

# TABLE OF CONTENTS

---

<i>List of Figures</i> .....	<i>xi</i>
<i>List of Tables</i> .....	<i>xiii</i>
<i>Preface</i> .....	<i>xv</i>

<b>Chapter 1</b>	<b>Introduction to Database Security</b> .....	<b>1</b>
	Introductory Example.....	2
	Unit Introduction .....	2
	1.1. The Scope of Database Security .....	4
	1.2. Security Models and Controls .....	8
	1.3. Database Security Challenges .....	13
	1.4. Database Security and the Internet.....	18
	Summary .....	22
	Review Questions.....	22
	Multiple Choice Questions .....	23
	References .....	24
<b>Chapter 2</b>	<b>Database Security Fundamentals</b> .....	<b>29</b>
	Introductory Example.....	30
	Unit Introduction .....	30
	2.1. Overview of Database Security Features .....	31
	2.2. Management in Database Security.....	34
	2.3. User Permission Control .....	39
	2.4. Cloud Audit Services.....	49
	Summary .....	53
	Review Questions.....	53
	Multiple Choice Questions .....	54
	References .....	55

<b>Chapter 3</b>	<b>Database Security Threats and Prevention</b> .....	<b>61</b>
	Introductory Example.....	62
	Unit Introduction.....	62
	3.1. Aspects of Database Security.....	63
	3.2. Origin of Security Threats.....	66
	3.3. Database Security Threats.....	67
	3.4. Preventive Measure for Database Security.....	76
	Summary.....	82
	Review Questions.....	82
	Multiple Choice Questions.....	83
	References.....	84
<b>Chapter 4</b>	<b>Database Security Policies</b> .....	<b>89</b>
	Introductory Example.....	90
	Unit Introduction.....	90
	4.1. Access Control Policies.....	92
	4.2. Administration Policies.....	100
	4.3. Identification and Authentication.....	102
	4.4. Auditing a Database System.....	103
	Summary.....	104
	Review Questions.....	104
	Multiple Choice Questions.....	105
	References.....	106
<b>Chapter 5</b>	<b>Database Security Revamp: Concepts and Techniques</b> .....	<b>111</b>
	Introductory Example.....	112
	Unit Introduction.....	112
	5.1. Insider Misuse and Anomaly Detection.....	114
	5.2. Data and User Profiling.....	117
	5.3. Access Path Model.....	123
	5.4. Security Reconfiguration.....	129
	5.5. Advancement in Database Security.....	133
	5.6. Gradual Re-Design Strategies.....	134
	Summary.....	136
	Review Questions.....	136

	Multiple Choice Questions.....	137
	References.....	138
<b>Chapter 6</b>	<b>Authorization and Authentication</b> .....	<b>145</b>
	Introductory Example.....	146
	Unit Introduction.....	146
	6.1. Security Violations.....	147
	6.2. Authorization (Access Rights).....	148
	6.3. User Access Control.....	150
	6.4. Granting of Privileges.....	150
	6.5. Notion of Roles.....	152
	Summary.....	156
	Review Questions.....	156
	Multiple Choice Questions.....	157
	References.....	158
<b>Chapter 7</b>	<b>Detection and Prevention of SQL Injection Attacks</b> .....	<b>161</b>
	Introductory Example.....	162
	Unit Introduction.....	162
	7.1. SQL Injection Attacks.....	164
	7.2. SQL Injection Attack Detection and Prevention.....	170
	7.3. Related Approaches.....	177
	Summary.....	181
	Review Questions.....	181
	Multiple Choice Questions.....	182
	References.....	183
<b>Chapter 8</b>	<b>Securing Data in Transit and at Rest</b> .....	<b>189</b>
	Introductory Example.....	190
	Unit Introduction.....	190
	8.1. Encryption.....	191
	8.2. Role of Encryption in Data Protection.....	192
	8.3. Encrypting Data-in-Transit.....	193
	8.4. Encrypt Data-at-Rest.....	205
	Summary.....	213
	Review Questions.....	213

Multiple Choice Questions .....	214
References .....	215
<b>Index .....</b>	<b>221</b>

## LIST OF FIGURES

---

- Figure 1.1. Illustration of data security principles
- Figure 1.2. Illustration of access control and other security services
- Figure 1.3. Illustration of authentication and authorization
- Figure 1.4. Illustration of access keys
- Figure 1.5. Illustration of data extraction challenges
- Figure 1.6. Illustration of secure database access
- Figure 1.7. Illustration of proxy server
- Figure 1.8. Illustration of firewall
- Figure 1.9. Illustration of the working of digital signatures
- Figure 2.1. Illustration of database security framework
- Figure 2.2. Description of the use of IAM
- Figure 2.3. Representation of the example of fine-grained permission management
- Figure 2.4. Description of flow of IAM using GaussDB (for MySQL)
- Figure 2.5. Illustration of 2 user, role, and permission
- Figure 2.6. Illustration of authorization
- Figure 2.7. Illustration of cloud audit service
- Figure 3.1. Illustration of database security aspects
- Figure 3.2. Representation of database security threats
- Figure 3.3. Illustration of SQL injection attack
- Figure 3.4. Illustration of denial-of-service attack
- Figure 4.1. Illustration of discretionary security policies
- Figure 4.2. Illustration of access control security policies
- Figure 4.3. Description of authorization rules
- Figure 4.4. Illustration of access control
- Figure 4.5. Illustration of role hierarchy
- Figure 4.6. Illustration of multiple parents
- Figure 4.7. Illustration of cyclic graph
- Figure 4.8. Illustration of administration policies