

Introduction générale :

La technologie de l'information (TI) est un Ensemble d'outils et de ressources technologiques permettant de transmettre, enregistrer, créer, partager ou échanger des informations, notamment les ordinateurs, l'internet (sites web, blogs et messagerie électronique, Cloud Computing). [10]

Les systèmes d'information sont un enjeu stratégique dans plusieurs domaines Parmi les évolutions récentes, le développement du Cloud Computing et la sécurité est devenu un sujet d'attention.

Le Cloud Computing est maintenant le fondement de plus l'utilisation d'Internet. Email, moteurs de recherche, réseaux sociaux, médias en streaming, et d'autres services sont désormais hébergés dans "le Cloud ". Les collections des grands serveurs des produits de base en cours d'exécution de coordination logicielles qui rend des hôtes individuels largement disponible. Alors que le Cloud Computing à coûts réduits et une commodité accrue, l'accessibilité et la centralisation du Cloud Computing crée également de nouvelles opportunités pour les failles de sécurité. [11]

La sécurité des systèmes d'information (SSI) est l'ensemble des moyens techniques, organisationnels, juridiques et humains nécessaires et mis en place pour conserver, rétablir, et garantir la sécurité du système d'information. Assurer la sécurité du système d'information est une activité du management du système d'information.

Il existe des chercheurs en sécurité qui ont étudié divers aspects de la sécurité du Cloud Computing à la fois une offensive et une perspective défensive. [11]

L'objectif de notre travail est une étude sur la sécurité d'un Cloud Computing.

Dans ce mémoire, nous adopterons une organisation comportant quatre différents chapitres. Les deux premiers présentent l'état de l'art sur les notions fondamentales du Cloud Computing et Les mécanismes de sécurité d'un Cloud Computing.

Dans le premier chapitre, nous définirons le Cloud Computing et éléments constitutifs du Cloud Computing, ainsi qu'un aperçu des types de Cloud Computing. A la fin de ce chapitre nous donnons une description sur l'architecture du Cloud Computing.

Dans le deuxième chapitre, il sera consacré pour présenter une étude sur les mécanismes de sécurité d'un Cloud Computing, nous commençons cette étude par les attaques et l'impact courant sur le Cloud. Puis nous introduisons les différentes

techniques utilisées pour la sécurité de données du Cloud, en présentant aussi l'historique des attaques dans le Cloud. Nous terminons ce chapitre par le contrôle de sécurité d'un Cloud.

Le troisième chapitre, la réalisation du système, en présentant le système open source OPENSTACK, ainsi nous expliquons les différences étapes pour l'installation de l'OENSTACK. et puis on a expliqué comment la création d'un espace Cloud sur OPENSTACK.

Le quatrième chapitre, nous allons présenter une étude sur la sécurité dans l'OpenStack, .et puis on a explique comment on utilise les outils de l'analyse les vulnérabilités d'un Cloud, et les outils de l'attaque. A la fin de ce chapitre nous allons présenter les outils de la sécurité.

Notre travail sera achevé par la conclusion générale qui va résumer nos objectifs estimés et les limites de notre réalisation tout en évoquant les problèmes que nous avons rencontrés et les améliorations envisageables.