

Contents

1	Introduction	1
1.1	Motivation	1
1.2	Contribution of the Book	4
1.2.1	Access Control Enforcement	4
1.2.2	Privacy Protection	5
1.2.3	Safe Data Integration	6
1.3	Organization of the Book	7
2	Overview of the State of the Art	9
2.1	Introduction	9
2.1.1	Chapter Outline	10
2.2	Basic Scenario and Data Organization	11
2.2.1	Parties Involved	11
2.2.2	Data Organization	12
2.2.3	Interactions	13
2.3	Querying Encrypted Data	15
2.3.1	Bucket-Based Approach	15
2.3.2	Hash-Based Approach	17
2.3.3	B+ Tree Approach	18
2.3.4	Order Preserving Encryption Approaches	20
2.3.5	Other Approaches	21
2.4	Evaluation of Inference Exposure	22
2.5	Integrity of Outsourced Data	24
2.6	Privacy Protection of Databases	26
2.7	Access Control Enforcement in the Outsourcing Scenario	27
2.8	Safe Data Integration	29
2.9	Chapter Summary	30
3	Selective Encryption to Enforce Access Control	31
3.1	Introduction	31
3.1.1	Chapter Outline	33

3.2	Relational Model	33
3.2.1	Basic Concepts and Notation	34
3.3	Access Control and Encryption Policies	35
3.3.1	Access Control Policy	35
3.3.2	Encryption Policy	36
3.3.3	Token Management	40
3.4	Minimal Encryption Policy	42
3.4.1	Vertices and Edges Selection	45
3.4.2	Vertices Factorization	47
3.5	$\mathcal{A}2\mathcal{E}$ Algorithm	48
3.5.1	Correctness and Complexity	53
3.6	Policy Updates	58
3.6.1	Grant and Revoke	59
3.6.2	Correctness	63
3.7	Two-Layer Encryption for Policy Outsourcing	65
3.7.1	Two-Layer Encryption	66
3.8	Policy Updates in Two-Layer Encryption	70
3.8.1	Over-encrypt	70
3.8.2	Grant and Revoke	71
3.8.3	Correctness	75
3.9	Protection Evaluation	76
3.9.1	Exposure Risk: Full_SEL	78
3.9.2	Exposure Risk: Delta_SEL	79
3.9.3	Design Considerations	80
3.10	Experimental Results	81
3.11	Chapter Summary	84
4	Combining Fragmentation and Encryption to Protect Data Privacy . .	85
4.1	Introduction	85
4.1.1	Chapter Outline	87
4.2	Confidentiality Constraints	88
4.3	Fragmentation and Encryption for Constraint Satisfaction	90
4.4	Minimal Fragmentation	91
4.4.1	Correctness	92
4.4.2	Maximal Visibility	92
4.4.3	Minimum Number of Fragments	93
4.4.4	Fragmentation Lattice	94
4.5	A Complete Search Approach to Minimal Fragmentation	96
4.5.1	Computing a Minimal Fragmentation	98
4.5.2	Correctness and Complexity	100
4.6	A Heuristic Approach to Minimize Fragmentation	102
4.6.1	Computing a Vector-minimal Fragmentation	102
4.6.2	Correctness and Complexity	105
4.7	Taking Attribute Affinity into Account	107
4.8	A Heuristic Approach to Maximize Affinity	109

4.8.1	Computing a Vector-minimal Fragmentation with the Affinity Matrix	110
4.8.2	Correctness and Complexity	113
4.9	Query Cost Model	115
4.10	A Heuristic Approach to Minimize Query Cost Execution	118
4.10.1	Computing a Vector-minimal Fragmentation with the Cost Function	119
4.10.2	Correctness and Complexity	122
4.11	Query Execution	123
4.12	Indexes	126
4.13	Experimental Results	130
4.14	Chapter Summary	133
5	Distributed Query Processing under Safely Composed Permissions ..	135
5.1	Introduction	135
5.1.1	Chapter Outline	137
5.2	Preliminary Concepts	137
5.2.1	Data Model	137
5.2.2	Distributed Query Execution	139
5.3	Security Model	141
5.3.1	Permissions	141
5.3.2	Relation Profiles	143
5.4	Graph-based Model	144
5.5	Authorized Views	147
5.5.1	Authorizing Permissions	149
5.5.2	Composition of Permissions	151
5.5.3	Algorithm	155
5.6	Safe Query Planning	159
5.6.1	Third Party Involvement	162
5.7	Build a Safe Query Plan	163
5.8	Chapter Summary	169
6	Conclusions	171
6.1	Summary of the Contributions	171
6.2	Future Work	172
6.2.1	Access Control Enforcement	172
6.2.2	Privacy Protection	173
6.2.3	Safe Data Integration	174
	References	175



<http://www.springer.com/978-1-4419-7658-1>

Preserving Privacy in Data Outsourcing

Foresti, S.

2011, XV, 180 p., Hardcover

ISBN: 978-1-4419-7658-1