République Algérienne Démocratique et Populaire

Ministère de l'enseignement Supérieur et de la Recherche Scientifique

Université Saad Dahleb Blida 1

Faculté des Sciences

Département Informatique

Projet de fin d'étude pour l'obtention du diplôme Master

Sécurité des Systèmes d'Information

Conception et réalisation d'une approche de recherche d'informatio sécurisée sur des données structurées cryptées dans un Cloud

Sujet proposé par :

Mr Boucenna Fateh.

Présenté par :

Merouane Yasmine.

Marakache Fouzia.

Supervisé par :

Mme Zahra Fatma Zohra.

Devant le jury :

Mme Fareh Présidente du jury.

Mme Ouahrani Examinatrice.

- Juillet 2019 -

BIBLIOTHEQUE DU CERIST

REMERCIEMENTS

Louanges à celui sans qui rien n'aurait été.

Nous adressons ensuite nos remerciements les plus sincères et les plus chaleureux à notre promotrice Mme ZAHRA pour son encadrement, ses conseils, et son aide.

Nos profonds remerciements vont à Mr BOUCENNA, notre Encadreur pour nous avoir proposé ce thème et aidé inconditionnellement à le réaliser tout au long de notre Stage, ainsi que pour son constant et réconfortant soutien.

Nous tenons à formuler notre reconnaissance aux membres du jury.

Nous tenons à remercier tous les employés de service de sécurité des systèmes d'information de CERIST (Alger) pour l'aide qu'ils nous ont apportée.

Et enfin, merci à tous ceux qui ont contribué de près ou de loin à nous apporter de l'aide.

BIBLIOTHEQUE DU CERIST

DEDICACE

Une fleur d'amour et de reconnaissance est dédiée à mes parents.

À mes sœurs : Warda, Wahiba, Ihcene et Soundous.

À mes frères : Youcef, Ayoub, Taher et Houcine.

À mon neveu : Ilyes.

À mes nièces : Maram, Lina et Tesnim.

À toute ma famille.

Et à tous mes amis.

Fouzia.

BIBLIOTHEQUE DU CERIST

DEDICACE

Une fleur d'amour et de reconnaissance est dédiée à mes parents.

À mon frère : Rabeh, Cherif, Faize.

À ma nièce : Tesnim.

À mes cousines : Houda, Fatima, Sabiha.

À toute ma famille.

Et à tous mes amis.

Yasmine.

BIBLIOTHEQUE DU CERIST

Résumé

Les propriétaires de données sont motivés de plus en plus à externaliser leurs données structurées sur des serveurs Clouds, pour bénéficier de ses multiples avantages. Ces données sont sensibles et elles doivent être protégées contre (les attaques externes / serveur Cloud). Dans ce contexte nous avons proposé et implémenté une solution qui permet d'effectuer une recherche efficace et sécurisée sur des données chiffrées structurées dans le Cloud. Nous avons choisi le chiffrement AES pour chiffrer les tables externalisés. Pour qu'on puisse appliquer l'indexation sur des données structurées on a proposé une méthode d'indexation basée sur le modèle vectoriel. L'index a été chiffré avec la méthode SKNN, et dans le but d'accélérer le processus de recherche un arbre binaire est exploité et démontré par des tests dont les résultats sont satisfaisants.

Mots-clés

Cloud computing, le modèle vectoriel, recherche d'information sur des données chiffrées, le chiffrement SKNN, le chiffrement AES.

BIBLIOTHEQUE DU CERIST

Abstract

Data owners are increasingly motivated to outsource their data on Cloud servers, to benefit from its many advantages. This data is sensitive and must be protected against (external attacks / Cloud server). In this context, we have proposed and implemented a solution that allows an efficient and secure search on encrypted data structured in the Cloud. We chose AES encryption to encrypt outsourced tables. In order to apply indexing to structured data, an indexing method based on the vector model has been proposed. The index was encrypted with the SKNN method, and in order to speed up the search process a binary tree is exploited and demonstrated by tests whose results are satisfactory.

Keywords

Cloud computing, the vector model, search for information on encrypted data, AES encryption, SKNN encryption.

BIBLIOTHEQUE DU CERIST

Table des matières

Introduction générale 1

Partie 1 : État de l'art

Chapitre 01 : Recherche d'information

1. Introduction 6
2. Définitions 6
   2.1. La recherche d'information 6
   2.2. Les systèmes de recherche d'information 6
3. Conception de base de la RI 7
   3.1. Document 7
   3.2. Requête 8
   3.3. Collection de documents 8
   3.4. Besoin en information 8
   3.5. Pertinence 8
      3.5.1. La pertinence Système 8
      3.5.2. Pertinence utilisateur 8
   3.6. Correspondance entre la requête et les documents 9
4. Indexation 9
   4.1. Indexation de documents 9
      4.1.1. Manuelle 9
      4.1.2. Semi-automatique 9
      4.1.3. Automatique 10

BIBLIOTHEQUE DU CERIST

Tables des matières

5. Modèles de recherche 11
5.1. L'appariement requête-document 11
5.2. Le Modèle Booléen 12
5.2.1. Les avantages du Modèle Booléen 13
5.2.2. Les inconvénients du Modèle Booléen 13
5.3. Le modèle Vectoriel (VSM : Vector Space Model) 13
5.3.1. Les avantages du modèle vectoriel (VSM : Vector Space Model) 14
5.3.2. L'inconvénient du modèle vectoriel (VSM : Vector Space Model) 14
5.4. Le modèle probabiliste (Probabilistic Model) 14
5.4.1. Les avantages du Modèle probabiliste (Probabilistic Model) 15
5.4.2. L'inconvénient du modèle probabiliste (Probabilistic Model) 15
6. Conclusion 15

Chapitre 2 : Cloud computing

1. Introduction 17
2. Définition 17
3. Différents services du Cloud computing 17
3.1. IaaS (Infrastructure as a Service/Infrastructure fournie en mode service) 17
3.2. PaaS (Platform as a Service / Plate-forme fournie en mode service) 18
3.3. SaaS (Software as a Service / Logiciel fourni en mode service) 18
4. Différents modèles du Cloud computing 18
4.1. Le Cloud privé 18
4.2. Le Cloud public 18
4.3. Le Cloud communautaire 19
4.4. Le Cloud hybride 19
5. Les caractéristiques essentielles d'un Cloud 19

BIBLIOTHEQUE DU CERIST

6. La sécurité des données dans le cloud 20

7. Conclusion 21

Chapitre 03 : Le chiffrement des données (Cryptographie)

1. Introduction 23

2. La cryptologie 23

3. Domaines de cryptographie 24

3.1. Chiffrement symétrique (Chiffrement à clé secrète) 24

3.1.1. Chiffrement AES 24

3.1.2. La méthode de cryptage SKNN 27

3.2. Chiffrement asymétrique (Chiffrement à clé publique) 30

3.1.1. Chiffrement RSA 30

4. Objectifs de la cryptographie 31

5. Conclusion 32

Chapitre 4 : La recherche d'information sur des données chiffrées dans le Cloud computing

1. Introduction 34

2. L'architecture générale d'un système de recherche d'information crypté 34

2.1. Architecture de système 34

2.2. Principe 35

3. Les approches de recherches sur une donnée cryptée dans la littérature 36

3.1.Méthode traditionnelle de la recherche sur des données cryptées 36

3.2. Une recherche sécurisée et dynamique avec plusieurs mots clés sur des données chiffrées en nuage 36

BIBLIOTHEQUE DU CERIST

3.2.2. Principe 37

3.2.3. Le fonctionnement de l'approche 37

3.2.4. Les avantages de l'approche 38

3.3. Recherche d'images cryptées sécurisée et efficace avec contrôle d'accès 39

3.3.1. Architecture de système 39

3.3.2. Principe 39

3.3.3. Le fonctionnement de l'approche 39

3.3.4. Les avantages de l'approche 40

3.4. Recherche par mot-clé flou vérifiable et efficace sur des données chiffrées dans le Cloud Computing 41

3.4.1. Architecture de système 41

3.4.2. Principe 41

3.4.3. Les objectifs de conception 42

3.4.4. Les techniques utilisées 43

3.5. EPCBIR : Schéma de récupération d'images basé sur le contenu, efficace et préservant la confidentialité, dans le cloud computing 44

3.5.1. Architecture du système 44

3.5.2. Principe 44

3.5.3. Le fonctionnement de l'approche 45

3.5.4. Les principales contributions 46

3.5.5.Les avantages de l'approche 46

3.6. Comparaison entre les techniques d'accélération 47

4. La recherche d'information sécurisée sur des données structurées dans le Cloud 48

5. Conclusion 48

BIBLIOTHEQUE DU CERIST

Tables des matières

Partie 2 : Conception et Implémentation

Chapitre 5 : Conception de l'approche proposée

1. Introduction 51

2. Description de l'approche proposée 51

2.1. Entités du processus de recherche……..……..52

2.2. Processus de recherche…….53

3. Analyse de sécurité 60

4.Conclusion 61

Chapitre 6 : Implementation et test

1.Introduction 63

2. L'environnement de travail et les outils de développement 63

2.1. Le système d'exploitation 63

2.2. Caractéristiques de l'ordinateur 63

2.3. Langage de programmation 63

3. Présentation de l'application 64

3.1. Les interfaces graphiques 64

4. Test et performances 71

5. Conclusion 72

Conclusion générale 73

Bibliographie.

BIBLIOTHEQUE DU CERIST