

---

# Contents

---

<b>Preface</b>	<b>xiii</b>
<b>1 A data-centric view of cloud security</b>	<b>1</b>
<i>Vimal Kumar, Sivadon Chaisiri, and Ryan Ko</i>	
Abstract	1
1.1 Introduction	1
1.2 Definitions and terminology	2
1.3 Need for new methods	4
1.3.1 Cryptography	6
1.3.2 Data provenance	7
1.3.3 Privacy and security laws and regulations	7
1.4 Classification of data security issues in cloud computing	8
1.4.1 Data at rest	9
1.4.2 Data in use	10
1.4.3 Data in transit	11
1.4.4 Cross-cutting issues	12
1.5 Conclusion	13
References	13
<b>2 Nomad: a framework for ensuring data confidentiality in mission-critical cloud-based applications</b>	<b>19</b>
<i>Mamadou H. Diallo, Michael August, Roger Hallman, Megan Kline, Henry Au, and Scott M. Slayback</i>	
2.1 Introduction	20
2.2 Nomad framework overview	22
2.2.1 Client management service	23
2.2.2 Cloud storage service	24
2.2.3 Operational overview	24
2.3 Homomorphic encryption background	27
2.3.1 BGV scheme	27
2.3.2 HELib	28
2.4 GPU-based acceleration of BGV FHE	29
2.5 Application: <i>CallForFire</i>	31
2.5.1 <i>CallForFire</i> operational workflow	32
2.6 Implementation	33

2.7	Experiments	34
2.7.1	Performance of the GPU-based parallelisation	34
2.7.2	<i>CallForFire</i> performance	37
2.8	Related work	38
2.9	Conclusion	39
2.10	Future research challenges	40
	References	40
<b>3</b>	<b>Preserving privacy in pre-classification volume ray-casting of 3D images</b>	<b>45</b>
	<i>Manoranjan Mohanty, Muhammad Rizwan Asghar, and Giovanni Russello</i>	
	Abstract	45
3.1	Introduction	45
3.2	Related work and background	47
3.2.1	Encrypted domain rendering	47
3.2.2	3D images	48
3.2.3	Volume ray-casting	48
3.3	System model	50
3.4	Proposed approach	52
3.5	Solution details	54
3.5.1	Data preparation	55
3.5.2	Ray-dependent rendering	56
3.5.3	Composition	57
3.6	Construction details	57
3.7	Security analysis	59
3.8	Implementation and experiment	61
3.9	Conclusions	63
	References	63
<b>4</b>	<b>Multiprocessor system-on-chip for processing data in cloud computing</b>	<b>65</b>
	<i>Arnab Kumar Biswas, S. K. Nandy, and Ranjani Narayan</i>	
4.1	Introduction	65
4.2	Current approaches to secure MPSoC cloud platforms	67
4.3	Threat model	68
4.3.1	Router attack description	68
4.3.2	The malicious effects of router attack	69
4.3.3	Examples of router attack	70
4.4	Countermeasure for unauthorized access attack	71
4.4.1	Runtime monitor	72
4.4.2	Restart monitor	75
4.4.3	Ejection address checker	77
4.4.4	Simulation and synthesis results	78

4.5	Countermeasure for misrouting attack	81
4.5.1	Local monitoring module	82
4.5.2	Intermediate manager	83
4.5.3	Simulation and synthesis results	84
4.6	Summary, future research directions, and further readings	84
	Acknowledgments	85
	References	85
<b>5</b>	<b>Distributing encoded data for private processing in the cloud</b>	<b>89</b>
	<i>Mark A. Will and Ryan K. L. Ko</i>	
	Abstract	89
5.1	Introduction	89
5.2	Summary of distributed encoding and related work	90
5.2.1	Encoding	90
5.2.2	Distribution	92
5.2.3	Custom hardware processors	94
5.3	String searching	94
5.3.1	Overview	94
5.3.2	Removing special characters	96
5.3.3	Approximate string searching	96
5.3.4	False positives	96
5.3.5	Building the search index	96
5.3.6	Distributed index	97
5.3.7	Results for searching over a document	98
5.3.8	Summary	99
5.4	Arbitrary computation	99
5.4.1	Overview	99
5.4.2	Distributed NAND Gate	101
5.4.3	Addition	103
5.4.4	Multiplication	104
5.4.5	Conditional	105
5.4.6	Proof-of-concept addition and multiplication	105
5.5	Security analysis	107
5.5.1	One set of the distributed data	107
5.5.2	Breaking into all systems	109
5.6	Little computational and network overhead	110
5.7	Concluding remarks	111
	Acknowledgements	112
	References	112
<b>6</b>	<b>Data protection and mobility management for cloud</b>	<b>117</b>
	<i>Dat Dang, Doan Hoang, and Priyadarsi Nanda</i>	
	Abstract	117
	Keyword	117

6.1	Introduction	118
6.2	Data mobility	119
6.2.1	Components of a data mobility model	120
6.2.2	Data mobility scenarios	121
6.3	Security mechanisms for data-in-transit	124
6.3.1	Geographic location-based mechanisms	125
6.3.2	Data-mobility-based policy and encryption mechanisms	125
6.3.3	Binding user and data location	126
6.3.4	Protecting cloud data using trusted third-party technologies	127
6.3.5	Data mobility based on location register database	127
6.4	A trust-oriented data protection framework	127
6.4.1	Mobility management model	129
6.4.2	Trust-oriented data protection framework	133
6.4.3	Implementation	134
6.4.4	Evaluation and results	138
6.5	Discussion and conclusion	145
6.5.1	Discussion	145
6.5.2	Conclusion	146
	References	146
<b>7</b>	<b>Understanding software-defined perimeter</b>	<b>151</b>
	<i>Chenkang Tang, Vimal Kumar, and Sivadon Chaisiri</i>	
	Abstract	151
7.1	Introduction	151
7.2	Background and related work	152
7.2.1	Firewalls	153
7.2.2	Virtual private network	154
7.2.3	Public key infrastructure	155
7.2.4	Transport layer security	155
7.2.5	Other SDP-like solutions	155
7.3	Software-defined perimeter	156
7.3.1	Overview of the software-defined perimeter framework	156
7.3.2	Software-defined perimeter architecture	157
7.3.3	Software-defined perimeter configurations	158
7.3.4	Software-defined perimeter workflow	158
7.3.5	Software-defined perimeter protocol	160
7.4	SDP security	166
7.5	Conclusion	167
	References	168

<b>8 Security, trust, and privacy for cloud computing in Transportation Cyber-Physical Systems</b>	<b>171</b>
<i>Wenjia Li, Jonathan Voris, and N. Sertac Artan</i>	
Abstract	171
8.1 Introduction	172
8.2 Transportation CPS	173
8.2.1 Vehicular and transportation networks	173
8.2.2 Vehicle-to-everything communication	173
8.2.3 Intra-vehicle Communication	175
8.3 Transportation cloud computing	176
8.3.1 Transportation cloud computing service taxonomy	176
8.4 TCPS attack surfaces	178
8.4.1 Modern intra-vehicle data networks and the cloud	178
8.4.2 Attack surfaces of future cloud-based V2X transportation networks	180
8.5 TCPS security mechanisms	181
8.5.1 Trust management for TCPS	182
8.5.2 Privacy for TCPS	186
8.6 Conclusion	187
References	188
<b>9 Review of data leakage attack techniques in cloud systems</b>	<b>197</b>
<i>Zirak Allaf and Mo Adda</i>	
Abstract	197
9.1 Introduction	197
9.2 Data state and vulnerabilities	198
9.2.1 Data-At-Rest	198
9.2.2 Data-In-Motion	199
9.2.3 Data-In-Use	199
9.3 Core technology vulnerabilities in cloud computing	200
9.3.1 Web technology	200
9.3.2 Virtualisation technology	200
9.3.3 Cryptography	201
9.4 Side and covert channel attack classification	201
9.4.1 Targeted data types	202
9.4.2 Source of leakage	202
9.4.3 Types of channel attacks	205
9.4.4 Techniques	207
9.4.5 A generic attack model	207
9.5 Mitigation countermeasures	210
9.5.1 OS level	211
9.5.2 Application level	211

9.5.3	Hardware level	211
9.5.4	Analysis or profile-based detection	212
9.6	Conclusion	213
	References	213

**10 Cloud computing and personal data processing: sorting-out legal requirements** **219**

*Ioulia Konstantinou and Irene Kamara*

	Abstract	219
	Keywords	220
10.1	Introduction: the emergence of cloud and the significance of a secure cloud	220
10.2	Cloud computing and the extra-territorial effect of EU data protection law	221
10.3	The EU legal framework on data protection	222
10.3.1	The Data Protection Directive 95/46/EC	223
10.3.2	The new General Data Protection Regulation	223
10.4	Data controller, data processor and cloud computing actors: assigning roles and responsibilities	224
10.4.1	Cloud client and cloud service provider	225
10.4.2	Sub-contractors	226
10.5	Duties and responsibilities of the cloud actors	228
10.5.1	Compliance with the general personal data processing principles	228
10.5.2	Technical and organisational measures of data protection and data security	230
10.5.3	Data protection impact assessments in cloud computing	234
10.5.4	Audits and certifications	234
10.6	Data flows and appropriate safeguards	235
10.6.1	Adequacy decisions	235
10.6.2	Alternative ways for data transfers by means of ‘appropriate safeguards’	236
10.7	Conclusions	238
	References	239

**11 The Waikato Data Privacy Matrix** **243**

*Craig Scoon and Ryan K. L. Ko*

	Abstract	243
11.1	Introduction	243
11.2	Background	244
11.2.1	Justification	244
11.2.2	Cloud computing	245
11.2.3	NSA leaks	246
11.2.4	PRISM	247

11.2.5	Trans-national agreements	247
11.2.6	Safe harbor to privacy shield	247
11.2.7	General data protection regulation	249
11.3	Legal cases	250
11.3.1	Schrems v. Data Protection Commissioner	250
11.3.2	Google Spain v. AEPD and Mario Costeja González	250
11.3.3	Apple v. FBI	251
11.3.4	The right to be forgotten concept	252
11.4	Related work in legal alignment	252
11.4.1	DLA Piper	252
11.4.2	Forrester Global Heat Map	253
11.4.3	International Data Protection Legislation Matrix	253
11.4.4	Baker & McKenzie's Global Privacy Handbook	253
11.5	Proposed solution	253
11.5.1	Data privacy matrix road map	254
11.6	Concluding remarks	255
11.6.1	Vision	255
	References	255
<b>12</b>	<b>Data provenance in cloud</b>	<b>261</b>
	<i>Alan Yu Shyang Tan, Sivadon Chaisiri, Ryan Ko Kok Leong, Geoff Holmes, and Bill Rogers</i>	
	Abstract	261
12.1	Data provenance and its application	261
12.1.1	What is data provenance?	261
12.1.2	Applying data provenance to data security	262
12.2	Data provenance in cloud	263
12.2.1	Scope of the discussion	263
12.2.2	Log files is not provenance	263
12.3	Acquiring data provenance from cloud	265
12.3.1	Active provenance collection	265
12.3.2	Reconstructing provenance	268
12.4	Conclusion and future challenges	270
	References	271
<b>13</b>	<b>Security visualization for cloud computing: an overview</b>	<b>277</b>
	<i>Jeffery Garae, Ryan K. L. Ko, and Mark Apperley</i>	
	Abstract	277
13.1	Introduction	277
13.1.1	Motivation and objectives for this chapter	278
13.1.2	Chapter outline	279
13.2	Background: security visualization and data security	280
13.2.1	Security visualization for data security	280

13.2.2 The need for security visualization	281
13.3 A security visualization standardization model	282
13.3.1 Effective security visualization approaches	282
13.3.2 Security Visualization Standard (SCeeL-VisT)	283
13.4 Security visualization intelligence framework	285
13.4.1 Security Visualization as a Cloud Service	285
13.4.2 Data Provenance as a Security Visualization Service	286
13.5 Security visualization intelligence model	288
13.5.1 Bitcoin visualization	288
13.5.2 Threat intelligence visualization	290
13.5.3 ForensicTMO – analytic tool	291
13.6 Concluding remarks	292
References	292

<b>Index</b>	<b>297</b>
--------------	------------