information Leakage in Optimal Anonymized and Diversified Data. **2008**, 30-44	3
312	L-Diversity Based Dynamic Update for Large Time-Evolving Microdata. **2008**, 461-469	4
311	Decomposition: Privacy Preservation for Multiple Sensitive Attributes. **2009**, 486-490	14
310	Data and Structural k-Anonymity in Social Networks. **2009**, 33-54	104
309	Location Diversity: Enhanced Privacy Protection in Location Based Services. **2009**, 70-87	74
308	Privacy Preserving Publication of Moving Object Data. **2009**, 190-215	5
307	Privacy-Preserving Classifier Learning. **2009**, 128-147	14
306	Reconstructing Data Perturbed by Random Projections When the Mixing Matrix Is Known. **2009**, 334-349	4
305	Privacy Risk Diagnosis: Mining l-Diversity. **2009**, 216-230	3
304	L-Cover: Preserving Diversity by Anonymity. **2009**, 158-171	3
303	On t-Closeness with KL-Divergence and Semantic Privacy. **2010**, 153-167	1
302	Privacy-Preserving Publishing Data with Full Functional Dependencies. **2010**, 176-183	6
301	Privacy and Anonymization as a Service: PASS. **2010**, 392-395	1
300	Anonymizing Transaction Data by Integrating Suppression and Generalization. **2010**, 171-180	18

299	Generalizing PIR for Practical Private Retrieval of Public Data. **2010**, 1-16	14
298	Understanding Privacy Risk of Publishing Decision Trees. **2010**, 33-48	3
297	Identifying the Risk of Attribute Disclosure by Mining Fuzzy Rules. **2010**, 455-464	3
296	Clustering with Diversity. **2010**, 188-200	14
295	A User-Oriented Anonymization Mechanism for Public Data. **2011**, 22-35	2
294	Distributed Privacy Preserving Data Collection. **2011**, 93-107	8
293	Attribute Based Anonymity for Preserving Privacy. **2011**, 572-579	2
292	Privacy Measures for Free Text Documents: Bridging the Gap between Theory and Practice. **2011**, 161-173	3
291	Privacy beyond Single Sensitive Attribute. **2011**, 187-201	3
290	On-the-Fly Generalization Hierarchies for Numerical Attributes Revisited. **2011**, 18-32	5
289	Privacy Preserving for Multiple Sensitive Attributes Based on l-Coverage. **2011**, 319-326	1
288	Noiseless Database Privacy. **2011**, 215-232	29
287	An Information-Theoretic Privacy Criterion for Query Forgery in Information Retrieval. **2011**, 146-154	6
286	Permutation Anonymization: Improving Anatomy for Privacy Preservation in Data Publication. **2012**, 111-123	8
285	Clustering-Based k-Anonymity. **2012**, 405-417	7
284	An Analysis of Privacy Preservation Techniques in Data Mining. **2013**, 119-128	7
283	Adaptive Differentially Private Histogram of Low-Dimensional Data. **2012**, 160-179	2
282	Data Privacy Using MASKETEERTM. **2012**, 151-158	0

281	An Efficient and Dynamic Concept Hierarchy Generation for Data Anonymization. **2013**, 488-499	2
280	Testing the Lipschitz Property over Product Distributions with Applications to Data Privacy. **2013**, 418-436	8
279	Using Safety Constraint for Transactional Dataset Anonymization. **2013**, 164-178	3
278	Behavioral Tendency Obfuscation Framework for Personalization Services. **2013**, 289-303	2
277	Preservation of Utility through Hybrid k-Anonymization. **2013**, 97-111	7
276	Anonymizing Data with Relational and Transaction Attributes. **2013**, 353-369	24
275	Privacy-Aware Set-Valued Data Publishing on Cloud for Personal Healthcare Records. **2017**, 323-334	2
274	Digital Earth Ethics. **2020**, 785-810	5
273	Game Theory for Next Generation Wireless and Communication Networks: Modeling, Analysis, and Design. **2019**,	25
272	Review of results on smart-meter privacy by data manipulation, demand shaping, and load scheduling. **2020**, 3, 605-613	8
271	Sanitization models and their limitations. **2006**,	6
270	Privacy and location anonymization in location-based services. **2009**, 1, 15-22	16
269	Social networks integration and privacy preservation using subgraph generalization. **2009**,	5
268	Private record matching using differential privacy. **2010**,	81
267	An online framework for publishing privacy-sensitive location traces. **2010**,	2
266	Preserving Patient Privacy When Sharing Same-Disease Data. **2016**, 7,	5
265	Protocols for Checking Compromised Credentials. **2019**,	12
264	Privacy-Preserving Classification with Secret Vector Machines. **2020**,	2

263	PMF. **2020**, 4, 1-21	31
262	Game Theory for Mobile Location Privacy. **2020**,	1
261	A Statistical Approach to Provide Individualized Privacy for Surveys. **2016**, 11, e0147314	15
260	PANDA. **2020**, 13, 3001-3004	5
259	An Overview of De-Identification Techniques and Their Standardization Directions. **2020**, E103.D, 1448-1461	1
258	VER□MAHREM□YET□SALDIRILAR, KORUNMA VE YEN□BR ZM NERS□**2018**, 4, 21-34	1
257	Evaluation of Privacy Risks of Patients' Data in China: Case Study. **2020**, 8, e13046	2
256	Stochastic Channel-Based Federated Learning With Neural Network Pruning for Medical Data Privacy Preservation: Model Development and Experimental Validation. **2020**, 4, e17265	3
255	SoK: Differential privacies. **2020**, 2020, 288-313	10
254	Blockchain-Based Data Sharing and Decentralizing Privacy. 235-240	3
253	Database Anonymization Techniques with Focus on Uncertainty and Multi-Sensitive Attributes. **2013**, 364-383	3
252	Ameliorating the Privacy on Large Scale Aviation Dataset by Implementing MapReduce Multidimensional Hybrid k-Anonymization. **2019**, 11, 14-40	1
251	Low Dimensional Data Privacy Preservation Using Multi Layer Artificial Neural Network. **2012**, 8, 17-31	11
250	Protecting User Privacy Better with Query l-Diversity. **2010**, 4, 1-18	3
249	The issues connected with the anonymization of medical data. Part 2. Advanced anonymization and anonymization controlled by owner of protected sensitive data. **2014**, 8, 13-24	1
248	Achieving Anonymization Constraints in High-Dimensional Data Publishing Based on Local and Global Data Suppressions. **2022**, 3, 1	
247	Privacy Preserving Parallel Clustering Based Anonymization for Big Data Using MapReduce Framework. 1-34	1
246	Towards an Anti-inference (K, l)-Anonymity Model with Value Association Rules. **2006**, 883-893	4

245 Towards a More Reasonable Generalization Cost Metric for K-Anonymization. **2006**, 258-261 4

244 Query Evaluation on a Database Given by a Random Graph. **2006**, 149-163 2

243 Indistinguishability: The Other Aspect of Privacy. **2006**, 1-17 9

242 Risk & Distortion Based K-Anonymity. **2007**, 345-358 1

241 Practical Issues on Privacy-Preserving Health Data Mining. **2007**, 64-75 2

240 Privacy Protection with Uncertainty and Indistinguishability. **2007**, 173-185

239 Personalized Privacy Preservation. **2008**, 461-485 3

238 Facilitating discovery on the private web using dataset digests. **2008**,

237 Understanding the privacy-efficiency trade-off in location based queries. **2008**, 4

236 Returning Lethe to Aletheia? Towards Anonymity in Semantic Data Federations.

235 Privacy preserving document indexing infrastructure for a distributed environment. **2008**, 1, 1638-1643

234 Mining Entropy l-Diversity Patterns. **2009**, 384-388

233 Privacy FP-Tree. **2009**, 246-260 1

232 Clustering-Based Frequency l-Diversity Anonymization. **2009**, 159-168 2

231 Context Quality and Privacy - Friends or Rivals?. **2009**, 25-40 1

230 An Active Global Attack Model for Sensor Source Location Privacy: Analysis and Countermeasures. **2009**, 373-393 4

229 On Sketch Based Anonymization That Satisfies Differential Privacy Model. **2010**, 397-400

228 On the Identification of Property Based Generalizations in Microdata Anonymization. **2010**, 81-96

227	Location Privacy. **2010**, 173-186	1
226	Synthesizing: Art of Anonymization. **2010**, 385-399	
225	eM2: An Efficient Member Migration Algorithm for Ensuring k-Anonymity and Mitigating Information Loss. **2010**, 26-40	4
224	Satisfying Privacy Requirements: One Step before Anonymization. **2010**, 181-188	13
223	A Privacy Preserving Service Broker Architecture for Data Sharing. **2010**, 450-458	
222	Privacy Disclosure Analysis and Control for 2D Contingency Tables Containing Inaccurate Data. **2010**, 1-16	
221	On-the-Fly Hierarchies for Numerical Attributes in Data Anonymization. **2010**, 13-25	3
220	Using Classification Methods to Evaluate Attribute Disclosure Risk. **2010**, 277-286	1
219	Reducing metadata complexity for faster table summarization. **2010**,	3
218	Regulatory Compliance. **2010**, 555-584	
217	Checking Anonymity Levels for Anonymized Data. **2011**, 278-289	1
216	An Improved l-Diversity Anonymisation Algorithm. **2011**, 81-86	
215	Validating Privacy Requirements in Large Survey Rating Data. **2011**, 445-469	
214	Protecting Information Privacy in the Electronic Society. **2011**, 20-36	
213	Effectiveness of Using Integrated Algorithm in Preserving Privacy of Social Network Sites Users. **2011**, 237-249	1
212	Impact of Outliers on Anonymized Categorical Data. **2011**, 326-335	1
211	On the Complexity of the l-diversity Problem. **2011**, 266-277	3
210	Data Anonymity in Multi-Party Service Model. **2011**, 21-30	2

209 Protecting Privacy of Sensitive Value Distributions in Data Release. **2011**, 255-270 2

208 Detecting dependencies in an anonymized dataset. **2012**, 1

207 A Formal Description for Multi-owner Privacy. **2012**, 689-695

206 A Model for Assessing the Risk of Revealing Shared Secrets in Social Networks. **2012**, 499-508 1

205 Privacy Hash Table. **2012**, 129-145

204 A Probabilistic Hybrid Logic for Sanitized Information Systems. **2012**, 500-513

203 Protecting Privacy by Multi-dimensional K-anonymity. **2012**, 7, 3

202 Preventing Re-identification While Supporting GWAS. **2013**, 39-53

201 Overview of Patient Data Anonymization. **2013**, 9-30

200 Conclusions and Open Research Challenges. **2013**, 65-69 0

199 Modeling and Respecting Privacy Specification when Composing DaaS Services*. **2012**, 9, 24-44

198 A Conceptual Framework for Social Network Data Security. **2013**, 58-86 2

197 Improved Algorithms for Anonymization of Set-Valued Data. **2013**, 581-594 1

196 Anonymity in Multi-Instance Micro-Data Publication. **2013**, 325-337

195 Preservation of Proximity Privacy in Publishing Categorical Sensitive Data. **2013**, 563-570 2

194 Defining Privacy Based on Distributions of Privacy Breaches. **2013**, 211-225 1

193 Subscription Privacy Protection in Topic-Based Pub/Sub. **2013**, 361-376 2

192 Assured Information Sharing (AIS)Using Private Clouds. **2014**, 215-255

191	A Multi-Constraint Anonymous Parameter Design Method Based on the Attribute Significance of Rough Set. **2014**, 345-350	
190	Privacy Preservation Techniques. **2014**, 23-50	2
189	A Unified Framework for Privacy Preserving Data Clustering. **2014**, 319-326	
188	Conceptual Framework and Architecture for Privacy Audit. **2014**, 17-40	
187	FACTS: A Framework for Anonymity towards Comparability, Transparency, and Sharing. **2014**, 120-135	
186	Background on Spatial Data Management and Exploration. **2014**, 21-47	
185	Location Privacy. **2014**, 211-225	
184	PrivacyFrost2: A Efficient Data Anonymization Tool Based on Scoring Functions. **2014**, 211-225	
183	A Quantitative Analysis of the Performance and Scalability of De-identification Tools for Medical Data. **2014**, 274-289	3
182	Database Security and Privacy. **2014**, 53-1-53-21	
181	An Approach to Achieving K-partition for Preserving Privacy by Using Multi-constraint Anonymous Parameter Based on Rough Sets. **2014**, 9,	
180	Study on Personalized Location Privacy Preservation Algorithms Based on Road Networks. **2015**, 35-45	
179	De-anonymising Social Network Posts by Linking with R□um□**2015**, 248-260	
178	Correlation Based Anonymization Using Generalization and Suppression for Disclosure Problems. **2015**, 581-592	1
177	A Privacy-Aware Access Model on Anonymized Data. **2015**, 201-212	
176	Anonymous Data Collection System with Mediators. **2015**, 141-160	
175	Privacy Preservation in Information Systems. **2015**, 4393-4402	
174	Location Semantics Protection Based on Bayesian Inference. **2015**, 297-308	1

173 Privacy-aware Wrappers. **2015**, 130-138 1

172 k-Anonymous Microdata Release via Post Randomisation Method. **2015**, 225-241 1

171 Security and Privacy in LTE-based Public Safety Network. **2016**, 317-364 1

170 Mining Representative Patterns Under Differential Privacy. **2017**, 295-302

169 Privacy and Utility Preservation for Location Data Using Stay Region Analysis. **2017**, 808-820

168 Analysis of Privacy Preserving Data Publishing Techniques for Various Feature Selection Stability Measures. **2017**, 582-591

167 (delta)-privacy: Bounding Privacy Leaks in Privacy Preserving Data Mining. **2017**, 124-142 0

166 Fine Grained Privacy Measuring of User Profile Over Online Social Network. **2018**, 371-379 1

165 Mutual Correlation-Based Anonymization for Privacy Preserving Medical Data Publishing. **2018**, 304-319

164 Improving Opinion Analysis Through Statistical Disclosure Control in eVoting Scenarios. **2018**, 45-59

163 Impact of Big Data on Security. **2018**, 326-350

162 Study on Data Anonymization for Deep Learning. **2018**, 762-767

161 Anonymisierung von Floating Car Data. **2018**, 285-295

160 Anonymity Online Current Solutions and Challenges. **2018**, 38-55

159 kazan: fayda temelli veri yay lama modeli. **2018**, 2018, 1

158 Stipulation-Based Anonymization with Sensitivity Flags for Privacy Preserving Data Publishing. **2019**, 445-454 2

157 Anonymization of System Logs for Preserving Privacy and Reducing Storage. **2019**, 162-179 2

156 Research on Social Networks Publishing Method Under Differential Privacy. **2019**, 58-72

155 Analytical Study on Privacy Attack Models in Privacy Preserving Data Publishing. **2019**, 1273-1293

154 Injecting Differential Privacy in Rules Extraction of Rough Set. **2019**, 175-187 0

153 An Efficient Hybrid Encryption Scheme for Large Genomic Data Files. **2019**, 214-230

152 Mutual Correlation-Based Anonymization for Privacy Preserving Medical Data Publishing. **2019**, 644-659

151 Combining Machine Learning and Statistical Disclosure Control to Promote Open Data. **2019**, 83-93

150 Risk-Based Privacy-Aware Information Disclosure. **2019**, 567-586

149 Hybrid Privacy Preservation Technique Using Neural Networks. **2019**, 454-472

148 Hybrid Privacy Preservation Technique Using Neural Networks. **2019**, 542-561

147 A Clustering Approach Using Fractional Calculus-Bacterial Foraging Optimization Algorithm for k-Anonymization in Privacy Preserving Data Mining. **2019**, 587-608 0

146 Privacy Protection Workflow Publishing Under Differential Privacy. **2019**, 382-394

145 Data Anonymization for Privacy Aware Machine Learning. **2019**, 725-737 2

144 Impact of Big Data on Security. **2019**, 2014-2038

143 Encyclopedia of Big Data Technologies. **2019**, 1478-1487

142 Analytical Study on Privacy Attack Models in Privacy Preserving Data Publishing. **2019**, 1518-1538

141 VER□MAHREM□YET□SALDIRILAR, KORUNMA VE YEN□BR □M NER□□21-34

140 A Study on Models and Techniques of Anonymization in Data Publishing. **2019**, 84-90 1

139 User Relationship Privacy Protection on Trajectory Data. **2020**, 1038-1045 1

138 SPARK-Based Partitioning Algorithm for k-Anonymization of Large RDFs. **2020**, 292-298

137 Comparative Analysis of Privacy Preserving Approaches for Collaborative Data Processing. **2020**, 199-206 0

136 Cluster-Based Anonymization of Assortative Networks. **2020**, 709-718

135 Oan: aykEkayEyDelimli fayda temelli mahremiyet koruma modeli. **2019**, 35, 355-368 1

134 Differentially Private Graph Clustering Algorithm Based on Structure Similarity. **2019**, 0

133 A Mixed Model for Privacy Preserving and Secure Sharing of Medical Datasets. **2020**, 406-415

132 Smart Contract-Driven Mechanism Design to Mitigate Information Diffusion in Social Networks. **2020**, 201-216

131 Derin Denmede Diferansiyel Mahremiyet. **2020**, 6, 1-16 1

130 A Method of Trajectory Anonymization with Adjustable Usefulness. **2020**, 140, 956-963

129 A Privacy-Preserving Approach for Continuous Data Publication. **2020**, 441-458

128 . **2020**, 1

127 k-Anonymous Crowd Flow Analytics. **2020**, 1

126 Semantic Location Privacy Protection Algorithm Based on Edge Cluster Graph. **2020**,

125 K-modes Based Categorical Data Clustering Algorithms Satisfying Differential Privacy. **2020**,

124 A Case Study of User Privacy based on WiFi Data in a Campus Setting. **2020**,

123 . **2020**, 1

122 Evaluation of Re-identification Risks in Data Anonymization Techniques Based on Population Uniqueness. **2020**, 1

121 Research on the Application of Blockchain in Credit Bank. **2020**,

120 An Analysis of Different Notions of Effectiveness in k-Anonymity. **2020**, 121-135 1

119	Utility-Enhancing Flexible Mechanisms for Differential Privacy. **2020**, 74-90	
118	PGLP: Customizable and Rigorous Location Privacy Through Policy Graph. **2020**, 655-676	1
117	Secure k-Anonymization Linked with Differential Identifiability (Workshop). **2020**, 307-316	
116	Safety Analysis of High-Dimensional Anonymized Data from Multiple Perspectives. **2020**, 94-111	
115	IoT in Healthcare. **2020**, 1-22	1
114	Privacy-Preserving Technologies. **2020**, 279-297	3
113	An Elastic Anonymization Framework for Open Data. **2020**, 108-119	
112	Old and New Data Mining Topics: Imbalanced Data Problem, Privacy-Preserving Data Mining and Data Mining by Image Processing. **2020**, 32, 9-12	
111	A Baseline for Attribute Disclosure Risk in Synthetic Data. **2020**,	7
110	Set-valued data publication with local privacy. **2020**, 13, 1234-1247	2
109	Smaller, Faster & Lighter KNN Graph Constructions. **2020**,	1
108	Privacy preserving defect prediction using generalization and entropy-based data reduction. **2021**, 25, 1369-1405	
107	Preserving the Privacy of COVID-19 Infected Patients Data Using a Divergent-Scale Supervised Learning for Publishing the Informative Data. **2022**, 35-47	1
106	Hybrid Privacy Preservation Technique Using Neural Networks. 229-246	
105	Analytical Study on Privacy Attack Models in Privacy Preserving Data Publishing. 98-116	0
104	A Privacy Protection Model for Patient Data With Multiple Sensitive Attributes. 44-60	
103	Privacy Inference Disclosure Control with Access-Unrestricted Data Anonymity. 126-148	
102	Privacy in Database Publishing: A Bayesian Perspective. **2008**, 461-487	

101	Privacy Preserving Publication: Anonymization Frameworks and Principles. **2008**, 489-508	
100	Privacy Protection through Anonymity in Location-based Services. **2008**, 509-530	6
99	An Empirical Study of Utility Measures for k-Anonymisation. **2008**, 15-27	1
98	Granulation as a Privacy Protection Mechanism. **2007**, 256-273	
97	Capture Inference Attacks for K-Anonymity with Privacy Inference Logic. **2007**, 676-687	1
96	Answering Queries Based on Imprecision and Uncertainty Trade-Offs in Numeric Databases. **2007**, 81-95	
95	Allowing Privacy Protection Algorithms to Jump Out of Local Optimums: An Ordered Greed Framework. **2008**, 33-55	2
94	Privacy Inference Attacking and Prevention on Multiple Relative K-Anonymized Microdata Sets. **2008**, 263-274	
93	Verification of the Security Against Inference Attacks on XML Databases. **2008**, 359-370	
92	How Anonymous Is k-Anonymous? Look at Your Quasi-ID. **2008**, 1-15	3
91	BSGI: An Effective Algorithm towards Stronger l-Diversity. **2008**, 19-32	3
90	T-rotation: Multiple Publications of Privacy Preserving Data Sequence. **2008**, 500-507	1
89	Non-stochastic hypothesis testing for privacy. **2020**, 14, 754-763	0
88	AnonFACES. **2020**,	1
87	A Qualitative-Driven Study of Irreversible Data Anonymizing Techniques in Databases. **2020**,	
86	Evaluation of the Privacy Risks of Personal Health Identifiers and Quasi-Identifiers in a Distributed Research Network: Development and Validation Study (Preprint).	
85	A Comprehensive Review of Blockchain Technology Implementation in the EV Charging Infrastructure. **2022**, 38-67	0
84	Utilization of Homomorphic Cryptosystems for Information Exchange in Value Chains. **2021**,	3

83	Simple Distribution of Sensitive Values for Multiple Sensitive Attributes in Privacy Preserving Data Publishing to Achieve Anatomy. **2021**,	
82	A Decision Process Model for De-Identification Methods on the Example of Psychometric Data. **2021**,	
81	Privacy and efficiency guaranteed social subgraph matching. 1	3
80	Privacy-Preserving Attribute-Based Access Control in Education Information Systems. **2021**, 327-345	0
79	Privacy Risk of Document Data and a Countermeasure Framework. **2021**, 29, 778-786	
78	Big Data Privacy Management: A Vision Paper. **2020**,	
77	Information Exposure From Relational Background Knowledge on Social Media. **2020**,	
76	imdpGAN: Generating Private and Specific Data with Generative Adversarial Networks. **2020**,	1
75	ASENVA: Summarizing Anatomy Model by Aggregating Sensitive Values. **2020**,	
74	Understanding the Potential Risks of Sharing Elevation Information on Fitness Applications. **2020**,	3
73	A New Blockchain-based Electronic Medical Record Transferring System with Data Privacy. **2020**,	1
72	Inferring the Meaning of Non-personal, Anonymized, and Anonymous Data. **2021**, 269-282	
71	PPQC: A Blockchain-Based Privacy-Preserving Quality Control Mechanism in Crowdsensing Applications. **2022**, 1-16	0
70	A Road Truncation-Based Location Privacy-Preserving Method against Side-Weight Inference Attack. **2022**, 12, 1107	1
69	Modelling imperfect knowledge via location semantics for realistic privacy risks estimation in trajectory data.. **2022**, 12, 246	
68	A new utility-aware anonymization model for privacy preserving data publishing.	0
67	Information Resilience: the nexus of responsible and agile approaches to information use. 1	
66	Security and Privacy Issues Related to Big Data-Based Ubiquitous Healthcare Systems. **2022**, 41-64	

65	A survey of data minimisation techniques in blockchain-based healthcare. **2022**, 205, 108766	1
64	Achieving Transparency Report Privacy in Linear Time. **2022**, 14, 1-56	
63	Publishing Triangle Counting Histogram in Social Networks Based on Differential Privacy. **2021**, 2021, 1-16	0
62	Heap Bucketization Anonymity—An Efficient Privacy-Preserving Data Publishing Model for Multiple Sensitive Attributes. **2022**, 10, 28773-28791	8
61	Privacy-Preserving Bin-Packing With Differential Privacy. **2022**, 3, 94-106	1
60	Introduction. **2022**, 1-4	
59	Privacy Preservation Technique Based on Sensitivity Levels for Multiple Numerical Sensitive Overlapped Attributes. **2022**, 38-55	
58	A Survey on Privacy-Preserving Data Publishing Models for Big Data. **2022**, 250-276	
57	A Comprehensive Assessment of Privacy Preserving Data Mining Techniques. **2022**, 833-842	2
56	Sovereign Digital Consent through Privacy Impact Quantification and Dynamic Consent. **2022**, 10, 35	
55	Differential privacy: a privacy cloak for preserving utility in heterogeneous datasets. **2022**, 10, 25-36	
54	Privacy Preservation in Social Network Data using Evolutionary Model. **2022**,	1
53	Deceptive Infusion of Data: A Novel Data Masking Paradigm for High-Valued Systems. 1-16	1
52	Enabling personal consent in databases. **2021**, 15, 375-387	
51	Gene Sequence Clustering Based on the Profile Hidden Markov Model with Differential Identifiability. **2021**, 2021, 1-9	
50	Research on Privacy Protection Technology for Data Publishing. **2021**,	1
49	A Novel Mixed Integer Programming Formulation for Data Perturbation. **2022**,	
48	An End-to-End Data Pipeline for Managing Learning Analytics. **2021**,	2

47	Large Scale Data Anonymisation for GDPR Compliance. **2022**, 325-335	0
46	Consent-driven data reuse in Multi-tasking Crowdsensing Systems: A privacy-by-design solution. **2022**, 101614	
45	When Differential Privacy Implies Syntactic Privacy. **2022**, 1-1	
44	Re-Identification in Differentially Private Incomplete Datasets. **2022**, 3, 62-72	3
43	Generating a trading strategy in the financial market from sensitive expert data based on the privacy-preserving generative adversarial imitation network. **2022**, 500, 616-631	
42	Optimization Design of Privacy Protection System Based on Cloud Native. **2022**, 599-615	
41	A Targeted Privacy-Preserving Data Publishing Method Based on Bayesian Network. **2022**, 1-1	1
40	Enhancing Privacy in Ride-Sharing Applications Through POIs Selection. **2022**,	1
39	Differential Privacy High-dimensional Data Publishing Method Based on Bayesian Network. **2022**,	
38	Localized Differential Location Privacy Protection Scheme in Mobile Environment. **2022**,	
37	A New Anonymization Model for Privacy Preserving Data Publishing: CANON.	
36	Utility-Preserving Biometric Information Anonymization. **2022**, 24-41	0
35	Scalable Distributed Data Anonymization for Large Datasets. **2022**, 1-14	0
34	Privacy Preserving in the Modern Era. **2022**, 1-24	0
33	Composite Privacy Preservation in Location Based Advertisement. **2022**,	0
32	Preserving Privacy of Social Media Data Using Artificial Intelligence Techniques. **2022**, 186-204	0
31	Enhanced k-Anonymity model based on clustering to overcome Temporal attack in Privacy Preserving Data Publishing. **2022**,	0
30	K-MNSOA: K-Anonymity Model for Privacy in the Presence of Multiple Numerical Sensitive Overlapped Attributes. **2023**, 69-79	0

29	Dimension-aware under spatiotemporal constraints: an efficient privacy-preserving framework with peak density clustering.	0
28	An Optimized Selection of Statistical Disclosure Control Methods: A Case Study Involving Microdata from the Polish Survey of Accidents at Work. **2022**, 63-78	0
27	Verfahren zur Anonymisierung und Pseudonymisierung von Daten. **2022**, 183-201	0
26	HTF: Homogeneous Tree Framework for Differentially-Private Release of Large Geospatial Datasets with Self-Tuning Structure Height.	0
25	Anomaly detection as a service: An outsourced anomaly detection scheme for blockchain in a privacy-preserving manner. **2022**, 1-1	0
24	Secure Method for De-Identifying and Anonymizing Large Panel Datasets. **2019**,	0
23	Blossom: Cluster-Based Routing for Preserving Privacy in Opportunistic Networks. **2022**, 11, 75	0
22	A Python library to check the level of anonymity of a dataset. **2022**, 9,	0
21	A Survey on´Privacy Preserving Synthetic Data Generation and´a´Discussion on´a´Privacy-Utility Trade-off Problem. **2022**, 167-180	0
20	Anonymization Methods for Privacy-Preserving Data Publishing. **2023**, 145-159	0
19	Comprehensive Analysis of Privacy and Data Mining Techniques. **2022**,	0
18	Secure Recommender System based on Neural Collaborative Filtering and Federated Learning. **2022**,	0
17	Privacy Preserving Enhancing Model for Multiple-sensitive Attributes. **2022**,	0
16	Optimally Designing Cybersecurity Insurance Contracts to Encourage the Sharing of Medical Data. **2022**,	0
15	Is Your Model Sensitive? SPEDAC: A New Resource for the Automatic Classification of Sensitive Personal Data. **2023**, 11, 10864-10880	0
14	Bottlenecks CLUB: Unifying Information-Theoretic Trade-Offs Among Complexity, Leakage, and Utility. **2023**, 18, 2060-2075	0
13	An anonymization-based privacy-preserving data collection protocol for digital health data. 11,	0
12	Efficient Bayesian Network Construction for Increased Privacy on Synthetic Data. **2022**,	0

11	Data Anonymization with Differential Privacy. **2022**, 1-5	0
10	Examining the Utility of Differentially Private Synthetic Data Generated using Variational Autoencoder with TensorFlow Privacy. **2022**,	0
9	Differentially Private Clustering Algorithm for Mixed Data. **2023**, 392-405	0
8	Clustering-Based Anonymization Technique using Agglomerative Hierarchical Clustering. **2022**,	0
7	On the Risks of Collecting Multidimensional Data Under Local Differential Privacy. **2023**, 16, 1126-1139	0
6	Data Sharing Privacy Metrics Model Based on Information Entropy and Group Privacy Preference. **2023**, 7, 11	0
5	Double Phased Algorithm for Frequent Sub Graph Mining with More Security. **2022**,	0
4	Boosted Hybrid Privacy Preserving Data Mining (BHPPDM) Technique to Increase Privacy and Accuracy. **2023**,	0
3	K-Anonymity-Based Privacy-Preserving and Efficient Location-Based Services for Internet of Vehicles Withstand Viterbi Attack. **2023**, 1016-1028	0
2	Apply Rough Set Methods to Preserve Social Networks Privacy: A Review. **2023**, 427-436	0
1	Geo-Graph-Indistinguishability: Location Privacy on Road Networks with Differential Privacy. **2023**, E106.D, 877-894	0