

Contents

Chapter 1. Overview of e-Health Architectures	1
Omessaad HAMDI	
1.1. Introduction	1
1.2. Definitions	2
1.2.1. e-Health	2
1.2.2. Telehealth.	2
1.2.3. m-Health	2
1.2.4. Telemedicine.	2
1.3. e-Health services.	3
1.4. Requirements for e-health systems	4
1.5. e-Health system architecture	5
1.5.1. Components of an e-health architecture	6
1.5.2. Features of e-health systems	6
1.6. e-Health system technologies.	8
1.6.1. Devices	8
1.6.2. Connecting technologies	9
1.6.3. Other technologies	10
1.7. Security in e-health systems	12
1.7.1. Security services	12
1.7.2. Legal environment for e-health systems.	13
1.8. Medical data security	14
1.8.1. Cryptography	14

1.8.2. Biometrics	16
1.8.3. Blockchain	17
1.9. Perspectives.	19
1.10. Conclusion.	20
1.11. References.	21

Chapter 2. Vulnerabilities in e-Health and Countermeasures 27

Aida BEN CHEHIDA DOUSS and Ryma ABASSI

2.1. Introduction.	27
2.2. The importance of digitization in healthcare systems.	28
2.3. The challenges of digitization in e-health systems.	30
2.4. Cyber-attacks in the healthcare sector	31
2.4.1. Profiles of cybercriminals.	32
2.4.2. Motivations of cybercriminals	33
2.4.3. Risks and repercussions	35
2.4.4. Types of attacks	36
2.5. Security incidents in the healthcare sector.	39
2.5.1. Example of a phishing attack.	40
2.5.2. Examples of ransomware attacks	40
2.5.3. Examples of data theft attacks	41
2.5.4. Examples of DDoS attacks	42
2.5.5. Example of an internal attack	42
2.6. Existing security measures for e-health systems	42
2.7. Recommendations for protecting e-health systems	45
2.7.1. Risk management methods	45
2.7.2. Technical and organizational recommendations.	46
2.7.3. Raising awareness and training	47
2.8. Conclusion	48
2.9. References.	49

Chapter 3. Security Policies for e-Health Systems 53

Ryma ABASSI

3.1. Introduction.	53
3.2. The concept of the security policy.	54
3.2.1. Definition	54

3.2.2. Modeling a security policy	57
3.3. Environment for specifying, validating and testing security policies	61
3.3.1. Specifying a security policy	61
3.3.2. The concept of executable security policy	63
3.3.3. Testing a security policy	64
3.4. Security services for e-health systems	66
3.4.1. The e-health concept	66
3.4.2. Comparison of national digital health infrastructure security policies	67
3.5. Security requirements for e-health platforms	69
3.5.1. Essential security functions.	69
3.5.2. Security models	70
3.6. Future security challenges for e-health	73
3.7. Conclusion	74
3.8. References.	74
Chapter 4. Adaptive, Dynamic, Decentralized Authorizations for e-Health	77
Tidiane SYLLA, Mohamed AYMEN CHALOUF, Léo MENDIBOURE and Francine KRIEF	
4.1. Introduction	77
4.2. Fundamental principles	79
4.2.1. Concept of e-health.	79
4.2.2. Context-aware computing and security in the IoT	81
4.2.3. Authentication and Authorization for Constrained Environments (ACE-OAuth)	86
4.2.4. Blockchain	89
4.3. Proposal for dynamic, decentralized adaptation of e-health authorizations	91
4.3.1. Threat model for the environment under consideration	91
4.3.2. Proposed architecture for dynamic, decentralized authorization management	92
4.4. Conclusion	100
4.5. References.	101

Chapter 5. Applying Blockchain to e-Health	107
Cyrine LAHSINI, Faiza HAMDY and Omessaad HAMDY	
5.1. Introduction	107
5.2. Blockchain technology	108
5.2.1. Blockchain fundamentals	108
5.2.2. Blockchain categories	110
5.2.3. Characteristics of the blockchain	112
5.3. Health sector	113
5.3.1. Patients	113
5.3.2. Doctors	114
5.3.3. Insurance sector	114
5.3.4. Pharmaceutical industry	115
5.3.5. Government	115
5.4. Issues and challenges for the healthcare sector	115
5.4.1. Quality	116
5.4.2. Coordination	117
5.4.3. Integrity	117
5.4.4. Transparency	118
5.4.5. Traceability	118
5.4.6. Interoperability	119
5.4.7. Data sharing	120
5.4.8. Costs	120
5.4.9. Data volume	121
5.5. Application of blockchain technology in e-health systems	122
5.5.1. Electronic health records	122
5.5.2. Pharmaceutical supply chain	123
5.5.3. Patient follow-up	124
5.5.4. Scientific research in the health sector	125
5.5.5. Analyzing medical data	126
5.6. Implementing blockchain technology in healthcare	127
5.6.1. MedRec	127
5.6.2. MedCredits	128
5.6.3. MIStore	128
5.6.4. Robomed	129
5.6.5. HealthChain	129
5.6.6. Medicalchain	129

5.7. Contribution of the blockchain solution	130
5.8. Conclusion	133
5.9. References.	134

Chapter 6. Using Biometrics to Secure Intra-BAN

Communications.	137
----------------------------------	-----

Omessaad HAMDJ, Mohamed AYMEN CHALOUF and Amal SAMMOUD

6.1. Introduction	137
6.2. Security for WBAN.	138
6.2.1. Architecture of an e-health system	138
6.2.2. Security requirements for WBANs	139
6.2.3. WBAN attacks.	140
6.3. Security solutions for intra-WBAN communications	140
6.3.1. TinySec	141
6.3.2. Biometric methods	141
6.3.3. ZigBee security	141
6.3.4. Bluetooth security.	141
6.3.5. Elliptical curve cryptography	142
6.4. Biometric data-based security solutions for WBANs	143
6.4.1. Biometrics	143
6.4.2. Examples of security approaches for intra-WBAN communications using biometrics.	145
6.4.3. The approach of Sammoud et al.	147
6.5. Discussion.	154
6.6. Conclusion	155
6.7. References.	158

Chapter 7. Using Biometrics for Authentication in e-Health Systems

Omessaad HAMDJ, Mohamed AYMEN CHALOUF and Amal SAMMOUD	161
--	-----

7.1. Introduction	161
7.2. e-Health systems.	162
7.2.1. Architecture	162
7.2.2. Security services	163

7.3. Authentication techniques	163
7.3.1. Authentication factors	164
7.3.2. Types of authentications	164
7.4. Biometric authentication.	166
7.4.1. Biometric features	166
7.4.2. Biometric system effectiveness	167
7.4.3. Performance measures for biometric systems	168
7.5. Multimodal authentication	168
7.6. Multi-factor authentication approaches for e-health system security.	169
7.6.1. Sammoud et al.'s approach.	173
7.7. Conclusion	178
7.8. References.	179

Chapter 8. Security of Medical Data Processing 183

Manel ABDELHEDI and Omessaad HAMDI

8.1. Introduction	183
8.2. Homomorphic encryption	185
8.2.1. Definition	185
8.2.2. Terminology	186
8.2.3. Partially homomorphic encryption	187
8.2.4. Somewhat homomorphic encryption.	190
8.2.5. Fully homomorphic encryption	191
8.2.6. Comparative study	193
8.2.7. Application of HE to secure e-health solutions	198
8.3. Attribute-based encryption	200
8.3.1. Key-policy attribute-based encryption.	201
8.3.2. Ciphertext-policy attribute-based encryption.	202
8.3.3. Comparative study	203
8.3.4. Application of ABE to secure e-health solutions	204
8.4. Conclusion	206
8.5. References.	207

Chapter 9. Artificial Intelligence for Security of e-Health Systems	213
Mohamed Aymen CHALOUF, Hana MEJRI and Omessaad HAMDI	
9.1. Introduction	213
9.2. e-Health systems	214
9.3. e-Health system security	215
9.3.1. Potential attacks	216
9.3.2. Security services	216
9.3.3. Security solutions	218
9.4. Artificial intelligence techniques	220
9.4.1. Machine learning	221
9.4.2. Deep learning	222
9.5. Intrusion detection based on artificial intelligence.	223
9.5.1. IDS based on supervised learning	224
9.5.2. IDS based on unsupervised learning	225
9.5.3. IDS based on deep learning.	226
9.6. AI-based IDS in WBANs	226
9.6.1. Tested learning techniques	227
9.6.2. Implementation and results	227
9.7. Conclusion	232
9.8. References.	233
List of Authors	237
Index	239