

# Table des matières

<b>Chapitre 1. Présentation des architectures de e-santé . . . . .</b>	<b>1</b>
Omessaad HAMDI	
1.1. Introduction. . . . .	1
1.2. Définitions . . . . .	2
1.2.1. E-santé . . . . .	2
1.2.2. Télésanté . . . . .	2
1.2.3. M-santé . . . . .	2
1.2.4. Télémédecine . . . . .	2
1.3. Services offerts par la e-santé . . . . .	3
1.4. Exigences des systèmes de e-santé . . . . .	4
1.5. Architecture des systèmes e-santé . . . . .	5
1.5.1. Composants d'une architecture e-santé . . . . .	6
1.5.2. Fonctionnalités des systèmes e-santé . . . . .	6
1.6. Technologies des systèmes e-santé . . . . .	8
1.6.1. Dispositifs . . . . .	8
1.6.2. Technologies de connexion . . . . .	10
1.6.3. Autres technologies. . . . .	10
1.7. Sécurité dans les systèmes e-santé . . . . .	12
1.7.1. Service de sécurité . . . . .	12
1.7.2. Environnement légal des systèmes e-santé . . . . .	13
1.8. Techniques de sécurité des données médicales . . . . .	14
1.8.1. Cryptographie . . . . .	14
1.8.2. Biométrie . . . . .	16
1.8.3. <i>Blockchain</i> . . . . .	18
1.9. Perspectives . . . . .	19
1.10. Conclusion . . . . .	20
1.11. Bibliographie . . . . .	21

## Chapitre 2. Vulnérabilités dans la e-santé et contre-mesures . . . . . 27

Aida BEN CHEHIDA DOUSS et Ryma ABASSI

2.1. Introduction . . . . .	27
2.2. Importance de la numérisation dans les systèmes de santé . . . . .	28
2.3. Enjeux de la numérisation dans les systèmes e-santé . . . . .	30
2.4. Cyberattaques dans le secteur de la santé . . . . .	30
2.4.1. Profils des cybercriminels . . . . .	32
2.4.2. Motivations des cybercriminels . . . . .	33
2.4.3. Risques et conséquences engendrés . . . . .	35
2.4.4. Types d'attaques . . . . .	36
2.5. Quelques incidents de sécurité dans le secteur de la santé . . . . .	39
2.5.1. Exemple d'attaque de <i>phishing</i> . . . . .	40
2.5.2. Exemples d'attaques avec un <i>ransomware</i> . . . . .	40
2.5.3. Exemples d'attaques de vol de données . . . . .	41
2.5.4. Exemples d'attaques DDoS . . . . .	41
2.5.5. Exemple d'attaque interne . . . . .	42
2.6. Mesures de sécurité existantes sur les systèmes e-santé . . . . .	42
2.7. Quelques recommandations relatives à la protection des systèmes e-santé . . . . .	45
2.7.1. Méthodes de gestion de risques . . . . .	45
2.7.2. Recommandations techniques et organisationnelles . . . . .	46
2.7.3. Sensibilisation et formations . . . . .	47
2.8. Conclusion . . . . .	48
2.9. Bibliographie . . . . .	49

## Chapitre 3. Politiques de sécurité pour les systèmes e-santé . . . . . 53

Ryma ABASSI

3.1. Introduction . . . . .	53
3.2. Notion de politique de sécurité . . . . .	54
3.2.1. Définition . . . . .	55
3.2.2. Modélisation d'une politique de sécurité . . . . .	57
3.3. Environnement de spécification, de validation et de test des politiques de sécurité . . . . .	61
3.3.1. Spécification d'une politique de sécurité . . . . .	62
3.3.2. Notion de politique de sécurité exécutable . . . . .	63
3.3.3. Test d'une politique de sécurité . . . . .	64

3.4. Services de sécurité des systèmes e-santé . . . . .	66
3.4.1. Notion de e-santé . . . . .	66
3.4.2. Comparaison des politiques de sécurité des infrastructures numériques nationales pour la santé . . . . .	67
3.5. Exigences de sécurité des plateformes de e-santé . . . . .	69
3.5.1. Fonctions de sécurité nécessaires. . . . .	70
3.5.2. Modèles de sécurité. . . . .	70
3.6. Défis futurs de sécurité pour la e-santé. . . . .	73
3.7. Conclusion . . . . .	74
3.8. Bibliographie. . . . .	75

## **Chapitre 4. Adaptation dynamique et décentralisée des autorisations pour la e-santé. . . . . 77**

Tidiane SYLLA, Mohamed AYMEN CHALOUF, Léo MENDIBOURE  
et Francine KRIEF

4.1. Introduction. . . . .	77
4.2. Principes fondamentaux . . . . .	79
4.2.1. Concept de e-santé . . . . .	79
4.2.2. Informatique et sécurité sensibles au contexte dans l'IdO . . . . .	81
4.2.3. Authentification et autorisation pour les environnements contraints (ACE-OAuth) . . . . .	86
4.2.4. <i>Blockchain</i> . . . . .	88
4.3. Proposition d'adaptation dynamique et décentralisée des autorisations pour la e-santé . . . . .	91
4.3.1. Modèle de menace de l'environnement considéré. . . . .	91
4.3.2. Architecture proposée pour la gestion dynamique et décentralisée des autorisations. . . . .	92
4.4. Conclusion . . . . .	99
4.5. Bibliographie. . . . .	100

## **Chapitre 5. Application de la *blockchain* dans la e-santé. . . . . 107**

Cyrine LAHSINI, Faiza HAMDI et Omessaad HAMDI

5.1. Introduction. . . . .	107
5.2. Technologie <i>blockchain</i> . . . . .	108
5.2.1. Bases de <i>blockchain</i> . . . . .	108
5.2.2. Catégories de <i>blockchain</i> . . . . .	110
5.2.3. Caractéristiques de la <i>blockchain</i> . . . . .	112

5.3. Secteur de la santé . . . . .	113
5.3.1. Patients . . . . .	113
5.3.2. Médecins . . . . .	114
5.3.3. Secteur de l'assurance . . . . .	114
5.3.4. Industrie pharmaceutique . . . . .	115
5.3.5. Gouvernement . . . . .	115
5.4. Enjeux et défis pour le secteur de la santé . . . . .	115
5.4.1. Qualité . . . . .	116
5.4.2. Coordination . . . . .	117
5.4.3. Intégrité . . . . .	117
5.4.4. Transparence . . . . .	118
5.4.5. Traçabilité . . . . .	118
5.4.6. Interopérabilité . . . . .	119
5.4.7. Partage des données . . . . .	120
5.4.8. Coûts . . . . .	120
5.4.9. Volume de données . . . . .	121
5.5. Application de la technologie <i>blockchain</i> dans les systèmes e-santé . . . . .	122
5.5.1. Dossier de santé électronique . . . . .	122
5.5.2. Chaîne d'approvisionnement en médicaments . . . . .	123
5.5.3. Suivi des patients . . . . .	124
5.5.4. Recherche scientifique dans le domaine de la santé . . . . .	125
5.5.5. Analyse des données médicales . . . . .	126
5.6. Mise en œuvre de la technologie <i>blockchain</i> dans le domaine de la santé . . . . .	127
5.6.1. MedRec . . . . .	128
5.6.2. MedCredits . . . . .	128
5.6.3. MIStore . . . . .	129
5.6.4. Robomed . . . . .	129
5.6.5. HealthChain . . . . .	130
5.6.6. Medicalchain . . . . .	130
5.7. Apport de la solution <i>blockchain</i> . . . . .	131
5.8. Conclusion . . . . .	133
5.9. Bibliographie . . . . .	134

## **Chapitre 6. Utilisation de la biométrie pour sécuriser les communications intra-BAN . . . . . 137**

Omessaad HAMDY, Mohamed AYMEN CHALOUF et Amal SAMMOUD

6.1. Introduction . . . . .	137
6.2. Sécurité des réseaux WBAN . . . . .	138

6.2.1. Architecture d'un système e-santé . . . . .	138
6.2.2. Exigences de sécurité dans les WBAN . . . . .	139
6.2.3. Attaques de sécurité liées aux WBAN. . . . .	140
6.3. Solutions de sécurité pour les communications intra-WBAN . . . . .	140
6.3.1. TinySec. . . . .	141
6.3.2. Méthodes biométriques . . . . .	141
6.3.3. Sécurité de ZigBee . . . . .	141
6.3.4. Sécurité de Bluetooth. . . . .	141
6.3.5. Courbes elliptiques (ECC). . . . .	142
6.4. Solutions de sécurité à base de données biométriques pour les WBAN . . . . .	143
6.4.1. Biométrie. . . . .	143
6.4.2. Exemples d'approches de sécurité des communications intra-WBAN utilisant la biométrie. . . . .	145
6.4.3. Approche de Sammoud <i>et al.</i> . . . . .	147
6.5. Discussion . . . . .	154
6.6. Conclusion . . . . .	157
6.7. Bibliographie. . . . .	157

## **Chapitre 7. Utilisation de la biométrie pour l'authentification dans les systèmes e-santé . . . . . 161**

Omessaad HAMDJ, Mohamed AYMEN CHALOUF et Amal SAMMOUD

7.1. Introduction. . . . .	161
7.2. Systèmes e-santé. . . . .	162
7.2.1. Architecture . . . . .	162
7.2.2. Services de sécurité. . . . .	163
7.3. Techniques d'authentification . . . . .	163
7.3.1. Facteurs d'authentification . . . . .	163
7.3.2. Types d'authentification . . . . .	164
7.4. Authentification par la biométrie . . . . .	166
7.4.1. Caractéristiques biométriques. . . . .	166
7.4.2. Efficacité d'un système biométrique. . . . .	167
7.4.3. Mesures de performance des systèmes biométriques . . . . .	168
7.5. Authentification multimodale . . . . .	168
7.6. Approches d'authentification multifacteur pour la sécurité du système e-santé . . . . .	169
7.6.1. Présentation de l'approche. . . . .	173
7.7. Conclusion . . . . .	178
7.8. Bibliographie. . . . .	179

**Chapitre 8. Sécurité du traitement des données médicales . . . . . 183**

Manel ABDELHEDI et Omessaad HAMDI

8.1. Introduction. . . . .	183
8.2. Chiffrement homomorphe . . . . .	185
8.2.1. Définition. . . . .	185
8.2.2. Terminologie. . . . .	186
8.2.3. Chiffrement partiellement homomorphe . . . . .	187
8.2.4. Chiffrement quelque peu homomorphe . . . . .	190
8.2.5. Chiffrement complètement homomorphe . . . . .	190
8.2.6. Étude comparative . . . . .	193
8.2.7. Application du HE dans la sécurisation des solutions e-santé . . .	198
8.3. Chiffrement par attributs . . . . .	199
8.3.1. <i>Key-Policy Attribute-Based Encryption</i> . . . . .	200
8.3.2. <i>Ciphertext-Policy Attribute-Based Encryption</i> . . . . .	201
8.3.3. Étude comparative . . . . .	203
8.3.4. Application du ABE dans la sécurisation des solutions e-santé . . .	204
8.4. Conclusion . . . . .	206
8.5. Bibliographie. . . . .	206

**Chapitre 9. Intelligence artificielle pour la sécurité en e-santé . . . . . 213**

Mohamed AYMEN CHALOUF, Hana MEJRI et Omessaad HAMDI

9.1. Introduction. . . . .	213
9.2. Systèmes e-santé. . . . .	214
9.3. Sécurité des systèmes e-santé . . . . .	215
9.3.1. Attaques possibles . . . . .	216
9.3.2. Services de sécurité. . . . .	216
9.3.3. Solutions de sécurité . . . . .	218
9.4. Techniques d'intelligence artificielle. . . . .	220
9.4.1. Apprentissage automatique . . . . .	221
9.4.2. Apprentissage profond . . . . .	222
9.5. Détection d'intrusion basée sur l'intelligence artificielle . . . . .	223
9.5.1. IDS basés sur l'apprentissage supervisé. . . . .	224
9.5.2. IDS basés sur l'apprentissage non supervisé . . . . .	225
9.5.3. IDS basés sur l'apprentissage profond. . . . .	226
9.6. IDS basés sur l'intelligence artificielle dans les WBAN . . . . .	226
9.6.1. Techniques d'apprentissage évaluées . . . . .	227
9.6.2. Implémentation et résultats . . . . .	227

9.7. Conclusion . . . . .	232
9.8. Bibliographie . . . . .	233
<b>Liste des auteurs . . . . .</b>	<b>237</b>
<b>Index . . . . .</b>	<b>239</b>