Index

A
access control 216, 220
access control framework 153
active intrusion prevention (AIP) 221
advanced business-centric personal data management system (ABC-PDMS) 177, 184
data protection in 184ive processes 186
alert correlation 20
alert fusion 20
anonymity 236
anonymization set 117
Anton et al. Study 101
artificial immune systems (AISs) 221
assessment view of system security 71
authentication approaches 216
authentication classification 39
availability 215

B
behavioral biometrics 219
binary-rewriter 160
Binding Corporate Rules (BCRs) 137
biometric-based authentication 219
boolean expressions 15

C
caracter-based authentication 217
cloaked query 120
cloud computing 153
encrypted data storage 155
security issues 151
virtualization paradigm 151
computational private information retrieval 8
Confab 238
confidentiality 215

d
Dale-Chall index (DCI) 98
data at rest (DAR) 177, 185
database PH indistinguishability 7
   up to frequency 9
database privacy homomorphism 5
data confidentiality 271
data in processing (DIP) 177, 185
data in transmission (DIT) 177, 185
data partitioning 199
data protection
   controls domain 185
   legislation domain 185
   policies and procedures domain 185
Data Protection Directive (95/46 134
data sharing 198, 203
Data Sharing Miner and Analyzer (DASMA) system 197
Denials of Service (DoS) attacks 19
detection techniques 274
DigNet age 176
distributed DoS 20
dynamic detection techniques 275

E
Electronic Medical Records (EMRs) 271, 276-277
elimination (hiding) techniques 274-275
embedding algorithm 260, 267
empirical study 227
encrypted data storage
   for cloud computing 155
existing secure information system (SIS) design 60
Expand Cloak algorithm 121-122
exploit-based DoS attacks 19
extensive game 241
extraction algorithm 261
F
Fair Information Practices (FIP) 94
False Accept Rate (FAR) 40
False Reject Rate (FRR) 40
feature analysis 20
feature extraction 35
Federal Information Security Management Act (FISMA) 182
Flesch Grade Level (FGL) 97-98, 100
Flesch Readability Score (FRES) 97, 100
flooding-based DoS attack 19
Fog Index (FI) 98
free text 34
Fry graph 99

G
Geographic Information System (GIS) 256, 258
global information security 165
globalization 163
Gradient Boosting Trees (GBT) Model 21-22
Graham Leach Bliley Act (GLBA) 91
graph components 257

H
Hadoop distributed file system (HDFS) 151
inadequacies 156
overview 156
secure query processing 156
SUN XACML implementation into 159
hierarchical fallback model 49
hierarchical identity model 240
Hilbert Cloak 124
Hochhauser Study 102
homomorphism 11
horizontal partitioning 199
Host-based Intrusion Detection Systems (HIDSs) 18-19
hybrid partitioning 200

I
IBM 4758 Cryptographic Coprocessor 155
identification classification 39
identity federation 238
I Love You virus 165
image-based authentication 217
imperceptibility 265
indistinguishability 5
inference channels 272
detection 270, 277-278, 280, 291
restriction 270, 277-278, 280, 291
information security 164
global nature of 164
information security breaches 271
information systems security 215, 221
main goals 214-215
In-lined Reference Monitors (IRM’s) 159
integrity 215
intrusion detection systems (IDS) 214-216, 220
intrusion prevention systems (IPS) 215-216
IP spoofing 20

J
Jensen and Potts Study 99
jurisdictional laws 92

K
k-anonymity
in Location-Based Services (LBS) 117
Kantarcioglu-Clifton model 7
keystroke biometric systems 33-34
four components 35
keystroke-duration 37
k-nearest-neighbor (kNN) classifier 39
knowledge-based authentication 216, 220
knowledge-based IDS 221

L
l-diversity
in Location-Based Services (LBS) 117
legal view of system security 74
Location-Based Services (LBS) 115
low-rate pulsing method 20

M
machine learning techniques 20
management view of system security 73
Mandatory Access Control (MAC) 271, 273, 275
mapping 11
maximum entropy probability distribution 289
Medical Knowledge Base (MKB) 276
memory tokens 219
mining shared data 198
### Index

**N**
- Network-based Intrusion Detection Systems (NIDSs) 18-19

**O**
- optimal identity exposure 242

**P**
- password security 218
- personal information exposure 236
- Personal Information Protection and Electronic Documents Act (PIPEDA) 180
- personalized query 120
- physiological biometrics 219
- Plan-Do-Check-Act (PDCA) 60, 76
- Platform for Privacy Preferences Project (P3P) 181
- Policy Decision Point (PDP) 159
- Policy Enforcement Point (PEP) 159
- possession-based authentication 219
- principal component analysis (PCA) 106
- privacy 134, 177-178
- privacy framework 134
  - business perspective 137
  - legal perspective 134
  - technical perspective 138
- privacy homomorphism 2, 4
- Privacy Impact Assessments (PIAs) 182
- privacy policies 92
- privacy policy statement 180
- privacy protection laws 179
- privacy protection solutions 181
- privacy protection threshold 287
- Private Information Retrieval problem (PIR) 8
- process view of system security 70

**Q**
- quansi-identifiers 117
- Query Anonymization Time (QAT) 124
- query homogeneity attack 116
- Query Success Rate (QSR) 125
- Question-and-answer-based authentication 217

**R**
- RationalExposure model 237
- raw keystroke data capture 35
- readability evaluation methods 97
- readability formulas 97
- Receiver Operating Characteristic (ROC) 34, 40
- Relative Anonymity Area (RAL) 125
- Relative Anonymization Area (RAA) 125
- releasing factor 198
- Requirements of Human Readable Policies 94
- resource view of system security 68
- robustness 266
- Role-Based Access Control (RBAC) 239

**S**
- safe queries 10
- sectoral laws 92
- secure cloud data management 152
- secure multipart computation (SMC) 155
- secure query processing with Hadoop 156
- Secure Virtual Machine (VM) Monitor 151
- security design methods 60
- security policies 215
- security requirements analysis 60
- security systems development 60
  - five methods 60
- Security Systems Development Life Cycle (SecS-DLC) 60
- signature-based IDS 221
- six-view perspective of system security (SVPSS)
  - applicability of the 76
  - assessment view 71
  - legal view 74
  - limitations 78
  - management view 73
  - process view 70
  - resource view 68
  - security risk determination 76
  - threat view 66
- smart tokens 219
- SMOG Index (SMOG) 99
- SMOG readability formula 92
- social cognitive theory 226
- static detection techniques 274
- steganalysis 264
- steganographic algorithm 256
- steganography 255
- Systems of Records Notices (SORNs) 182

**T**
- theoretical model 226
- threat view of system security 66
Index

token-based authentication 219
tuple-wise encryption 15

U
unauthorised data observation 271
unsafe queries 10
unweighted m-match, k-Nearest-Neighbor (m-kNN) procedure 40-41

V
vertical partitioning 200

W
Weighted m-match, k-Nearest-Neighbor (Wm-kNN) procedure 40-41
Whitmore, James J. 62-63