UNIVERSITÉ KASDI MERBAH OUARGLA

Faculté des Nouvelles Technologies de

L'Information et de la Communication

Département d'Informatique et des Technologies de l'Information

Mémoire

En vue de l'obtention du diplôme de

MASTER PROFESSIONEL

Domaine : Informatique et Technologie de l'Information

Filière : Informatique

Spécialité : Réseau convergence et sécurité

Thème

Une approche de sécurité basée sur authentification dans Cloud Computing

Présenté par :

- Ghezal Hadjer
- Belghit Karima

Soutenu publiquement le : 01/07/2017

Devant le jury composé de :

M. Said Bachir	Président	Maître assistant A	UKM Ouargla
M. Bekkari Foad	Rapporteur	Maître assistant A	UKM Ouargla
M. Euschi Salah	Examinateur	Maître assistant A	UKM Ouargla

Année universitaire : 2016/2017

Remerciement

En préambule à ce mémoire nous remercions ALLAH qui nous aide et nous donne la patience et le courage durant ces longues d`années d'études.

Nous souhaitons adresser nos remerciements les plus sincères aux personnes qui nous ont apporté leur aide et qui ont contribué à l'élaboration de ce mémoire ainsi qu'à la réussite de cette formidable année universitaire.

Ces vifs remerciements vont tout d'abord au corps professoral et administratif de la Faculté ***des Nouvelles Technologies de L'Information et de la Communication****, pour la richesse et la qualité de leur enseignement et qui déploient de grands efforts pour assurer à leurs étudiants une formation actualisée.*

Nous tenons à remercier sincèrement Monsieur ***Meflah Mohammed Salim****, notre encadreur qui, en tant que Directeur de mémoire, s`est toujours montré à l'écoute et par sa disponibilité tout au long de la réalisation de ce mémoire, ainsi pour l'inspiration, l'aide et le temps qu'il a bien voulu nous consacrer*

C'est avec une immense fierté qui j'adresse mes remerciements les plus distingués à tous ***mes enseignants de l'Informatique*** *qui nous ont transmis leur savoir et nous ont assuré la meilleure des formations.*

Notre dernier mot s'adresse à ***tous les membres du jury*** *d`avoir accepté de juger notre travail.*

Dédicace

Je dédie ce travail

A ma très chère mère ***Fatima***

A mon très cher Père ***lhaj Tayeb***

A mes très chers frères ***Madjid*** *et* ***Ibrahim***

A ma très chère sœur ***Mona****, son mari* ***Amar***
Et leurs enfants ***Adam*** *et* ***Hodaifa***

A ma très chère sœur ***Sarah***

A tous les membres de ma famille, petits et grands

A mes chères ami(e)s et collègues
Hichem, Mebarka, Amina, Malek, Khaoula, Narimen,Yousra,
Houssem,Yasmin, Hadjer, Hind, Chaima

A mon binôme, ma sœur, mon amie ***Karima***

Hadjer

Dédicace

A ma très chère mère ***Malika***

A mon cher Père ***AbdelKarim***

A mes très chers frères ***Imad, Akram*** *et* ***Chahine***

A ma très chère sœur ***Kaouther***

A tous les membres de ma famille, petits et grands

A mes chères ami(e)s

Sami, Fethi, Ramzi, Othman, Samia, Yasmine, Cappella, Raja, Aldja

A mon binôme, ma sœur, mon amie ***Hadjer***

Karima

Table des matières

Liste des figures

Liste des tables

Introduction Générale

Introduction

De nos jours, l'utilisation d'Internet et des nouvelles technologies, pour satisfaire l'évolution continue des besoins de différents types d'utilisateurs (affaire, particulier), fait partie de la vie quotidienne. Toute information est disponible partout dans le monde à tout moment. Cela n'était pas possible il y a quelques années. Récemment, un nombre important de possibilités d'accès à l'information publique et privée sont apparues. Ainsi, nous avons un accès généralisé à grand débit à Internet grâce au déploiement de dispositifs fixes, mobiles ou encore sans fil qui permettent la connexion à Internet sans presque se soucier de la limitation géographique.

Aujourd'hui, différents types d'utilisateurs consultent leurs courriers en ligne via des Webmail, rédigent des documents de collaboration en utilisant les navigateurs web, exécutent des applications et stockent des données dans des serveurs situés sur Internet et non dans leurs propres ordinateurs. De plus, ces services ainsi que d'autres sont utilisés d'une façon transparente pour l'utilisateur et sont donc perçus comme étant des services offerts par un nuage (Cloud) sans en connaître les détails. Cela signifie que de nombreux utilisateurs et organisations peuvent éviter l'installation de certaines applications sur leurs infrastructures ou peuvent avoir plus de puissance de calcul en utilisant les ressources de ce Cloud grâce à Internet. De plus, ces utilisateurs peuvent construire leurs propres Clouds privés et les administrer selon leurs propres politiques de gestion. Ainsi, la plupart des entreprises essayent de réduire leurs coûts d'exploitation et de traitement grâce à des techniques de virtualisation. Ces techniques et usages ont conduit à l'émergence d'un nouveau concept appelé Cloud Computing qui permet d'offrir plusieurs types de services avec une meilleure utilisation des ressources des infrastructures et une réduction de leurs coûts d'exploitation.

Le Cloud Computing est un terme utilisé pour décrire à la fois une plateforme et un type d'application. En tant que plateforme, le Cloud Computing fournit, configure et reconfigure les serveurs. Ces serveurs peuvent être des machines physiques ou encore des machines virtuelles. D'autre part, le Cloud Computing permet à des applications d'être étendues pour devenir accessible à travers Internet. A cet effet, des grands centres de données et des serveurs puissants sont utilisés pour héberger ces applications qui peuvent être utilisées grâce à des services Web. Le Cloud Computing est devenu l'une des plus importantes technologies ces

derniers temps et fait l'objet de plusieurs études dans différents domaines en égard à la multiplicité des possibilités de service offert qu'il propose.

La sécurité est l'un des défis à relever les plus importants pour l'adoption du Cloud. En effet, les données sont des éléments très précieux pour les utilisateurs. Les entreprises veulent toujours s'assurer que ces données sont sécurisées. La confiance des utilisateurs est naturellement plus importante lorsque les données sont traitées, stockées et contrôlées en interne. L'externalisation du traitement ou encore du stockage de ces données dans un environnement de Cloud Computing s'accompagne d'un risque de sécurité. En effet, les données peuvent être compromises à différentes étapes de leur cycle de vie lorsqu'elles sont stockées ou traitées dans le Cloud. Les risques de sécurité peuvent apparaître lors du transfert de ces données du réseau interne de l'entreprise vers le Cloud pour y être stockées ou traitées, ou encore lors du processus de restauration des données. Ainsi, la transition vers une utilisation massive des services du Cloud s'accompagne de plusieurs défis de sécurité et de confidentialité, principalement en raison de la nature dynamique du Cloud et le fait que dans cet environnement les composants logiciels et matériels qui permettent d'offrir un service appartiennent à de multiples domaines de confiance. Par conséquent, la garantie des services de sécurité dans un environnement de Cloud est beaucoup plus difficile.

Problématique

Le cloud computing, comme tout système informatique réparti, est continuellement exposé à de nombreuses menaces aux origines diverses [41]. Ainsi, la sécurité du cloud est aujourd'hui une préoccupation très importante des fournisseurs et utilisateurs [42, 43].

Pour se prémunir des attaques reposant sur l'utilisation des réseaux, des mécanismes de sécurité réseau sont déployés pour protéger les données hébergées dans les infrastructures virtuelles. Les pare-feu sont responsables du filtrage de paquets afin de contrôler l'accès réseau. Les systèmes de détection d'intrusion sont en charge de détecter les attaques survenant sur les canaux de communication. L'objectif des administrateurs de sécurité (des clients ou des fournisseurs) est de prévenir et de détecter les attaques tout en ne perturbant pas le bon fonctionnement du cloud. Rendre les pare-feu et systèmes de détection d'intrusion efficaces conjointement n'est pas une tâche aisée. En effet, les produits déployés doivent être maintenus à jour, correctement configurés et positionnés sur le réseau. De plus, les environnements cloud évoluent constamment au cours du temps.

Organisation du mémoire

Dans le cadre de ce mémoire nous réalisons un état de l'art afin de relever le défi de recherche dans un environnement de Cloud Computing, nous analyserons la technologie de Cloud Computing et les services qui la composent.

Puis nous analyserons les défis de sécurité dans le domaine d'authentification dans le Cloud et les solutions proposées.

Chapitre 1 : Cloud Computing

Introduction

Le terme (Cloud) vient du monde des télécommunications, lorsque les médecins ont commencé à l'aide de services de réseaux privés virtuels (VPN) pour les communications de données [1]. Traiter de l'informatique en nuage, logiciel de calcul, l'accès aux données et des services d'entreposage qui ne nécessitent pas de connaissances de l'utilisateur final de l'emplacement physique et la configuration du système qui est de la prestation des services. Le Cloud Computing est une tendance récente dans ce qui déplace les données informatiques et loin de bureau et ordinateurs portables dans les grands centres de données [2].

La définition du Cloud Computing fourni par le National Institute of Standards and Technologie (NIST) dit que : « le Cloud Computing est un modèle de pratique permettant, à la demande d'un accès réseau à un pool partagé de ressources informatiques configurables (par ex., réseaux, serveurs, applications et services de stockage) qui peuvent être configurés rapidement et avec un minimum d'effort de gestion de parution ou le fournisseur de l'interaction [3] » Avec la prolifération à grande échelle de l'internet dans le monde, les applications peuvent maintenant être livrés en tant que services sur internet. Par conséquent cela réduit le coût global.

L'objectif principal de l'informatique en nuage est de faire une meilleure utilisation des ressources distribuées, les combiner pour obtenir un débit plus élevé et être capable de résoudre des problèmes de calcul à grande échelle. Cloud Computing traite de la virtualisation, l'évolutivité, l'interopérabilité, de qualité de service et de la prestation des services du Cloud, à savoir les secteurs privé, public et hybride.

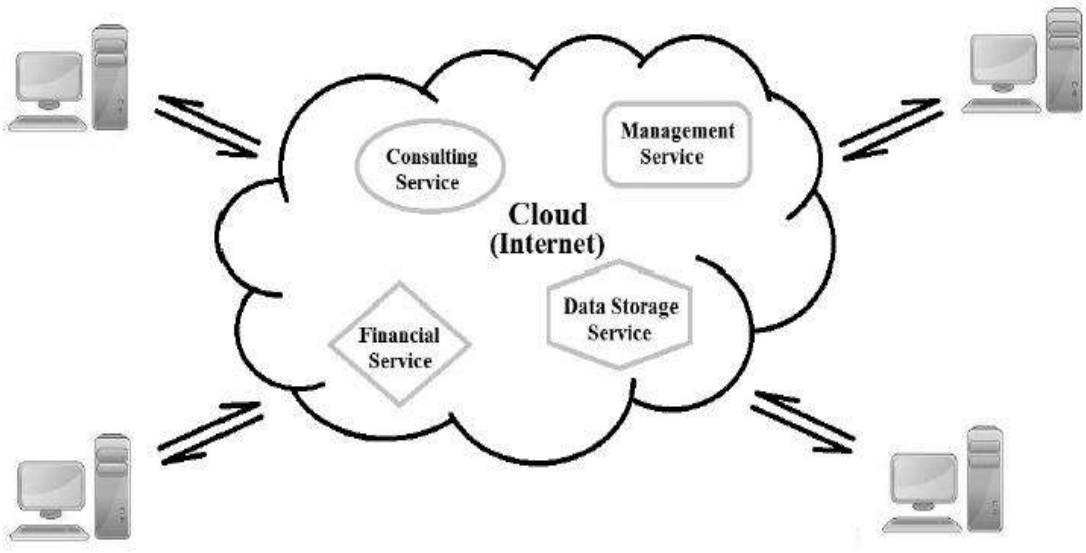

Figure 1: Cloud Computing**[4].**

1.1 Historique

Le concept sous-jacent de l'informatique en nuage a été introduit en 1960 par John McCarthy. Il est d'avis que « peut être un jour de calcul service organisé comme un public. [5] » Aussi les caractéristiques du Cloud Computing ont été explorées pour la première fois en 1966 par Douglas Parkhill dans son livre, le défi de l'Utilitaire informatique [5]. L'histoire du terme Cloud est du monde des télécommunications, où les entreprises de télécommunications ont commencé à offrir des services de réseaux privés virtuels (VPN) avec une qualité de service comparable à un coût beaucoup plus faible. Avant d'abord, ils ont fourni VPN point à point dédiée des circuits de données qui a été un gaspillage de bande passante. Le Cloud Computing s'étend désormais à couvrir cette infrastructure réseau et serveurs.

De nombreux acteurs de l'industrie ont sauté dans le Cloud Computing et l'a mis en œuvre. Amazon a joué un rôle clé et a lancé l'Amazon Web Service (AWS) en 2006. Également Google et IBM ont lancé des projets de recherche dans le Cloud Computing. L'Eucalyptus est devenu la première plate-forme open source pour le déploiement de Clouds privés.

1.2 Définition

La notion de Cloud fait référence à un nuage, tel que nous avons l'habitude de l'utiliser dans des schémas techniques lorsque nous voulons représenter Internet. Un réseau comme Internet est constitué d'une multitude de systèmes fournissant des services. Le Cloud Computing est

dans cette lignée : un ensemble de services et de données consommables fournis aux utilisateurs [6].

1.3 Caractéristiques de l'informatique en nuage

- Dans le Cloud Computing, les utilisateurs accèdent aux données, applications ou tout autre service à l'aide d'un navigateur, peu importe l'appareil utilisé et l'endroit des utilisateurs. L'infrastructure qui est généralement fourni par un tiers est accessible avec l'aide de l'internet. Le coût est réduit à un niveau que l'infrastructure est fournie par un tiers et n'a pas besoin d'être acquis pour des tâches de calcul intensif.
- Moins ils sont les compétences requises pour la mise en œuvre.
- Service fiable peut être obtenu par l'utilisation de plusieurs sites qui est adapté pour la continuité de l'activité [9] et de reprise après sinistre [9]. Cependant, parfois, de nombreux services de Cloud Computing ont subi des pannes et dans de tels moments ses utilisateurs peuvent difficilement faire quoi que ce soit [10].
- Le partage des ressources et les coûts entre une grande collection d'utilisateurs permettent à l'utilisation efficace de l'infrastructure.
- L'entretien est plus facile en cas d'applications de Cloud Computing car qu'ils n'ont pas besoin d'être installé sur chaque ordinateur de l'utilisateur.
- Facilité de paiement à la consommation permet de mesurer l'utilisation de l'application par le client sur des bases régulières.
- Les performances peuvent être surveillées et donc il est évolutif.
- La sécurité peut être aussi bonne ou meilleur que les systèmes traditionnels parce que les fournisseurs sont en mesure de consacrer des ressources à la résolution des problèmes de sécurité que de nombreux clients ne peuvent pas se permettre. Cependant, la sécurité demeure une préoccupation importante lorsque les données sont tout à fait confidentielles. Cela retarde l'adoption du Cloud Computing dans une certaine mesure [11,12].

1.5 Type du Cloud Computing

Le Cloud Computing est composé de trois type, que nous allons exposer :

1.5.1 Iaas (Infrastructure as a Service)

Il s'agit de la mise à disposition, à la demande, de ressources d'infrastructures dont la plus grande partie est localisée à distance dans des Data-centers.

L'IaaS permet l'accès aux serveurs et à leurs configurations pour les administrateurs de l'entreprise. Le client a la possibilité de louer des clusters, de la mémoire ou du stockage de données. Le coût est directement lié au taux d'occupation. Une analogie peut être faîte avec le mode d'utilisation des industries des commodités (électricité, eau, gaz) ou des télécommunications, Eucalyptus est un exemple d'infrastructure [13].

1.5.2 Paas (Plateform as a Service)

Il s'agit des plateformes du nuage, regroupant principalement les serveurs mutualisés et leurs systèmes d'exploitation. En plus de pouvoir délivrer des logiciels en mode SaaS, le PaaS dispose d'environnements spécialisés au développement comprenant les langages, les outils et les modules nécessaires.

L'avantage est que ces environnements sont hébergés par un prestataire basé à l'extérieur de l'entreprise ce qui permet de ne disposer d'aucune infrastructure et de personnel de maintenance et donc de pouvoir se consacrer au développement.

1.5.3 Saas (Software as a Service)

Concept consistant à proposer un abonnement à un logiciel plutôt que l'achat d'une licence.

On oublie donc le modèle client-serveur et aucune application n'est installée sur l'ordinateur, elles sont directement utilisables via le navigateur Web. L'utilisation reste transparente pour les utilisateurs, qui ne se soucient ni de la plateforme, ni du matériel, qui sont mutualisés avec d'autres entreprises.

Le SaaS remplace l'ASP, aussi appelé fournisseur d'applications hébergées ou FAH, ou application service provider en anglais ou ASP, qui est une entreprise qui fournit des logiciels ou des services informatiques à ses clients au travers d'un réseau.

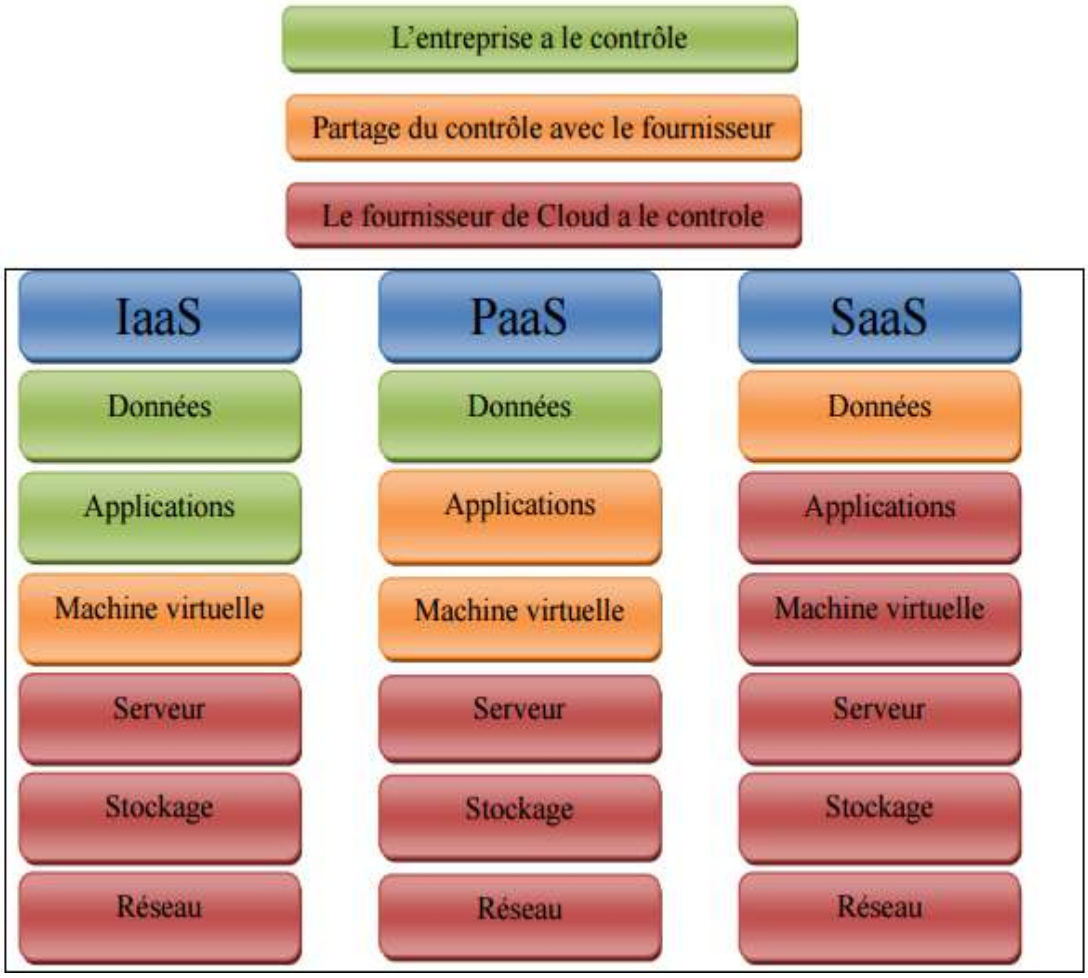

Figure 2:Répartirions des responsabilités dans le Cloud Computing **[15].**

Deux principales différences avec l'ASP traditionnel sont qu'une simple interface web est utilisée côté client dans tous les cas (pas de client lourd), et que le SaaS propose une seule instance de logiciel qui évolue indépendamment des clients. Avec l'arrivé du Haut débit, les logiciel en mode SaaS deviennent utilisables sans problème.

La figure ci-dessous (**Figure 4**) présente les trois couches du Cloud Computing ainsi que leurs acteurs en donnant un compromis flexibilité/simplicité. En Cloud, la flexibilité est obtenue grâce à la virtualisation des systèmes d'exploitation. La plateforme est exécutée via des machines virtuelles et les ressources peuvent être allouées et libérées à la demande. Ainsi, l'IaaS est considéré comme le service le plus flexible.

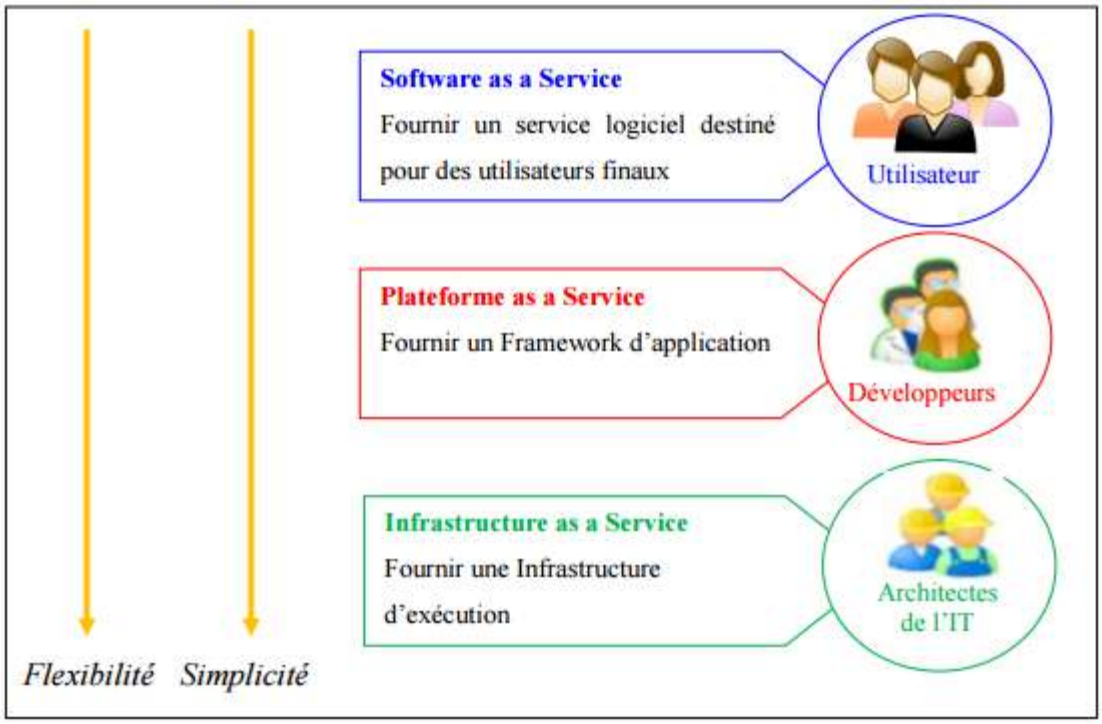

Figure 3:Les différents niveaux des services du Cloud Computing

1.5.4 Avantages et inconvénients des services

Du point de vue économique, le Cloud Computing est essentiellement une offre commerciale d'abonnement économique à des services externes. Selon le National Institute of Standards and Technology, il existe trois catégories de services qui peuvent être offerts en Cloud Computing: IaaS, PaaS et SaaS[16]. Les avantages et les inconvénients de ces services ce résume dans le tableau ci-dessous.

	Avantage	Inconvénient
SaaS	✓ Pas d'installation ✓ Plus de licence ✓ Migration ✓ Accessible via un abonnement	✓ Logiciel limité ✓ Sécurité ✓ Dépendance des prestataires
PaaS	✓ Pas d'infrastructure nécessaire ✓ Pas d'installation ✓ Environnement hétérogène	✓ Limitation des langages ✓ Pas de personnalisation dans la configuration des machines virtuelles
IaaS	✓ Administration ✓ Personnalisation ✓ Flexibilité d'utilisation ✓ Capacité de stockage infini	✓ Sécurité ✓ Besoin d'un administrateur système ✓ Demande pour les acteurs du Cloud des investissements très élevés

Tableau 1: Avantage et inconvénients des services Cloud Computing [13][14].

1.6 Avantages et inconvénients du Cloud Computing

1.6.1 Avantages

- **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 [13].

1.6.2 Inconvénients

- **La bande passante peut faire exploser le budget :**

La bande passante qui serait nécessaire pour mettre cela dans le Cloud est gigantesque, et les coûts seraient tellement importants qu'il est plus avantageux d'acheter le stockage nous-mêmes plutôt que de payer quelqu'un d'autre pour s'en charger.

- **Les performances des applications peuvent être amoindries :**

Un Cloud public n'améliorera définitivement pas les performances des applications.

- **La fiabilité du Cloud :**

Un grand risque lorsqu'on met une application qui donne des avantages compétitifs ou qui contient des informations clients dans le Cloud.

- **Taille de l'entreprise :**

Si l'entreprise est grande alors ses ressources sont grandes, ce qui inclut une grande consommation du Cloud. Du coup il serait peut-être plus intéressant à mettre au point son 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. [13].

1.7 Modèles de déploiement

Il existe différents modèles de déploiement du Cloud, chacun avec ses avantages et ses inconvénients.

1.7.1 Cloud public

Dans un Cloud public les CSP offrent leurs ressources comme services au grand public.
Ce modèle peut être détenu, géré et exploité par une entreprise ou une organisation académique ou gouvernementale, ou une combinaison entre eux. Le Cloud public offre plusieurs avantages aux utilisateurs, y compris l'absence de coûts d'investissement élevés sur les infrastructures et le déplacement des risques vers les fournisseurs d'infrastructure.
Mais, ces utilisateurs n'ont pas un contrôle fin sur les données, le réseau et les paramètres de sécurité, ce qui entrave l'efficacité de ce modèle de déploiement.

1.7.2 Cloud privé

Le Cloud privé est conçu pour une utilisation exclusive par une seule organisation. Un Cloud privé peut être construit et géré par l'organisation, une tierce partie, ou une combinaison des deux. Il offre le plus haut degré de contrôle sur les performances, la fiabilité et la sécurité. Cependant, il est souvent critiqué car il est similaire aux serveurs propriétaires traditionnels

qui ne fournissent pas les avantages du Cloud comme l'absence de coûts d'investissement élevés.

1.7.3 Cloud communautaire

C'est un Cloud qui partage des infrastructures entre plusieurs organismes d'une communauté spécifique avec des préoccupations communes (la mission, les exigences de sécurité, la politique, etc..). Ces infrastructures sont gérées par un ou plusieurs organismes de la communauté, une tierce partie, ou une combinaison de ces entités. Ce modèle de déploiement offre les avantages d'un Cloud public comme la structure de facturation de type «payez ce que vous utilisez», mais aussi les avantages d'un Cloud privé en termes de confidentialité et de sécurité d'une façon générale. Les coûts sont répartis sur moins d'utilisateurs qu'un Cloud public (mais plus qu'un Cloud privé), de sorte qu'une partie des économies potentielles de Cloud sont réalisées.

1.7.4 Cloud hybride

Un Cloud hybride est une combinaison de déploiement des modèles de Cloud (public, privé et communauté) qui tente de remédier aux limitations de chaque approche. Dans un Cloud hybride, une partie du service de l'infrastructure s'exécute dans des Clouds privés tandis que la partie restante est dans des Clouds publics. Un Cloud hybride offre plus de flexibilité qu'un Cloud public ou privé, puisqu'il fournit un meilleur contrôle et une meilleure sécurité pour les données d'application des utilisateurs par rapport aux Clouds publics et une tarification avantageuse par rapport aux Clouds privés. Cependant, la conception d'un Cloud hybride nécessite une étude détaillée afin de déterminer la meilleure répartition entre les composantes de Cloud public et privé.

Pour la plupart des organisations, le choix du modèle de Cloud dépend du cas d'utilisation et des exigences du CSU « Cloud Service User » (sécurité, QoS, etc.).

Conclusion

Aujourd'hui, avec le Cloud, il est possible de déployer facilement une application à travers le monde. Cela permet aux entreprises de ne pas être obligées d'être implantées physiquement dans un pays pour aller à la rencontre de leurs clients locaux et de leur proposer leurs services. Dans ce **chapitre,** nous avons réalisé une présentation générale du Cloud Computing, son historique, ses caractéristiques, ses modèles de services et de déploiement, ainsi que les outils d'implémentation et de simulation.

Dans cet environnement de Cloud, le défi demeure en ce qui concerne la sécurité et la confiance, la localisation des données, etc. Ainsi, dans le **chapitre** suivant, nous présenterons un état de l'art sur l'authentification dans le Cloud Computing.

Chapitre 2 :

La sécurité Dans le Cloud Computing

2.1 Introduction

Depuis sa jeunesse, le Cloud Computing a été de révolutionné les modes de stockage et de traitement des données, des mécanismes sont envisagés et mis en œuvre. Elle a permis à la demande de la disponibilité des services tels qu'un logiciel, plate-forme, et infrastructure (SaaS, PaaS, IaaS respectivement) et ainsi constitué une solution économique pour répondre à la fluctuation constante à la demande de ressources informatiques et de stockage par les entreprises qui était en pleine croissance [18]. Aujourd'hui, la rondelette somme de 32 milliards est calculée pour être consacrée à l'infrastructure informatique en nuage par année, selon l'International Data Corporation, Le marché de l'entreprise intelligence [19]. Cela représente 33% du total des dépenses d'infrastructure informatique. Plus loin, les dépenses d'infrastructure de Cloud Computing devrait atteindre 52 milliards de dollars en 2019 soit 43% du total des dépenses. Le nuage est responsable de fournir des services en temps réel tels que le stockage des données, applications et du traitement des données pour les consommateurs à travers l'internet. Les consommateurs peuvent stocker à distance leurs données dans le Cloud et pourrez profiter de la rémunération des services évolutifs à la demande [20]. Comme une technologie émergente, il offre de grandes possibilités mais avec son juste part de problèmes, peut-être la plus importante est comment assurer la sécurité et la vie privée des utilisateurs du Cloud ?. Comme dans les paradigmes traditionnels, l'authentification joue un rôle majeur dans la sécurité dans le Cloud Computing. L'authentification de l'utilisateur est un régime important afin que seuls les utilisateurs autorisés puissent accéder au serveur. Ce chapitre résume les méthodes d'authentification existantes en Cloud Computing, présente un système de classification pour les différentes méthodes et de souligner les avantages et inconvénients de chacune des méthodes.

2.2 Pourquoi la sécurité dans le Cloud Computing ?

En utilisant les données de débarquement et le Cloud computing, beaucoup d'entreprises peuvent réduire considérablement leurs coûts. Cependant, en dépit des tonnes de fond de l'informatique en nuage, de nombreux propriétaires d'entreprises ont commencé à s'inquiéter au sujet de la sécurité. Dans l'environnement d'informatique en nuage, les employés peuvent facilement accéder, falsifier et divulguer les données. Un tel comportement est parfois un désastre pour un grand et célèbre société.

Le chiffrement est une sorte de moyen idéal pour résoudre ce genre de problème, alors que pour les clients qui utilisent le système de Cloud Computing ne peut pas utiliser de telles données chiffrées. Les données originales doivent être utilisées dans la mémoire de l'hôte dans le cas contraire, la machine hôte VM ne peut pas faire d'applications sur demande. Par exemple, l'Amazon EC2 est l'un des fournisseurs de services qui ont le privilège de lire et modifier les données de la part des clients. Il n'y a pas de sécurité pour les clients qui utilisent ce service.

Certains fournisseurs de développement offre une certaine méthode technique visant à éviter la sécurité traité de l'intérieur. Par exemple, certains fournisseurs limitent le pouvoir d'accès et de gérer le matériel, contrôler les procédures, et à réduisent au minimum le nombre de membres du personnel qui a le privilège d'accéder aux parties de l'infrastructure essentielle. Cependant, chez le fournisseur principal, l'administrateur peut également accéder à la machine client VM. [21].

2.3 Définition de la sécurité

La sécurité du Cloud peut être définie comme étant l'ensemble des moyens techniques, organisationnels, juridiques et humains nécessaires pour protéger les données, les applications et l'infrastructure associée au Cloud contre une faiblesse d'ordre logicielle ou matérielle qui peut être exploitée par une ou plusieurs menaces internes ou externes.

La sécurité du Cloud implique des concepts tels que la sécurité des réseaux et du matériel ainsi que les stratégies de contrôle déployées afin de protéger les données, les applications et l'infrastructure d'un environnement de Cloud [22].

2.4 Services de sécurité dans un enivrement de Cloud

La sécurité assure les services importants tels que l'authentification, le contrôle d'accès, la confidentialité, l'intégrité, la disponibilité et la non-répudiation. Par conséquent, ces services deviennent des composants importants que nous devons utiliser lors de la conception d'un système de Cloud sécurisé [23][24][25].

L'authentification est définie comme étant l'assurance que l'entité qui demande l'accès est celle qu'elle prétend être. L'authentification permet au CSP (Cloud Service Provider) de faire confiance à l'identité du CSU (Cloud Service User) suite à une vérification afin de lui permettre l'accès aux ressources déployées dans le Cloud. Une procédure d'authentification

qui manque de robustesse peut conduire à un accès non autorisé aux comptes des utilisateurs dans un Cloud, et par conséquent à une violation de la confidentialité et de la vie privée. Le contrôle d'accès est défini comme étant la capacité de décider, en fonction de l'identité authentifié d'une entité, qui est autorisé à accéder aux ressources du Cloud pour manipuler des données, exécuter des programmes et effectuer des actions.

La confidentialité se réfère à la capacité de permettre seulement aux parties autorisées d'avoir l'accès aux données et aux logiciels protégés dans le Cloud. Par conséquent, dans un environnement de Cloud l'utilisateur est tenu de déléguer la confiance au CSP qui doit assurer la confidentialité en utilisant par exemple le processus de chiffrement et de déchiffrement. La puissance de tout système de cryptographie, qui sera déployé dans un environnement de Cloud, repose sur la technique de distribution des clés d'une façon sécurisée afin de permettre à deux entités d'utiliser ces clés lors de l'échange de données.

De plus, le CSP doit protéger la vie privée des CSU. La vie privée est le désir d'un

CSU d'avoir une garantie de confidentialité relative à ses données personnelles. Dans ce contexte, l'environnement de Cloud présente un certain nombre de défis juridiques relatifs à la confidentialité.

L'intégrité se réfère à la protection des données et des logiciels dans le Cloud contre la suppression, la modification et l'ajout non autorisés qui peuvent être volontaires ou involontaires. Les CSP mettent en œuvre un ensemble d'interfaces logicielles ou des API que les CSU utilisent pour gérer et utiliser leurs services dans le Cloud. La sécurité de ces services dépend fortement de la sécurité de ces interfaces ou API car si un CSU non autorisé prend le contrôle de ces interfaces, il pourrait modifier, supprimer ou ajouter des données. Par conséquent, les CSP doivent sécuriser ces interfaces afin de maintenir l'intégrité des données et des services d'une façon générale.

La disponibilité se réfère à la propriété d'un système de Cloud d'être accessible et utilisable sur demande par une entité autorisée. Les services du Cloud présentent une forte dépendance vis à vis des ressources réseau et leur disponibilité. Le système de Cloud doit avoir la capacité de poursuivre ses activités même si une panne a eu lieu.

La non-répudiation est définie comme étant la capacité d'assurer qu'une partie d'un contrat ou d'une communication ne peut pas nier la réception d'un message ou d'être la source d'un message envoyé. Ainsi, dans un environnement de Cloud, le CSP doit assurer la traçabilité de tous les accès ou encore les modifications apportées aux ressources et aux données dans des registres vérifiables.

2.5 Les domaines de la sécurité

Tous les domaines de l'informatique sont concernés par la sécurité d'un système d'information. En fonction de son domaine d'application, la sécurité informatique se décline en [46] :

2.5.1 Sécurité physique

- Accès physique
- Contrôle et traçabilité des accès
- Sécurisation de l'environnement
- Redondance matérielle
- Résilience [26].

2.5.2 Sécurité logique

- Sécurité des serveurs virtuels
- La Colocation sécurisée
- Segmentation réseau
- Sécurité de l'interface d'administration
- Sécurité des accès et des identités :
    - **Authentification**
    - Sécurisation des accès
    - Accessibilité du service hébergé
    - Adaptabilité aux pics de charge
    - Impact de la gestion des mises a jour de sécurité sur la certification [26].

2.5.3 Sécurité des données

- Responsabilité juridique de la sécurité et de la confidentialité des données dans le Cloud
- Protection et récupération des données
- Intégrité des données (RBAC)

- Chiffrement des données
- Réversibilité : changer de Cloud [26].

2.6 Tendance d'authentification récente en Cloud Computing

Un certain nombre de chercheurs travaillent à trouver des méthodes d'authentification forte pour le Cloud Computing. Un certain nombre de méthodes d'authentification sont en pratique. Dans cette section, un examen critique des divers travaux de recherche est effectué. Pour simplifier l'examen, de nouvelles approches sont divisées en différentes catégories. Dans chaque catégorie, la pratique actuelle et les recherches récentes sont discutés.

2.6.1 Frameworks d'authentification, les modèles et architectures

Dans la dernière décennie, beaucoup de développement a eu lieu dans le domaine du modèle d'authentification. Nombre de Framework, modèles et architectures ont été proposées par les chercheurs. L'une des architectures d'authentification a été proposée par Chow et al. [27]. L'architecture est basée sur la méthode « Ce qu'un individu a l'habitude de voir. » Ils ont proposé une méthode d'authentification pour les utilisateurs mobiles. Cette architecture d'authentification est basée sur l'historique des sites web que l'utilisateur visite. D'une part, il est pratique et facile à utiliser, d'autre part, il ne peut pas être utilisé comme un remplacement pour l'authentification régulière dans les secteurs à haut risque, comme les banques. Dans une autre recherche de premier plan par Z.Shen et al. [38], [29] une architecture de référence proposée pour régler les problèmes de gestion de l'identité pour le Cloud Computing. Comme l'étape suivante dans la recherche d'une nouvelle méthode d'authentification a été proposée par l'œuvre de l'authentification mobile lié à l'Infrastructure à clé publique durant la phase de connexion. Lee et autre [30, 2010] a présenté un système où l'infrastructure à clé publique est mis en œuvre. **PKI** est une collection de matériel, logiciel, politique, les procédures et les personnes travaillant ensemble. Le modèle d'authentification (**CAM**) proposé par Kim et Hong [31, 2011] offre non seulement un cadre d'authentification plus souple mais aussi plus sûr conduit à la gestion des informations d'identification, à l'administration de divers appareils mobiles tels que smart phone, smart pad, etc. L'inconvénient de cette méthode est l'absence de protocole d'identification sécurisée.

2.6.2 Les mots de passe jetons et l'authentification par carte à puce

Dans la méthode « Une personne possède quelque chose » la catégorie technique d'authentification de base est les jetons. L'authentification des jetons vient dans deux formes de base - matériel et logiciel. Ces jetons sont utilisés dans les appareils courants tels que les téléphones portables. Les jetons matériels sont des dispositifs physiques qui génère un temps passe et dont la validité ne dure que pour l'événement d'authentification unique. Le principal inconvénient est le coût de la distribution et de la sécurité. Jeton logiciel se présente comme une solution aux problèmes soulevés par les jetons matériels.

En serveurs distribués, Serveur EAP-TLS Les cartes à puce offrent la sécurité et la simplicité. Urien et autres [32,2010] dans leur proposition de recherche un paradigme basé sur une grille de cartes à puce construit sur un contexte de cartes à puce SSL. Ils ont présenté l'évolutivité du serveur lié aux grilles de la carte à puce dont le calcul distribué gère l'accord de nombreuses sessions d'authentification.

Les jetons de logiciel sont en coopération en PC portables et PC de bureau. Quorica[33,2009] - Un logiciel intelligent, les jetons sont utilisés avec les téléphones intelligents et les périphériques USB. Leur popularité est due au fait que ces jetons n'ont pas besoin d'être transportés et conservés à l'abri comme les jetons matériels. Une alternative au logiciel token est le jeton à la demande, qui est un ancien mot de passe entré dans une application pour l'authentification. La technique présentée par Dinesha et Agarwal[34] génération de mot de passe propose par la concaténation de mots de passe à plusieurs niveaux. L'authentification s'effectue à différents niveaux d'organisation, niveaux d'utilisateurs et l'équipe. De niveau de l'utilisateur, l'utilisateur authentifié est autorisé à accéder à une ressource nuage particulière. L'avantage de cette technique est qu'elle utilise une approche multi-niveaux. Il est assez difficile de rompre la sécurité multi-niveaux par rapport à niveau unique. L'inconvénient de cette méthode est qu'il y a un risque d'un mot d'être piraté par l'ingénierie sociale et d'autres attaques non techniques.

2.6.3 Les méthodes d'authentification biométrique

Les authentifications biométriques sont de plus en plus populaires de jour en jour dans les systèmes de sécurité critiques. Les techniques biométriques dépendent de l'utilisateur et ses caractéristiques personnelles. La politique commune de biométrie comprend les empreintes digitales, reconnaissance vocale, la reconnaissance faciale, Palmaires, La forme de la main,

reconnaissance de la rétine. Chaque système de reconnaissance biométrique peut être analysé sur la base de plusieurs facteurs tels que le temps, consistance, acceptabilité, unicité, nombre de fausses alarmes, etc. Le principal inconvénient de ces systèmes est l'exigence d'un périphérique de numérisation pour l'authentification des utilisateurs, ce qui n'est pas applicable pour les utilisateurs d'Internet et à distance. Une recherche exhaustive est menée afin de simplifier les méthodes d'authentification biométrique de l'utilisateur pour le Cloud. Certains des travaux de recherche importants sont discutés ici.

Dans le domaine de l'authentification biométrique basé sur la voix, Zhu et autre [35,2011] a proposé une nouvelle approche dans laquelle un modèle d'impression pour l'authentification vocale a été utilisé. Le système d'authentification est effectué en deux étapes. En premier « La phase d'inscription » et deuxième « La phase d'appariement ». Cette méthode n'utilise que la caractéristique biométrique pour authentifier l'utilisateur. Un modèle est préférable d'employer le mot traditionnel et caractéristique biométrique pour l'authentification du client Cloud. Dans le domaine de la reconnaissance des empreintes digitales, Wang, [36,2011] a proposé un système basé sur le partage de secret des données biométriques d'empreintes digitales. Dans leur approche ils divisent et stockent dans le cadre de données d'empreintes digitales sur une carte à puce et d'une partie de celui-ci sur le serveur. Cela rend plus difficile l'attaque comme l'attaquant a besoin de briser deux clés plutôt qu'une.

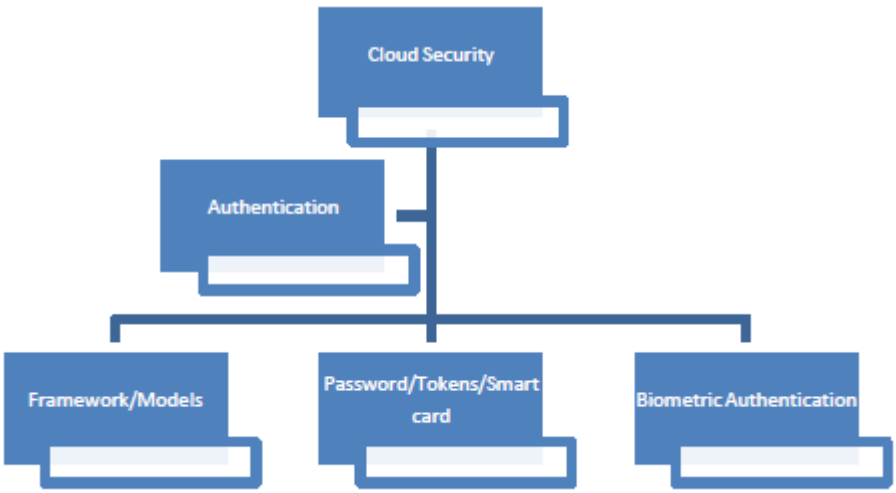

Figure 4: Orientations de recherche dans le domaine de la sécurité du Cloud Computing

2.9 L'authentification traditionnelle dans le Cloud Computing

L'authentification est l'un des aspects clés de tout système de sécurité. Un service d'authentification est la garde vigilante à l'entrée de la forteresse numérique ; sa responsabilité est de vérifier l'identité de toute partie qui demande l'entrée (c.-à-d., l'accès au système) ; il vérifie certains pouvoirs afin de s'assurer qu'une entité n'est en effet ce qu'il prétend lui-même d'être. L'authentification est utilisée pour établir la confiance dans les utilisateurs et aussi est une excellente manière de trouver l'accès aux données stockées.

Les niveaux d'assurance d'authentification devraient être selon la sensibilité de l'application, l'information de l'accès et le risque. [38].

Mécanisme	Idée	Avantages	Inconvenants
Un Framework et son application aux utilisateurs mobiles	Vérifier l'identité à partir d'un nombre de facteurs relié à l'utilisateur.	L'authentification se fait sur le comportement des clients, de sorte que le vol de l'appareil n'est pas une menace.	Le score d'authentification est vérifié par rapport à un certain seuil. Par conséquent, un meilleur résultat dépend de l'application.
ID de l'utilisateur/ mot de passe **(User ID/ Password)**	D'un pré-enregistrement d'utilisateur et votre mot de passe secret	Populaire, simple et facile à déployer	Il doit être renouvelé fréquemment
L'ouverture de session unique **(Single Sign-On)**	Une étape d'authentification pour de multiples applications.	Convivial	Toute violation de la sécurité de connexion sur plusieurs applications
mot de passe jetable **(One time Password)**	Borne. Généralement utilisée dans l'authentification multi facteur	Facile à utiliser ; Compatible avec l'authentification par mot de passe	La production et la transmission sécurisée de l'OTP est difficile
Module de confiance mobile **(Module Trusted**	Puce pour l'authentification matérielle	Optimisés pour les appareils mobiles ; faible encombrement	Le déploiement et la gestion est difficile

Mobile)			
L'authentification biométrique **(biometric Authentication)** [37]	Authentification basée sur des caractéristiques biologiques de l'utilisateur.	Les algorithmes font la voix imprimée inversible.	Taille de livre de code base de données dépend du nombre d'utilisateurs. D'où l'augmentation du nombre d'utilisateurs entraîne une augmentation de la surcharge

Tableau 2: Une comparaison des mécanismes d'authentification traditionnels avec les avantages et les inconvénients

2.10 Les protocoles d'authentification PPP (point a point protocole)

Windows Server 2003 et Windows XP prennent en charge les protocoles d'authentification PPP:

2.10.1 Protocole d'authentification PAP

Les plus anciennes formes de modèles d'authentification utilisée lorsque les droits d'accès de l'utilisateur sont envoyés en texte clair. Ce n'est pas la forme la plus sûre de transmettre des informations d'authentification comme n'importe qui peut utiliser un programme tiers sniffer et saisir ces nom d'utilisateur et mot de passe en texte clair qu'elles ne sont pas cryptées. La prochaine chose qui se passe, c'est le news d'un serveur d'être compromise en raison de l'attaque d'intrus. Éviter d'utiliser PAP autant que vous le pouvez [39].

2.10.2 Challenge-Handshake Authentication Protocol ou CHAP

CHAP est meilleur que PAP comme il utilise l'authentification cryptée mécanisme qui permettrait de protéger l'utilisateur et le mot de passe d'être envoyé si la destination NAS Server ne prend pas en charge cette méthode d'authentification. Essentiellement, Le mot de passe réel n'est pas transmis sur le réseau, Au lieu lorsque la connexion PPP est établie, le

serveur NAS envoie un mot de passe associé avec un ID de session pour le client distant. Puis le client distant utilise un MD5 (Message Digest version 5) algorithme de hachage pour répondre à la chaîne, avec l'utilisateur et une réponse à la table de hachage défi avec son pseudo , ID et mot de passe réseau.

CHAP n'est certainement pas un meilleur choix que PAP où le mot de passe est envoyé sous forme de texte en clair. Mais dans le mot de passe CHAP est mêlé à forme de hachage comme une réponse à la chaîne envoyée par le serveur NAS. Une fois la réponse à la table de hachage défi est reçue du serveur NAS qui connait déjà le mot de passe, authentifie l'utilisateur immédiatement. Défis pour l'envoi de maintien de CHAP à l'utilisateur de répondre et vérifier son identité plusieurs fois au cours de la connexion permettant une connexion plus sécurisée contre toute intrusion. L'avantage qui a CHAPpar rapport au PAP est la façon dont un utilisateur est authentifié sur un accès commuté ou une connexion PPP direct [39].

2.10.3 MS-CHAP Challenge-Handshake Authentication Protocol Microsoft

MSCHAP est un mécanisme d'authentification chiffrée qui fonctionne très similaire de CHAP. Nous avons vu lorsqu'un serveur NAS envoie un défi pour le client composé d'un ID de session et d'une chaîne de hachag au client distant puis, le défi est de retour avec l'ID de session et MD5 en fonction d'une réponse hachée. L'introduction de MD5 a donné un niveau de sécurité supplémentaire, où le texte a été remplacé par le hachage des mots de passe. MS-CHAP a donné plusieurs attributs à la transmission sécurisée de mot de passe sur le fil en ajoutant plus de code d'erreur, conscients des attributs tels que, code mot de passe expiré, prochain niveau de cryptage entre le client et le serveur qui permet à l'utilisateur de changer de mot de passe il y a tout en étant connecté au serveur NAS ou lors de processus d'authentification. Le cryptage supplémentaire entre le client et le serveur est pris en charge par l'aide d'une clé de cryptage. Le cryptage des données à l'appui par MPPE (Microsoft Point to Point Encryption)[39].

2.10.4 EAP (Extensible Authentication Protocol)

L'EAP a été récemment présenté comme le nouveau protocole d'authentification PPP basé sur MS CHAP v2. Pendant la phase d'authentification EAP n'est pas dans l'image ! C'est la plus grande différence entre l'EAP et d'autres méthodes. Le EAP n'effectue pas d'aucune sorte d'authentification, elle ne négocie de dans-fait le type EAP et l'utilisateur l'authentification se

fait par le contrôleur de domaine qui maintient l'utilisateur de la base de données, d'obtenir des informations d'identification de l'utilisateur d'une vérification par rapport à un contrôleur de domaine.

Jusqu'à ce que MS-CHAP v2, cette authentification qui se passe seulement à la NAS server avec la base de données utilisateur mais avec EAP, C'est dans une base de données utilisateur centrale titulaire ou un contrôleur de domaine uniquement.

L'EAP est un nouveau protocole d'authentification PPP qui permet une méthode d'authentification arbitraire. Une fois l'utilisateur connecté sur PPP, serveur NAS recueille immédiatement les références de l'utilisateur et les envoie à un serveur RADIUS ou contrôleur de domaine pour la vérification [39].

2.10.5 Le protocole d'authentification Kerberos « Le Service d'authentification (comme MS Exchange) »

Le premier échange de messages est un échange entre un client et le Service d'authentification (KDC). L'échange est utilisé pour obtenir un ticket et la clé de session pour une utilisation avec un serveur lorsqu'il n'y a pas de créances qui ont été obtenues au préalable. Cet échange est généralement initié par un client, habituellement au début d'une session de connexion, pour obtenir des informations d'identification pour le Service de tickets, qui peut ensuite être utilisé pour obtenir des billets pour d'autres serveurs. Dans le cas d'un serveur dont les pouvoirs ne peuvent pas être négociés à l'aide du TGS, cet échange est également utilisée pour obtenir un ticket pour un tel serveur.

Cet échange se compose de deux messages, la première étant une demande du client pour le KDC dans lequel il précise les pouvoirs qu'il veut avoir et aussi certaines options. La seconde est la réponse du KDC, contenant le ticket et la clé de session à utiliser. Les clés secrètes (habituellement tirées à partir d'un mot de passe) sont utilisés pour le chiffrement [40].

Conclusion

L'utilisation de la technologie Cloud Compting a crée un besoin de sécurisér les informations existantes dans l'espace partagé de ressources, c'est pour cela que les protocoles d'authentification ont été adaptés pour protéger et vérifier l'identité des utilisateurs

Chapitre 3 : Réduction de charges des serveurs d'authentification

3.1 Introduction

Le protocole CHAP (Challenge Handshake Authentication Protocol), défini par la RFC en 1994, est un protocole d'authentification basé sur la résolution d'un « défi » (en anglais « challenge »), c'est-à-dire une séquence à chiffrer avec une clé et la comparaison de la séquence chiffrée ainsi envoyée.

CHAP peut être utilisé dans tous types de systèmes d'authentification qui se baser sur une information secrète (réseaux de nouvelles génération (3G-4G), sites web, application Cloud)

3.2 CHAP (Challenge-HandshakeAuthentication Protocol)

C'est la forme sécurisée d'authentification cryptée à l'aide de Message Digest 5(MD5).

Message Digest 5 est un modèle de hachage normalisé, c'est à dire une méthode de transformation des données en un résultat unique qui ne peut plus retrouver sa forme d'origine.

Grâce au protocole CHAP, les connexions réseau et d'accès à distance peuvent se connecter à pratiquement tous les autres serveurs PPP de manière sécurisée [44].

3.3 Fonctionnement du protocole CHAP

● Le protocole CHAP utilise un système de défi réponse qui consiste de la part du serveur à envoyer au client une clé destinée à chiffrer le nom d'utilisateur et le mot de passe dés lors que le client fait sa demande d'accès[44].

● Avec le protocole CHAP, l'authentification se fait en cinq étapes :

- Le serveur envoie une requête contenant son nom : c'est le défi
- Le client transforme ce défi avec sa clé et l'algorithme MD-5
- Le client envoie son résultat au serveur : c'est la réponse
- Le serveur applique le même algorithme avec la clé du client, puis compare son résultat avec celui du client

- Le serveur accorde ou rejette la connexion

3.4 Les avantages et les inconvénients du protocole CHAP

3.4.1 Avantages

- CHAP assure une protection maximale grâce à l'utilisation de la méthode défi réponse.
- CHAP peut être employé pour l'authentification de systèmes différents [44].

Le fait de répéter cette méthode au cours des connexions permet de limiter le temps d'exposition à une quelconque attaque.

3.4.2 Inconvénients

- Le secret doit être disponible sous la forme de texte.
- Evolutivité difficile dans les grandes installations.
  Chaque secret doit être maintenue à chaque côté de la connexion.

Il est donc réservé à des personnes confirmées afin que la sécurité au niveau de l'authentification soit maximale [44].

3.5 Eléments du protocole

Types de messages utilisés [45]

1. Challenge
2. Response
3. Success
4. Failure

Message 'Challenge' : Principal attribut

- Le défi 'challenge' (le nonce) : une valeur aléatoire déterminée par le demandeur qui est imprévisible et unique.

Message 'Response' : Principaux attributs

A. Le nom d'usager,
B. Le MD5 (16 octets de MD5) de la chaîne identificateur, Mot de passe secret, nonce (la valeur de challenge)

Messages 'Success' ou 'Failure'

- Deux messages sans attributs (simplement typés) pour indiquer que la valeur reçue correspond à la valeur calculée ou non.

3.6 Sécurité du CHAP

- CHAP résiste aux écoutes des mots de passe ('sniffing').
- CHAP résiste aux attaques de répétition.
- CHAP ne résiste pas à une écoute puis attaque à dictionnaire.
- CHAP est incapable de résister à toute attaque de type insertion

D'un programme dans le flot des échanges qui peut aussi modifier lesmessages ('active wiretapping', 'spoofing')[45].

- CHAP est peu pratique pour une utilisation distribuée
    - Obligation de stocker les mots de passe en clair.
    - Le service d'authentification doit être réalisé dans tous les pointsd'accès à un réseau (NAS, routeurs …) => Améliorations nécessaires.
- Variante propriétaire ARAP
    - ARAP 'Appletalk Remote Access Protocol'
    - Protocole bidirectionnel (Authentification mutuelle client-serveur)
    - Avec challenge/réponse utilisant le DES pour le hachage.
- Variante propriétaire MS-CHAP ('Microsoft CHAP')

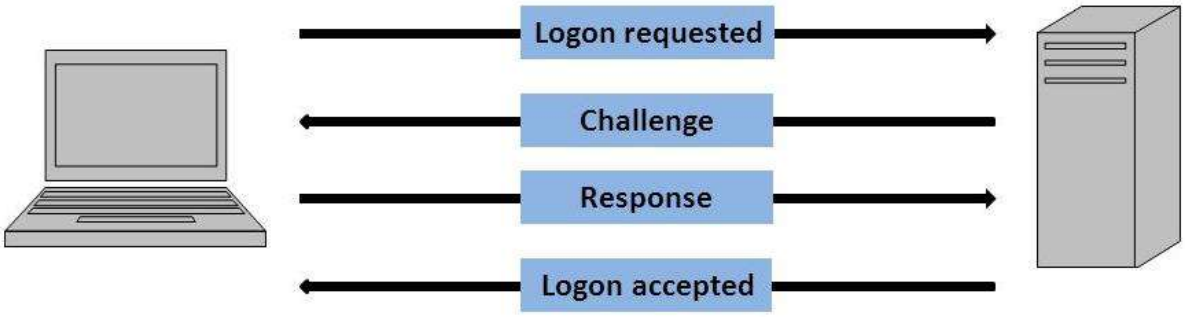

Figure 5 : Principe de fonctionnement du Protocol CHAP.

3.7 Objective

L'objective de ce chapitre est de réaliser la conception et la mise en œuvre d'une solution à l'une des inconvénients du Protocol CHAP.

La solution proposée est de réaliser un système de distribution de charge, qui va partager la charge d'un serveur d'authentification sur plusieurs serveurs.

3.8 Le langage de programmation Microsoft C#

Microsoft C# (prononcez C sharp) est un nouveau langage de programmation qui a été conçu pour permettre la création d'une large gamme d'applications d'entreprise s'exécutant sur le .NET Framework. Évolution du Microsoft C et du Microsoft C++, C# est simple, moderne, à sécurité de type et orienté objet. Le code C# est compilé en tant que code managé, c'est-à-dire qu'il bénéficie des services du Common Language Runtime (CLR). Ces services incluent l'interopérabilité entre les langages, un garbage collection et une sécurité améliorée.

C# est présenté en tant que Visual C# dans la suite Visual Studio .NET. La prise en charge de Visual C# comprend les modèles de projet, les concepteurs, les pages de propriétés, les Assistants Code, un modèle objet et d'autres fonctionnalités de l'environnement de développement. La bibliothèque de programmation de Visual C# n'est autre que le .NET Framework. [47]

3.9 L'algorithme de distribution de charge

Nous avons implémenté un algorithme de distribution de charge basé sur le nombre de sessions actives sur chaque serveur, cet algorithme distribue les demandes d'authentification dans la file (`RequettesChallenge`) en sélectionnant le serveur qui a le moins de charge.

L'instruction (`lock`) est utilisée pour déclarer une ressource critique.

```
Tant que (!stop)
{
	si (RequettesChallenge.Count > 0 )
	{
		int min = ServeursChap[0].Charge;
		int ind = 0;
		pour (int i=0; i< ServeursChap.Count; i++)
		{
			si (ServeursChap[i].Charge < min)
			{
				min = ServeursChap[i].Charge;
				ind = i;
			}
		}
		if (ServeursChap[ind].ChallengeRequests.Count < 100000)
		{
			int t = RequettesChallenge.Premier();
			RequettesChallenge.Defiler();
			lock (ServeursChap[ind].ChallengeRequests)
			{
				ServeursChap[ind].ChallengeRequests.Enfiler(t);
			}
		}
	}
	else
	{
		Thread.Sleep(1000);
	}
}
```

3.10 Conception de l'application

3.10.1 Diagramme de classes

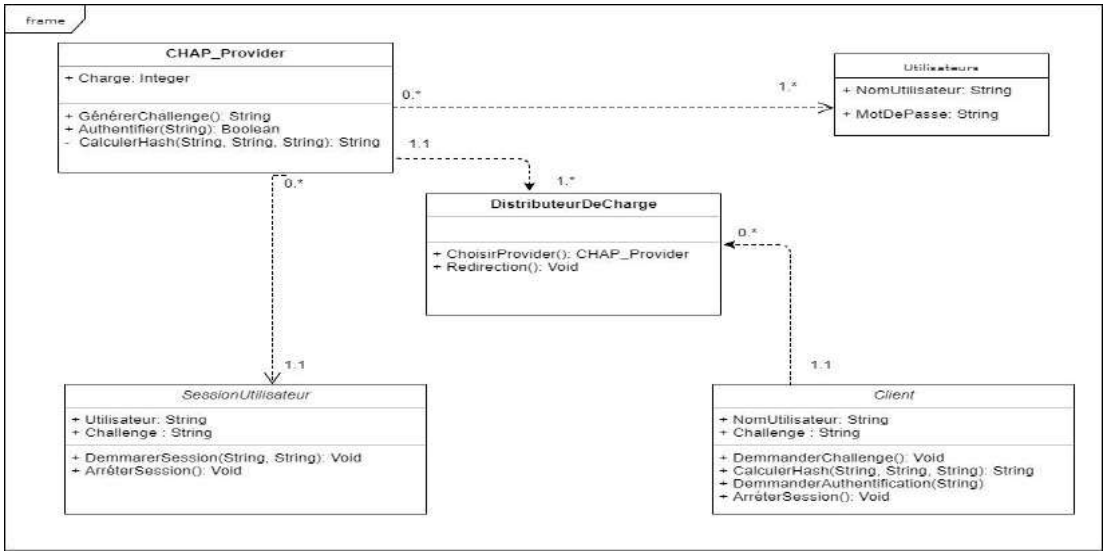

Figure 6 : Diagramme de classes

3.10.2 Diagramme d'activité

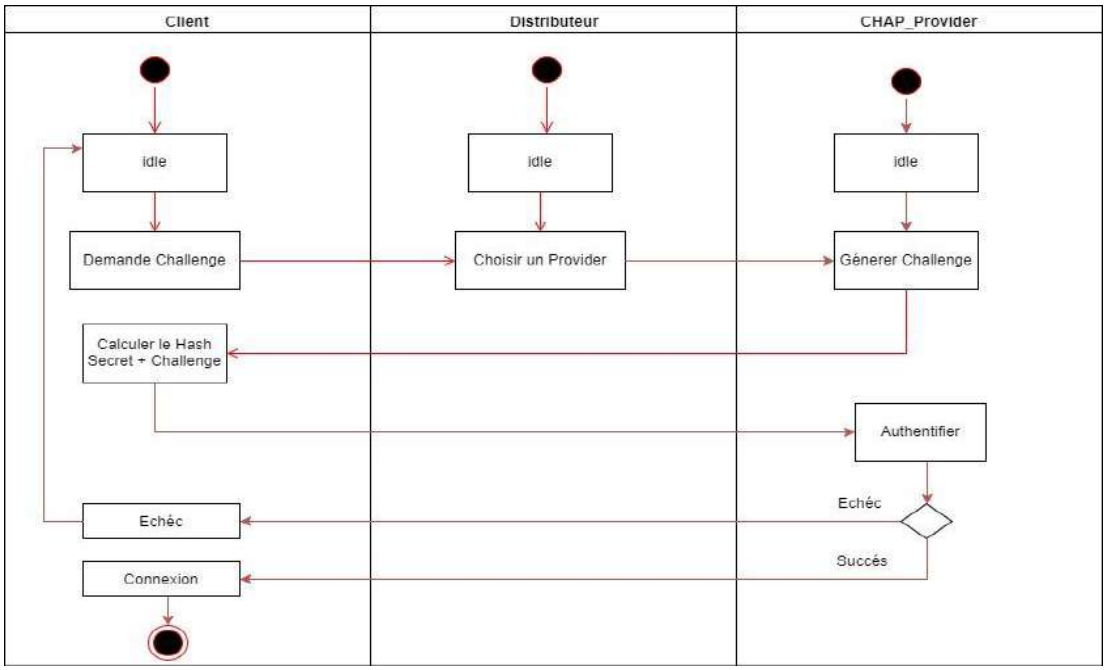

Figure 7: Diagramme d'activité

3.11 Interface d'utilisateur

Dans l'interface d'utilisateur, nous avons inclue l'état de chaque serveur d'authentification, ainsi que des statistiques relié à leur performance.

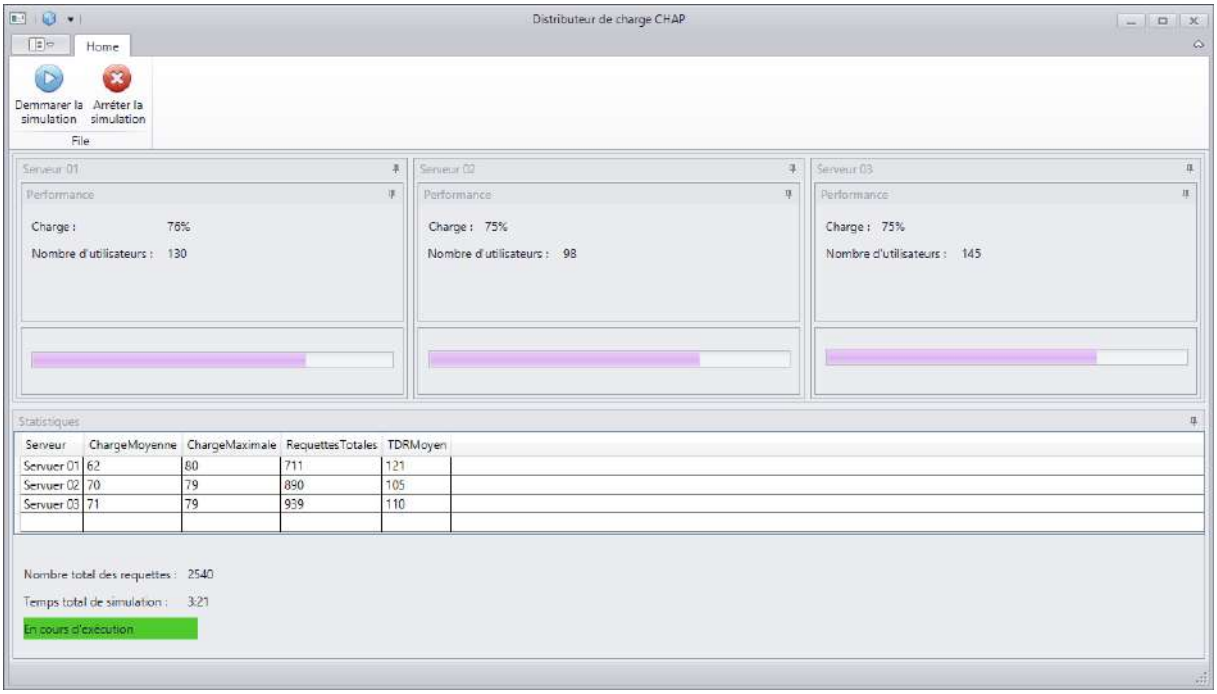

Figure 8 : Interface d'utilisateur

3.12 Analyse des résultats

Nous avons réalisé un nombre de tests pour évaluer la performance de cette solution.

La station de test se composé d'un processeur à 4 cœurs physiques (8 cœurs logiques grâce à la technologie Hyper-Threading).

3.12.1 Test 1 : Serveur d'authentification unique

Dans le premier cas, nous testons la performance de l'implémentation de l'algorithme standard de CHAP (qui utilise un seul serveur), pour une période de test de 2 minutes.

Les résultats suivants représentent les moyennes obtenues après 10 tests :

Nombre de processus	Nombre totale des requêtes traités	Temps moyen de traitement par requête	Nombre maximum de sessions concurrentes
1	460	4.35ms	311

Tableau 3: les moyennes obtenues après 10 tests

3.12.2 Test 2 : 3 Serveurs d'authentification et un distributeur de charge

Dans le deuxième cas, nous testons la performance de l'implémentation de l'algorithme standard de CHAP (qui utilise un seul serveur), pour une période de test de 2 minutes.

Les résultats suivants représentent les moyennes obtenues après 10 tests :

Nombre de processus	Nombre totale des requêtes traités	Temps moyen de traitement par requête	Nombre maximum de sessions concurrentes
3	2720	4.6ms	850

Tableau 4 : les moyennes obtenues après 10 tests

Nous observons que le nombre de requêtes traité dans la mémé période a augmenté de ~600% grâce au traitement parallèle des requêtes.

Conclusion

Dans ce chapitre, nous avons réalisé la conception et la mise en œuvre d'une solution d'un des inconvénients du protocole CHAP (Evolutivité difficile).

La solution proposé a été de réaliser un système de distribution de la charge du serveur d'authentification, sur plusieurs serveurs.

Après l'analyse des résultats, nous avons observé une amélioration dans la performance du système multiserveur de 600% en comparant avec le système mono-serveur grâce au traitement parallèle.

Il est théoriquement possible d'augmenter la performance en utilisant le traitement parallèle du CPU pour réduire le temps de hashage considérablement.

Ce travail prouve qu'il est possible d'améliorer la performance des protocoles d'authentification pour augmenter la fiabilité des applications Cloud.

Conclusion générale

L`objectif de ce mémoire est d`implémenter une stratégie de sécurité dans l`informatique des nuages (Cloud).

Dans ce travail nous présentons l'importance et les principes d'authentification des utilisateurs dans le domaine de Cloud Computing.

Dans le premier chapitre nous avons réalisé un état de l'art du Domaine de Cloud Computing, ces objectives et ces types.

Ensuite nous avons présenté les méthodes et les protocoles utilisés pour authentifier les utilisateurs ainsi que leurs avantages et inconvénients.

Enfin, nous avons réalisé une solution pour l'inconvénient de difficulté d'évolutivité dans le protocole CHAP, l'un des protocoles d'authentification les plus utilisés.

Ce travail contribue à la facilitation de l'utilisation du protocole CHAP dans les grandes installations, et à des perspectives d'implémentation dans les applications Cloud et d'amélioration de la méthode de traitement utilisé.

Bibliographie

1. **Harauz, John, Kaufinan, Lorti M. et Potter, Bruce.***Data Security in the World of Cloud Computing.* Copublished by the IEEE Computer and Reliability Societies, Kherva (Mahesana), Gujarat, India : July/August 2009.

2. **Dikaiakos, Marios D., et al.***Cloud computing : Distributed Internet Computing for IT and Scientific Research.* IEEE Internet Computing, Kherva (Mahesana), Gujarat, India : September/October 2009.

3. National Institute of Standards and Technology - Computer Security Resource Center. *www.csrc.nist.gov.* [En ligne]

4. **BEGIN, M.-E.***An egee comparative study: Grids and clouds – evolution or revolution.* EGEE III project Report, s.l. : 2008.

5. *http://en.wikipedia.orglwikilCloud_computing.* [En ligne]

6. **Wygwam.** Le Cloud Computing : Réelle révolution ou simple évolution ? *http ://www.wygwam.com/documents/cloud-computing.* [En ligne] 2015.

7. **L. Vaquero; L. Merino, J. Caceres; M. Lind;.***A break in the clouds : towards a cloud definition.* s.l. : ACM SIGCOMM Computer Communication Review.

8. NIST Definition of Cloud Computing v15. *http ://www.nist.gov/itl/cloud/upload/cloud.* [En ligne] October accédé en 2015.

9. *http://en.wikipedia.orglwikilCloud_computing.* [En ligne]

10. http://www.computerweekly.com/ArticlesI2009/02124/234988/googlemail-collapses.htm. [En ligne]

11. Are security issues delaying adoption of cloud computing ? *http://www.networkworld.com/news/2010/022210-virtualization-c1oud-security-debate.html.* [En ligne]

12. Security of virtualization, cloud computing divides IT and security pros. *http://www.networkworld.com/newsI201 0/02221 O-virtualizationc1oud-security-debate.html.* [En ligne]

13. **Vincent Kherbache and all.***Cloud Computing.* s.l. : IUT Nancy Charlemagne, 2009/2010.

14. *Le Cloud Computing, Définition et impact pour les SSII.* 2012.

15. **Pascal Sauliere.***Cloud et sécurité.* s.l. : Microsoft tech.days, 2011.

16. **Chee, Brian J.S. et Jr, Curtis Franklin.***Cloud Computing: Technologies and Strategies of the Ubiquitous Data Center.* s.l. : CRC Press, 2010.

17. **MOHAMAD HAMZE.***Autonomie, sécurité et QoS de bout en bout dans un environnement de Cloud Computing.* 07 décembre 2015.

18. **S.Marston, Z.Li, S.Bandyopadhyay, J.Zhang, A. Ghalsasi.***Cloud computing – The business perspective.* Decision Support Systems, s.l. : April 2011.

19. *Worldwide Cloud IT Infrastructure Market Growth Expected to Accelerate to 21% in 2015, Driven by Public Cloud Datacenter Expansion, According to IDC.* International Data Corporation (IDC) Worldwide Quarterly Cloud IT Infrastructure Tracker, s.l. : 2015.

20. **K.Ren, C.Wang, Q. Wang.***Security Challenges for the Public Cloud.* IEEE Internet Computing, s.l. : 2012.

21. **Hu1, Fei, et al.***A Review on Cloud Computing:Design Challenges in Architecture and Security.* Department of Electrical and Computer Engineering, University of Alabama, Tuscaloosa, AL, USA, USA : March, 2011.

22. Cloud. *https ://fr.wikipedia.org/wiki/S%C3%A9curit%C3%A9_du_-cloud#whatnewaboutcloudcomputing.* [En ligne] 2015.

23. **Zissis Dimitrios; Lekkas Dimitrios.***Addressing cloud computing security issues.* s.l. : Third IEEE International Conference on Coud Computing Technology and Science, 2012. pp. 583–592.

24. **ITU-T.***Focus Group on Cloud Computing.* 2012.

25. **W.Stallings.***Network security essentials : applications and standards.* 2005.

26. **Philippe Hedde.***LIVRE BLANC " SÉCURITÉ DU CLOUD COMPUTING ".* Paris : s.n., 2010.

27. **Chow, et al.***Authentication in the Clouds .A Framework and its Application to Mobile Users.* CCSW‟10, Chicago, Illinois, USA : 2010.

28. **Shen, Z., et al.***Cloud Computing System Based on Trusted Computing Platform.* International Conference on Intelligent Computation Technology and Automation (ICICTA), s.l. : 2010.

29. **Celesti, A., et al.***Security and Cloud Computing: InterCloud Identity Management Infrastructure.* 19th IEEE International Workshop onEnabling Technologies: Infrastructures for CollaborativeEnterprises (WETICE), s.l. : 2010.

30. **Lee, S., et al.***Two factor authentication for Cloud computing.* International Journal of KIMICS, s.l. : August 2010.

31. **Kim, J. et Hong, S.***One-Source Multi-Use System having Function of Consolidated User Authentication.* YES-ICUC, s.l. : 2011.

32. **Urien, Pascal, Marie, Estelle et Kiennert, Christophe.***An Innovative Solution for Cloud Computing Authentication: Grids of EAP-TLS Smart Cards.* Fifth International Conference on Digital Telecommunications, s.l. : 2010.

33. **Quorica.***Buisness Analysis Evolution of Strong Authentication.*

34. **A, Dinesha H.***Multi-level Authentication Technique for Accessing Cloud Services.* International Conference on Computing Communication and Applications (ICCCA), IEEE, s.l. : February 2012.

35. **Zhu, Hua-Hong, et al.***IEEE international Conference on Cloud and Service Computing on Voiceprint-Biometric Template Design and Authentication Based on Cloud Computing Security.*

36. **Wang, P., Ku, C. C; Wang, T. C;.** A New Fingerprint Authentication Scheme Based on Secret-Splitting for Enhanced Cloud Security. *www.intechweb.org.* [En ligne] 2011.

37. **Jivanadham, L. B. et YoshiakiKatayam, A.K.M. MuzahidulIslam.***Cloud Cognitive Authenticator (CCA) A Public Cloud Computing Authentication Mechanism.* IEEE, s.l. : 2013.

38. **Yadav Ankita; Nagendra Kumar;.***A Survey of Authentication Methods in Cloud computing.* 2016.

39. *PPP_Authentication_Protocols in cloud.* 11 MARS 2016.

40. **Sven Groot.***The Kerberos Authentication Protocol.* 23 June 2005.

41. **CVE Details.** The ultimate security vulnerability datasource. *http://www.cvedetails.com/browse-by-date.php.* [En ligne] 30/06/15.

42. **Netmedia - Enjeux IT.** Où en sont les DSI en région en 2014. *http://www.vmwaretour2014.com/IMG/pdf/pleniere_vmware_tour_2014.pdf.* [En ligne] 30/06/15.

43. **PAC CloudIndex.** Le niveau de maturité Cloud des organisations françaises a franchi un palier. *http://www.cloudindex.fr/content/tous-les-résultats.* [En ligne] 30/06/15.

44. **Hicham RICHA.***Mot de passe sécurisé, systèmes d'authentification S/Key et par jeton de contrôle, protocoles d'authentification pour PPP : PAP, CHAP et EAP*. France : Institut des Sciences Cognitives , 2016.

45. **Florin Gérard.***Sécurité des niveaux liaison et réseau Réseaux Privés Virtuels 'RPV' VPN 'Virtual Private Networks'.* suisse : Laboratoire CEDRIC, 2001.

46. **Florent Nolot.***Les principes de la sécurité.* Paris : université de reims champagne-ardenne.

47. https://msdn.microsoft.com/fr-fr/library/aa287558(v=vs.71).aspx *(05/07/2017)*

Liste Des Abréviations

VPN:VirtualPrivate Network

« Réseau privé virtuel **»**

NIST: National Institute of Standards and Technology

« Institut national des normes et de la technologie »

AWS: Amazon Web Service

« Service Web Amazon »

IBM: International Business Machines Corporation

« International Business Machines Corporation »

IaaS:infrastructure as a service

«Infrastructure en tant que service »

PaaS: Platform as a service

« Plate-forme en tant que service »

Saas:software as a service

« Logiciel en tant que service »

ASP: Application Service Provider

« Fournisseur de services application »

QoS: Quality of Service

« Qualité de service »

CSP: Cloud Service Provider

« Fournisseur de services Cloud »

CSU: Cloud Service User

« Utilisateur de services Cloud »

VM: Virtual Machine

« Machine virtuelle »

EC2: Amazon Elastic Compute Cloud

« Amazon Elastic Compute Cloud »

API: Application Programming Interface

« Interface de programmation d'application »

PKI: Public Key Infrastructure

« Infrastructure à clés publiques »

USB: Universal Serial Bus

« Bus Universel en Série »

PPP: Point-to-Point Protocol

« Protocole point à point »

PAP: PasswordAuthentication Protocol

« Protocole d'authentification par mot de passe »

CHAP: Challenge Handshake Authentication Protocol

« Protocoled'authentification de Handshake Challenge »

NAS: Network Attached Storage

« Serveur de stockage en réseau »

MD5: Message Digest 5

« Message Digest 5 »

MS-CHAP: Microsoft-Challenge-Handshake Authentication Protocol

« Microsoft-Challenge-Handshake Authentication Protocol »

MD4: Message Digest4

« Message Digest 4 »

MPPE: Microsoft Point to Point Encryption

« Microsoft Point to Point Encryption »

EAP: ExtensibleAuthentication Protocol

« Protocole d'authentification extensible »

RADIUS: RemoteAuthentication Dial-In User Service

«Service à distance d'authentification à distance»

KDC: Key Distribution Center

« Centre de distribution de clés »

TGS: Ticket Granting Service

« Service d'attribution de billets »

ARAP: Appletalk Remote Access Protocol

« Protocole d'accès à distance Appletalk »

Résumé

Dans ce mémoire on a étudié les enjeux de la sécurité dans le cloud computing, nous nous somme basés sur l`authentification comme solution de sécurité. Le protocole CHAP (Challenge Handshake Authentication Protocol) a été utilisé. On a amélioré le protocole CHAP afin de permettre une meilleure évolutivité à l'aide d'un module de distribution de charge. Nous avons implémenté notre application en utilisant le langage C# et .NET Framework.

Grâce à l'exploitation du processeur multi-cœurs et la technologie Hyper-Threading, nous avons réalisé une augmentation importante dans la performance du protocole CHAP jusqu'à 600%.

Mots clés : Cloud Computing, sécurité, attaques, protocole d`authentification, CHAP.

Abstract

In this brief we studied the stakes of security in the cloud computing, we rely on the authentication as solution of security. The Challenge Handshake Authentication Protocol (CHAP) was used. The CHAP protocol has been improved to allow for better scalability with a load distribution module. We implemented our application using C # and .NET Framework.

Thanks to the use of the multi-core processor and the Hyper-Threading technology, we have achieved a significant increase in CHAP performance up to 600%.

Keywords: Cloud computing, security, attacks, authentication protocol, CHAPS

ملخص

فيهذهالورقةدرسنامجالالأمنفيالحوسبةالسحابية،وركزنا علىالمصادقة كحل لضمان الحماية، استعملنا بروتوكول CHAP (Challenge-HandshakeAuthentication Protocol) بعد تحسينه لحل مشكلة قابلية التوسع باستخدام وحدة لتوزيع الضغط، انجزنا هذا البرنامج باستعمال لغة C# و .NET Framework.

بفضل إستغلال المعالجات متعددة النواة و تقنية Hyper-Threading تمكننا من الحصول على ارتفاع في أداء البروتوكول بنسبة تصل إلى 600%.