

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 d'une solution Cloud
sécurisée pour le ministère de la santé**

Elaboré par:

ABDELHAI Kamel
KHEMACHE Nabil

Encadré par :

M. TANDJAOUI Djamel

Soutenu devant le jury :

- **M. MEZIANE Abdelkrim** **Président**
- **Mme. BENMEZIANE Souad** **Examineur**
- **M. AMIRA Abdelouahab** **Examineur**

Remerciements

*Nous remercions le bon Dieu de nous avoir accordé la force et le temps
d'achever cet humble travail*

Ce travail est le fruit du cursus que nous avons suivi au niveau du CERIST, par conséquent le mérite revient à tous ceux qui ont contribué de près ou de loin à cette formation.

Nous tenons tout d'abord à remercier notre promoteur M.TANDJAOUI Djamel pour avoir eu l'obligeance de nous accepter pour ce travail et qui, avec ses orientations et ses remarques pertinentes, a eu l'amabilité de partager avec nous son savoir et ses expériences.

Un grand merci à M. MEZIANE qui à été très accueillant et serviable en acceptant de nous accorder un peu de son temps très précieux, et pour les éclaircissements et information qu'il nous a donné.

Nous exprimons nos sincères sentiments de gratitude et de remerciements pour le personnel du service formation du CERIST, sans oublier tous les enseignants qui ont assuré notre formation.

Nous remercions aussi les membres du jury pour avoir bien voulu juger notre travail.

Un grand merci à tout le personnel du CERIST pour le bon accueil et l'hospitalité qui nous ont été offerts tout au long de notre séjour au sein de cet établissement respectable.

A toute la promotion 2012-2013 pour les moments inoubliables que nous avons passé ensemble.

« Si les constructeurs bâtissaient des immeubles comme les programmeurs écrivent des programmes. Le premier pivot qui passe détruirait la civilisation »

Deuxième loi de Weinberg [8].

A tous ceux qui, nourris de sciences et de savoir, sont morts de faim,

A mes très chers parents, à mon épouse et à mes enfants, à mon frère et à mes sœurs, à tous ceux pour qui je compte.

Nabil

*A tous ceux qui, nourris de sciences et de
savoir, sont morts de faim,*

*A mes très chers parents, à mon épouse
et à ma fille, à mes frères et à mes sœurs,
à tous ceux pour qui je compte.*

Kamel

Résumé

Les technologies de l'information et de la communication ont modifié en profondeur les pratiques médicales et les relations entre patients et professionnels de la santé partout dans le monde.

En tant que modèle général pour la fourniture de services informatiques, l'informatique en nuage présente un vaste champ d'applications au secteur de la santé en Algérie tant sur le plan de la sécurité des masses importantes de données stratégiques générées par les différents établissements que sur le plan d'organisation et de structuration du système d'information et du stockage à partir du moment où les établissements de la santé n'ont pas les compétences requises pour la gestion et le maintien d'une infrastructure aussi lourde.

L'objectif de ce mémoire est de proposer une solution de Cloud privé sécurisée pouvant être déployée par le ministère de la santé, cette solution doit entre autre répondre à des exigences de sécurité et de fonctionnement qui garantissent la protection adéquate des données sensibles qui seront stockées et de l'infrastructure entière. Cette solution sera constituée de quatre Datacenters répartis sur le territoire national, ils seront connectés entre eux à travers le réseau ARN et nous utiliserons des lignes spécialisées pour relier les établissements de la santé à cette infrastructure.

Mots clés : Cloud Computing, Sécurité informatique, Solution privé de Cloud.

Table des matières

Introduction générale	1
1. Généralités sur le Cloud Computing	3
1.1 Définition du Cloud Computing	3
1.2 Caractéristiques communes du Cloud Computing	5
1.3 Qualités du Cloud Computing	7
1.4 Les services offerts par le Cloud Computing	10
1.5 Types de Cloud Computing	12
1.6 Modèle de référence du Cloud Computing	12
1.7 La virtualisation	14
1.7.1 Présentation	14
1.7.2 Les différentes techniques de virtualisation	15
1.7.3 Solutions de virtualisation	17
1.8 Le stockage dans le Cloud	19
1.9 Quelques solutions libres de Cloud Computing	20
1.10 Solutions de virtualisation dans le Cloud computing	22
1.11 Conclusion	22
2. La sécurité dans le Cloud	23
2.1 Vu d'ensemble de la sécurité dans le Cloud	23
2.2 Inquiétude vis-à-vis de la sécurité	26
2.3 Risques majeures relatifs aux Clouds computing	29
2.4 Eléments architecturaux de la sécurité	34
2.4.1 Exigences de sécurité pour l'architecture	34
2.4.2 Sécurité physique	35
2.4.3 Normes et stratégies de sécurité du Cloud	36
2.4.4 Synchronisation de l'heure au niveau du Cloud	37
2.4.5 Gestion des identités	37
2.4.6 Gestion des accès	37
2.4.7 Gestion des clés	37
2.4.8 Audit du système et du réseau	38
2.4.9 Surveillance de la sécurité	38
2.4.10 Complexité des hyperviseurs	39
2.4.11 Protection coté serveur	40
2.4.12 Protection coté client	40
2.4.13 Protection des données	41
2.4.14 Résilience	41
2.5 Conclusion	42
3 Motivations et architecture du Cloud privé	43
3.1 Problématique	44
3.2 Exigences pour le système d'information	47
3.3 Avantages de l'informatisation du secteur de la santé	48
3.4 Solutions possibles pour l'informatisation	49
3.4.1 Déploiement d'un système d'information traditionnel	49
3.4.2 Migration vers Cloud public	50
3.4.3 Déploiement d'un Cloud privé	51
3.5 Pourquoi le Cloud privé ?	51

3.6 Solution proposée	52
3.6 Conclusion	56
4 Implémentation de la solution	57
4.1 Prérequis	57
4.2 Implémentation du Cloud et choix des technologies	58
4.3 Implémentation de la sécurité au niveau du Cloud	62
4.3.1 Stratégies et politique de sécurité du Cloud	62
4.3.2 Sécurité physique	62
4.3.3 Installation d'un serveur de temps	63
4.3.4 Gestion des identités et contrôle des accès	63
4.3.5 Sécurisation des communications et des accès	64
4.3.6 Surveillance de la sécurité	64
4.3.7 S Suppression des logiciels malveillants	64
4.3.8 Protection des données	65
4.3.9 Utilisation d'une base de données de configuration	66
4.3.10 Améliorer la Résilience	66
4.4 Evaluation de la sécurité	67
4.6 Le maillon faible	78
4.7 Conclusion	78
Conclusion générale et perspectives	79