

République Algérienne Démocratique et Populaire
Ministère de L'Enseignement Supérieur de la Recherche Scientifique
Centre de Recherche sur l'Information Scientifique et technique



Mémoire pour l'obtention du diplôme
De Post-Graduation Spécialisée en Sécurité Informatique

Thème

Conception et implémentation d'une plate- forme de recherche sur une base de données chiffrées

Jury :

- **Président** : DBAH Adel
- **Membre**: KHEMISSA Hamza
- **Membre**: DERKI Mohamed
Sadek

Présenté par :

- Merdaci Adel.
- Elhoussaoui Abdelkrim.

Encadré par:

- M.BOUCENNA Fateh.

promotion - 2017 /2018 -

Sommaire

Introduction générale	1
Chapitre 1: Sécurité dans les bases de données.....	6
1. Sécurité	7
1.1. Propriétés principales.....	8
1.2. Processeur de sécurité.....	9
1.3. Attaque.....	9
1.4. Types d'attaques.....	10
1.5. Qui attaque?	10
1.6. Les risques encourus.....	10
2. Politique de sécurité.....	13
3. Les moyens de sécurité.....	13
3.1 Vues	13
3.2 L'authentification des utilisateurs	14
3.3 Le contrôle d'accès des utilisateurs.....	14
3.4 Protection des données de l'utilisateur.....	16
3.5 Audit des accès de l'utilisateur.....	17
4. La protection d'une base de données	19
4.1 Connaitre son besoin.....	19
4.2. Une sécurité en amont	19
4.3. Supervision	20
4.4. Sensibiliser les DBA.....	20
4.5. Durcir le socle système	20
4.6. Renforcer la couche BD	20
4.7. Méthodes d'accès.....	21
4.8. Chiffrer les flux de données.....	21
5. Conclusion	22
Chapitre 2: Cryptographie dans les bases de données	23
Introduction	24

1.	Contraintes pour chiffrer des bases de données ?.....	25
2.	Problématique du chiffrement des bases de données :.....	26
2.1	Les différents niveaux de chiffrement des bases de données :.....	26
2.1.1	Au niveau stockage :	28
2.1.2	Au niveau de base de données :	29
2.1.3	Au niveau applicatif :	30
3.	Chiffrement de la table :.....	32
3.1	Comment chiffrer la table ?.....	32
4.	Conclusion :.....	34
Chapitre 3: Recherche d'information dans des bases de données cryptées		36
Introduction		37
1.	cryptage interrogeable	38
1.1	Le problème.....	38
1.2	définition (indexation cryptée).....	39
2.	Principaux produits prenant en charge les bases de données chiffrées.....	40
3.	Synthèse.....	443
4.	Cadre proposé	44
5.	Conclusion :	45
Chapitre 4 Conception de l'approche proposée:		46
Introduction/motivation.....		47
1.	Problèmes	47
2.	Modèle de menace.....	48
3.	Architecture générale	49
4.	La structure de données utilisée par l'approche proposée :	51
6.	Description de l'approche proposée.....	53
7.	Description de l'approche proposée améliorée :.....	55
8.	Conception de l'approche avec UML :	57
8.1	Digramme de cas d'utilisation :	59
8.2	Diagramme de Classe :.....	61

8.3 Diagramme de Séquence :	62
8.4 Diagramme de Déploiement :	64
9. Analyse de sécurité :	65
10. Conclusion :	66
Chapitre 5: Implémentation et test	67
Introduction :	68
1. Environnement et outils de développement :	68
1.1. Système d'exploitation :	68
1.2. Caractéristiques de l'ordinateur :	68
1.3. Choix du langage de programmation :	68
1.3.1 Le JDK :	69
1.3.2 NetBeans :	69
1.3.3 JDBC :	69
1.3.4 RMI :	69
1.3.5 Choix du SGBD :	70
1.3.6 Oracle VM Virtual Box:	70
2. Présentation de l'application :	71
2.1. L'index et le chiffrement :	71
3. Fonctionnement de l'application :	71
3.1. Les serveurs :	72
3.2 Les base de données :	72
3.2. Propriétaire de données :	74
3-2-1 L'opération d'ajout des données :	75
3-2-2 L'opération de suppression des données :	76
3-2-3 L'opération de modification des données :	77
3-2-4 L'opération d'indexation et de chiffrement des indexes :	77
3.3. Client :	78
4.Conclusion :	80
Conclusion générale :	81