République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université A/Mira de Béjaïa
Faculté des Sciences Exactes
Département d'Informatique

Mémoire de Master professionelle
en Informatique
Option
Administration et sécurité des réseaux
Thème

La sécurité des données dans le Cloud Computing

Présenté par

M^{elle} ***BERKANI*** **Nassima**
M^{elle} ***MOUSSAOUI*** **Salima**

Soutenu devant le jury composé de :

Président	M^{r} ***BOUDRIES*** **Abdelmalek**
Promotrice	M^{elle} ***SELLAMI*** **Lynda**
Examinateur	M^{r} ***BAADACHE*** **Abdarrahmane**
Examinatrice	M^{me} ***HALFOUNE*** **Nadia**

Promotion 2015/2016

Dédicaces

Je dédie ce modeste travail à :

A mes trés chers parents, qui sont la cause de mon existence dans cette vie, Pour leur soutient, leur patience et leur amour qui m'ont donné la force pour continuer mes études,
A mon trés chér mari pour son soutien qui ma donné le courage de continuer ainsi que toute la famille Aoulmi ,
A mon chér frère Allaoua et sa femme Samia ,
A mon chér frère Aziz et sa femme Assia,
A ma chére sœur Dalila et son mari Tahar,
A mes chéres sœurs Naima et Wissam à qui je souhaite une bonne continuation dans leurs études,
A mon oncle Hanafi et sa femme Souhila ainsi que toute mes tantes ,
A mes nièces (Aya,Fariel,Lyna et Anaïs) et neveux (Islem,Rafik,Wassim,Aymen et Hocine) ,
A toutes mes meilleurs amies et cousines, dont la liste est longue surtout Sylia , Lydia et Wissam
A toute ma grande famille,
A mes amies et collègues, et tous ceux qui m'ont aidé ,
A ma binôme salima et sa famille.

BERKANI Nassima

Dédicaces

Je dédie ce modeste travail à :
A mes très chers parents qui n'ont jamais cessé de me soutenir tout au long de mon parcours d'étude,
A mon cher frère Nassim et son épouse Kahina,
A mes chers frères Nadjim et Hakim,
A ma chère sœur Nassima et son époux Yazid,
A ma chère sœur Karima et son époux Lamine,
A ma très chère niéce Imane et mes trés chers neveux Ibrahim, Youcef et Wassim,
A mes très chères copines,
Et a tous mes amis (es).
A ma binôme Nassima et sa famille.

A tous ceux dont les noms n'y figurent pas pour une raison ou une autre trouve l'expression de ma profonde gratitude.

MOUSSAOUI Salima

Remerciements

En premier lieu,nous remercions DIEU le tout puissant, maître des cieux et de la terre, qui nous a éclairé le chemin et permis de mener à bien ce travail.

Nous tenons également à exprimer toute notre reconnaissance à notre promotrice Madame SELLAMI Lynda, qui s'est toujours montré disponible et à l'écoute durant toute la réalisation de ce présent mémoire et qui a su guider et structurer nos idées grâce à ses précieux conseils.

Nos profonds remerciements s'adressent aux membres de jury qui nous font honneur en acceptant d'évaluer notre travail.

Un énorme merci à nos familles et amis pour leurs éternel soutient et la confiance qu'ils ont en nos capacité.

Enfin, nous remercions tous ceux qui ont contribué de près ou de loin à l'aboutissement de ce modeste travail.

Résumé

Cloud Computing est une révolution économique et technologique, dans lequel les ressources informatiques sont fournies en tant que service via internet. En particulier, ces ressources peuvent être provisionnées de façon dynamique et libérées en fonction de la demande de service et avec un effort minimal de gestion. Le Cloud Computing présente une meilleure solution pour gérer les données, les infrastructures, etc. Cependant, la sécurité des données en transit dans le Cloud Computing reste un challenge pour les fournisseurs du Cloud. En effet, ces données sont la cible de plusieurs attaques réseau, qui ont pour but d'interrompre, d'intercepter, de modifier et de fabriquer des informations. Par conséquent, il est essentiel de faire face à ces attaques et intrusions en vue d'améliorer l'utilisation et l'adoption de Cloud. A travers ce mémoire nous présentons une étude détaillée sur la sécurité des données dans le Cloud en fournissant les plus importantes solutions existantes dans ce domaine. Ensuite, nous allons proposer une solution de sécurisation basant sur le chiffrement des données.

Mots-clés : Cloud Computing, Sécurité des données, Attaques, Solutions,chiffrement des données.

Abstract

Cloud Computing is an economic and technological revolution in which computing resources are provided as a service over the Internet. In particular, these resources can be dynamically provisioned and released according to the service request and with minimal management effort. It presents a better solution for managing data, infrastructure, etc. However, security of data in transit in the Cloud remains a challenge for Cloud providers. Indeed, these data are the target of many network attacks that are aimed to interrupt, intercept, modify and manufacture information. Therefore, it is essential to face these attacks and intrusions to improve the use and adoption of Cloud. Through this paper we present a detailed study on data security in the Cloud by providing the most extensive existing solutions in this area. Then we will offer a security solution based on data encryption.

Keywords : Cloud Computing, Data security, Attacks, Solutions, Data encryption.

Table des matières

Liste des figures

Liste des abréviations

ACL : Access Control List.
AES : Advanced Encryption Standard.
API : Application Programming Interface.
CRM : Customer Relationship Management.
DES : Data Encryption Standard.
DoS : Denial of Service.
DSI : Direction des Systèmes d'Information.
ECC : Elastic Compute Cloud.
EDI : environnement de Développement Intégré
ENS : Ecole National Supérieur
FAT : File Allocation Table.
GRH : Gestion des Ressources Humains.
IaaS : Infrastructure as a Service.
IAM : Identity and Access Management.
IBM : International Business Machines.
IMEI : International Mobile Equipment Identity.
IMSI : International Mobile Subscriber Identity.
IP : Internet Protocol.
IPSEC : Internet Protocol Security.
MITM : Man In The Middle.
NIST : National Institute of Standards and Technology.
NT : Nouvelle Technologie.
OTP : One Time Password.
PaaS : Platform as a Service.
PIN : Personal Identification Number.
SaaS : Software as a Service.
SLA : Service Level Management.
SSL : Secure Socket Layer.
SSS : Simple Storage Service.
SQL : Structured Query Language.
SQS : Simple Queue Service.
RSA : Rivest Shamir and Adleman.
TLS : Transport Layer Security.
TIC : Technologies de l'Information et de la Communication.
TVDc : Trusted Virtual Data Center.
URL : Uniform Resource Locator.
VM : Virtual Machine.

VM CO : Virtual Machine Company.
VMM : Virtual Machine Monitor.
VPN : Virtual Private Network.
XML : Extensible Markup Language.

Introdution Générale

L'informatique a toujours évolué, au gré des nouvelles technologies, pour répondre à de nouvelles demandes. L'informatique est centralisée avec l'avènement des centres de données et surtout, elle se dématérialise et devient " l'informatique dans les nuages " ou Cloud Computing.

Le Cloud Computing consiste en une interconnexion et une coopération de ressources informatiques, situées dans diverses structures internes, externes ou mixtes et dont le mode d'accès est basé sur les protocoles et standards Internet. Le Cloud Computing est devenu ainsi, le sujet le plus débattu aujourd'hui dans le secteur des technologies de l'information. Face à l'augmentation continuelle des coûts de mise en place et de maintenance des systèmes d'information, les entreprises externalisent de plus en plus leurs services informatiques en les confiant à des entreprises spécialisées comme les fournisseurs de Cloud. L'intérêt principal de cette stratégie pour les entreprises réside dans le fait qu'elles ne paient que pour les services effectivement consommées. Quant au fournisseur du Cloud, son but est de répondre aux besoins des clients en dépensant le minimum de ressources possibles.

Avec le developpement des services et moyens informatique pour le Cloud Computing, des problèmes de sécurité sont apparus mettant en péril la sécurité des données ce qui fait de ce point l'un des principaux challenge du Cloud, en effet la sécurité des données externalisées est un thème très convoité. La sécurité du Cloud Computing est l'ensemble des moyens techniques, organisationnels, juridiques et humains nécessaires qui sont mise en place pour conserver, rétablir, et garantir la sécurité . Assurer la sécurité du Cloud Computing est une activité du management du Cloud. Pour une meilleure sécurité du Cloud il est important de protéger la console de restitution des données nécessaires à la délivrance du service, et se soucier également de son emplacement géographique et de la localisation dont elle dépend.

Dans le cadre de ce mémoire, nous nous sommes intéressés à la sécurité des données

dans le Cloud Computing qui est le premier frein à l'adoption du Cloud. Pour remédier à ce problème plusieurs efforts de recherche ont été entrepris, ces dernières années, visant à sécuriser et protéger les données dans le Cloud Computing, mais une protection parfaite est loin d'être évidente à cause de la diversité des problèmes et attaques possibles.
Notre solution proposée permet de résoudre quelques problèmes liés à la sécurité des données et de détecter si les données ont été altérées ou non.

Pour cela, nous avons entrepris notre étude selon les quatre chapitres suivants :

Le ***premier chapitre*** propose quelques notions fondamentales et généralités à propos du Cloud Computing.

Dans le ***deuxiéme chapitre***, nous entamerons la sécurité dans le Cloud Computing, nous présentons les services de sécurité exigés, les différentes attaques possibles, ainsi que les solutions de sécurité proposées dans la littérature.

Le ***troisiémé chapitre*** est consacré aux problémes de sécurité des données dans le Cloud ainsi que les solutions proposées dans la littérature.

Dans le ***quatriéme chapitre***, nous proposons une approche de sécurité pour protéger les données dans le Cloud Computing, ensuite nous présentons et discutons les résultats de notre programmation.

Enfin, nous conclurons notre travail en résumant les connaissances acquises.

1

Introduction au Cloud Computing

1.1 Introduction

Les technologies de l'information et de la communication (TIC) se développent plus rapide et de manière progressive. Dans ces dernières années il y a une nouvelle destination, son but est d'améliorer les services dans le domaine TIC, il s'agit du "Cloud Computing". Ce dernier est un nouveau concept informatique qui consiste à proposer des services informatiques sous forme de services à la demande, accessibles de n'importe où, n'importe quand et par n'importe qui. Cette nouvelle technologie permet à des entreprises d'externaliser le stockage de leurs données et de leur fournir une puissance de calcul supplémentaire pour le traitement de grosse quantité d'information.

Dans ce chapitre nous donnons quelques généralités sur le Cloud Computing, à savoir sa définition, ses différents types, les services qu'il offre, ses avantages et inconvénients, ainsi certaines notions pour la bonne compréhension de ce concept.

1.2 Un bref historique

La première énonciation du concept du Cloud Computing date de 1960, quand John McCarthy affirmait que la ressource informatique serait accessible et consommée par le public de la même façon que la distribution d'eau et d'énergie [1].

Le concept du Cloud Computing a été adopté pour la première fois en 2002 par Amazon, un leader du e-business, qui avait investi dans un parc de machines immense, dimensionné pour absorber la charge importante des commandes faites sur leur site au moment des fêtes de Noël, mais relativement inexploité le reste de l'année. Sous-dimensionner leur parc aurait causé des indisponibilités de leur site au moment des pics, mettant ainsi en péril leur business pendant les fêtes (soit une grosse partie de leur chiffre d'affaires). Leur idée a donc été d'ouvrir toutes ces ressources inutilisées aux entreprises, pour qu'elles les louent à la demande. Depuis, Amazon investit massivement dans ce domaine et continue d'agrandir son parc et ses services.

1.3 Définition

Le terme Cloud Computing se traduit en français par " Informatique dans les nuages ", est un concept qui représente l'accès à la demande, à des informations et services situés sur un serveur distant. L'idée principale à retenir est que le Cloud n'est pas un ensemble de technologies, mais un modèle de fourniture, de gestion et de consommation de services et de ressources informatiques. La notion de Cloud Computing est vaste et le concept ne peut être réduit à une simple définition. En effet de nombreuses définitions existent, en voici les principales d'entre elles :
NIST (National Institute of Standards and Technology) définit le Cloud Computing comme suit : " Le Cloud Computing est l'ensemble des disciplines, pratiques, technologies et modèles commerciaux utilisés pour délivrer comme un service à la demande et par le réseau des capacités informatiques (logiciels, plateformes, matériels) " [2].
Pour le groupe de travail CIGREF (Reseaux des grandes entreprises) le Cloud Computing est défini par les quatre points suivant [3] :

- Un Cloud est toujours un espace virtuel.
- Contenants des informations qui sont fragmentées.
- Les fragments sont toujours dupliqués et répartis dans cet espace virtuel, lequel peut être sur un ou plusieurs supportsphysiques.

- Et qui possède "une console (programme) de restitution"permettant de reconstituer l'information.
  Pour Génération NT (Nouvelle Technologie) :" Le Cloud Computing est un concept d'organisation informatique qui place Internet au cœur de l'activité des entreprises, il permet d'utiliser des ressources matérielles distantes pour créer des services accessibles en ligne " [4].

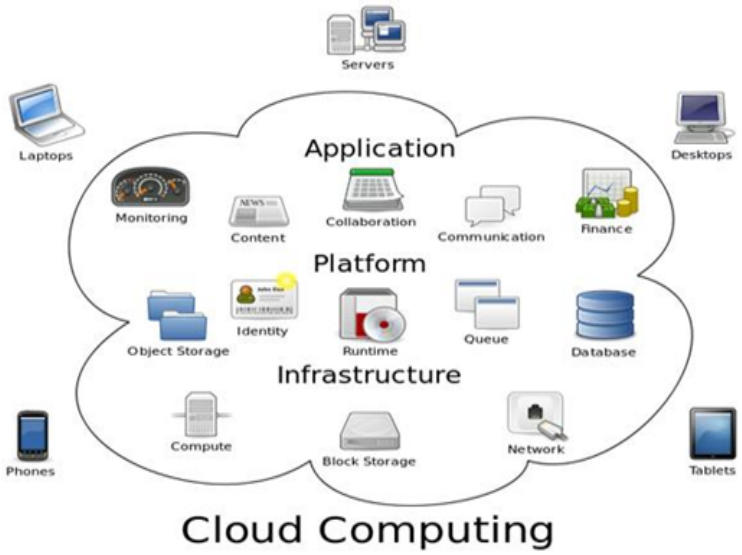

FIG. 1.1 – Les déférents compoants du Cloud Computing.

1.4 Objectifs

L'objectif principal du Cloud Computing est de créer une communauté de pratique sur le concept de Cloud Computing.Les objectifs spécifiques poursuivis sont :

- Fournir des données objectives sur le domaine en construisant une base d'informations dynamiques ;
- Susciter l'intérêt et provoquer la réflexion des parties prenantes sur le domaine ;
- Stimuler la participation, la collaboration et favoriser l'enrichissement de la base d'informations sur le domaine ;
- Aassurer la permanence et la visibilité de la communauté de pratique sur le Cloud Computing.

1.5 Caractéristiques du Cloud Computing

les principales caractéristiques du Cloud Computing sont :

- **Elasticité :**Elle définit la capacité d'une infrastructure donnée à s'adapter de manière-dynamique au changement [5].
- **pay-as-you-use :**Le coût est proportionnel à l'usage, donc l'utilisateur paye pour exactement ce qu'il utilise [6].
- **Self-service (à la demande) :**Les ressources sont disponibles au moment et là où le client le souhaite [6].
- **Mesure de la qualité de services :** évaluer et garantir un niveau de performance et de disponibilité adapté aux besoins spécifiques des clients.
- **Accès réseau universel :** L'accès aux ressources est très rapide et à l'aide d'un réseau (Internet), par des protocoles standards en manière très élasticité [7].
- **" Mise en commun de ressources (pooling) :**Dans un environnement de type Cloud Computing, on ne pense pas en nombre de serveurs, taille de disques, nombre de processeurs ,etc mais en puissance de calcul, capacité totale de stockage, bande passante disponible grace a la virtualisation [2].
- **Multi-tenancy (Multi location)** :Sur le Cloud une même application peut être utilisée par plusieurs clients en même temps, en préservant la sécurité et les données privées de chaque client. Cela est possible en utilisant des outils de virtualisation qui permettent de partager un serveur sur plusieurs utilisateurs [8].
- **Disponibilité :**La haute disponibilité de la plate-forme est obtenue grâce à la mise en place de techniques de redondance et/ou réplication. Donc le Cloud fournit un service fiable et non sensible à la défaillance [5].
- **Auto-guérison :** Tout système Cloud doit contenir une ou plusieurs copies de chaque application déployée , de telle façon qu'en cas de disfonctionnement de l'application en cours, l'application en copie vient la remplacer. Les applications en copies doivent être maintenues et mise à jours à chaque fois que l'application en cours est modifiée [9].
- **SLA (Service Level Management) :** Avec les services Cloud, un client peut négocier le niveau de service qu'il lui convient et il doit payer pour cela. Dans le cas où les ressources Cloud sont en surcharge, le système crée d'autres entités d'applications Cloud en utilisant les outils de virtualisation disponible afin de respecter les termes du contrat SLA [10].

1.6 Eléments du Cloud Computing

Les éléments pouvant constitué le système Cloud sont les suivant :

1.6.1 La virtualisation

La virtualisation est la principale technologie dans le Cloud,elle permet une gestion optimisée des ressources matérielles en disposant de plusieurs machines virtuelles sur une machine physique. C'est une technologie qui permet une plus grande modularité dans la répartition des charges et la reconfiguration des serveurs en cas d'évolution ou de défaillance momentanée.
Le principe de virtualisation permet d'intégrer les différents serveurs de façons plus flexible pour faciliter l'utilisation.
Le but de la virtualisation est de faire la transparence d'utilisation et l'efficacité d'exploitation des ressources, d'assurer le fonctionnement des différents services et la séparation entre de multiples locataires (utilisateurs) impliqués dans un matériel physique [11].

1.6.2 L'infrastructure

L'infrastructure informatique du Cloud est un assemblage de serveurs, d'espaces de stockage et de composants réseau organisés de manière à permettre une croissance incrémentale supérieure à celle que l'on obtient avec les infrastructures classiques. Ces composants doivent être sélectionnés pour leur capacité à répondre aux exigences d'extensibilité, d'efficacité, de robustesse et de sécurité. Les serveurs d'entreprise classiques ne disposent pas des capacités réseau, de la fiabilité ni des autres qualités nécessaires pour satisfaire efficacement et de manière sécurisée les accords de niveau de service SLA (Service Level Agreement). Par ailleurs, les serveurs d'un Cloud affichent des coûts de fonctionnement moins élevés et ils peuvent être plus fiables s'ils ne sont pas tous équipés de disques internes [7].

1.6.3 Le Datacenter

Un centre de traitement de données, en anglais " datacenter " est un site physique sur lequel sont regroupés des équipements constituants le système d'information de l'entreprise (mainframes, serveurs, baies de stockage, équipements réseaux et de télécommunications, etc.). Il peut être interne ou externe à l'entreprise, exploité ou non avec le soutien de prestataires. Il comprend en général un contrôle sur l'environnement (climatisation, système de prévention contre l'incendie, etc.), une alimentation d'urgence et redondante, ainsi qu'une sécurité physique élevée. Des particuliers ou des entreprises peuvent venir y stocker leurs données suivant des modalités bien définies [12]. Nous distinguons quatre formes de Cloud

Computing (voir figure 1.3) : Le Cloud public, le Cloud privé, le Cloud hybride et le Cloud communautaire.Dans ce qui suit, nous décrivons chacun d'eux en détail :

FIG. 1.2 – Exemple d'un Centre de données (Datacenter).

1.6.4 La plateforme collaborative

Une plate-forme de travail collaboratif est un espace de travail virtuel. C'est un outil, parfois sous la forme d'un site internet qui centralise tous les outils liés à la conduite d'un projet et les met à disposition des acteurs (clients). L'objectif du travail collaboratif est de faciliter et d'optimiser la communication entre les individus dans le cadre du travail ou d'une tâche [12].

1.7 Les formes de déploiement du Cloud Computing

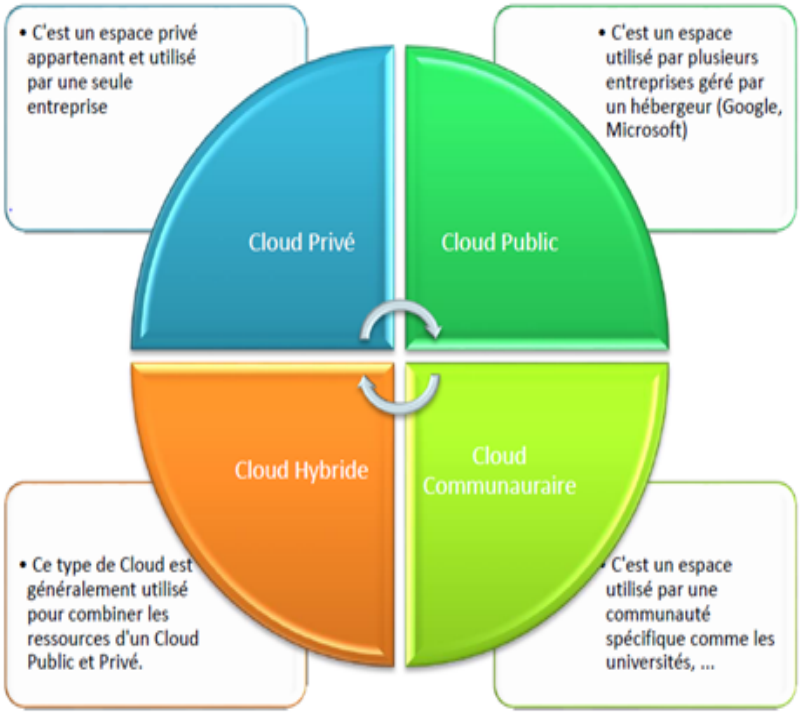

FIG. 1.3 – Modèles de déploiements du Cloud Computing [6].

1.7.1 Le Cloud public

Le Cloud public également le premier apparu, son principe est d'héberger des applications, en général des applications Web, sur un environnement partagé avec un nombre illimité d'utilisateurs. C'est un ensemble des services et des ressources accessibles par Internet et géré par un prestataire externe (fournisseur), ces ressources et services sont partagés entre plusieurs clients, utilisés à la demande et à tout moment sans savoir où elles existent, aussi ces services peuvent être gratuits ou payants. En cas des services payants, il existe des contrats SLA (Service Level Agreement) entre les clients et les fournisseurs, SLA est un document qui définit la qualité de service requise entre les deux [13].

1.7.2 Le Cloud privé

Un Cloud privé est un ensemble des services et des ressources disponible à un seul client par exemple une entreprise, il peut être géré par l'entreprise elle-même, ou bien avec ses branches, dans ce cas il s'appelle "Le Cloud privé Interne", en d'autre façons il peut

être géré par un prestataire externe loué par l'entreprise, dans ce cas s'appelle "Le Cloud privé Externe ", il est accessible via des réseaux sécurisés de type VPN (Virtual Private Network). L'avantage de ce type de Cloud par rapport au Cloud public réside dans l'aspect de la sécurité et la protection des données [10].

1.7.3 Le Cloud hybride

Cloud hybride est la cohabitation et la communication entre un Cloud privé et un Cloud public dans une organisation partageant des données et des applications. C'est -à-dire on peut déporter nos applications vers un Cloud public qui consommera des données stockées et exposées dans un Cloud privé, ou bien faire communiquer deux applications hébergées dans deux Clouds privés distincts, ou encore consommer plusieurs services hébergés dans des Cloud publics différents [14].

1.7.4 Le Cloud Communautaire

Un Cloud communautaire est utilisé par plusieurs organisations qui ont les mêmes intérêts. Dans une telle architecture, l'administration du système peut être effectuée par l'une ou plusieurs des organisations partageant les ressources du Cloud.Ainsi cela peut porter sur l'hébergement d'une application métier très spécialisée, mais commune à de très nombreuses entreprises, qui décident de fédérer leurs efforts [15].

1.8 Les services du Cloud Computing

Le Cloud Computing peut être subdivisé en 3 couches (voir la figure 1.4) : La couche infrastructure (IaaS) est gérée par les architectes réseaux, la couche plateforme (PaaS) destinée aux développeurs d'applications et finalement la couche applicative (SaaS) qui est le produit final pour les utilisateurs.

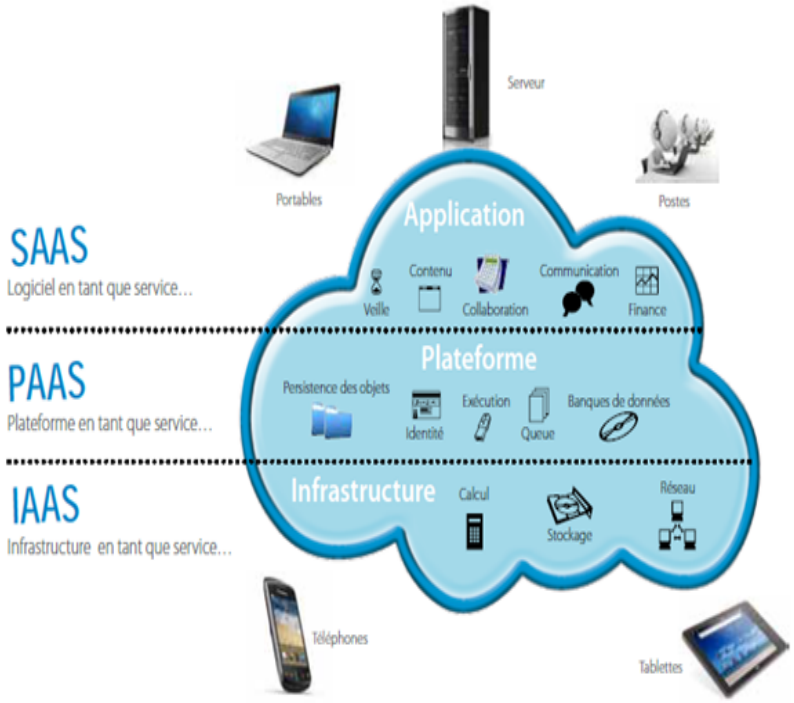

FIG. 1.4 – Les différentes couches du Cloud Computing.

1.8.1 IaaS (Infrastructure as a Service)

C'est un modèle où l'entreprise dispose d'une infrastructure informatique (des capacités de calcul, de stockage et d'une bande passante suffisante) qui se trouve en fait chez le fournisseur. Cette infrastructure est mise à disposition de façon à gérer automatiquement la charge de travail requise par les applications. Cependant, l'entreprise y a accès sans restriction, comme si le matériel se trouvait dans ses locaux. Ceci lui permet de s'affranchir complètement de l'achat et de la gestion du matériel. L'entreprise exploite le matériel comme un service à distance. Cette couche permet à l'entreprise de se concentrer en premier sur ses processus métiers sans se préoccuper du matériel [16].

1.8.2 PaaS (Platform as a Service)

C'est une plateforme d'exécution, de déploiement et de développement des applications. La PaaS regroupe la partie développeur (client) et système (fournisseur) du Cloud Computing. Elle propose des fonctions qui privent le développeur de la gestion des utilisateurs ou des questions de disponibilité par exemple. Le développeur a ainsi uniquement besoin d'héberger son application pour qu'elle soit disponible en SaaS [14].

1.8.3 SaaS (Software as a Service)

C'est la mise à disposition par Internet d'applications informatiques (logiciels) comme un service dans le cadre d'un abonnement, les données sont aussi stockées sur un serveur de l'opérateur SaaS. Il n'y a donc aucun pré requis sur le poste client si ce n'est d'avoir un accès réseau au Cloud (en général Internet). Le déploiement, la maintenance, la supervision du bon fonctionnement de l'application et la sauvegarde des données, sont alors de la responsabilité du fournisseur de services.
C'est en quelque sorte la partie visible du Cloud Computing pour l'utilisateur final, qui n'a plus besoin d'installer l'application sur son poste, et qui accède à son compte par le Web, sur un environnement sécurisé [7].

1.9 Principales applications du Cloud

De nombreuses applications du Cloud ont été proposées .Les principales applications que l'on trouve sur les Clouds sont les suivant [16] :

- La messagerie ;
- Les outils collaboratifs et de web-conferencing ;
- Les environnements de développement et de test ;
- Automatisation de la force de vente et la Business Intelligence ;
- La gestion de la relation client (CRM) ;
- Utilitaires bureautiques ;
- Archivage et sauvegarde de données ;
- Les applications d'ingénierie mathématique (modélisation 3D, simulation, CAO,etc) ;
- Les applications financières (analyse des marchés d'actions, analyses sur le long terme,etc) ;
- Comptabilité (gestion de trésorerie, de facturation,etc) ;
- Ressources humaines (gestion de recrutement, de la paie,etc).

1.10 Acteurs du Cloud Computing

La technologie Cloud a était adoptée par les plus grandes entreprise à travers le monde, vu les avantages qu'elle offre. Les principaux acteurs du Cloud Computing qui se positionnent sont :

1.10.1 Amazon

Amazon est devenu le fournisseur de service Cloud le plus connu dans le monde, grâce à l'ensemble des services Cloud qu'il offre ainsi que les contributions qu'il propose[7]. Parmi les services offerts par Amazon, on trouve :

- **Amazon ElasticCompute Cloud (Amazon EC2) :** Pour le redimensionnement et la configuration dynamique des ressources de calcul.
- **Amazon SimpleDB :** Pour le stockage et l'indexation automatique de données dans le Cloud.
- **Amazon Simple Storage Service (Amazon S3) :** Pour la fourniture d'interface web simple pour la synchronisation des traitements des données stockées par Amazon SimpleDB.
- **Amazon CloudFront :** Pour la livraison et la diffusion distribuées des données à travers le globe en utilisant des points et des sites d'approvisionnement éparpillés un peu partout sur Internet.
- **Amazon Simple Queue Service (Amazon SQS) :** Pour la sauvegarde et le stockage de messages lors de l'acheminement vers leurs destination, afin d'éviter la perte de données, et de faciliter la visualisation de message par tous les intervenant dans la chaine de communication sur le Cloud (clients, développeurs, partenaire d'affaire etc.).

1.10.2 Google

En 2008, Google a lancé son Cloud public orienté pour les services Web offrant une plateforme (PaaS) nommée " Google App Engine " fournit une grande puissance de traitement et une grande capacité de stockage, et permettant l'hébergement d'applications Python ou Java, ainsi que des applications SaaS regroupées dans la gamme " Google App " [18].
Les services App Engine sont les suivants :

- URL Fetch (service de rapatriement d'URL) ;
- Messagerie ;
- Manipulation d'Images ;
- Taches planifiées ;

- Stockage distribué de données (comprend un moteur de recherche et la gestion des transactions).

1.10.3 Microsoft

Microsoft fournit une plate-forme Cloud intitulé Windows Azure. il s'agit d'une offre d'hébergement des applications, de données et de services de stockage, synchronisation des données, bus de messages, contact, etc. [17]. Windows azure offre également un ensemble de services pour :

- La gestion de base de données dans le Cloud, avec SQL-based web service, ce qui permet d'accéder à ces derniers à distance par d'autres partenaires ou par des utilisateurs mobiles ;
- La réutilisation de composants, avec les services .Net, qui offrent un ensemble d'outils pour accélérer le développement et le déploiement d'application dans le Cloud ;
- La fourniture d'un ensemble de kits avec services Live qui représente un centre de documentation d'API et d'échantillonnage pour la mise en route des applications basées Windows azure.

1.10.4 IBM

IBM offre essentiellement un service de consultation et d'aide à l'immigration vers le Cloud, qui permet un suivit complet des clients lors du transfert de leur données et applications vers le Cloud. IBM propose un modèle économique sur lequel se base l'évaluation des coûts d'immigration vers le Cloud, par la suite IBM fournit des conseils métiers qui permettent aux clients de prendre les bonnes décisions quant à la création et l'utilisation de leurs Cloud privé/public. Sur le plan sécurité, IBM propose une architecture unifiée qui vise à ré-architecturer les systèmes traditionnels afin de les adapter aux besoins des clients, notamment pour l'isolement l'authentification, l'accès et la gestion de ressources virtuel dans le Cloud [17].

1.10.5 Salesforce

Salesforce fut le premier hébergeur de Cloud en 1999. La principale application proposée par Salesforce est la CRM (Customer Relationship Management). Il offre aussi des fonctionnalités de marketing, analyse, gestion des ressources humains (GRH), gestion de vente, etc.
Salesforce propose aussi une plateforme pour le développement et le déploiement des ap-

plications de gestion. Ainsi, force.com qui est fournit par Salesforce permet de créer des applications de gestion à la demande [16].

1.10.6 Sun

Sun Microsystem a annoncé en 2009 un service Cloud public ouvert aux développeurs, aux étudiants et à tous ceux qui ne veulent pas dépenser beaucoup d'argent pour se doter d'une infrastructure serveur. Sun Open Cloud est composé de deux services : le Sun Cloud Storage Service et le Sun Cloud Compute Service. Les services offerts sont assez similaires à ceux d'Amazon Web Service[16].

1.11 Avantages du Cloud Computing

Le Cloud Computing présente de nombreux avantages, en voici les plus principaux [11] :

- **Un démarrage rapide :** Le Cloud Computing permet de tester le business plan rapidement, à coûts réduits et avec facilité .
- **L'agilité pour l'entreprise :** Résolution des problèmes de gestion informatique simplement sans avoir à s'engager à long terme .
- **Un développement plus rapide des produits :** Réduction du temps de recherche pour les développeurs sur le paramétrage des applications .
- **Pas de dépenses de capital :** Plus besoin des locaux pour élargir les infrastructures informatiques .
- **Réduction des coûts :** Les utilisateurs ne payent que ce qu'ils consomment. Forte économie en coût et énergie notamment dans les cas de besoins non constants ou linéaires.
- **Mobilité :** Les utilisateurs peuvent à tout moment et à partir de n'importe quel appareil (Ordinateurs, Smartphones, Lap top,etc) avoir accès aux données, applications, serveurs ou plate-forme indépendamment du terminal [19].

1.12 Limites du Cloud Computing

Le Cloud Computing présente les inconvénients (limites) suivantes :

- **Connexion Internet obligatoire :** L'accès aux services du Cloud Computing se fait par le baillet de l'Internet. La rupture de la connexion Internet implique la perte d'accès aux applications et aux données [19].

- **Sécurité des données :** Dans le cas du Cloud Computing, l'entreprise devra connecter ses postes à Internet, et les exposer à un risque d'attaque et d'intrusion, et de vol de données par piratage [19].
- **La bande passante peut faire exploser votre budget :** La bande passante qui serait nécessaire pour stocker les données dans le Cloud est gigantesque, et les coûts seraient tellement importants qu'il est plus avantageux d'acheter le stockage plutôt que de payer quelqu'un d'autre pour s'en charger [19].
- **Stockage de données :** Le stockage physique des données dans le Cloud est effectué par les fournisseurs des services ce qui limite la manipulation de ces dernier par les clients [17].
- **Identification des clients :** Avec l'utilisation croissante du Cloud et l'utilisation multi location de ces ressources, il devient de plus en plus difficile d'identifier par qui et de quel endroit les données ont était modifiées [17].
- **Taille de l'entreprise :** Si votre entreprise est grande alors vos ressources sont grandes, ce qui inclut une grande consommation du Cloud. Vous trouverez peut-être plus d'intérêt à mettre au point votre propre Cloud plutôt que d'en utiliser un externalisé. Les gains sont bien plus importants quand on passe d'une petite consommation de ressources à une consommation plus importante [20].

1.13 Conclusion

Au cours de ce chapitre, nous avons essayé de faire un survol sur les principaux concepts et points clés du Cloud Computing. La naissance du Cloud Computing a donné un nouveau mode de consommation de l'informatique et a changé la manière d'investissement des entreprises dans les infrastructures informatiques. Un coût faible, stockage évolutif illimité et une grande puissance de calcul sont les promesses du Cloud Computing. Tandis que la sécurité est l'une des plus grandes préoccupations des responsables informatiques lorsqu'il est question de Cloud Computing.

Dans le chapitre suivant, nous concentrerons sur la présentation de la sécurité dans le Cloud Computing, qui permet de garantir la confidentialité, l'intégrité, l'authenticité et la disponibilité des informations.

2

La Sécurité dans le Cloud Computing

2.1 Introduction

La sécurité du Cloud est un sous domaine du Cloud Computing en relation avec la sécurité informatique. Elle implique des concepts tels que la sécurité des réseaux, du matériel et les stratégies de contrôle qui sont déployées afin de protéger les données, les applications et l'infrastructure associées au Cloud Computing. Un aspect important du Cloud est la notion d'interconnexion avec divers matériels qui rend difficile et nécessaire la sécurisation de ces environnements.

Dans ce chapitre, nous évoquant la sécurité dans le Cloud Computing. Nous commencerons par les objectifs et services de sécurité, ensuite nous présenterons les problèmes de sécurité dans le cloud ainsi que les différents attaquants. Enfin, nous terminerons avec les différents types d'attaques sur le Cloud Computing et leurs solutions.

2.2 Objectifs et principaux services de la sécurité

La sécurité informatique c'est l'ensemble des moyens mis en œuvre pour réduire la vulnérabilité d'un système contre les menaces accidentelles ou intentionnelles.
Afin d'assurer un transfert de données sécurisé sur les réseaux de communication, un certain nombre de services de sécurité sont requis. La sécurité informatique vise généralement cinq principaux objectifs [21] :

- **Authentification :** Consiste à s'assurer de l'identité d'un utilisateur, c'est-à-dire de garantir à chacun des correspondants que son partenaire est bien celui qu'il croit être. Un contrôle d'accès peut permettre (par exemple par le moyen d'un mot de passe qui devra être crypté) l'accès à des ressources uniquement aux personnes autorisées. Sans l'authentification, un attaquant peut se faire passer par un autre utilisateur pour mener son attaque dans le réseau.
- **Confidentialité :** Est un service qui assure que seules les personnes autorisées aient accès aux ressources échangées.
- **Intégrité :** C'est garantir que les données sont bien celles que l'on croit être. Vérifier l'intégrité des données consiste à déterminer si les données n'ont pas été altérées ou modifiées sans autorisation préalable durant la communication.
- **Disponibilité :** Veille à ce que les services ou les ressources demandées soient disponibles.Elle permet de maintenir le bon fonctionnement du système d'information. L'objectif de la disponibilité est de garantir l'accès à un service ou à des ressources.
- **Non répudiation :** C'est la possibilité de vérifier que l'envoyeur et le destinataire sont bien les parties qui disent avoir respectivement envoyé ou reçu le message. Autrement dit, la non-répudiation de l'origine prouve que les données ont été envoyées, et la non-répudiation de l'arrivée prouve qu'elles ont été reçues.

Ces objectifs de sécurité nécessitent l'emploi de certains mécanismes et services de sécurité à mettre en œuvre. Un mécanisme de sécurité peut être défini comme un processus ou un dispositif, qui vise à détecter, ou empêcher ou se remettre d'une attaque de sécurité. Les mécanismes de sécurité tels que la sténographie, le chiffrement,hachage, etc. sont couramment utilisés pour assurer la sécurité d'unsystème. Un service de sécurité peut être identifié comme un service de traitement ou de communication visant à améliore la sécurité des données et les transferts d'information sur entité. Ces services aident dans la lutte contre les attaques de sécurité. Les services de sécurité emploient habituellement un ou plusieurs mécanismes pour atteindre ses objectifs.

2.3 Problèmes de sécurité dans le Cloud Computing

En ce qui concerne le Cloud, la sécurité est une des premières préoccupations des entreprises qui transfèrent des éléments de leur infrastructure vers le Cloud. Il existe par ailleurs une contradiction, certaines entreprises craignent la perte d'informations capitales (brevet, données clients), les atteintes à leur réputation, les actes malveillants et les interruptions de services. Cependant, les entreprises reconnaissent que le Cloud Computing peut améliorer leur sécurité car les prestataires doivent répondre aux exigences de sécurité et aux obligations réglementaires, tout en garantissant des performances et le respect des contrats de niveau de service(SLA).
L'utilisation fréquente du Cloud Computing fait apparaître plusieurs risques et problèmes de sécurité [22] :

- **Accès :** Dans le domaine du Cloud Computing, les besoins sécuritaires portent aussi sur le contrôle d'accès et la gestion des identités. Il s'agit de mettre en place des contrôles précis afin de filtrer efficacement les personnes autorisées à utiliser les applications de l'entreprise portées dans le Cloud.
- **Disponibilité :** La disponibilité assure l'accès fiable et rapide aux données en nuage ou aux ressources du Cloud Computing par le personnel approprié. La disponibilité garantit que les systèmes fonctionnent correctement en cas de besoin. En outre, ce concept garantit que les services de sécurité du système de Cloud sont en ordre de marche.
- **La charge du réseau :** Dans une stratégie Cloud, on devra être attentif à la disponibilité du réseau et donc des services. Il est donc important pour un DSI (Direction des Systèmes d'Information) de valider avec son fournisseur les engagements de services (SLA) et sa maîtrise des enjeux sécuritaires physique et logique, sa performance et le débit du réseau proposé. Il est nécessaire de renforcer la sécurité du Cloud Computing, éviter l'indisponibilité ou les vols de données et limiter les attaques par déni de service en élargissant le périmètre de sécurité au-delà du centre de données. Une stratégie globale de sécurité Web est à mettre en place.
- **Intégrité :** Le concept de l'intégrité des informations du Cloud exige que les trois principes suivants soient remplis :
  . Les modifications des données ne sont pas faite par le personnel ou des processus non autorisés.
  . Les modifications non autorisées des données ne sont pas faites par le personnel ou processus autorisés.
  . Cohérence des données interne et externe.

- **Sécurité des données :** La sécurité de l'ensemble de données devient un enjeu pour la DSI. Les domaines principaux de la sécurité des données dans le Cloud peuvent se distinguer de la manière suivante :
  . La protection des données contre les failles, les attaques, les pertes, les malveillances.
  . La localisation des données.
  . L'accès aux données.
  Il faut donc sauvegarder, stocker, partager, archiver et sécuriser l'ensemble des données de l'entreprise.
- **Lieu de données :** Le lieu géographique de stockage des données est un point important qui est d'ailleurs d'actualité avec ce que l'on appelle " le Cloud Souverain" et "le Cloud en France". Un contrat de service déterminera les traditionnels aspects juridiques et légaux, et devra spécifier le pays de l'exécution du contrat car chaque pays dispose d'une législation.
- **La séparation des données :** Le Cloud Computing travaille souvent sur le principe de plusieurs baux, de sorte que ses serveurs sont partagés par différents partis avec l'intention de l'hébergement de données et applications. La séparation des données du client devient souvent un défi avec les données d'un parti qui est accessible à partir de l'autre parti. Cela pose de graves défis au maintien de la vie privée du client et souvent conduit à la violation de données sensibles qui peuvent être spécifiques aux clients.

2.4 Classification des attaquants

Avec l'avènement d'Internet, la cybercriminalité est devenue de plus en plus répandue. Les crimes sont commis par de simples adolescents ou par de vrais professionnels :

2.4.1 Les scripts kiddies

La catégorie de pirate le plus commun inclus des adolescents. Cela est souvent en jouant avec des scripts et autres programmes téléchargés depuis Internet et au hasard, ces scripts sont utilisés contre des ciblesaléatoires. Script kiddies sont heureusement plus faciles à détecter. Malgré leur niveau de qualifications faible voire nul, les scripts kiddies sont parfois une menace réelle pour la sécurité des systèmes.D'une part les scripts kiddies sont très nombreux, et d'autre part ils sont souvent obstinés au point de passer parfois plusieurs jours à essayer toutes les combinaisons possibles d'un mot de passe, avec le risque d'y parvenir bien que souvent.

2.4.2 Vrais pirates

Au-delà des scripts kiddies,c'est la catégorie des vrais pirates,qui sont avant tout "des passionnés des réseaux". Ils veulent comprendre le fonctionnement des systèmes informatiques et tester à la fois les capacités des outils et leurs connaissances. Généralement ils ont un niveau relativement élevé de connaissances et de créativité. Les vrais hackers aiment explorer et exploiter les faiblesses de tout type de système de bases de données, serveurs d'applications, serveurs Web, etc. La plupart des hackers affirment s'introduire dans les systèmes par passion pour l'informatique et pas dans l'objectif de détruire ou de voler des données.

2.4.3 La menace interne

La troisième catégorie est représentée par le pirate intérieur. En général c'est des employés ou anciens employés d'une entreprise qui agissent par vengeance personnelle ou dans le cadre de l'espionnage économique. De nombreuses grandes entreprises ont tendance à négliger cette menace. La plupart des systèmes de détection d'intrusions ont été principalement orientés vers la détection d'intrusions par Internet uniquement.

2.4.4 Structures organisées

La quatrième et la dernière catégorie concerne les pirates des gouvernements et les terroristes ou criminelles des organisations. Leurs motivations sont d'ordre économique ou idéologique.

2.5 Classification des attaques

De plus en plus le monde se dirige vers le CloudComputing, il devient plus sophistiqué et augmente ainsi l'intérêt des attaquants à trouver de nouvelles vulnérabilités et exposant. Le Cloud Computing fait face à un certains types d'attaques. Une attaque représente n'importe quelle action qui compromet la sécurité des informations détenues par une organisation ou un individu.
Il existe différentes attaques sur le Cloud Computing dont les plus potentielles sont discutées ci-dessous :

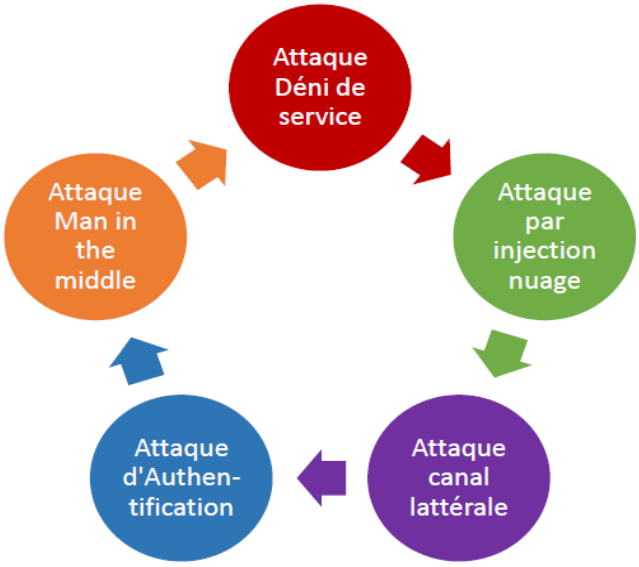

FIG. 2.1 – Types d'attaques dans le Cloud Computing.

2.5.1 Attaque déni de service (DoS Attacks)

principe

C'est un type d'attaque visant à rendre indisponible les services ou ressources d'une organisation pendant un temps indéterminé. Il s'agit la plupart du temps d'attaques à l'encontre des serveurs d'une entreprise, afin qu'ils ne puissent être utilisés et consultés. Les attaques par déni de service sont un fléau pouvant toucher tout serveur d'entreprise ou tout particulier relié à internet. Le but d'une telle attaque n'est pas de récupérer ou d'altérer des données, mais de nuire à la réputation des sociétés ayant une présence sur internet et éventuellement de nuire à leur fonctionnement si leur activité repose sur un système d'information. D'un point de vue technique, ces attaques ne sont pas très compliquées, mais ne sont pas moins efficaces contre tout type de machine possédant un système d'exploitation (Windows, Linux, Unix commercial) ou tout autre système. Certains Cloud Security Alliance a identifié que le nuage est plus vulnérable aux attaques par déni de service, car il est utilisé par de nombreux utilisateurs qui le rend beaucoup plus dommageable. Le principe des attaques par déni de service consiste à envoyer des paquets IP ou des données de taille ou de constitution inhabituelle, afin de provoquer une saturation ou un état instable des machines victimes et de les empêcher ainsi d'assurer les services réseau qu'elles proposent [23, 24].

On distingue habituellement deux types de dénis de service :

- Les dénis de service par saturation, consistant à submerger une machine de requêtes, afin qu'elle ne soit plus capable de répondre aux requêtes réelles ;
- Les dénis de service par exploitation de vulnérabilités, consistant à exploiter une faille du système distant afin de le rendre inutilisable

Solution

Pour limiter l'attaque DoS nous pouvons classer le trafic sur la base de l'autorisation, de sorte que nous pouvons bloquer le trafic qui identifie comme non autorisé et permettre au trafic qui est à identifier comme autorisé. Pour ce pare-feu peut être utilisé pour autoriser ou refuser le trafic sur la base de protocoles d'accès, des ports ou des adresses IP. Aujourd'hui, la plupart des commutateurs ont une capacité de limitation de vitesse sur la base de la liste de contrôle d'accès qui peut fournir le taux de limitation automatique, le trafic de forme, le filtrage IP faux, contraignant et peut profondément inspecter les paquets. Comme pour les commutateurs et routeurs ont aussi une certaine capacité tel queles listes de contrôle d'accès (ACL), et des limitations de vitesse qui peut être réglé manuellement pour créer des règles. Demande de matériel d'extrémité peut être utilisé sur les réseaux en colligation avec les routeurs et les commutateurs qui peuvent analyser les paquets de données dès leur entrée dans le système de réseau pour vérifier leur autorité et leur priorité afin que le flux de la circulation peut être contrôlée. L'attaquant DoS peut envoyer tous le trafic sur paquet attaqué à une interface nulle ou à une interface non existante, ce qui contribue à réduire l'effet des attaques DoS [25, 26].

2.5.2 Attaque par injection nuage (Malware Injection Attacks)

Principe

Dans Malware Attaque, un attaquant tente d'injecter un service malveillant ou une machine virtuelle dans le nuage. Dans ce type d'attaque l'attaquant crée son propre module de mise en œuvre de services malveillants (SaaS ou PaaS) ou une instance de machine virtuelle (IaaS), et essaye de l'ajouter au système Cloud. Ensuite, l'attaquant doit se comporter de manière à en faire un service valide au système Nuage qui est une nouvelle instance de mise enœuvre de services parmi les instances valides. Si l'attaquant parvient, le Cloud redirige automatiquement les demandes d'utilisateur valide à la mise en œuvre de services malveillants, et le code de l'attaquant commence à s'exécuter. Le scénario principal derrière l'attaque par injection Nuage est qu'un attaquant transfère une instance de services malveillants dans les nuages afin qu'il puisse obtenir l'accès aux demandes de service de la victime. Pour ce faire, l'attaquant doit obtenir le contrôle sur les données de la victime dans

le nuage. Selon la classification, cette attaque est le principal représentant de l'exploitation de la surface d'attaque du service du nuage. Le but de cette attaque peut être quelque chose dans lequel un attaquant est intéressé ; il peut comprendre des modifications de données, les modifications de fonctionnalités complètes ou inverser les blocages [25, 27].

Solution

Dans le Cloud Computing l'application du système gérée par le client est considérée avec une grande efficacité et intégrité. Donc, pour éviter l'attaque par injection nuage, nous pouvons combiner l'intégrité avec le matériel ou on peut utiliser le matériel à des fins d'intégrité parce que pour un attaquant, il est difficile d'empiéter dans le niveau IaaS. Pour cela, nous pouvons utiliser un système de table d'allocation de fichiers (FAT). En l'utilisant, nous pouvons déterminer la validité et l'intégrité de nouvelle instance en comparant l'instance actuelle et précédente. A cet effet, nous avons besoin de déployer un hyperviseur du côté du fournisseur. Dans le Cloudl'hyperviseur du système est considéré comme la partie la plus sûre et sophistiquée dont la sécurité ne peut pas être brisée par tous les moyens. L'hyperviseur est responsable de la planification de tous les cas et les services que nous pouvons faire pour vérifier la table d'allocation de fichiers, pour valider et intégrer une instance de client. Une autre approche est que nous pouvons maintenir les informations de la versionde typeplate-forme d'un utilisateur client pour accéder le Clouddans la première phase quand un client ouvre un compte et peut utiliser ces informations pour vérifier la validité de la nouvelle instance du client [28].

2.5.3 Attaque Canal latéral (Side Channel Attacks)

Principe

Un attaquant tente de compromettre le système duCloud en plaçant une machine virtuelle malveillante à proximité d'un système de serveur cible du Cloud, puis lancer une attaque à canal latéral. L'Attaque canal latéral a émergé comme une sorte de menace efficace pour la sécurité ciblant la mise en œuvre du système des algorithmes de cryptographie. Évaluation des systèmes cryptographiques résistant aux attaques canal latéral est donc importante pour la conception de système sécurisé. Attaques à canal latéral utilisent deux étapes :

- **VM CO- Residence et placement :** Un attaquant peut souvent placer son instance sur la même machine physique comme une instance cible.
- **VM Extraction :** La capacité d'un exemple malveillant d'utiliser des canaux latéraux à apprendre des informations sur les cas de co-résident.

Il peut être très facile d'obtenir des informations secrètes à partir d'un périphérique donc la sécurité contre les attaques à canal latéral dans le Cloud Computing devrait être fournie [25].

Solution

Pare-feu virtuel

Le pare-feu est un ensemble de programmes connexes qui protègent les ressources des utilisateurs d'autres réseaux et imposteur. Dans cette approche, le pare-feu virtuel s'exécute dans le serveur du Cloud. Il est possible de détecter les nouvelles machines virtuelles malveillantes dans l'environnement du Cloud Computing. Avec l'aide du serveur de pare-feu virtuel ces types d'attaques peuvent être empêchés dans des environnements du Cloud. L'attaquant tente de placer des machines virtuelles dans des environnements du Cloud. Ce système de pare-feu virtuel bloque ces types de nouveaux emplacements de machines virtuelles malveillantes [29].

Chiffrage et déchiffrage

Les attaques à canal latéral peuvent être évitées dans les environnements du Cloud Computing au moyen de pare-feu virtuels. Cela peut empêcher les attaques à canal latéral dans ces environnements. Afin de fournir une plus grande sécurité pour le Cloud, les données et les informations confidentielles utilisent un chiffrement et déchiffrement. Les données côté client sont cryptées de façon aléatoire qui utilise le concept de confusion et de diffusion. Les différentes clés de sécurité et les différents algorithmes de chiffrement sont utilisées pour chiffrer les données côté de client. Même si les attaques à canal latéral peut se produire il est difficile de décrypter les données de client. Ce qui offre une plus grande sécurité aux environnements Cloud Computing [29, 30].

2.5.4 Attaque d'Authentification (Authentication Attacks)

Principe

Ce type d'attaques peut être facilement produit dans les environnements du Cloud. Les attaquants ciblent facilement les serveurs par ces types d'attaques d'authentification. Les attaquants ciblent le mécanismequi est suivi par l'utilisateur. Le mécanisme utilisé pour l'authentification est capturé et les attaquants tentent d'accéder à des informations confidentielles. Ils utilisent les différents mécanismes de décryptage pour transférer les données plus confidentielles. Le fournisseur de services stocke la valeur clé des utilisateurs et doit être autorisé avant d'accéder à un service [31, 32].

Solution

Ce problème se pose lors de l'utilisation d'un mécanisme d'authentification simple tel qu'un simple nom d'utilisateur et mot de passe. Plusieurs mécanismes d'authentification doivent être établis dans les environnements pour éviter ces types d'attaques [23, 32].

2.5.5 Man-In-The-Middle (Cryptographic Attacks)

Principe

Dans cette attaque l'attaquant intercepte les messages lors d'échange des clés publiques, puis les retransmet, en substituant sa propre clé publique de sorte que les deux parties originales semblent encore communiquer les uns avec les autres. L'expéditeur du message ne reconnaît pas que le récepteur est un attaquant inconnu en essayant d'accéder ou de modifier le message avant de retransmettre au récepteur. Ainsi, l'attaquant contrôle l'ensemble de la communication [33].

Dans une attaque de l'homme au milieu (MITM) voir figure (2.2), une communication entre deux ordinateurs (ici un ordinateur personnel à gauche et un serveur à droite) est interceptée par un tiers, ici MITM. L'ordinateur et le serveur semblent converser ensemble mais tous les messages transitent en fait par MITM, qui peut les lire et se faire passer pour l'une des deux parties.

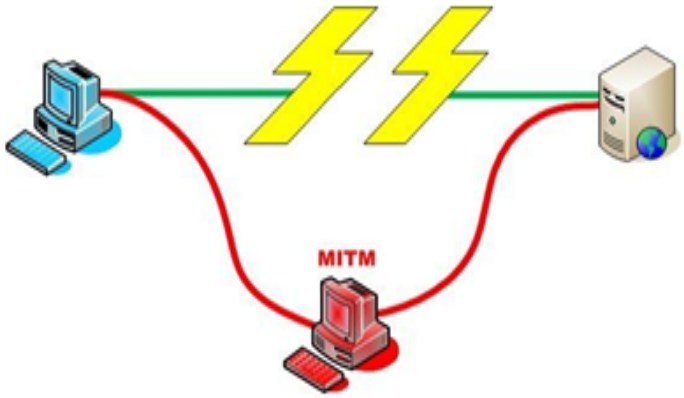

FIG. 2.2 – Attaque Man In The Middle

Solution

Ce type d'attaques est évité par le mécanisme d'authentification approprié. Le cryptage est utilisé pour le côté de l'expéditeur et le déchiffrement est utilisé pour le côté récepteur. Ce dispositif doit être utilisé. L'attaquant ne peut pas modifier les données cryptées. Plusieurs algorithmes de cryptage et de décryptage sont utilisés tel que AES, DES, triple DES, etc. [23].
plusieurs solutions sont utilisées contre MITM qui sont :

- L'utilisation de mot de passe parce qu'un mot de passe à usage unique est à l'abri des attaques MITM.
- L'analyse médico-légale des attaques MITM (adresse IP du serveur, Est-ce que le certificat auto signé ?, Est-ce que d'autres clients, ailleurs sur l'Internet, également obtiennent le même certificat ?, Le certificat est-il signé par une autorité de confiance ?).
- L'authentification mutuelle, avec de nombreuses implémentations client et serveur, la confiance initiale est confirmée seulement par une vérification de chemin entre le client et le serveur. Avec l'authentification mutuelle, le serveur vérifie le client et le client vérifie le serveur pour assurer que les communications légitimes sont échangées. La vérification peut être effectuée en utilisant des clés publiques et privées.

2.6 Conclusion

Les attaques affectent l'environnement duCloudComputing. Elles conduisent à la perte de données et aussi perte financière pour les propriétaires, les fournisseurs et les utilisateurs du Cloud. Les attaques doivent être évitées avant qu'elles se produisent. Pour une utilisation efficace du CloudComputing, nous devons réduire et éviter les attaques de vulnérabilités et d'améliorer la sécurité en appliquant les différentes solutions et techniques d'atténuation appropriées possibles.

Dans le chapitre qui suit nous entamerons le probléme de sécurité dans le Cloud Computing.

3

Sécurité des données dans le Cloud Computing

3.1 Introduction

Le Cloud Computing est devenu incontournable dans la mise en place et la fourniture des services informatiques pour les entreprises. Aujourd'hui, plusieurs entreprises considèrent le Cloud Computing comme une force majeure qui a modifié de façon significative l'ensemble de la technologie d'information, la façon dont les centres de données sont construits, la façon dont les logiciels sont déployés, le traitement des mises à jour ; etc. Il leur permet de remplacer les coûts en capitaux par des coûts variables, de bénéficier d'importantes économies d'échelle, de cesser de deviner la capacité nécessaire, ainsi il offre une vitesse et souplesse accrues. Malgré ces avantages, la sécurité des données reste un sujet d'inquiétude pour les entreprises et représente un frein majeur pour l'adoption de cette technologie.

Pour atténuer le problème de sécurité, nous présentons à travers ce chapitre un état de l'art sur la sécurité des données dans le Cloud Computing en étudiant les différentes solutions proposées dans ce domaine.

3.2 Cycle de vie de la donnée dans le Cloud Computing

Le cycle de vie des données dans le Cloud est décomposable en cinq (5) grandes étapes : Le transfert des données, le stockage des données, l'utilisation, la récupération et la destruction des données [34].

3.2.1 Phase de transit (transfert) des données

Les phases liées à l'envoi des données depuis les systèmes internes d'une entreprise vers le Cloud ou à leur rapatriement sont les plus matures. Oû les données peuvent être chiffrées en internes par l'entreprise et ensuite envoyées, ou alors on utilise une couche de transport intégrant cette fonction de chiffrement. Dans cette seconde catégorie, les protocoles standards qui sont IPSEC (Internet Protocol Security) et SSL (Secure Socket Layer) sont très répandus. En liaison avec une authentification basée sur des clés asymétriques (certificats à clé publique par exemple), ces protocoles permettent de transmettre des données en toute sécurité vers ou depuis le Cloud , ainsi les systèmes deviennent fiables et faciles à utiliser.

3.2.2 Phase de stockage des données

Une fois les données arrivées dans le Cloud, celles-ci sont stockées. En l'absence de standards reconnus, la mise en œuvre des fonctions de chiffrement est dépendante du fournisseur du service. Certains d'entre-eux vont proposer des systèmes dont le fonctionnement n'est peut-être pas toujours très clair. Dans le cas où les données sont déposées dans le Cloud afin d'assurer leur disponibilité, le mieux est de chiffrer les données avant de les envoyer. Cette tâche sera réalisés par le client du Cloud. Evidemment, dans le cas d'un service de type SaaS (Software as a Service) le chiffrement ne pourra être réalisé que par le fournisseur, le client final ayant un rôle quasi inexistant dans cette étape de chiffrement.

3.2.3 Utilisation des données dans le Cloud

Une machine virtuelle (VM) déployée sur un Cloud de type IaaS (Infrastructure as a Service). Cette VM utilise un système de fichier pour stocker le système d'exploitation, les applicatifs et les données des applications. Même si on chiffre le système de fichier, les clefs de déchiffrement doivent être présentes dans la VM pour que celle-ci puisse fonctionner. Un attaquant pourrait donc, s'il arrive à récupérer ces clefs, accéder aux données présentes sur le disque de la VM. Dans ce cas précis, la sécurité des données va reposer sur les mesures de contrôle d'accès mises en place pour accéder aux données, cela tant pour les accès externes que pour les accès des administrateurs et exploitants du Cloud. Avoir confiance en son

fournisseur est donc plus important quand on lui confie des VM, idem pour une application positionnée dans le Cloud (web mail, application de CRM, gestion documentaire, etc.)

3.2.4 La récupération des données

Il est indispensable d'avoir la garantie de disposer des moyens pour la récupération de données en cas de problèmes autres que les cas de non-disponibilité. La récupération doit pouvoir s'effectuer dans des conditions de délais respectant les contraintes exprimées et les besoins métiers. La dissémination des données doit toutefois être effectuée de façon transparente pour l'utilisateur du Cloud.

3.2.5 La destruction des données

Une fois que des données ont été récupérées depuis un Cloud, il est important de s'assurer leur destruction. Il convient de demander quels sont les engagements, moyens et procédures mis en œuvre par un fournisseur pour effacer toute trace de vos données. Dans ce cas, le chiffrement peut être utilisé. En effet, sans la clé pour les déchiffrer, des données préalablement chiffrées sont totalement inutilisables. Donc pour détruire des données, il suffit de détruire la clé de chiffrement. C'est ce concept qui permet de s'assurer que des données sont bien inaccessibles même dans le cas extrême où un fournisseur de Cloud vient de détruire la clé sans prévenir.

3.3 Mesures de protection

A chaque étape de cycle de vie des données, différentes mesures peuvent être mises en œuvre pour assurer la sécurité des données. Les mesures de protection sont de deux types : Le contrôle d'accès et le chiffrement.

3.3.1 Le contrôle d'accès

Contrôler l'accès aux données s'appuie sur des mécanismes d'authentification. Une personne, un système ou un programme doit être fiable (saint) afin de pouvoir accéder aux données. L'ensemble des techniques, systèmes et moyens de contrôle d'accès sont regroupés sous l'acronyme IAM (Identity and Access Management) [34].

3.3.2 Le chiffrement

Grâce à un logiciel spécifique, un individu peut " crypter " ses propres documents. Ainsi, leur accès est limité dans la mesure où il faut avoir la clé de déchiffrement pour pouvoir les

lire. Par conséquent, la personne qui détient la clé est la seule à pouvoir avoir accès aux documents [34].

3.4 Différentes solutions proposées

L'informatique dans les nuages est un nouveau modèle de prestation de service informatique utilisant de nombreuses technologies existantes. Mais, On voit apparaitre aujourd'hui des Cloud spécifiques à des besoins fonctionnels comme le Cloud d'archivage ou le Cloud poste de travail, donc pour chacun d'eux une sécurité adaptée à leurs fonctions est appliquée. Il faut également penser à une approche de sécurité adaptée en fonction du service Cloud comme par exemple l'IaaS avec une gestion de sécurité de l'infrastructure et des identités forte ou encore le PaaS centrée sur l'application et ses données.
Les considérations à prendre en compte pour adopter une solution de sécurité sont donc nombreuses et complexes. Ce qui est sûr, c'est que le Cloud a permis de faire évoluer la sécurité dans des domaines multiples comme l'évolution de la gestion des logs, la fédération d'identité et le multiple login.
La sécurité est souvent considérée comme le frein principal à l'adoption des services du Cloud Computing. C'est ainsi que de nombreux travaux ont été consacrés à la recherche de solutions pour remédier à ce problème.
Nous présentons dans cette partie les principaux travaux de recherche qui ont proposé des solutions pour assurer la sécurité de données dans les nuages.

3.4.1 Sécurité des accès et du stockage de données dans le Cloud

Jensen et al ont énumérés les différentes techniques utilisées dans le Cloud Computing pour sécuriser les accès aux données et ils ont dégagé les lacunes de ces techniques pour mettre en œuvre leur solution qui est basée sur le protocole TLS (Transport Layer Security) et la cryptographie XML (Extensible Markup Language) [35]. Cette solution vient répondre au problème de navigateur web qui présente des lacunes au niveau sécurité. L'idée proposée consiste à utiliser le protocole TLS et à adapter le navigateur en intégrant la cryptographie XML. Cependant Wang et al ont proposés une solution qui se base sur le code erasure-correcting afin de permettre la redondance et garantir la fiabilité des données [36]. Ils ont utilisé le jeton homomorphique pour l'exactitude du stockage et pour localiser les erreurs. La solution proposée est capable de détecter la corruption des données lors du stockage, elle peut garantir la localisation des données erronées et identifier le serveur qui a un mauvais comportement [36].
Danwei et Yanjun ont proposés un algorithme de sécurité qui assure la restauration des données en cas d'échec de certains serveurs. Il s'agit d'un algorithme de séparation de don-

nées [37]. Cet algorithme n'est qu'une extension du théorème fondamental de K équation en algèbre, l'algorithme du partage de la clé secrète de Shamir qui est un algorithme de cryptographie basé sur le partage du secret (nombre aléatoire), l'algorithme de stockage de données en ligne d'Abhishek [38] et la théorie du nombre. L'idée est de partager la donnée d en k parties d= d1, d2, d3 ;jusqu'a dk. Ce partage est fait à l'aide de l'algorithme de séparation de données pour les stocker ultérieurement sur des serveurs choisis aléatoirement noté S= s1, s2, s3 jusqu'a,Sm avec m>k. Le processus de stockage de données dans les nuages se fait donc sur deux étapes, la première consiste à diviser et stocker les données sur un serveur choisi arbitrairement et la deuxième consiste à pouvoir restituer ces données. A travers ces processus , les données sont prêtes à être transférées, stockées, traitées, en toute sécurité puisqu'elles sont cryptées. Les chercheurs ont déduit que la complexité temporelle de l'algorithme est la même pour générer k bloc de données et pour la restauration des données. Ils ont prouvé que même si un attaquant envahit un nœud de stockage, vole un bloc de données et essaie de rétablir la série de données, la complexité temporelle nécessaire pour faire les traitements ne peut pas être supportée par les environnements informatiques actuels. Parmi les autres avantages qui distinguent cette proposition on trouve la capacité de restaurer les données même si un ou plusieurs nœuds de stockage ne sont pas disponibles ce qui ne peut pas être le cas avec une solution traditionnelle de cryptographie.

3.4.2 Sécurité logique de l'informatique dans le Cloud

Dans les nuages IAAS (Infrastructure as a service), les utilisateurs ont accès aux machines virtuels (VM) sur lesquels ils peuvent installer et exécuter leurs logiciels. Ces machines virtuelles sont créées et gérées par un moniteur de machine virtuel (VMM) qui est une couche logicielle entre la machine physique et le système d'exploitation. Le VMM contrôle les ressources de la machine physique et crée plusieurs machines virtuelles qui partagent ces ressources.

Les machines virtuelles ont des systèmes d'exploitation indépendants exécutant des applications indépendantes et sont isolées les unes des autres par le VMM. Ce type de dispositif a provoqué beaucoup de problèmes de vulnérabilité de la machine virtuelle ce qui a poussé les auteurs à travailler dans ce domaine pour trouver des solutions efficaces. Zhou et al. ont proposés une solution pour éliminer la vulnérabilité de la machine virtuelle [39]. La découverte des limites de l'hyperviseur XEN utilisé par AMAZON était leur point de départ. Ils ont proposés quatre approches pour améliorer la performance de cet hyperviseur qui sont basées sur la loi de Poisson, la loi de Bernoulli, la loi uniforme et enfin la loi exacte. Après une comparaison entre les quatre nouveaux modèles, ils ont déduit que la stratégie basée sur la loi de Poisson est la meilleure dans la pratique pour empêcher le vol de cycle. Wei et al. [40] ont proposés un système de gestion des images de la machine virtuelle qui contrôle

l'accès et la provenance de ces images à travers des filtres et des scanners qui permettent de détecter et réparer les violations en utilisant les techniques de fouille de données, ce système s'appelle Mirage. S. Berger et al. ont aussi développés une technologie qui réponds aux problèmes rencontrés par la machine virtuelle. Cette technologie est appelée Trusted Virtual Data Center (TVDc) [41], elle assure que les charges de travail ne peuvent être facturées qu'au client qui ont bénéficié du service. Elle assure aussi dans le cas de certains programmes malveillants comme les virus qu'ils ne peuvent pas se propager et elle permet également de prévenir les problèmes de mauvaise configuration. La TVDc utilise la politique d'isolement qui se base sur la séparation des ressources matérielles utilisées par les clients .Elle gère le centre de données, l'accès aux machines virtuelles et le passage d'une machine virtuelle à une autre.

3.4.3 Modèle de sécurité des données proposées dans le Cloud

L'approche en couches est présentée dans la figure (3.1) où la première couche est responsable de l'authentification de l'utilisateur. La deuxième couche est responsable de l'anonymisation des données et de la protection de la vie privée des utilisateurs et la troisième couche est responsable de la récupération des données et du déchiffrement [42, 43].

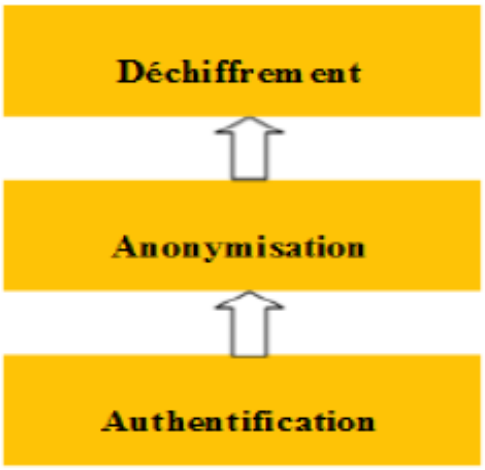

FIG. 3.1 – Modèle de sécurité de données dans le Cloud [42].

3.4.4 Mécanisme OTP

Mécanisme one time password (OTP) ou le mot de passe à usage unique est un mot de passe qui n'est valable que pour une session ou une transaction. L'utilisation d'une authentification multi facteur avec OTP réduit les risques associés avec la connexion au système

depuis un poste de travail non sécurisé [44]. OTP est comme un système de validation qui fournit une couche supplémentaire de sécurité pour les données et les informations sensibles en demandant un mot de passe qui est uniquement valable pour une seule connexion. De plus, ce mot de passe n'est plus choisi par l'utilisateur, mais généré automatiquement par une méthode de précalculé, ce qui va éliminer certaines lacunes associées aux mots de passe statiques telles que les lacunes de longévité du mot de passe, de simplicité du mot de passe et d'attaque par force brute. OTPs sont générés du côté du serveur et envoyés à l'utilisateur en utilisant un canal de télécommunication. Ils ne sont pas susceptible aux utilisateurs malveillants de trouver le nom d'utilisateur et mot de passe pour accéder à la ressource. On ne peut rien faire pour obtenir dans le cloud sans la bonne combinaison de nom d'utilisateur, le mot de passe et le mot de passe à usage unique. Afin de sécuriser le système d'une manière plus efficace, l'OTP généré doit être difficile à estimer, retrouver, ou tracer par les pirates. Par conséquent, il est très important de développer des algorithmes de génération d'OTP sécurisé [45]. Plusieurs éléments peuvent être utilisés pour générer un mot de passe à usage unique difficile à deviner [46], à savoir, International Mobile Equipment Identity (IMEI), International Mobile Subscriber Identity (IMSI), nom d'utilisateur, PIN, minute, heure, etc.

3.4.5 Techniques de chiffrements

Des recherches actuelles permettront sans doute d'utiliser des données cryptées avec des applications dans le Cloud. En effet, aujourd'hui, les données doivent être en clair pour pouvoir être utilisée par des applications sur le Cloud. Si les données sont chiffrées, le résultat sera lui aussi chiffré (exemple d'une requête SQL qui retournera un résultat chiffré) [47]. L'utilisation d'une clé n'est pas possible ici, car sinon, elle sera publiée sur Internet (Figure 3.2).

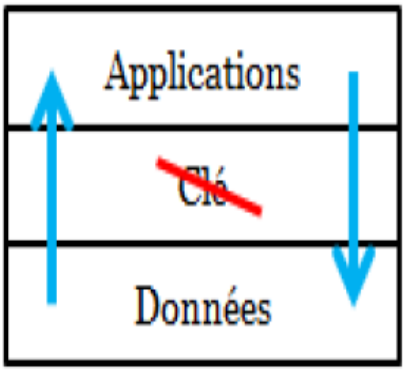

FIG. 3.2 – Principe de chiffrement sans clé [47].

On peut stocker ou archiver des données cryptées, mais une application cloud ne peut pas travailler sur des données cryptées. Les recherches pour remédier à ce problème ont mené à essayer de mettre en place une solution pour utiliser des données cryptées malgré tout (les recherches de Craig Gentry). La méthode consiste à mettre en place un algorithme totalement homomorphique [36]. Ce dernier fonctionne pour des opérations d'additions. Les plus avancées dans ces recherches sont les chercheurs de l'ENS Lyon, et une partie de leur travail va aussi consister à améliorer la complexité de l'algorithme qui est un réel problème lorsque la clé devient très grande. Ces recherches pourraient constituer l'avenir de la sécurité du cloud computing.

FIG. 3.3 – Fonctionnement du Cloud sur des données chiffrées sans clé de sécurité [47].

On peut donc voir que l'algorithme d'analyse va pouvoir donner la possibilité aux applications de travailler sur les données chiffrées (Figure 3.3).

3.4.6 Approches pour la sécurité des données dans le Cloud

La protection de la vie privée et la sécurité des données sont primordiales dans l'utilisation des services Cloud. Il existe plusieurs travaux réalisés dans ce domaine. Des modèles, des approches et des techniques sont proposées afin de protéger les données.
Dans [48], Singh et Singh ont proposés un système d'authentification à plusieurs niveaux visant à renforcer la sécurité dans les transactions financières. Dans [49], Satish et Anita ont proposés une méthode de faux écran pour assurer l'authentification à deux niveaux dans le Cloud Computing. Dans [50], Tandis et al. ont proposés une méthode utilisant le code d'authentification de message dans laquelle la clé cryptographique, le message et la fonction de hachage sont concaténés ensemble pour assurer l'authentification. Dans [51], Parsi

et Sudha ont proposés une méthode utilisant l'algorithme RSA(Rivest Shamir and Adleman) pour l'authentification et le transfert sécurisé de données. Cette méthode implique une phase de génération de clé, le chiffrement et le déchiffrement. Dans [52], l'auteur a proposé une technique de sécurité de données dans le Cloud par la combinaison des mécanismes différents à savoir, l'authentification multi-facteur par un mot de passe à usage unique et le code d'authentification d'une empreinte cryptographique de message avec une clé. Dans [53], le concept de signature numérique avec l'algorithme RSA a été proposé pour crypter les données avant de les transmettre sur le réseau. Cette technique permet de résoudre le problème de l'authentification et de la sécurité en utilisant les techniques d'anonymisation. Dans [54], Balasaraswathi et Manikandan ont proposés une architecture de Cloud multiple basée sur le partitionnement de données chiffrées avec une approche dynamique afin de sécuriser l'information en transit ou stockée.
Nous avons analysé plusieurs approches de transfert sécurisé de données, ces approches se focalisent principalement sur les paramètres d'authentification. En effet, les données en transit vers le Cloud peuvent être attaquées par différents intercepteurs non autorisés. Une méthode particulière ne suffit pas à traiter toutes les questions de sécurité et de confidentialité des données. Par conséquent, différentes techniques et mécanismes intégrés devraient être utilisés.

3.4.7 Les autres approches

On voit apparaitre aujourd'hui des Cloud spécifiques à des besoins fonctionnels comme le Cloud d'archivage ou le Cloud poste de travail, donc pour chacun une sécurité adaptée à leurs fonctions. Il faut donc penser à une approche de sécurité adaptée en fonction du service cloud également comme par exemple l'IaaS avec une gestion de sécurité de l'infrastructure et des identités forte ou encore le PaaS centrée sur l'application et ses données.
Les considérations à prendre en compte pour adopter une solution de sécurité sont donc nombreuses et complexes. Ce qui est sûr, c'est que le Cloud a permis de faire évoluer la sécurité dans des domaines multiples comme l'évolution de la gestion des logs, la " fédération d'identité " et le " multiple login ".

3.5 Discussion

Nous avons présenté dans la partie précédente quelques travaux qui proposent de résoudre les problèmes liés à la sécurité dans le cloud computing. Quelques approches semblent être pertinentes et assurent un niveau de sécurité acceptable mais qui reste insuffisant. En plus, ces travaux ont mis en évidence de nouveaux problèmes : Danwei et Yanjun ont relevés la redondance des données [55]. Mais ça n'empêche pas que l'idée proposée par ces cher-

cheurs est très faible pour sécuriser le transfert des données à travers le réseau et élimine le problème de non disponibilité du service en cas de panne de l'un des serveurs. Jensen et al. ont proposés d'utiliser le protocole TLS et adapter le navigateur en intégrant la cryptographie XML. Une telle proposition n'est pas suffisante pour assurer la sécurité du transfert sur les réseaux puisqu'elle est basée sur une technologie dont ses faiblesses sont bien connues. On ce qui concerne l'idée proposée par Wang et ces collaborateurs [36], elle est basée sur le chiffrement homomorphique qui est la réponse à la question de confidentialité des données lors de transfert et lors de traitement dans le Cloud. Néanmoins, le laboratoire de recherche en cryptographie dans le Cloud de Microsoft a annoncé que cette nouvelle façons de chiffrer les données n'en est encore qu'à ces débuts et qu'ils sont loin de pouvoir l'exécuter sur les machines virtuelles des données cryptées avec le chiffrement homomorphique.
Généralement les solutions existantes pour sécuriser le transfert et les traitements des données sont basées sur la cryptographie des données qui n'est pas toujours une solution complète pour protéger les données, en plus le mécanisme de cryptage et de décryptage des données peut être intensive sur les processeurs ce qui engendre un gaspillage des ressources une chose que les fournisseurs des nuages ne veulent pas.

3.6 Conclusion

Le Cloud Computing est une technologie très prometteuse permettant à ses clients de réduire les coûts d'exploitation, d'administration etc. Tout en augmentant l'efficacité, toutefois, l'adoption de cette technologie reste faible, et cela revient aux problèmes de sécurité en particulier la sécurité des données échangées sur le réseau internet. Afin de résoudre ces problèmes et d'améliorer l'adoption et l'utilisation de cette technologie, nous avons étudiéles aspects de sécurité des données du Cloud, ensuite nous avons présenté les différentes solutions existantes.

Dans le prochain chapitre nous présenterons notre solution ainsi que la mise en pratique de cette derniére.

4

Proposition et validation de la solution apportée basée sur le chiffrement

4.1 Introduction

L'objectif du Cloud Computing est d'offrir de manière transparente des ressources informatiques à ses clients. Le Cloud doit être fiable sécurisé et performant c'est pour cela que l'ère du Cloud oblige les entreprises de toute nature et de n'importe quelle taille à protéger leur patrimoine informationnel critique de manière plus réactive. Fournissant des informations de sécurité exploitables, c'est dans ce contexte que nous apportons notre collaboration afin d'améliorer le service de sécurité des données et des ressources du Cloud.

Nous consacrons ce chapitre à la présentation de notre solution qui est basée principalement sur le chiffrement, au choix de l'idée sur laquelle elle s'appuie ainsi qu'à son fonctionnement illustré par un diagramme. Enfin nous allons terminer par une phase de validation de la solution présentée.

4.2 Problématique

Le Cloud Computing est un modèle permettant de favoriser un accès ubiquitaire, commode et sur demande à un ensemble partagé de ressources informatiques configurables (des réseaux, serveurs, ressources de stockage et logiciels) pouvant être déployées rapidement avec un minimum de gestion ou d'intervention de la part du prestataire de service. L'accès aux données hébergées dans le Cloud est exposé à des risques de perte, de modification et d'altération. Pour remédier à ces risques des mécanismes de sécurité sont déployés à savoir les mécanismes d'authentification qui sont mis en place par les fournisseurs de service.
Cependant, Les entreprises clientes doivent considérer les points suivants :

- Les types d'informations qui sont accessibles dans le Cloud et qui peut y accéder et comment sont-elles isolées des éléments non sécurisés.
- Les droits pour l'envoie et la réception des données sensibles en dehors du périmètre de l'entreprise.
- Les mécanismes de sécurité qui garantissent la confidentialité des données de l'entreprise au sein du cloud public
- L'envoie des données sensibles et l'accès aux données.

4.3 Objectifs

Vu les problèmes de sécurité des données dans le Cloud Computing, notre travail s'articule autour des objectifs suivants :

- Protéger les données de toute perte.
- Récupérer les données en toute sécurité.

Notre objectif est le développement d'une application qui permet de résoudre les problèmes liés à la sécurité des données et de détecter si les données ont été altérées ou non.

4.4 Description du fonctionnement de la proposition

Afin de protéger les données partagées dans l'environnement du Cloud Computing contre les tentatives d'accès non autorisé et les risques de perte, de modification et d'altération, nous proposons une solution (application) basée sur le chiffrement et la reconstitution (déchiffrement) des données.

Notre solution est composée des étapes suivantes (voir figure 4.1) :

- **Authentification :** L'accès au Cloud se fait par authentification, l'utilisateur demande l'accès au Cloud en insérant le mot de passe et le login. Cette phase se fait lors de la connexion au Cloud et elle est effectuée par le Cloud server provider.
- **Chiffrement de la donnée :** Une fois que le client du Cloud a été authentifié, la donnée est décomposée en N blocs d'informations de taille prédéfinie par le Cloud server provider et le client, après qu'une réorganisation de ces données est effectuée de tel sorte que les cases de même niveau dans chaque bloc sont regroupées et placées dans un autre bloc (les premiére cases des N blocs forment un nouveau bloc, et même principe pour les deuxiémes cases des N blocs et ainsi de suite).
- **Reconstitution de la donnée :** Après avoir transféré la donnée, la reconstitution de cette dernière est obligatoire en appliquant l'inverse du chiffrement. Une fois la réception des blocs de données est effectuées, leur réorganisation est entamée pour la reconstitution des N blocs de données ; de tel sorte que pour former le premier bloc des N blocs, les premiéres cases de chaque blocs recus sont regroupées ensemble dans le même bloc et ainsi de suite jusqu'à en arriver a former les N blocs. La donnée transférée est reconstituée en regroupant les données des N blocs.
- **Vérification de la donnée :** Cette étape permet de détecter si la donnée a été altérée ou non, en comparant la donnée récupérée (reconstituée) à celle envoyée.

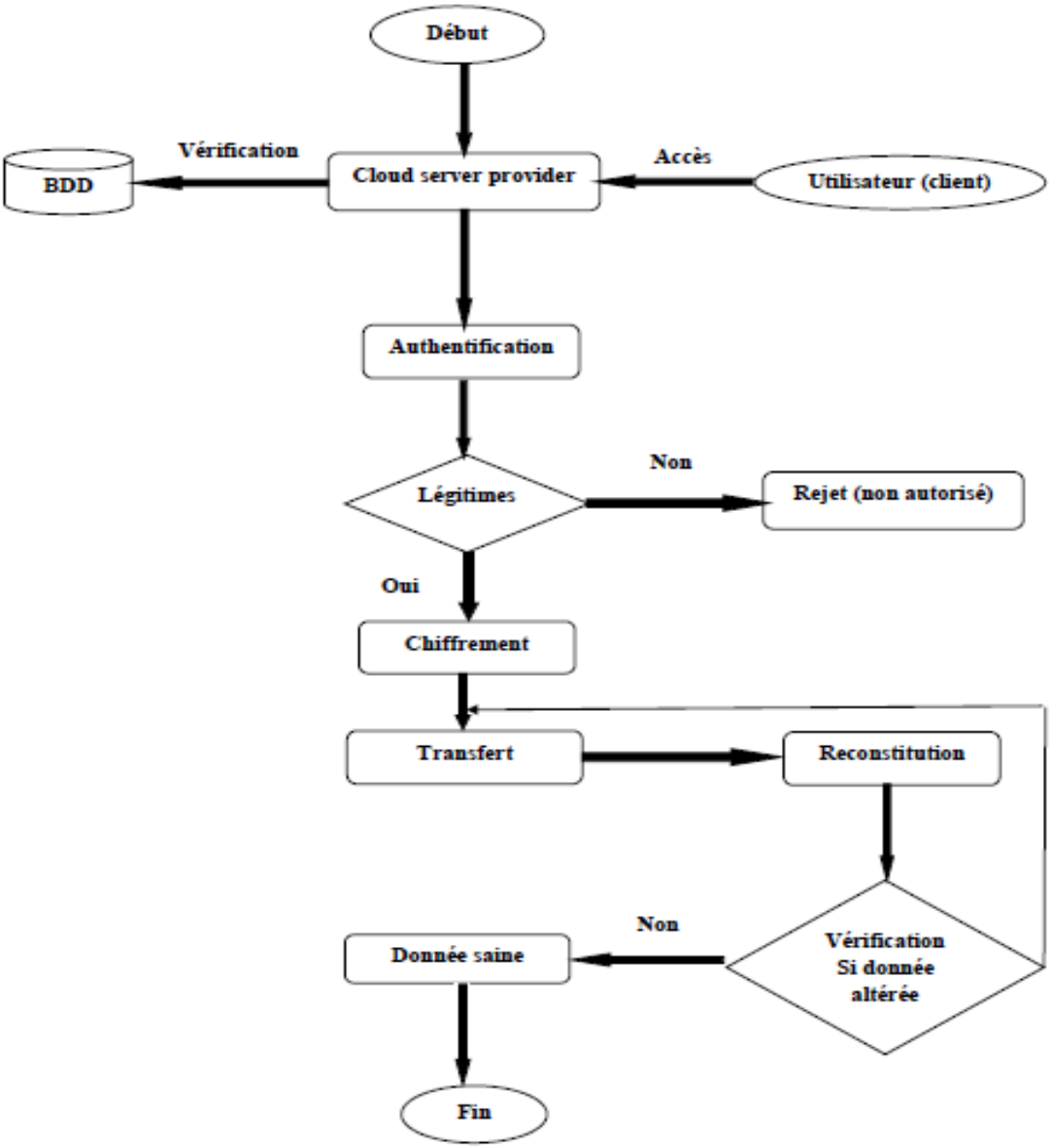

FIG. 4.1 – Diagramme de fonctionnement de la solution proposée.

4.5 Réalisation de la solution proposée

4.5.1 Environnement de développement

Environnement logiciel

Nous avons implementé notre solution en langage Java avec l'outil de développement NetBeans pour coder le programme.

Langage de programmation Java

Java est à la fois un langage de programmation informatique orienté objet et un environnement d'exécution informatique portable, développé par Sun Microsystems. Il permet de créer des logiciels compatibles avec de nombreux systèmes d'exploitation (Windows, Linux, Macintosh, Solaris). Java donne aussi la possibilité de développer des programmes pour téléphones portables et assistants personnels. Enfin, ce langage peut être utilisé sur internet pour des petites applications intégrées à la page web ou encore comme langage serveur.

NetBeans environnement de développement

NetBeans est l'environnement de Développement Intégré (EDI) supporté par SUN. Il est particulièrement bien adapté pour le développement d'applications WEB. Il remplace l'IDE Java Studio Creator. C'est un IDE moderne offrant un éditeur avec des codes couleurs et un ensemble de signes, des modèles de projets multi-langage et de différents types (application indépendante, distribuée, plugin, mobiles,etc), le refactoring, l'éditeur graphique d'interfaces et de pages web pour supporter le programmeur dans son travail. Il permet d'accéder rapidement à la documentation détaillée, de naviguer dans les sources et de faire des recherches d'usage des classes, méthodes et propriétés. NetBeans indique à l'utilisateur les erreurs et fait des propositions pour y remédier.

4.6 La mise en œuvre de la solution

Dans cette partie, nous allons présenter les interfaces de notre réalisation.

4.6.1 Interface client pour la réception des données

La figure suivante (figure 4.2) représente l'interface client aprés avoir reçu la donnée.

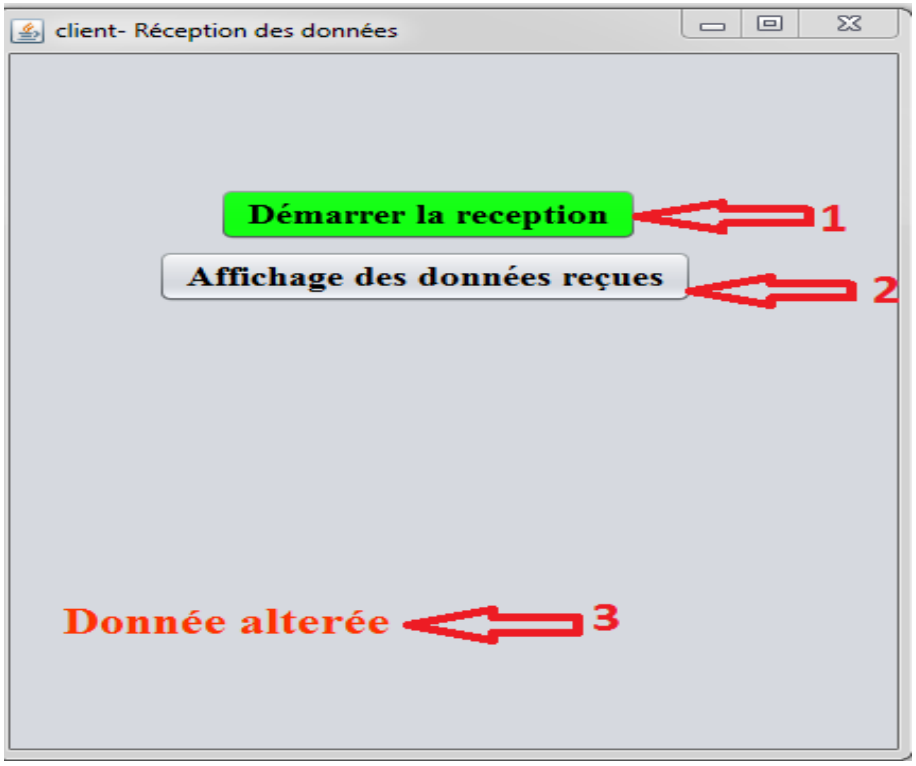

FIG. 4.2 – L'interface du client-Réception des données.

1. Le client demande des données du Cloud en démarrant la réception des données.
2. Bouton pour l'affichage des données recues :
   -Vérifier si la donnée a été altéré, cette étape se fait automatiquement.
   -Afficher un message "donnée altérée" si la donnée a été altéré, "donnée non altérée" sinon (illustré par 3).

4.6.2 Interface envoie des données

La figure suivante (figure 4.3) représente l'interface de l'envoie des données au niveau du Cloud server provider.

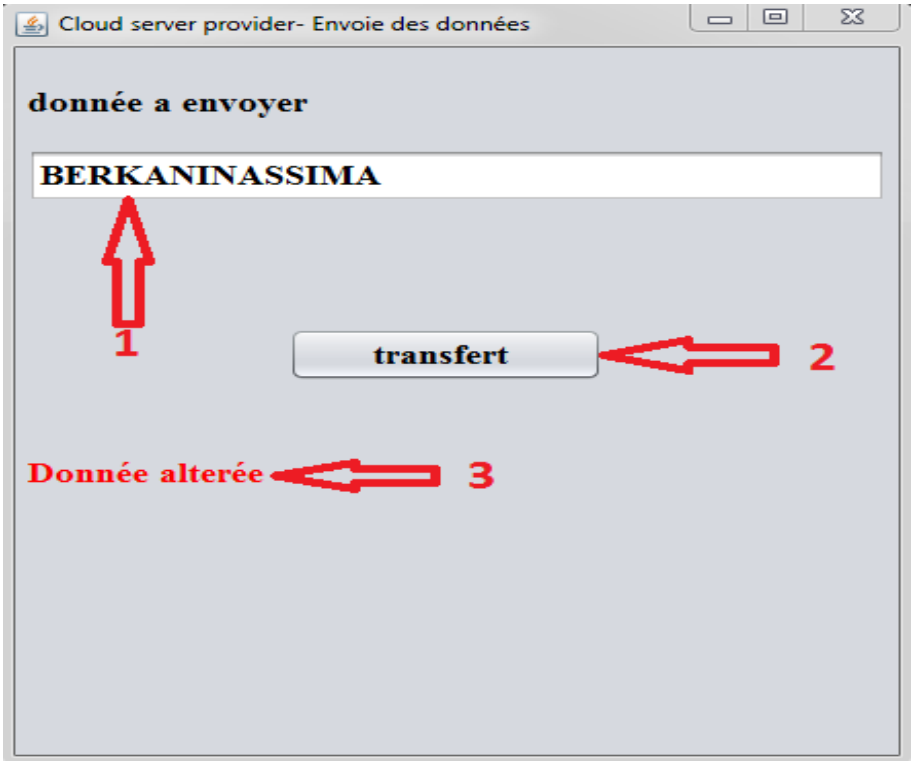

FIG. 4.3 – l'interface du Cloud server provider-envoie des données.

1. Donnée à envoyer au client.
2. Envoie de la donnée.
3. Affichage d'un message : "donnée altérée" si la donnée reçue par le client a été altérée, "donnée non altérée" sinon.

4.7 Conclusion

Ce chapitre a été consacré à la présentation et la validation de notre solution afin de remédier au problème de sécurité des données dans le Cloud Computing. Nous avons également illustré un diagramme représentant les étapes de la solution proposée ainsi que la mise en œuvre de la solution proposée.

Conclusion générale et Perspectives

Le Cloud Computing est un nouveau concept de déploiement de systèmes informatique, il offre beaucoup d'avantages en termes de puissance de calcul, de temps de réponse et de réduction des coûts. Les utilisateurs peuvent bénéficier pleinement des services Cloud qui permettent de satisfaire leurs besoins à la demande. Toutefois, comme chaque avancée technologique, externaliser ses ressources informatiques apporte aussi sa part de risques, notamment en termes de sécurité des données, car si l'utilisateur ne peut pas avoir ses propres ressources de manière sécurisée, à tout moment et à partir de n'importe quel emplacement géographique, alors l'efficacité, les avantages et même la définition du Cloud Computing seront mis en péril. On observera alors une baisse d'adoption du Cloud voir même une perte des clients.

Dans ce mémoire, nous avons essayé de développé une application basée sur le chiffrement qui permet de détecter si les données ont été altérées ou non.
La principale motivation qui a régi ce travail est la proposition d'une approche basée sur le chiffrement afin de protéger les données contre les tentatives d'accès non autorisé et les risques de perte, de modification et d'altération.

Sur la base du travail réalisé nous dressons les perspectives suivantes :
-Il serait intéressant de simuler la proposition sur un environnement Cloud Computing réel pour vérifier nos résultats envisagés et pour avoir de meilleures performances.
-Il parait important de comparer notre approche avec d'autres approches.

Bibliographie

[1] J. McCarthy, Informatique utilitaire : http ://computinginthe-cloud.wordpress.com/2008/09/25/ utility-cloud computingflashback-to-1961-prof-john-mccarthy/ (accédé Juin 2016).

[2] P. Mell, T. Grance, The NIST Definition of Cloud Computing, Recommendation of NIST. Special Publication 800-145, 2011. http ://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

[3] J-F Pépin, S. Bouteiller, A-S. Boissard, J. Watrinel, Fondamentaux du Cloud computing- le point de vue des grandes entreprise. Réseau de Grandes Entreprises (CIGREF). Mars 2013. http ://www.eurocloud.fr/doc/cigref2.pdf

[4] AE. Youssef, Exploring Cloud Computing Services and Applications, Journal of Emerging Trends in Computing and Information Sciences, Vol. 3, No. 6, 2012.

[5] N. Degroodt. L'élasticité des bases de données sur le cloud computing. Mémoire de master en sciences informatiques. Université libre de bruxelles. Université d'Europe, 2010.

[6] B. AZRIA, J. CHERKI, L'impact du Cloud Computing dans les PME, mémoire, Ecole supérieure de génie informatique ESGI, 2014.

[7] S.Lanani. Une approche BPM (Business Process Managment) par composition d'applications dans le cloud computing. Mémoire de magister, Université Mohamed Khider de Biskra, 2015.

[8] http ://whatiscloud.com/cloud_characteristics/multi_tenancy

[9] D. Yuanshun, X. Yanping, Z.Gewei. Self-healing and Hybrid Diagnosis in Cloud Computing. Proceedings CloudCom of 1st International Conference on Cloud Computing. Beijing, China, pp. 45-56, 2009.

[10] R. Buyya, S.k. Garg, R.N.Calheiros. SLA-oriented resource provisioning for cloud computing : Challenges, architecture, and solutions. Proceedings of the International Conference on Cloud and Service Computing (CSC),Hong Kong, China,pp. 1-10, 2011.

[11] I. Laribi. La mise en place de la solution Openstack, Université de Tlemcen, 2014.

[12] L.F. NOUMSI. Etude et mise en place d'une solution "cloud computing " privée dans une entreprise moderne : cas de CAMTEL. Ecole nationale supérieure des postes et télécommunications, 2012.

[13] J.B. Baraban. Private cloud, public cloud et hybrid cloud, 2010 My saas. http : //mysaas.fr/2010/10/04/private-Cloud-publique-Cloud-et-hybrid-Cloud/.

[14] A.A.Y. Elwessabi. Une approche basée agent mobile pour le cloud computing. Mémoire de magister. Université HADJ LAKHDAR - BATNA, 2014.

[15] P.P. Codo. Conception d'Une Solution de Cloud Computing Privé Basée sur un Algorithme de Supervision Distribué : Application aux Services IAAS. Ecole Polytechnique d'Abomey-Calavi (EPAC), 2012.

[16] F. Liu, J. Tong, J. Mao, R. Bohn, J. Messina, L. Badger and D, NIST SP 500-292, NIST Cloud Computing Reference Architecture ?, Leaf, 2011.

[17] H. Saouli. Découverte de services web via le Cloud computing à base d'agents mobiles. Thèse de doctorat. Université Mohamed Khider de Biskra, 2015.

[18] A.Prunier. Le Cloud Computing : Réelle révolution ou simple évolution. Wygwan bureau d'expertise technologique. pp. 62, 2011.

[19] http ://www.renaudvenet.com/cloud-computing-avantages-et-inconvenients-2011-01-26.html

[20] K. Maioua, A. Mansouri. Approche basée Agents Mobiles intelligents dans un environnement de cloud Computing. Mémoire de master. Université Kasdi Merbah Ouargla, 2014.

[21] Y. Lescopy. La sécurité informatique. Post BTS R2i. vol. 1, no. 6, 2002.

[22] S.N. Dhage, B.B. Meshram, Intrusion detection system in cloud computing environment. Int. J. Cloud Computing. vol. 1, no. 2/3, 2012.

[23] T.K. Subramaniam, B. Deepa. Security attack issues and mitigation techniques in cloud computing environments. International Journal of Ubicomp (IJU. Vol.7, No.1, Janvier 2016. http ://aircconline.com/iju/V7N1/7116iju01.pdf

[24] A. M. Lonea, D. E. Popescu, H. Tianfield. Detecting ddos attacks in cloud computing environment, International Journal of Computers. Communications & Control, vol. 8, no. 1, 2013.

[25] P. Chouhan, R. Singh. Security attacks on cloud computing with possible solution. International Journal of Advanced Research in Computer Science and Software Engineering. Vol. 6, Issue 1, Janvier 2016 ISSN : 2277 128X. http ://ijarcsse.com/docs/papers/Volume_6/01_January2016/V6I1-0140.pdf

[26] M. H. Sqalli, F. Al-Haidari, K. Salah. Edos-shield-a two-steps mitigation technique against edos attacks in cloud computing. in Utility and Cloud Computing (UCC). 2011 Fourth IEEE International Conference, pp. 49-56, IEEE, 2011.

[27] S. Qaisar, K. F. Khawaja. Cloud computing : network/security threats and counter measures. Interdisciplinary Journal of Contemporary Research in Business. Vol. 3, No. 9, Janvier http ://www.journal-archieves14.webs.com/1323-1329.pdf

[28] K. Zunnurhain, S. Vrbsky. Security attacks and solutions in clouds. In Proceedings of the 1st international conference on cloud computing. pp. 145-156, Citeseer, 2010.

[29] B. Sevak. Security against side channel attack in cloud computing. International Journal of Engineering and Advanced Technology (IJEAT. vol. 2, no. 2, pp. 183, 2013.

[30] Q.Luo, Y.Fei. Algorithmic collision analysis for evaluating cryptographic systems and side channel attacks. In : Hardware-Oriented Security and Trust (HOST). IEEE International Symposium, pp. 75-80, 2011.

[31] S.Subashini, V.Kavitha. A survey on Security issues in service delivery models of Cloud Computing. J Netw Comput Appl. vol. 1, no. 1, pp. 34, 2011.

[32] W.Li, L.Ping. Trust model to enhance Security and interoperability of Cloud environment. In : Proceedings of the 1st International conference on Cloud Computing. Springer Berlin Heidelberg, Beijing, China, pp. 69-79, 2009.

[33] M.K. Stine, R. Kissel. Guide for mapping types of information and information systems to security categories. National Institute of Standards and Technology. NIST 800-60, 2008.

[34] J.F Audenard.Comprendre la protection des données dans le cloud. Publication Orange Business Services, 17 Mars 2011.

[35] J. Schwenk, L.L Lacono, M. Jensen, N. Gruschka. On technical security issues in cloud computing. IEEE International Conference on Cloud Computing, 2009.

[36] C.Wang, K.Ren, Q.Wang, W.Lou. Ensuring data storage security in cloud computing. In the 17th IEEE InternationalWorkshop on Quality of Service (IWQoS'09). Charleston, South Carolina, July.2009.

[37] D. Chen, Y. He. A study on secure data storage strategy in cloud computing. Journal of Convergence Information Technology. Vol. 5, no.7, september.2010.

[38] A. Parakh, S. Kak. Online data storage using implicit security. Information Sciences. vol.179, no 3323-3331, 2009.

[39] F. Zhou, M. Goel, P. Desnoyers, R. Sundaram. Scheduler vulnerabilities and attacks in cloud computing. College of Computer and Information Science Northeastern University. Boston, USA, march.2011.

[40] J. Wei, X. Zhang, G. Ammons. Managing security of virtual machine images in a cloud environment. Proceedings of the 2009 ACMworkshop on Cloud computing security. New York, 2009.

[41] F. Hu, M. Qiu, J. Li, T. Grant, D. Tylor, S. McCaleb, L. Bulter, R. Hamner. A review on cloud computing : design challenges in architecture and security. Journal of Computing and Information Technology - CIT 19,1,25-55. pp. 17, 2011.

[42] E. M. Mohamed, H. S. Abdelkader, S. El-Etriby, Enhanced data security model for cloud computing. In Informatics and Systems (INFOS). 8th International Conference. pp. CC-12, 2012.

[43] A. Irudayasamy, L. Arockiam, N. Veeraragavan. Enhancing Data Security during Transit in Public Cloud. International Journal of Engineering and Innovative Technology (IJEIT). Volume 3, Issue 1, July 2013

[44] D. Chen, H. Zhao. Data security and privacy protection issues in cloud computing. pp. 647-651, 2012.

[45] S. Balakrishnan, G. Saranya, S. Shobana, S. Karthikeyan. Introducing effective third party auditing (tpa) for data storage security in cloud. International Journal of Computing and Technology. pp. 397-400, June 2011.

[46] F. Aloul, S. Zahidi, W. El-Hajj. Two factor authentication using mobile phones. In Computer Systems and Applications AICCSA, IEEE/ACS International Conference. pp. 641-644, 2009.

[47] D. Gelibert, F. Smili, J. Derock, L. Ratsihorimanana, M. Dreyer, T. Gervaise. La sécurité et la Virtualisation. Polytech Lyon, Livre Blanc, Mai 2012.

[48] S. Maninder, S. Sarabjeet. Design and implementation of multi -tier authentication scheme in cloud, International Journal of Computer Science Issues. vol. 9, no. 2.

[49] K. Satish, G. Anita. Multi-authentication for cloud security : a framework. International Journal of Computer Computing and Engineering Technology (IJCSET). vol. 5, no. 4, Apr. 2014.

[50] A. S.Ezhil, B.Gowri, S.Ananthi. Privacy-preserving public Auditing in cloud using HMAC International Journal of Recent Technology and Engineering (IJRTE) ISSN : 2277-3878, Volume-2, Issue-1, March 2013.

[51] P. Kalpana, S. Singaraju. Data security in cloud computing using RSA algorithm. International Journal of Research in Computer and Communication technology (IJRCCT). ISSN 2278-5841, Vol 1, Issue 4, pp. 143-146, September 2012.

[52] P. Pankaj, C. Inderveer. A secure data transfer technique for cloud computing. THAPAR UNIVERSITY, August 2014.

[53] U. Somani, K. Lakhani, and M. Mundra. Implementing digital signature with RSA encryption algorithm to enhance the data security of cloud in cloud computing. International Conference on Parallel Distributed and Grid Computing (PDGC).

[54] V. R. Balasaraswathi, S. Manikandan. Enhanced security for multi-cloud storage using cryptographic data splitting with dynamic approach. In Advanced Communication Control and Computing Technologies(ICACCCT). International Conference, pp. 1190-1194, 2014.

[55] Danwei Chen, Yanjun He, A Study on Secure Data Storage Strategy in Cloud Computing, Journal of Convergence Information Technology, Vol. 5, no. 7, September 2010.