République Algérienne Démocratique et Populaire
Ministère de l'enseignement supérieur et de la recherche scientifique
Université Larbi Tébessi - Tébessa
Faculté des Sciences Exactes et des Sciences de la Nature et de la Vie
Département : Mathématiques et Informatique

Mémoire de fin d'étude
Pour l'obtention du diplôme de MASTER
Domaine : Mathématiques et Informatique
Filière : Informatique
Option : Réseau et sécurité informatique

Thème

Un Framework de sécurité pour les applications du mobile cloud computing

Présenté Par :
Asma
Boumendjel

Devant le jury :

Mr Derdour Makhlouf	*MCA*	*Univérsité Larbi Tébessa*	*Président*
Mr Samir Tag	*MAA*	*Univérsité Larbi Tébessa*	*Examinateur*
Mr Mohamed Amroune	*MCA*	*Univérsité Larbi Tébessa*	*Encadreur*

Date de soutenance : 22/06/2019

Résumé:

La poussée incessante des activités de recherche visant à accroître les capacités des appareils mobiles aux ressources limitées, en exploitant des ressources Cloud hétérogènes, ont créé une nouvelle impulsion en matière de recherche appelée mobile Cloud computing. Cependant, cette relocalisation rapide dans le Cloud a alimenté des problèmes de sécurité et de confidentialité, les données des utilisateurs quittant la sphère de protection de leurs propriétaires pour entrer dans le Cloud.

Des efforts importants ont été déployés dans les universités et les milieux de la recherche consacrent leurs efforts à l'étude et à la création de framework sécurisés dans un environnement en nuage, mais il existe un déficit de solutions pour une étude approfondie des frameworks de sécurité dans un environnement en nuage mobile. Nous mettrons en évidence les problèmes de sécurité actuels dans l'environnement et l'infrastructure en Cloud computing mobile , étudierons divers framework de sécurité des données et fournirons une taxonomie des framework de sécurité des données à la pointe de la technologie, ainsi qu'une connaissance approfondie des questions de recherche ouvertes pour assurer la sécurité et la confidentialité des données dans plate-forme informatique en nuage mobile.

Notre travail consiste à construire un framework de sécurité pour le mobile Cloud computing. Ce framework combine des techniques de sécurité comme le cryptage pour la sécurisation des données et un réseau de neurones convolutionnel pour l'authentification via la reconnaissance faciale.

Mot clés: mobile cloud computing, framework, reconnaissance facial, sécurité, deep Learning

Abstract:

The relentless push for research to increase the capabilities of resource-constrained mobile devices by leveraging heterogeneous cloud resources has created a new research impulse called mobile cloud computing. However, this rapid relocation to the cloud has fueled security and privacy issues as users' data leaves the protection sphere of their owners to enter the cloud. Major efforts have been made Universities and research communities are devoting their efforts to the study and creation of secure frameworks in a cloud environment, but there is still a research gap for an in-depth study of security frameworks in a mobile cloud environment.

We will highlight current security issues in the mobile Cloud environment and infrastructure, investigate various data security frameworks, and provide taxonomy of state-of-the-art data security frameworks, as well as In-depth knowledge of open research questions to ensure data security and privacy in a mobile cloud computing platform.

Our job is to build a security framework for mobile Cloud computing this framework combines security techniques such as encryption for data security and a convolutional neural network for authentication via face recognition.

Key words: mobile cloud computing, framework, facial recognition, security, deep Learning .

ملخّص:

إنّ الضّغط الذّؤوب للبحوث من أجل زيادة قدرات الأجهزة المحمولة محدودة الموارد من خلال الاستفادة من الموارد السّحابيّة غير المتجانسة قد خلق دفعة بحثيّة جديدة تسمّى الحوسبة السّحابية المتنقّلة. ومع ذلك، فقد أدّى هذا النّقل السّريع إلى السّحابة إلى إثارة مشكلات تتعلّق بالأمان والخصوصيّة لأنّ بيانات المستخدمين تترك مجال حماية أصحابها لتدخل إلى السّحابة.لقد بذلت جهود كبيرة من قبل الجامعات ومجتمعات البحث التي تكرّس جهودها لدراسة وإنشاء أطر آمنة في بيئة سحابيّة ، ولكن رغم ذلك هناك فجوة في البحوثات لإجراء دراسة متعمّقة للأطر الأمنيّة في بيئة سحابيّة متنقّلة.ولذلك سنقوم بتسليط الضوء على مشكلات الأمان الحالية في بيئة البنى السّحابية المتنقلة والبنية التّحتية،وسنبحث في مختلف أطر أمان البيانات ، ونوفر تصنيفًا لأطر عمل أمان البيانات المتطورة ، وكذلك سنوفّر معرفة متعمقة للأسئلة المفتوحة في الأبحاث المتعلقة بضمان أمن البيانات والخصوصية في منصّة الحوسبة السّحابية المتنقّلة.عملنا يتمثل في بناء إطار أمان للحوسبة السّحابية المتنقّلة. يجمع هذا الإطار بين تقنيات الأمان مثل التّشفير لأمان البيانات والشّبكة العصبيّة التلافيفيّة للمصادقة وتحديد هويّة المستخدمين عبر التعرف على الوجه.

كلمات مفتاحيّة : الحوسبة السّحابية المتنقّلة, الإطار, التعرف على الوجه,الأمن,التعلم العميق.

Remerciements

Je tiens à remercier ma mère de
m'avoir encouragé durant toute la durée de mes études et de m'avoir apporté un soutien indispensable à ma réussite.
Je tiens avant tout à exprimer ma profonde gratitude, mes sincères remerciements et ma haute considération à mon encadreur de PFE le professeur monsieur Mohamed Amroune, professeur à l'université chikh laarbi tebessi pour ses bons conseils sans lesquels il m'aurait été impossible de mener à terme ce projet de recherche.

Liste des figures

Table des matières

Introduction Générale

Depuis sa création, le paradigme de Cloud computing a acquis une grande popularité dans l'industrie et le monde universitaire [67]. L'accès économique, évolutif, opportun, omniprésent et à la demande aux ressources partagées sont certaines des caractéristiques du Cloud qui ont entraîné le transfert des processus métier vers le Cloud. Le Cloud computing attire l'attention de la communauté des chercheurs en raison de son potentiel à offrir des avantages considérables à l'industrie et à la communauté [67][68][69]. Les ressources sont fournies aux utilisateurs et libérées en fonction des demandes du pool de ressources partagées [67]. L'approvisionnement en ressources à la demande assure l'allocation optimale des ressources et est également rentable [67]. Les consommateurs (particuliers et organisations professionnelles) n'ont plus besoin d'investir beaucoup dans l'infrastructure des technologies de l'information (TI) [67]. Les clients utilisent les ressources fournies par le Cloud et paient en fonction de l'utilisation. D'autre part, les fournisseurs d'informatique en nuage peuvent réutiliser des ressources dès qu'elles sont libérées par un utilisateur particulier, ce qui améliore l'utilisation des ressources.

La sécurité est l'un des plus gros obstacles qui entravent l'adoption du Cloud computing Plusieurs entreprises et organisations de recherche hésitent à faire totalement confiance au Cloud computing pour transférer leurs données aux fournisseurs de services tiers [70]. de nombreuses solutions ont été apportées pour résoudre les problèmes de sécurité dans le Cloud computing uniquement pour assurer un niveau de confort d'utilisation des ressources Cloud, chacune de ces solutions a traité un problème de sécurité ou une faille dans le système Cloud, de nombreux frameworks de sécurité ont également été développés et fournis objectifs de sécurité tels que confidentialité , sécurité du stockage des données, authentification et intégrité, etc.

La structure du mémoire :

nous avons divisé le mémoire en deux parties: le premier comprend les chapitres 1 et 2 dans lesquels nous allons parler en détail de mobile Cloud computing, de sa définition, de son architecture et comprendre les problèmes de sécurité le concernant, ainsi que de l'état de l'art des solutions et des cadres existants, Dans la deuxième partie, chapitre3, nous allons présenter notre contribution qui consiste en un framework de sécurité qui assure l'authentification des utilisateurs et la sécurité du stockage des données dans le Cloud.

Partie1 : état de l’art

Chapitre1 : dans ce chapitre, nous verrons tous les aspects du Cloud computing, comprendrons ce qu'est le Cloud computing, son architecture, ses types, ses services, ses modèles, ses fonctionnalités, ses applications, ses avantages et, enfin, nous terminerons par une conclusion

Chapitre 2 : dans ce chapitre, nous aborderons les problèmes de sécurité dans le Cloud computing et les travaux existants.

Partie 2 : Contribution

Chapitre 3 : Dans ce chapitre, nous présenterons notre système qui est un cadre de sécurité qui authentifie et vérifie l’identité des utilisateurs du cloud et assure la sécurité du stockage des données.

Chapitre 1

Mobile cloud computing

1. Introduction :

Le concept Cloud computing mobile est relativement nouveau dans la recherche. Il apporte divers avantages pour les appareils mobiles car il permet l'utilisation de ressources et de services Cloud. Au cours des cinq dernières années, les services Cloud, qui étaient auparavant perçus comme une solution risquée adaptée aux services non essentiels, étaient désormais répandus dans la grande majorité des entreprises ayant une impact sur la grande majorité de leurs fonctions.[33]

Selon une étude récente réalisée en 2017 par Forrester Press Les plates-formes de Cloud public, les services métiers et les applications atteindront 236 milliards de dollars, avec un CAGR (Compound annual growth rate) croissant de 22% entre 2015 et 2020. Le marché des applications de Cloud computing augmentera plus rapidement, avec un total de 17% supérieur à celui de 2014.[34] Aussi Les analystes d'IDC (international data corporation) ont également déclaré qu'au moins la moitié des dépenses informatiques seraient basées sur le Cloud en 2018, atteignant 60% de toutes les infrastructures informatiques et 60 à 70% de toutes les dépenses en logiciels, services et technologies d'ici 2020. Il est également prédit que la même année, le Cloud sera le mécanisme de diffusion préféré des analyses. [34]

2. Cloud computing :

2.1. Historique de Cloud computing :

Le Cloud computing est l'une des technologies les plus innovantes de notre époque. Vous trouverez ci-dessous un bref historique du Cloud computing.

Au début des années 1960 L'informaticien John McCarthy a mis au point le concept de partage du temps, qui permet à l'Organisation d'utiliser simultanément un ordinateur central coûteux.

En 1969 L'idée d'un «réseau informatique intergalactique» (concept de réseau informatique semblable à celui d'Internet actuel) a été introduite par J.C.R. Licklider, responsable du développement d'ARPANET (réseau d'agences de projets de recherche avancée). Sa vision était que tous les peuples du monde soient interconnectés et puissent accéder aux programmes et aux données de n'importe quel site, de n'importe où. [35]

En 1970, l'utilisation de logiciels de virtualisation tels que VMware est apparue. Il devient possible d'exécuter simultanément plusieurs systèmes d'exploitation dans un environnement isolé. Après cela, en 1997, le terme «Cloud computing » a été défini pour la première fois par le professeur Ramnath Chellappa à Dallas en 1997 comme «un paradigme informatique où être déterminé par une logique économique plutôt que par des limites techniques. "[35]

Maintenant que Cloud computing est devenue une réalité, elle était adoptée par des fournisseurs tels que

Salesforce et Amazon de 1999 à 2014, jusqu'à maintenant.la figure ci-dessous résume tout sur l'histoire du Cloud computing :

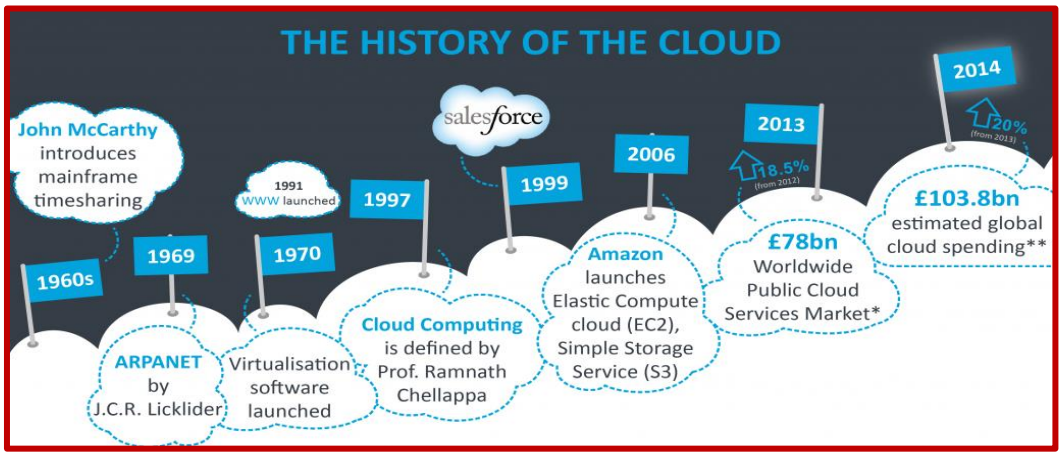

Figure 1 : historique de Cloud computing [35].

2.2. Définition de Cloud computing :

Imaginez vous cette scénario : si vous voulez regarder un film sur Netflix, vous allez Juste besoins d'un navigateur dans votre pc et d'une connexion internet rien d'autre, tout simplement parce que l'ensemble des films dont vous avez la disposition sont hébergé chez Netflix, et Netflix vous met a disposition un catalogue des films à la demande sous forme des services dont vous payer l'abonnement .c'est similaire au Cloud computing,

« En effet, le Cloud est la fourniture de services technologiques de toutes sortes (e mail, stockage, outils bureautiques, CRM,...) immédiatement et sur demande.il permet d'utiliser des moyens technologiques inédits jusqu'à présent en raison de sa souplesse » [3].

2.3. Les composants de Cloud computing :

Le Cloud computing comprend des clients, des centres de données et des serveurs Distribués [18].

- **Clients:** utilisateurs tels que des ordinateurs, des ordinateurs portables, des tablettes, des téléphones portables ou des assistants numériques personnels(PDAS).
- **Centres de données:** Il s'agit d'un ensemble de serveurs sur lesquels l'application est hébergée. La virtualisation est faite où
  plusieurs instances de serveurs virtuels sont créées.
- **Serveur distribué:** Serveurs qui ne résident pas localement et qui sont géographiquement éloignés.

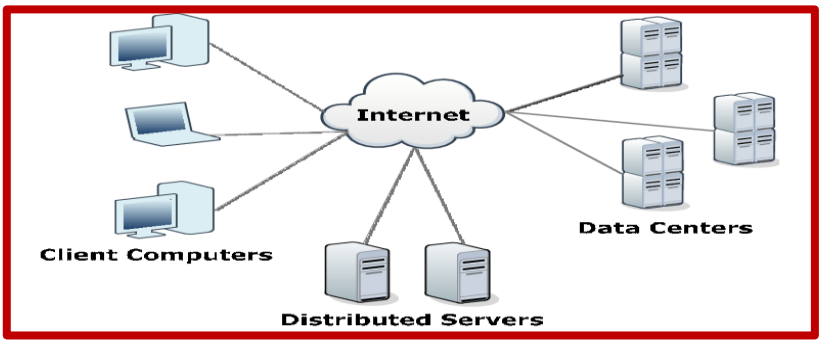

Figure 2 : les composants de Cloud computing [37]

2.4. Caractéristiques principale :

NIST (National Institute of Standards and Technology) a définit le Cloud computing autour de 5 points essentiels [32] :

- **Sur demande :** Un consommateur peut provisionner unilatéralement des capacités informatiques, telles que le temps du serveur et le stockage réseau, selon son besoins automatiquement sans nécessiter d'interaction humaine avec chaque fournisseur de services.
- **Large accès au réseau :** Les fonctionnalités sont disponibles sur le réseau et accessibles via des mécanismes standard qui favorisent l'utilisation de plates-formes client hétérogènes ou épaisses (par exemple, téléphones mobiles, tablettes, ordinateurs portables et stations de travail).
- **Mise en commun des ressources (resource pooling) :** les ressources informatiques du fournisseur sont mises en commun pour servir plusieurs consommateurs à l'aide d'un modèle multi-locataire, différentes ressources physiques et virtuelles étant affectées et réaffectées de manière dynamique en fonction de la demande des utilisateurs. le client n'a généralement aucun contrôle ni aucune connaissance sur l'emplacement exact des ressources fournies mais peut éventuellement spécifier l'emplacement à un niveau d'abstraction supérieur (par exemple, pays, état ou centre de données). Les exemples de ressources incluent le stockage, le traitement, la mémoire et la bande passante du réseau.
- **Élasticité rapide:** les capacités peuvent être provisionnées et libérées de manière élastique, dans certains cas automatiquement, pour s'adapter rapidement à la demande. Pour le consommateur, les fonctionnalités disponibles pour le provisionnement semblent souvent illimitées et peuvent être adaptées à n'importe quelle quantité à tout moment.
- **Service mesuré :** L'utilisation des ressources peut être surveillée, contrôlée et rapportée, offrant une transparence à la fois au fournisseur et au consommateur du service utilisé. Il est important que toutes les conditions, garanties et garanties de service soient indiquées dans le Contract SLA (Service Level Agreement).

2.5. Les modèles de service :

Il ya 3 modèle d'utilisation du Cloud computing et chacun de ces modèle joue un rôle spécifique [3] :

2.5.1. Software as a Service (SaaS) :

Fournit des applications prêtes à l'emploi, s'exécutant sur l'infrastructure de fournisseur Cloud et accessibles via le navigateur du client. Exemple de cas d'usage est l'accès à des applications en ligne de messagerie ou bureautique.et évidement les utilisateurs finaux sont la population cible de SaaS.

2.5.2. Platform as a Service (PaaS) :

Fournit en plus de l'infrastructure technique comme le IaaS des composants logiciels intégrés comme l'instance des middlewares et des contextes d'exécution, par exemple des serveurs d'application ou des bases de données. Dans ce model le client doit gérer l'ajout des applicatifs, cette offre permet de se focaliser sur le développement des applications.les développeurs sont donc la population cible.

2.5.3. Infrastructure as a Service (IaaS) :

Correspond à la partie infrastructure du Cloud plus concrètement il fournit des instances d'OS et l'infrastructure sous-jacent comme(les serveurs, les réseaux, stockage…) comme exemple de cas d'usage on a par exemple la mise a disposition d'une VM temporaire pour les tests ou une augmentation d'espace de stockage. Dans ce modèle l'utilisateur de service doit gérer l'ajout des middlewares et des applicatifs le rest est géré par le fournisseur Cloud.vue le cas d'usage on voie que la population cible de IaaS sont les exploitants informatiques. La Figure ci-dessous représente les différentes couches du Cloud computing de la couche la moins visible pour les utilisateurs finaux à la plus visible.

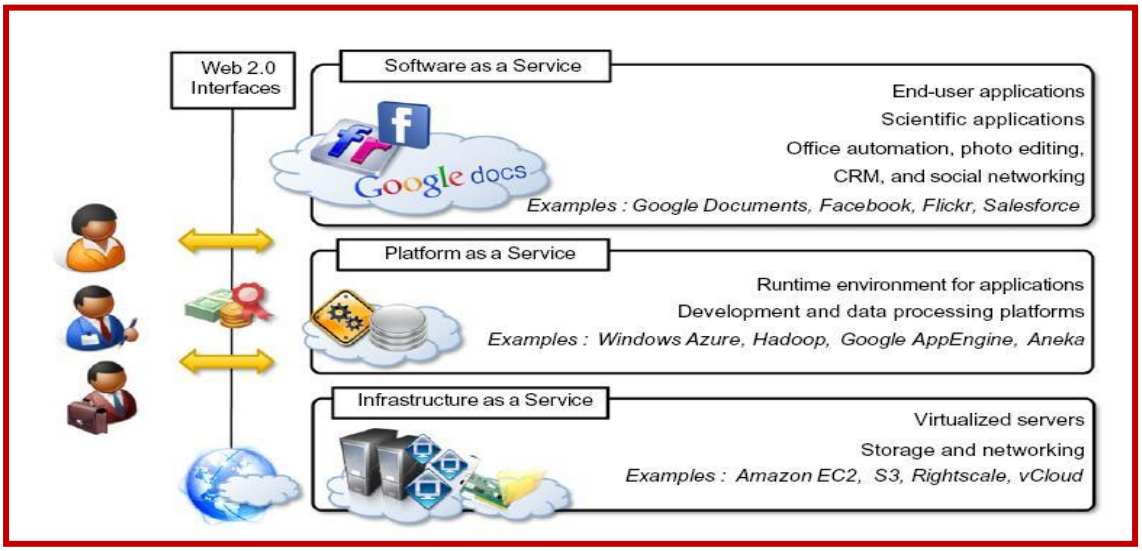

Figure 3 : les 3 couches du Cloud computing [15]

2.6. Les quatre modèles de déploiement :

2.6.1. CLOUD PRIVE :

« Ces ressources physiques peuvent être hébergées dans une infrastructure propre à l'entreprise et étant sous son contrôle, à sa charge donc de contrôler le déploiement des applications.
L'infrastructure peut être placée dans les locaux de l'organisation ou à l'extérieur. Le Cloud privé peut aussi désigner un Cloud déployé sur une infrastructure physique dédiée et mise à disposition d'un fournisseur de services. » [4]

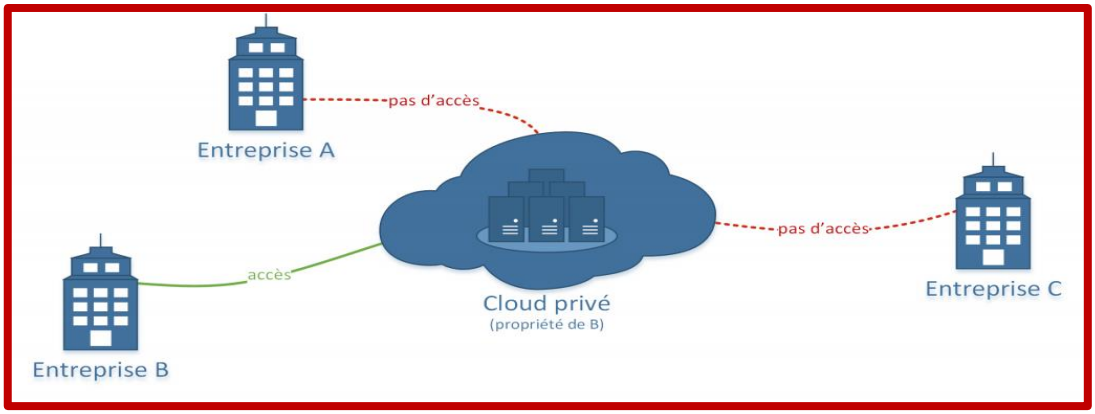

Figure 4 : Cloud privé [36]

2.6.2. CLOUD PUBLIC

« L'infrastructure Cloud est ouverte au public ou à de grands groupes industriels. Cette infrastructure est possédée par une organisation qui vend des services Cloud. Pour les consommateurs, il n'y a donc aucun investissement initial fixe et aucune limite de capacité. Les fournisseurs de Cloud public facturent à l'utilisation et garantissent une disponibilité de services au travers des contrats SLA. » [4].

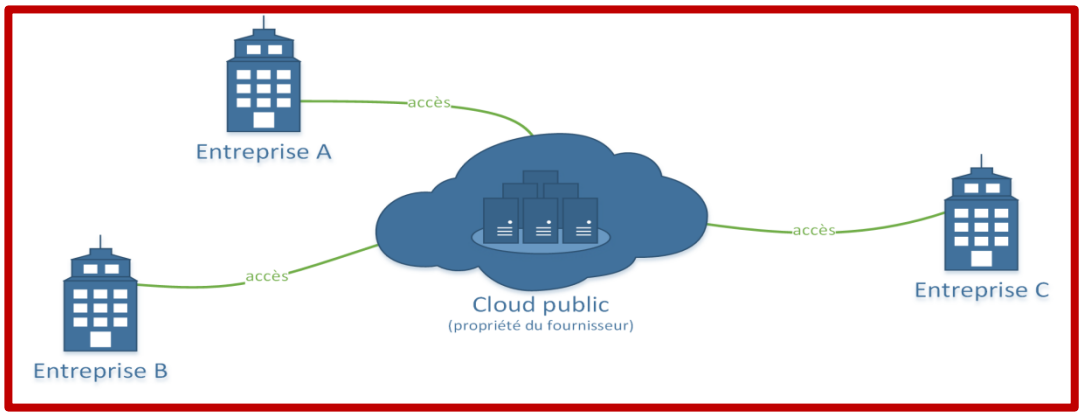

Figure 5 : Cloud public [36]

2.6.3. CLOUD HYBRIDE

« Un Cloud Hybride est l'utilisation de plusieurs Clouds, publics ou privés. Ces infrastructures sont

liées entre elles par la même technologie qui autorise la portabilité des applications et des données. C'est une excellente solution pour répartir ses moyens en fonction des avantages recherchés. » [4].

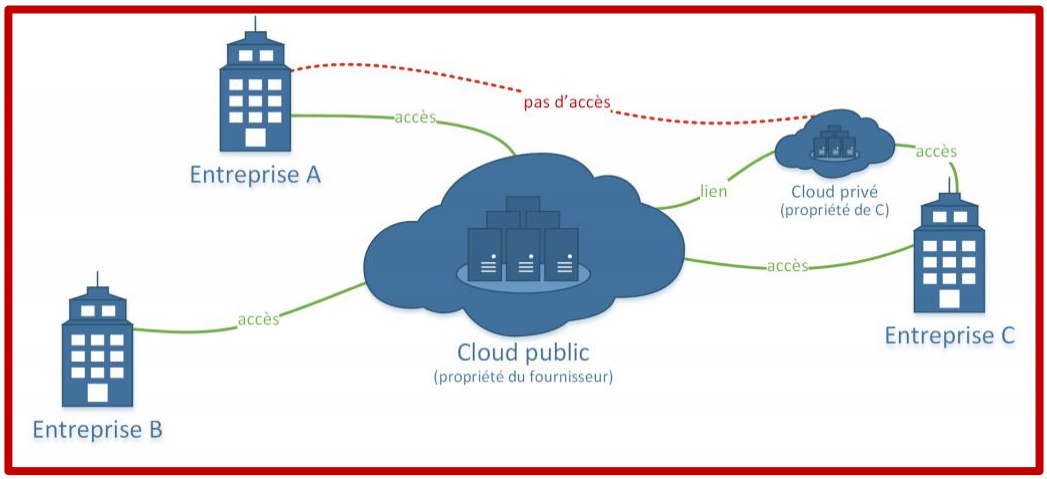

Figure 6 : Cloud hybride [36]

2.6.4. Les Clouds communautaires

« Les Clouds communautaires offrent une infrastructure qui est partagée par plusieurs organisations et prend en charge une communauté spécifique. Ils peuvent être gérés par ces organisations ou par un tiers et peuvent exister dans, ou hors des, locaux de celles-ci ». [4]

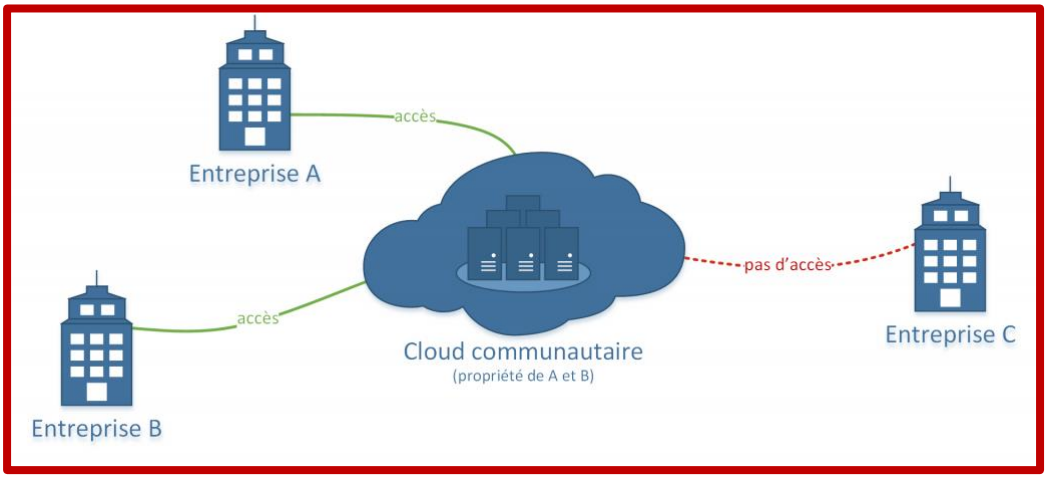

Figure 7 : Cloud communautaire [36]

2.7. Les acteurs du Cloud :

L'architecture de référence du Cloud computing définie par Nist regroupe cinq acteurs différents liés au Cloud computing: consommateur, fournisseur, auditeur, courtier, opérateur .la figure (8) les résume [45] :

- **Fournisseur Cloud :** Personne, organisation ou entité chargée de mettre un service à la disposition des parties intéressées.

Un fournisseur d'informatique en Cloud acquiert et gère l'infrastructure informatique nécessaire à la fourniture des services, exécute le logiciel d'informatique en nuage qui fournit les services et prend les dispositions nécessaires pour fournir les services en nuage aux utilisateurs d'informatique en Cloud par le biais d'un accès réseau.

- **Consommateur Cloud :** Une personne ou une organisation qui entretient une relation commerciale avec les fournisseurs de services Cloud et utilise le service de ces fournisseurs.

  Un consommateur du Cloud parcourt le catalogue de services proposé par le fournisseur Cloud, demande le service approprié, établit des contrats de service (SLA) avec le fournisseur de service et utilise le service. Le client en Cloud peut être facturé pour le service fourni et doit organiser les paiements en conséquence. "

- **Auditeur Cloud :** Un auditeur dans le Cloud est une partie pouvant effectuer un examen indépendant des contrôles des services dans le Cloud avec l'intention d'exprimer une opinion à ce sujet. Des audits sont effectués pour vérifier la conformité aux normes en examinant des preuves objectives.

  Un auditeur de Cloud peut évaluer les services fournis par un fournisseur du Cloud en termes de contrôles de sécurité, d'impact sur la confidentialité, de performances, etc.

- **Courtier Cloud(Cloud Broker) :** Au fur et à mesure que l'informatique en Cloud évolue, l'intégration des services en nuage peut s'avérer trop compliquée à gérer. Un consommateur en Cloud peut demander des services en Cloud à un courtier en Cloud au lieu de contacter directement un fournisseur de Cloud. Par conséquent, le courtier est une entité qui gère l'utilisation, les performances et la fourniture de services de Cloud computing, et négocie les relations entre les fournisseurs de cloud et les consommateurs de Cloud. "

- **Opérateur Cloud (Cloud carrier) :** Un intermédiaire qui fournit la connectivité et le transport des services de Cloud computing des fournisseurs aux consommateurs. Les opérateurs de Cloud offrent un accès aux consommateurs via des réseaux, des télécommunications et d'autres dispositifs d'accès.

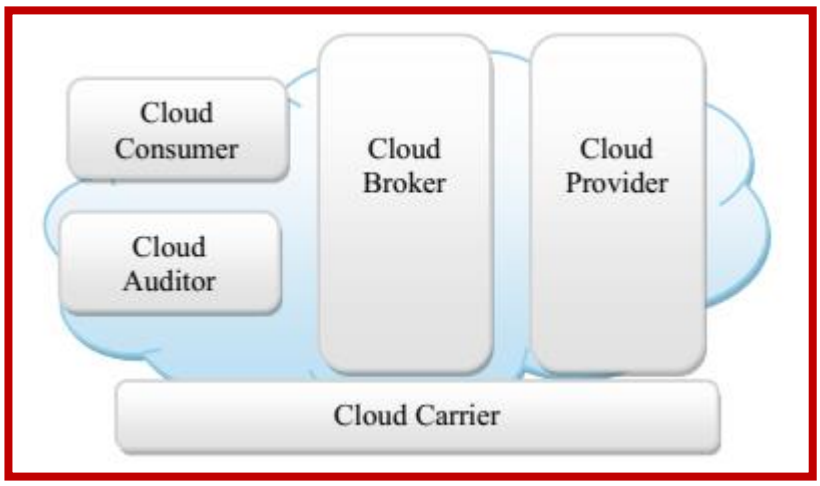

Figure 8 : Les acteurs de Cloud computing [45]

2.8. Les principaux fournisseurs de services dans le Cloud computing :

Selon l'enquête annuelle sur l'état du Cloud réalisée par RightScale en 2018 auprès de 997 professionnels de l'informatique (Figure 9), Amazon Web Services reste le leader des fournisseurs d'infrastructure Cloud. Cependant, des entreprises comme Microsoft Azure, Google Cloud et IBM Cloud rattrapent rapidement leur retard: selon l'enquête, 45% des répondants utilisent déjà leurs applications sur Azure, 18% sur Google Cloud et 10% sur IBM Cloud, tandis que de nombreux autres sont encore sur la phase d'expérimentation. [44]

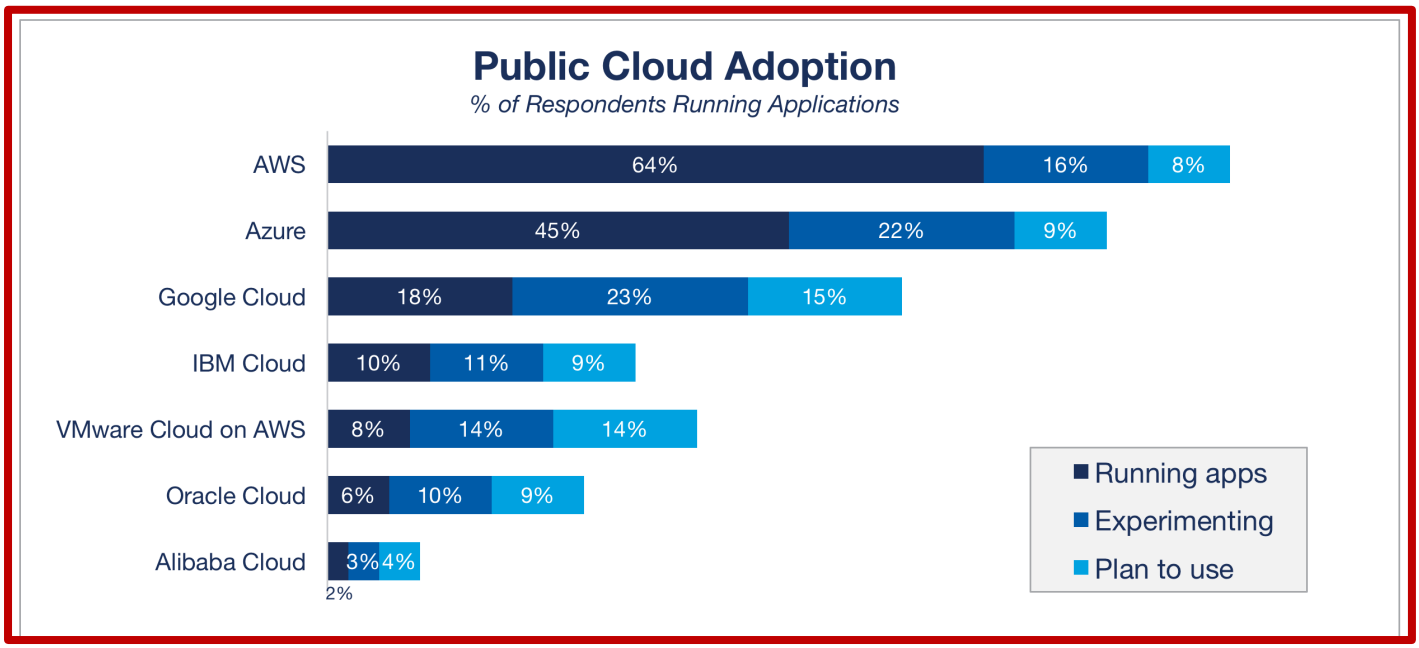

Figure 9: les tops fournisseurs de services en 2018 [44].

Dans ce qui suite on va discuter Les principaux fournisseurs de service selon leur classement : Amazon, Microsoft, IBM, Google, Salesforce [10] [39].

2.8.1. Amazon :

« Amazon Web Services » (AWS) Aujourd'hui propose de nombreux services en ligne, à commencer par l'IaaS probablement le plus connu : Elastic Compute Cloud (EC2). « Amazon EC2 présente un environnement informatique vraiment virtuel, vous permettant d'utiliser des interfaces de service Web pour lancer des instances avec une variété de systèmes d'exploitation, de les charger avec votre environnement d'applications personnalisées, de gérer les autorisations d'accès à votre réseau, et d'exécuter votre image en utilisant autant ou aussi peu de systèmes que vous le désirez. Amazon propose également des services PaaS avec « Amazon Simple Storage » (Amazon S3), un service de stockage en ligne. Et de nombreux autres services mentionnons rapidement Amazon SQS un système de gestion de files d'attentes pour stocker les messages alors qu'ils se déplacent entre les ordinateurs, Amazon DynamoDB qui permet de créer en quelques clics une base de données NoSQL (non-relationnel).

2.8.2. Microsoft : Microsoft a créé sa plate-forme hybride Azure, regroupant trois grandes catégories: SaaS, PaaS et IaaS, afin de relever les défis commerciaux de divers secteurs (financier, distribution, fabrication, santé, jeux, gouvernement, etc.).

2.8.3. IBM : Le Cloud IBM (anciennement Bluemix) est une plateforme complète qui englobe les environnements publics, privés et hybrides. Il offre le plus large éventail de produits et de ressources pour toutes les charges de travail.

2.8.4. Google : Google mise beaucoup sur le Cloud computing et propose des services PaaS et SaaS. A grande échelle, les solutions de Google dans le Cloud sont surtout connues des consommateurs privés au travers des ses Google Apps telles que Google Docs, Calendar ou encore Gmail. Toutes ces « web apps » sont dans le Domaine du SaaS et gratuites pour une utilisation privée. Google App Engine dont la première version beta est sortie en avril 2008 est le service PaaS de Google. Au départ le service ne supportait que le développement d'applications en Python. Depuis, le support de Java Virtual Machines (JVMs) a été ajouté et permet de développer des applications non seulement en Java mais aussi au moyen de JRuby, JPython, Scala ou Clojure.

2.8.5. Salesforce : Salesforce.com est une société pionnière dans le domaine du SaaS, elle a été créée en 1999 déjà par Marc Benioff. Les solutions de Salesforce.com sont regroupées dans différentes grandes catégories : Sales Cloud, Service Cloud, Force.com et Chatter Collaboration Cloud :

- **Sales Cloud :** l'outil de CRM (Customer Relationship management) par excellence disponible en plus de 25 langues et accessible depuis des appareils mobiles. Le produit fournit des outils de gestion des comptes et contacts clients, outils marketing, de ventes, plateforme de discussion, AppExchange un catalogue de services développés pour Salesforce par des tierces parties.
- **Service Cloud :** Un service client de nouvelle génération permettant aux entreprises d'être plus sociable et collaborative. Service Cloud propose des services rapides et réactifs intégrant tous les canaux de communication ; du centre d'appel aux réseaux sociaux.
- **Chatter Collaboration Cloud :** est une plateforme de collaboration en temps réel reprenant un peu la forme d'un réseau social.
- **Force.com :** une solution PaaS qui permet de créer des applications au moyen de Visualforce (un Framework pour la création d'interfaces graphiques) et Apex, un langage de programmation propriétaire qui reprend la syntaxe de Java mais qui est plus tourné vers la gestion des bases de données

Figure 10 : les fournisseurs des services Cloud [38]

2.9. La Virtualisation :

la virtualisation en informatique est la création d'un version virtuel (pas réel) de quelque chose , tel que du matériel, un logiciel, une plate-forme, un système d'exploitation, un stockage ou un périphérique réseau.[18]

La technique de la virtualisation est une caractéristique indispensable du Cloud Computing qui donne une grande flexibilité, une bonne sociabilité, une réduction des coûts remarquable et un énorme gain de temps. De plus la machine virtuelle ne tombe pratiquement jamais en panne par exemple En cas de défaillance d'un serveur, la machine virtuelle sera redémarrée sur l'autre serveur virtualisé, restaurant les services requis avec une interruption de service minimale [18]. Il existe différentes techniques de virtualisation. Pour les comprendre, il est d'abord important de comprendre ce qu'est un hyperviseur.

2.9.1. Hyperviseur :

Un hyperviseur ou un moniteur de machine virtuelle (VMM) est un logiciel, un micro logiciel ou un matériel informatique qui crée et exécute des machines virtuelles. Un ordinateur sur lequel un hyperviseur exécute une ou plusieurs machines virtuelles est appelé une machine hôte et chaque machine virtuelle est appelée une machine invitée. L'hyperviseur présente aux systèmes d'exploitation invités une plate-forme d'exploitation virtuelle et gère l'exécution des systèmes d'exploitation invités. (Wikipedia)

2.9.1.1. Types d'hyperviseur :

- **Hyperviseurs natifs de type 1 :** Ces hyperviseurs s'exécutent directement sur le matériel de l'hôte pour contrôler le matériel et gérer les systèmes d'exploitation invités. Pour cette raison, ils sont parfois appelés hyperviseurs nus.
- **Hyperviseurs ou hébergés de type 2:** Ces hyperviseurs fonctionnent sur un système d'exploitation conventionnel, tout comme les autres programmes informatiques. Un système

d'exploitation invité s'exécute en tant que processus sur l'hôte. Les hyperviseurs de type 2 extraient les systèmes d'exploitation invités du système d'exploitation hôte.

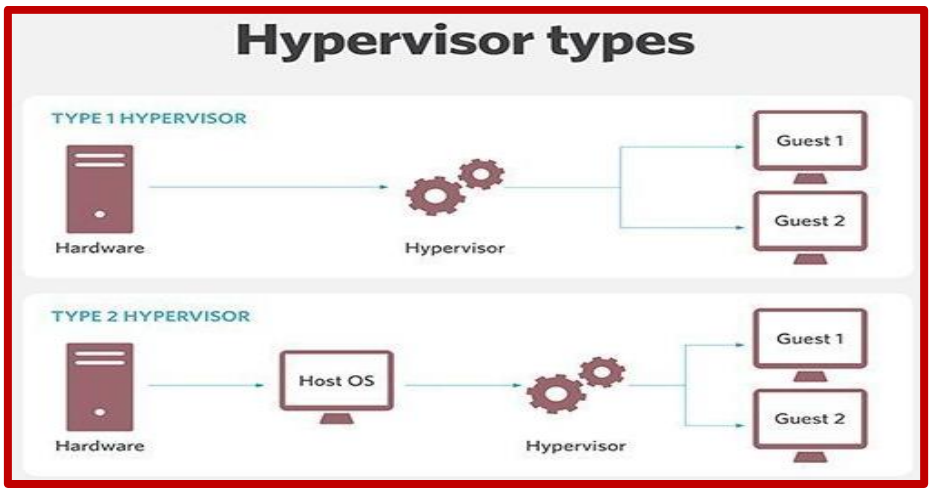

Figure 11 : Les types d'hyperviseur [43].

2.9.2. Techniques de virtualisation :

Il existe plusieurs types de virtualisation utilisés dans le Cloud computing: la virtualisation de matérielle/serveur, la virtualisation poste de travail/client, et la virtualisation de stockage. [26] Dans cette section, nous allons discuter les techniques de virtualisation [27] :

2.9.2.1. Virtualisation complète : En virtualisation complète, le code source du système d'exploitation invité n'est pas modifié. Ainsi, lorsqu'il est exécuté, le système d'exploitation invité n'est pas conscient de la virtualisation. la virtualisation complète est géré par les deux types d'hyperviseurs précédemment mentionné.

2.9.2.2. Para Virtualisation : Il fait référence à la collaboration entre le système d'exploitation invité et l'hyperviseur afin d'améliorer les performances. Cette collaboration implique la modification du code source du système d'exploitation invité pour appeler directement, à l'aide d'hypercall, l'hyperviseur permettant d'exécuter des instructions privilégiées. Donc, le système d'exploitation invité est conscient d'être virtualisé.

2.9.2.3. La virtualisation assistée par le matériel:

Il consiste à utiliser les composants physiques d'un ordinateur pour supporter le logiciel de création et de gestion de machines virtuelles (VM) [31]. Pour simplifier les techniques de virtualisation, les fournisseurs de matériel tels qu'Intel et AMD ont introduit de nouvelles extensions pour la virtualisation.

3. Cloud computing Mobile :

3.1. informatique mobile (mobile computing) :

Avant de passer au Cloud computing mobile, nous devons d'abord comprendre ce qu'est l'informatique mobile. C'est une forme d'interaction homme-machine par laquelle un ordinateur se déplace ou se transporte au cours d'une utilisation normale. L'informatique mobile repose sur un ensemble de trois concepts majeurs: matériel, logiciel et communication. Les concepts de matériel peuvent être considérés comme des appareils mobiles, tels que les smartphones et les ordinateurs portables. Les logiciels d'informatique mobile regroupent les nombreuses applications mobiles des périphériques, telles que le navigateur mobile, les logiciels anti-virus et les jeux. Le problème de communication concerne l'infrastructure des réseaux mobiles, les protocoles et la fourniture de données. Ils doivent être transparents pour les utilisateurs finaux. [42]

3.1.1. caractéristiques :

- **Mobilité:** Dans un réseau informatique mobile, les nœuds mobiles peuvent établir une connexion avec d'autres, même des nœuds fixes d'un réseau câblé, via la station de support mobile (MSS) pendant leur déplacement.[42]
- **Diversité des conditions de réseau:** Les réseaux utilisés par les nœuds mobiles ne sont pas uniques. Ces réseaux peuvent être un réseau câblé à large bande passante ou un réseau étendu sans fil (WWAN) à faible bande passante ou même déconnecté. [42]
- **cohérence de fréquence et déconnexion:** En raison de la limitation de la charge de la batterie, de la charge de la communication sans fil, des conditions du réseau, etc., les nœuds mobiles ne conservent pas toujours la connexion, mais se déconnectent et restent cohérents avec le réseau sans fil de manière passive ou active.[42]
- **Communication réseau asymétrique:** Les serveurs de point d'accès et les autres MSS permettent une capacité de réception / envoi puissante, alors que cette capacité dans les nœuds mobiles est relativement faible. Ainsi, la largeur de bande de communication et la surcharge entre la liaison descendante et la liaison montante sont divergentes. [42]
- **faible fiabilité:** En raison des signaux, les réseaux mobiles sont sensibles aux interférences et à la surveillance, par conséquent, un système de réseau informatique mobile doit être envisagé à partir de terminaux, réseaux, plates-formes de bases de données, ainsi que de développement d'applications pour résoudre le problème de sécurité. [42]

3.1.2. Problèmes et Défis :

Comparé au réseau câblé traditionnel, le réseau informatique mobile peut être confronté à divers problèmes et défis, tels que perturbation du signal, sécurité, délai de transfert, puissance limitée, capacité informatique réduite, etc., en raison de l'environnement sans fil et de nombreux nœuds

mobiles. En outre, la qualité de service (QoS) du réseau informatique mobile est beaucoup plus facilement affectée par les reliefs, les conditions météorologiques et les bâtiments.

3.2. Définition du Cloud computing mobile :

Aepona [19] décrit le MCC comme un nouveau paradigme pour les applications mobiles, dans lequel le traitement et le stockage des données sont transférés du périphérique mobile vers des plates-formes informatiques puissantes et centralisées situées dans le Cloud. Ces applications centralisées sont ensuite accessibles via la connexion sans fil basée sur un client natif léger ou un navigateur Web sur les périphériques mobiles. [20]

MCC a permis aux utilisateurs d'avoir à la fois une puissance de calcul et une capacité de stockage en ligne illimitées. Malheureusement, les appareils mobiles ont une puissance de traitement limitée, une faible capacité, du stockage, peu de fonctionnalités de sécurité, une connectivité problématique et une faible consommation d'énergie. Cela posera toujours des problèmes pour les applications nécessitant des capacités de calcul élevées et une grande capacité de stockage pour fonctionner dans un environnement mobile. [5] Afin d'augmenter la capacité de calcule, la capacité de stockage et la durée de vie de la batterie des appareils mobiles, ces activités exigeantes un calcul élevé et une grande capacité de stockage doivent être transférées vers le Cloud. Plus important encore, la sécurité des données reste un sujet de préoccupation et constitue le principal obstacle à l'adoption généralisée du Cloud computing mobile. [5][6] L'architecture de Mobile Cloud Computing est illustrée dans la figure [9] :

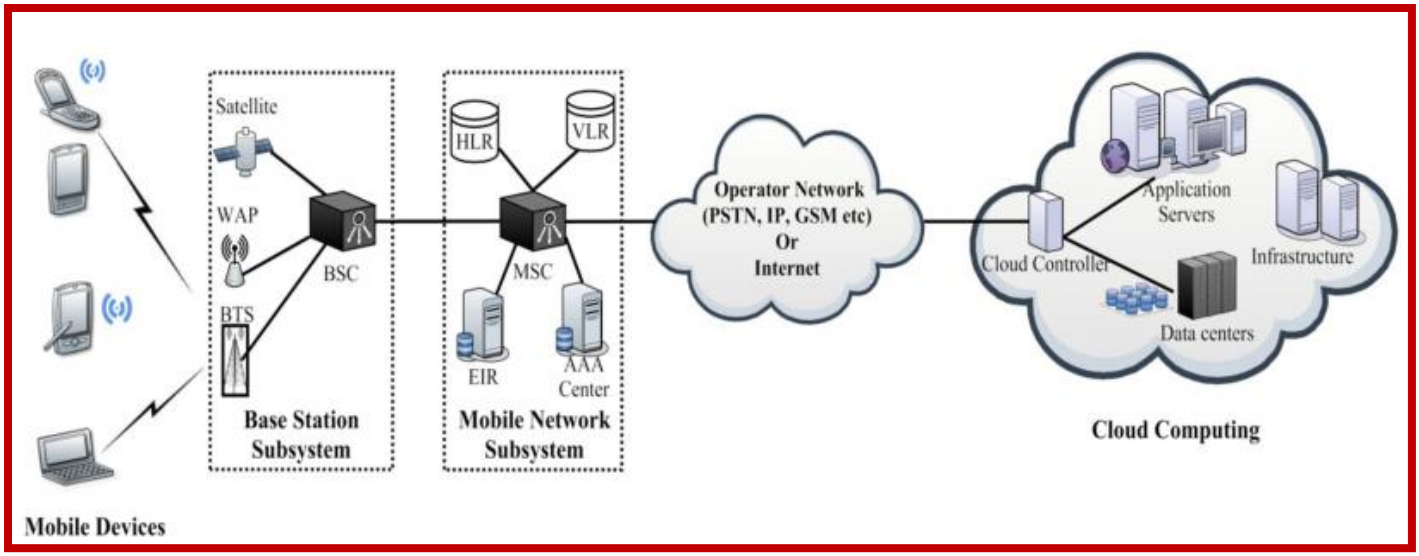

Figure 12 : architecture du Cloud computing mobile [12].

3.3. Description de l'architecture :

Les appareils mobiles tels que les ordinateurs portables, les assistants numériques personnels (PDA) et les appareils de poche peuvent accéder aux services Cloud via un réseau mobile ou des points d'accès sans fil (WAP). Les appareils mobiles sont connectés aux réseaux mobiles via des stations de base

(BTS) ou des satellites chargés de contrôler les connexions et les interfaces fonctionnelles entre les réseaux mobiles et les appareils mobiles. Ils transmettent les demandes et les données des utilisateurs mobiles aux contrôleurs de stations de base (BSC) qui sont en outre connectés au centre de commutation mobile (MSC) fournissant une large gamme de services de réseau mobile tels que AAA (authentification, autorisation et comptabilité).sur la base du registre de localisation du domicile (HLR), du registre de localisation du visiteur (VLR), du centre AAA, du registre d'identité de l'équipement (EIR) et des données des abonnés stockées dans des bases de données.[12]

Les demandes des abonnés sont ensuite acheminées vers le Cloud via l'Internet. Dans le cas WAP, les appareils mobiles se connectent aux points d'accès via Wi-Fi, qui se connecte ensuite au fournisseur de services Internet (ISP) pour fournir la connectivité Internet. La connectivité Wi-Fi est plus efficace que le réseau mobile GSM, Connexions GPRS, 3G, LTE, 4G car elles offrent une faible latence et consomment moins d'énergie. À l'intérieur du Cloud, les contrôleurs du Cloud se connectent aux centres de données et aux serveurs d'applications pour traiter les demandes et fournir aux utilisateurs mobiles les services de nuage correspondants reposant sur une architecture omniprésente, la virtualisation et une architecture orientée services.[12]

3.4. Avantages du Cloud computing mobile :

Vous trouverez ci-dessous certains des avantages pour ceux qui proposent des services et des applications basés sur le Cloud computing [28] [29] [30]:

- **Économies de coûts:**

  Le Cloud promet de réduire les coûts d'acquisition, de fourniture et de maintenance de la puissance de calcul, un avantage particulièrement important en période d'incertitude économique. En permettant aux clients d'acheter uniquement les services informatiques nécessaires, au lieu d'investir dans des infrastructures informatiques complexes et coûteuses, elles peuvent réduire les coûts de développement, de test et de maintenance des systèmes nouveaux et existants.

- **Accès mobile:**

  Le Cloud computing permet d'accéder à des ressources informatiques et de stockage de grande puissance à toute personne disposant d'un dispositif d'accès au réseau.

- **Evolutivité :**

  Un autre avantage du Cloud computing est qu'il permet aux utilisateurs d'ajuster les ressources en fonction de l'évolution des besoins de l'entreprise. Cela peut être fait en développant l'infrastructure informatique car la plupart des interfaces de Cloud computing sont conviviales.

- **Maximisation des ressources :**

Le Cloud computing réduit le fardeau des ressources informatiques pour de nombreuses entreprises et agences en maximisant les ressources du pool de Cloud computing.

- **Collaboration :**

  La collaboration est un terme dans lequel un groupe de personnes peut travailler ensemble en ligne. En utilisant un environnement informatique en ligne, la collaboration est plus facile qu'avant, Google Docs en est un bon exemple.

- **Personnalisation :**

Le Cloud computing est une plate-forme où nous pouvons nous adapter à nos besoins en cours de réaménagement. Il offre une plate-forme pour créer et modifier des applications afin de répondre à une diversité de tâches et de défis.

3.5. Les inconvénients :

- **Sécurité des données :**

  La sécurité des données sera toujours l'une des préoccupations majeures du Cloud computing. Il est important que les utilisateurs mobiles échangent et stockent leurs informations sensibles via le réseau dans un environnement sécurisé. En effet, si ces données ne sont pas protégées, elles peuvent causer des dommages importants. Il est également fortement recommandé de choisir le fournisseur de services le plus fiable, capable de protéger vos données en toute sécurité. [41]

- **Problèmes de connectivité et de performance :**

  Comme le Cloud computing mobile dépend d'Internet, cela peut affecter votre accès et votre utilisation. Parfois, vous pouvez penser que les performances ne répondent pas à vos attentes. Par conséquent, il est préférable de vérifier les antécédents de votre fournisseur de services avant de lancer le service. Malgré le maintien de normes de maintenance élevées, les fournisseurs de services Cloud peuvent être confrontés à de graves pannes.[41]

- **Dépendance et verrouillage du fournisseur (vendor lock-in) :**

Parfois, il devient difficile de migrer d'un fournisseur de services à un autre. C'est ce qu'on appelle le «verrouillage du fournisseur » ou « vendor lock-in en englais ». Par conséquent, il est très important de vérifier les termes et conditions énoncés dans le contrat SLA et les autres options avant de choisir un fournisseur, car il peut s'avérer difficile de passer ultérieurement à un autre fournisseur. [41]

Avec l'émergence de ressources en Cloud telles que le traitement et le stockage, les utilisateurs mobiles n'ont pas besoin de capacités de traitement et de stockage de données élevées sur leurs appareils mobiles. Et puisque les applications développées pour le Cloud mobile sont différentes de celles développées pour les plates-formes natives telles qu'iPhone ou Android. Les fournisseurs de solutions pour applications mobiles

ont commencé à proposer des navigateurs mobiles, qui permettent aux utilisateurs d'accéder aux applications depuis le site Web, évitant ainsi de devoir télécharger l'application sur l'App Store. [41]

4. Les Applications de Cloud computing mobile :

Diverses applications mobiles ont profité des avantages du MCC. Dans cette section, nous discuterons quelques applications typiques du MCC [1] [20] [21] [22] [23]:

❖ Mobile Commerce :

M-Commerce est une nouvelle perspective et une nouvelle architecture pour le commerce via les appareils mobiles. Il a été développé pour fournir les capacités du commerce à l'aide de la technologie sans fil. Les applications de commerce mobile sont divisées en trois catégories finance, shopping et publicité. [1]

❖ Mobile-Learning :

L'apprentissage mobile (m-Learning) est conçu sur la base de l'apprentissage électronique (e-Learning) et de la mobilité. Cependant, les applications m-Learning traditionnelles présentent des limitations en termes de coût élevé des périphériques et du réseau, d'un faible taux de transmission sur le réseau et de ressources pédagogiques limitées [21], [22], [23]. Des applications m-Learning basées sur le Cloud sont introduites pour résoudre ces limitations. Par exemple, en utilisant un Cloud avec une grande capacité de stockage et une capacité de traitement puissante, les applications fournissent aux apprenants des services beaucoup plus riches en termes de taille de données (informations), de vitesse de traitement plus rapide et de durée de vie de la batterie plus longue. [20]

❖ Soins de santé mobiles (Mobile Healthcare) :

Dans les environnements de soins de santé, les appareils informatiques mobiles permettent un accès plus rapide et plus simple aux données, permettant ainsi de mieux prendre en charge les patients. Les services de santé mobiles (m-soins de santé) permettent aux patients d'être surveillés à tout moment et en tout lieu grâce à la technologie sans fil. En outre, les appareils mobiles sensibles à la santé peuvent détecter le Rythme cardiaque et la pression artérielle pour alerter le système d'urgence. [1]

❖ Le jeu mobile (m-gaming) :

Le jeu mobile (m-game) est un marché potentiel générant des revenus pour les fournisseurs de services. M-game peut décharger complètement le moteur de jeu nécessitant d'importantes ressources informatiques (par exemple, un rendu graphique) sur le serveur dans le Cloud, et les joueurs n'interagissent qu'avec l'interface d'écran de leurs appareils. [20]

❖ Gouvernement mobile:

« Le gouvernement mobile (M-Gouvernement) est l'extension du gouvernement électronique aux plates-formes mobiles pour utiliser les services et applications du gouvernement à l'aide de périphériques mobiles intégrés à l'infrastructure Internet sans fil.il implique le déploiement des services et de l'administration du gouvernement sur des appareils mobiles afin de rendre les services gouvernementaux disponibles à tout moment et en tout lieu. »[40]

5. Conclusion

Le Cloud computing mobile est l'une des tendances futures de la technologie mobile, car elle combine les avantages de l'informatique mobile et de l'informatique en Cloud, offrant ainsi des services optimaux aux utilisateurs mobiles.

Dans ce chapitre, nous avons fourni un aperçu du Cloud computing mobile, de ses services et de ses modèles. Nous avons décrit les deux concepts le Cloud computing et le Cloud computing mobile et discuté les avantages du Cloud computing mobile et ses applications

Chapitre 2

Sécurité dans le cloud

1. Introduction :

La sécurité est l'un des défis les plus critiques pour le Cloud computing mobile. Le Cloud computing mobile pose de nombreux problèmes de sécurité, tels que le contrôle de l'accès aux données, la distribution des données sur une infrastructure distribuée, l'intégrité des données, la disponibilité des services, la sécurité des communications et la sécurité des applications. En outre, la mobilité ajoute des problèmes de sécurité plus difficiles. [60]

De plus, l'un des principaux problèmes non résolus pour les fournisseurs de services Cloud et leurs clients est la difficulté de déterminer qui est responsable de quelles mesures et contrôles de sécurité. Les fournisseurs de services sont responsables de la création de services et de fonctionnalités conformes aux normes de protection des données et de confidentialité d'un côté, et le client peut configurer et utiliser ces services d'une manière compatible avec son secteur d'activité et son emplacement de l'autre côté. Les fournisseurs de services peuvent créer des contrôles opérationnels pour protéger les données des clients sur le Cloud. Les clients doivent utiliser ces contrôles pour empêcher le partage de données involontaire. Les fournisseurs de services sont responsables de l'obtention des certifications et de la signature des contrats de niveau de service (SLA), tandis que les clients sont responsables de la vérification des rapports d'audit et des certificats du fournisseur de services conformément aux exigences de confidentialité de leurs données d'organisation. La frontière entre ces responsabilités n'est pas claire et dépend donc de l'accord signé entre le client et les fournisseurs de services et sur le service de Cloud et le modèle de déploiement utilisé. [12]
Dans ce chapitre, nous aborderons les menaces et les problèmes de sécurité liés au Cloud computing mobile et l'état de l'art des solutions existantes.

2. sécurité informatique en mobile Cloud computing :

2.1. Définition de La sécurité du Cloud computing :

La sécurité informatique, en général, fait référence à toutes les ressources techniques, organisationnelles, juridiques et humaines requises et mises en place pour garantir que les ressources matérielles ou logicielles d'une organisation ne sont utilisées que dans le cadre prévu et pour assurer la protection des informations contre l'accès, utilisation, divulgation, perturbation, modification ou destruction pour assurer la confidentialité, l'intégrité et la disponibilité .[61] [62]

2.2. Les causes d'insécurité :

Généralement il ya 5 type des faille informatique on va les détailler un peu ci dessous [11] :

2.2.1. Les failles physiques :

la plupart des entreprises ou de l'administration sont ignorant de l'importance de la sécurité au matériel informatique. L'attaquant peut simplement trouver des excuses comme effectuer des tests, effectuer de la maintenance ou nettoyer pour accéder.

Exploiter cet accès physique pour voler un mot de passe, effacer des données, en usurper l'identité d'un autre ou injecter des programmes malveillants peut causer des dommages catastrophiques à une entreprise.

2.2.2. Les failles réseaux : Malgré tous les efforts déployés pour faire en sorte que les réseaux informatiques s'appuient sur des normes et standard strictes et efficaces, il existe toujours des problèmes de vulnérabilités du réseau. Ces problèmes résident dans la complexité de la résolution des problèmes qui varient en fonction de la taille du réseau.

2.2.3. Les failles systèmes : Cette faille est aussi compliquée que le système d'exploitation lui-même, car ils intègrent différentes techniques et mécanismes de sécurité tels que mots de passe, journaux, séparation des privilèges, etc. cette complexité, ainsi que la mauvaise configuration et les faiblesses de certains mécanismes des systèmes d'exploitation représentent un danger pour les utilisateurs. Par exemple, la complexité d'un mécanisme de sécurité amène les utilisateurs à le désactiver et une mauvaise configuration peut entraîner l'arrêt ou la surcharge du système.

2.2.4. Les failles applicatives : Ce type de faille peut être dû à une mauvaise conception, non-traitement des exceptions, faille dans le langage de programmation. Ils peuvent causer de nombreux problèmes qui affectent le fonctionnement du système.

2.2.5. Les failles Web : Tout d'abord, même si le Web représente une grande partie de l'Internet, il ne s'agit pas d'une seule et même chose. le monde du web représente la combinaison de différent protocole, réseaux, système et application. Les failles web peuvent être causées par l'une des failles précédemment citées ou par des failles qui résident au niveau des protocoles et des standards du fonctionnement du web.

3. Les différents types d'attaque informatique :

Techniquement, nous pouvons simplement définir une attaque par l'exploitation de l'une des failles précédemment citée à des fins illégales. Il y a cinq types d'attaque que nous détaillons comme suit [17]:

3.1. L'attaque passive : une attaque passive est un type d'attaque dans lequel l'attaquant surveille simplement l'activité du réseau dans le cadre de la reconnaissance. Une attaque passive est difficile à détecter car l'attaquant n'attaque pas activement aucune machine cible ni ne participe à un trafic réseau. Un attaquant capturant des paquets du réseau est un exemple d'attaque passive.

3.2. L'attaque active : une attaque active est un type d'attaque par lequel l'attaquant lance une attaque active contre les serveurs cibles. En attaque active, l'attaquant envoie activement du trafic pouvant être détecté.

3.3. Attaque rapprochée: une attaque rapprochée est un type d'attaque où l'attaquant est physiquement proche du système cible. L'attaquant peut bénéficier des avantages d'être physiquement proche des équipements cibles.

3.4. Attaque interne: une attaque interne est une attaque d'utilisateurs internes, qui utilisent leurs informations d'identification d'accès et leur connaissance du réseau pour attaquer les ordinateurs cibles.

3.5. Attaque de distribution: les attaques de distribution sont les attaques utilisant des portes dérobées introduites dans des systèmes matériels ou logiciels au moment de leur fabrication. Une fois que le matériel ou le logiciel est devenu opérationnel, les attaquants peuvent exploiter la porte dérobée pour attaquer les périphériques cibles.

4. Les Objective de sécurité :

Les objectives de Tout Framework de sécurité des données selon FISMA « *Federal Information Security Management Act* », sont La confidentialité, l'intégrité, la disponibilité [12]:

- **Confidentialité:** ce principe garantit que seuls l'expéditeur et le destinataire/s doivent accéder au message. Il empêche l'accès non autorisé aux données et la perte de confidentialité entraîne une interception.
- **Intégrité:** garantit la livraison correcte du message au (x) destinataire (s) prévu (s) sans aucune modification. La perte d'intégrité conduit à une attaque par modification.
- **Disponibilité:** Cela garantit que les parties autorisées peuvent accéder aux informations quand elles le souhaitent. Refuser l'accès à l'information entraîne une attaque par déni de service dans laquelle des utilisateurs légitimes se voient refuser l'accès aux ressources.

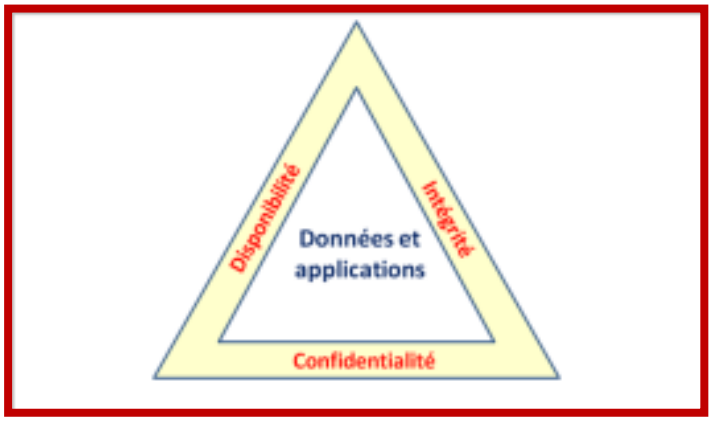

Figure 13 : Triad CIA de la sécurité. [61]

Outre ces objectives, La norme ISO 7498-2 à défini l'authentification et la non-répudiation et le contrôle d'accès comme des services permettant d'augmenter la sécurité .on va les résumer ci-dessous [12] :

- **Authentification:** il est utile d'établir la preuve des identités indiquant que le nœud en communication est ce qu'il prétend être. L'absence de mesures d'authentification conduit à une attaque contre la fabrication.
- **La non-répudiation:** Ce principe veille à ce que l'expéditeur ne peut pas nier plus tard pour ne pas envoyer le message.
- **Contrôle d'accès:** il garantit l'utilisation des ressources et des services du réseau par les seuls utilisateurs autorisés. Il agit comme un pont entre la confidentialité, l'intégrité et l'authenticité. Il commence par l'authentification et identifie ensuite qui peut «accéder» à quoi, où l'accès comprend la lecture des données (confidentialité) et l'écriture (intégrité).

5. Problèmes et attaques possible dans le Cloud computing mobile :

Le Cloud computing mobile est en constante évolution et requiert des mécanismes d'identification et d'authentification sécurisés, fiables et non répudiés. La sécurité est la seule peur qui empêche l'adoption du Cloud computing et du Cloud computing mobile, même si elle fournit un large éventail de ressources. Dans cette section, on va traiter plusieurs problèmes de sécurité, menaces et attaques éventuelles. Ces problèmes ont été résumés dans la Figure (18).

5.1. Problèmes infrastructurels et architecturaux :

Ces problèmes sont la sécurité de la virtualisation, la sécurité du réseau, les problèmes de séparation des données, les attaques d'initiés et les problèmes d'interface administrative. [12]

5.1.1. Sécurité de la virtualisation:

La virtualisation, l'un des composants majeurs du Cloud computing, permet à plusieurs utilisateurs de stocker des données à l'aide d'applications fournies par des fournisseurs SaaS et de partager des services à la demande. Cela présente un potentiel élevé d'intrusion dans les données des locataires si leurs données ne sont pas séparées correctement au niveau physique et au niveau de l'application. En effet il entraîne de nombreux risques, tels que l'échec d'isolation entre plusieurs machines virtuelles (VM) s'exécutant sur une même machine physique, les attaques entre machines virtuelles, l'injection de code malveillant dans l'application, etc.. par exemple l'exploitation de la vulnérabilités d'hyperviseur pour contourner l'authentification et augmenter les privilèges [14], l'attaque « VM Escape » permet à un attaquant de briser une couche d'isolation pour exécuter une application avec les privilèges root de

l'hyperviseur et obtenir un accès au système d'exploitation hôte et aux autres machines virtuelles exécutées sur la machine hôte, la figure ci-dessous montre comment l'attaque VM escape se lance :

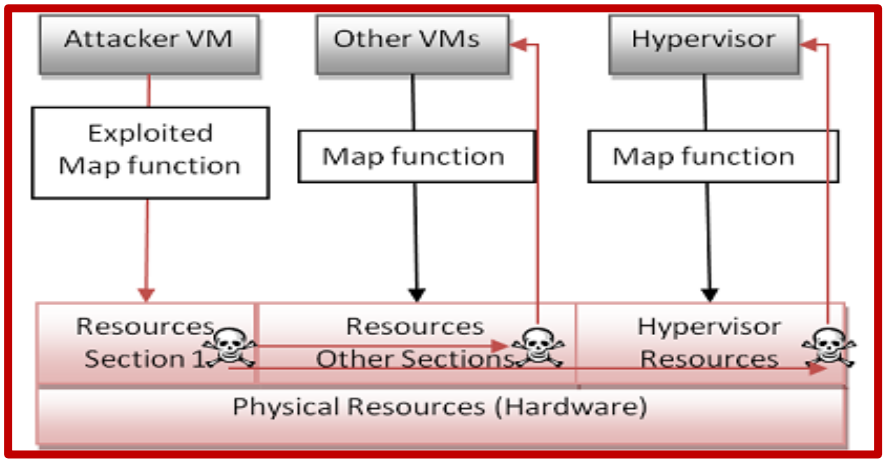

Figure 14 : attaque sur l'hyperviseur de type (VM Escape)

Un autre exemple est l'utilisation de rootkit qui est un ensemble de programmes ou d'outils utilisés par un attaquant pour obtenir des privilèges d'administrateur sur une machine, soit en déchiffrant son mot de passe, soit en exploitant la vulnérabilité de l'hyperviseur. Les rootkits basés sur des machines virtuelles permettent à un attaquant d'exécuter du code malveillant pour détruire des programmes anti-malware .Pour se défendre contre de telles attaques, un contrôle exhaustif des hyperviseurs et une forte isolation entre les ordinateurs virtuels sont nécessaires, ce qui empêche un attaquant d'injecter du code malveillant dans l'ordinateur virtuel du voisin.

5.1.2. La sécurité du réseau :

Il traite les communications et configurations réseau. Les vulnérabilités inhérentes aux protocoles Internet tels que ARP, HTTP, TCP permettent à un attaquant d'exploiter le système Cloud et ses ressources par le biais des attaques tel que man-in-th-middle, DDOS, d'empoisonnement ARP et DNS (ARP/DNS poisoning), de détournement de session (session hijacking), etc. Les données sont obtenues d'une entreprise et stockées sur le Cloud donc Les techniques de cryptage réseau telles que SSL et TLS sont nécessaires pour assurer une protection contre de telles attaques. Dans de qui suit on va expliquer les attaques MITM (man-in-the-middle), DDOS and ARP/DNS poisoning précédemment cité :

5.1.2.1. Attaque man-in-the-middle (MITM) : C'est une forme d'espionnage actif dans laquelle L'attaquant établit des connexions indépendantes avec les victimes et transmet des messages entre elles, leur faisant ainsi croire qu'ils se parlent directement via une connexion privée alors qu'en réalité, l'intégralité de la conversation est contrôlée par l'attaquant. L'attaque man-in-the-middle ne peut réussir que lorsque l'attaquant peut usurper l'identité de chaque terminal à la satisfaction de l'autre [47]. La figure ci-dessous montre comment MITM fonctionne :

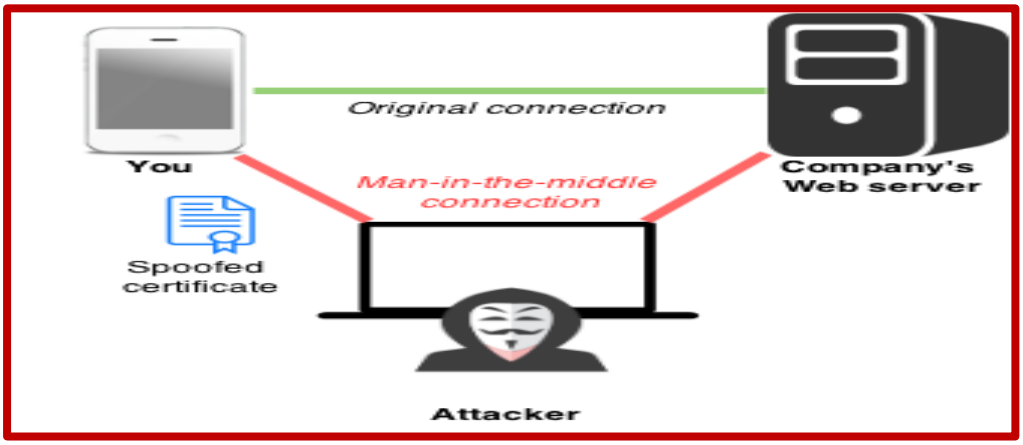

Figure 15: L'attaque man-in-the-middle [49]

5.1.2.2. L'attaque par déni de service distribué (DDOS) : l'attaque DDOS est la version distribuée de l'attaque DOS (déni de service) ce type d'attaque sur un réseau conçu pour le mettre à genoux en l'inondant de trafic inutile. Le déni de service distribué est une sorte d'attaque dans laquelle l'attaquant crée une machine zombie en l'infectant via Internet. Ensuite, ces machines infectées sont utilisées pour attaquer la victime. Lorsque les attaques / le trafic provenant d'un aussi grand nombre de machines infectées sont dirigés vers une victime, ses ressources telles que le processeur, la bande passante et la mémoire commencent à s'épuiser et cette ressource particulière devient indisponible pour les consommateurs. [48] [56]

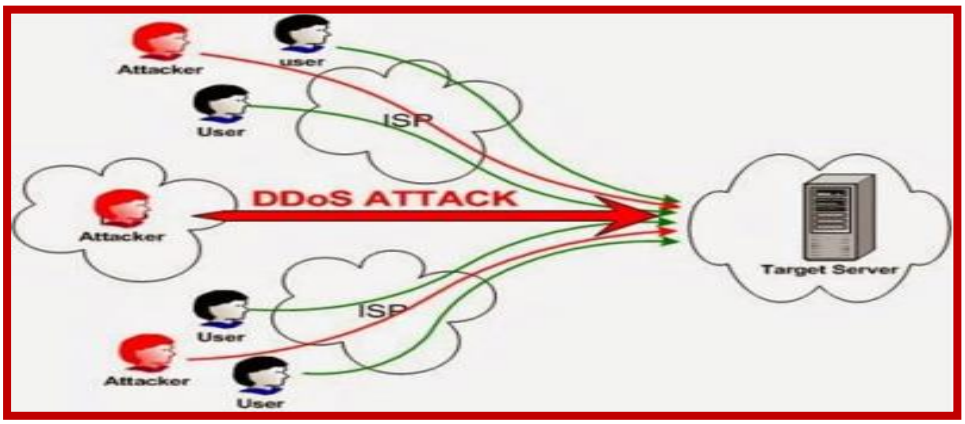

Figure 16: attaque par déni de service distribué [48]

5.1.2.3. Empoisonnement ARP/DNS : Avec l'empoisonnement du cache ARP/DNS ou les attaques par usurpation d'ARP, un intrus peut facilement emprunter l'identité d'un autre hôte et avoir accès à des informations sensibles. De plus, ces attaques peuvent être facilement effectuées en utilisant des outils largement disponibles et faciles à manipuler spécialement conçus à des fins d'attaque. [58]

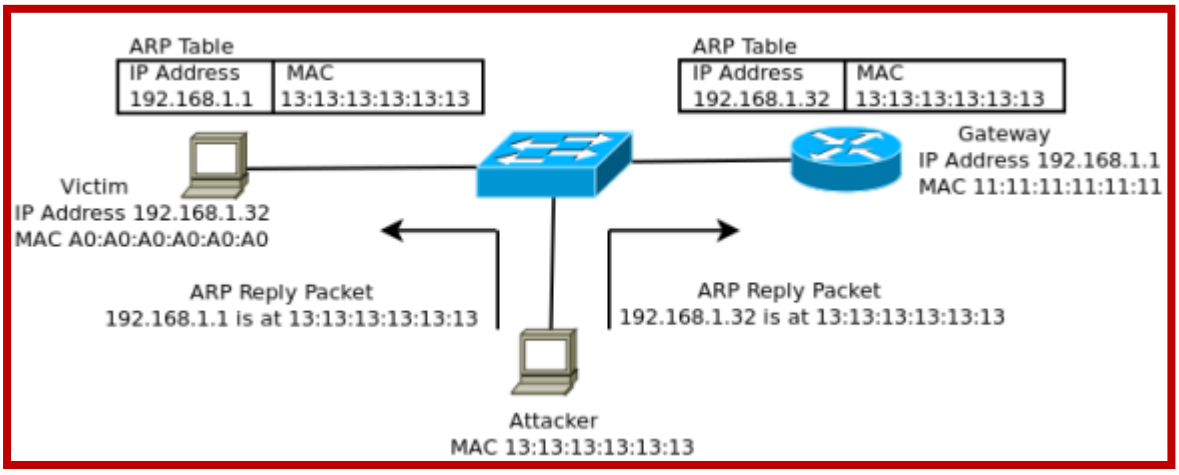

Figure 17: attaque par Empoisonnement d'ARP [58]

5.1.3. Vols d'identité:

Il s'agit d'une forme d'acte frauduleux dans lequel une entité prétend être quelqu'un d'autre pour accéder à des ressources ou obtenir des informations bancaires et autres informations critiques. L'attaque par usurpation d'identité ou (spoofing attack en englais) incluse DNS spoofing, IP spoofing, ARP spoofing, métadonnée spoofing, phishing, ils sont toutes des formes de vol d'identité. Par exemple Un intrus obtient l'adresse IP d'un utilisateur légitime et modifie les en-têtes de paquets TCP / IP pour se faire passer pour un hôte de confiance et cache son identité afin de lancer une attaque de type IP spoofing. L'attaque d'usurpation d'identité peut être utilisée pour pirater un navigateur, surcharger des cibles avec du trafic et voler des informations. Lors d'une attaque par usurpation d'ARP, un intrus lie son adresse MAC à l'adresse IP d'une machine virtuelle légitime sur un réseau et envoie des messages ARP usurpés qui aboutissent à l'envoi de données destinées à l'adresse IP de l'hôte légitime à la machine virtuelle intrus rattachée au même commutateur virtuel.

5.1.4. Applications et interfaces non sécurisées:

Des interfaces utilisateur et des API faibles peuvent exposer une entreprise à plusieurs risques de sécurité. Les défauts de conception et d'architecture des applications entraînent des attaques par injection de logiciels malveillants telles que l'injection SQL, l'injection de système d'exploitation, l'injection XSS (cross-site Scripting), etc. Un adversaire compromet le système Cloud en injectant un code malveillant dans un service ou une instance de machine virtuelle illicite, susceptible de modifier ou de bloquer les fonctionnalités du service. Le protocole SSL assure une communication sécurisée entre le navigateur de l'utilisateur et le serveur grâce à l'utilisation de certificats SSL qui peuvent être vérifiés par le navigateur de L'utilisateur. La connexion sécurisée SSL peut être interrompue en imitant un serveur légitime via une attaque par empoisonnement du certificat SSL afin d'intercepter des informations sensibles.

5.1.5. Attaquant interne :

Un attaquant interne peut facilement nuire au réseau ou au système car il a des privilèges pour accéder au système et est très familier avec l'architecture du réseau et les procédures de sécurité du système. L'employé interne peut être un employé malveillant travaillant pour le fournisseur de Cloud ou un employé d'une entreprise utilisant des services de Cloud

5.1.6. Abus de services Cloud:

ou (Cloud abuse en englais) Cela signifie utiliser des services Cloud à des fins malveillantes, telles que casser des clés de chiffrement, partager des logiciels piratés ou propager des programmes malveillants en lançant des attaques DDoS et des attaques de phishing, car il était difficile de les utiliser avec un ordinateur standard. Des contrôles de validation / vérification appropriés lors de la phase d'enregistrement initiale et une surveillance constante du trafic réseau peuvent empêcher de telles attaques.

5.2. Problème de gouvernance et de confidentialité :

Des problèmes de gouvernance tels que le verrouillage des données fournisseur (vendor lock-in en englais), le contrôle des données et de la sécurité résultent de différences entre les architectures Cloud sous-jacentes et de la perte des contrôles administratifs d'un client dans un environnement Cloud. Accéder à la plate-forme Cloud qui stocke les données de divers utilisateurs et organisations compromet la confidentialité, l'intégrité et l'authenticité (CIA). [12]

« Dans ce cas, l'accord de niveau de service (SLA : Service Level Agreement) doit jouer un rôle crucial pour défendre l'intérêt du client ». [3]

5.3. Problème de conformité :

Cette dimension traite la disponibilité du service et les capacités d'audit. Les accords de niveau de service (SLA) garantissent la disponibilité de service requise et les procédures à adopter pour garantir un certain niveau de sécurité. Les clients, les fournisseurs de services et des tiers effectuent des audits pour évaluer en permanence les services de sécurité et de disponibilité. [12] Les fournisseurs de SaaS doivent tenir compte de certains cadres réglementaires et législatifs lors du stockage des informations relatives à la confidentialité dans le Cloud, telles que HIPAA (health insurance, portability and accountability act), privacy act, the Fair and Accurate Credit Transaction Act (FACTA). [3]

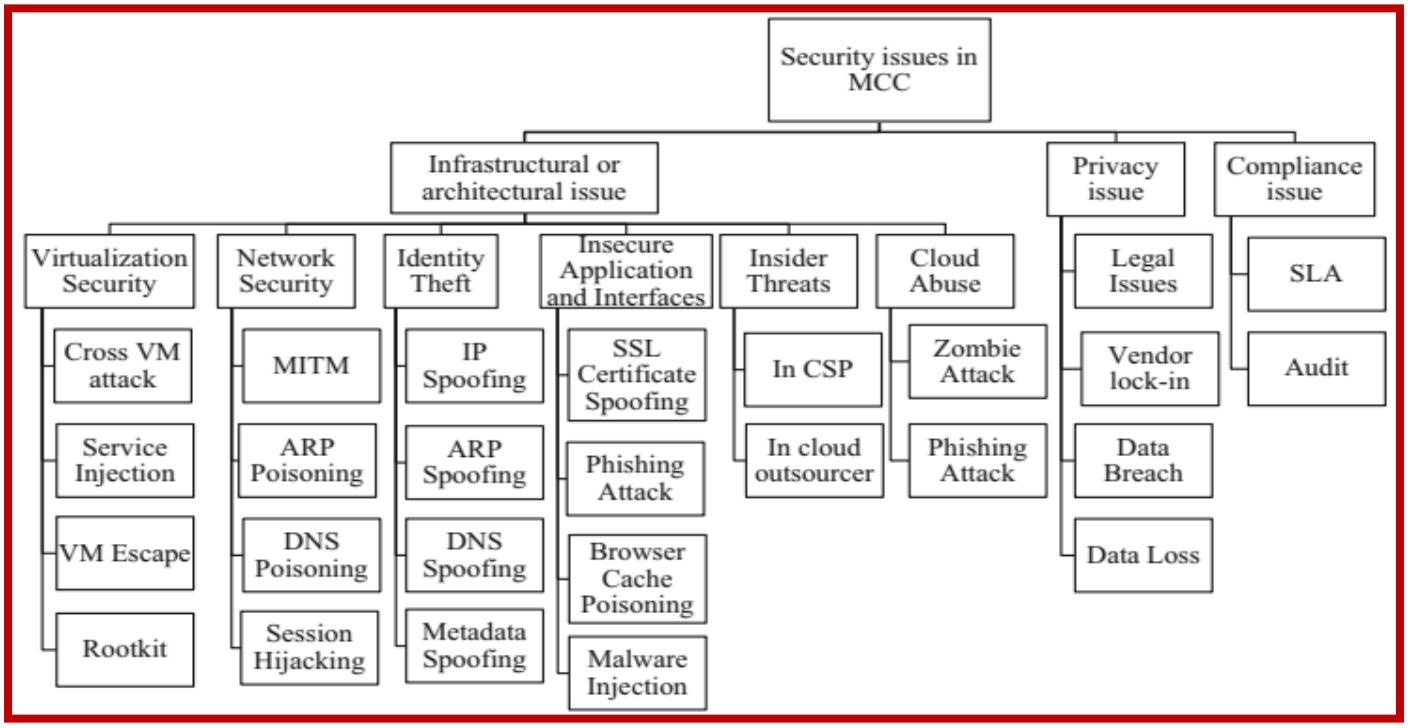

Figure 18 : taxonomie des problèmes et attaques dans le Cloud.

6. Les différentes travaux et solutions existant:

Lors de la sécurisation des données dans le Cloud, nous devons déterminer les états possibles montré dans la figure (19) dont lesquels les données peuvent se produire et les contrôles disponibles pour cet état. Avec la prolifération d'Internet et du Cloud computing ces dernières années, la protection des données statique est considérée comme aussi importante que la protection des données en transit. Les états possibles des données sont les suivants [12]:

- **Données en transit:** les données telles que la voix, la vidéo, le texte et les métadonnées sont supposées être en mouvement une fois qu'elles ont quitté le contrôle de l'entreprise et sont transférées sur le réseau ou dans le Cloud, et inversement, leur cryptage est donc essentiel. Cela implique non seulement la communication avec un composant extérieur au service Cloud, mais également la communication entre réseaux virtuels. Il doit être protégé contre les attaques d'espionnage au moyen de protocoles cryptographiques tels que SSL ou TLS en établissant un canal crypté et authentifié.
- **Les données statiques :** Il fait référence aux données inactives qui sont stockées physiquement sur un NAS (Network attached storage), SAN (Storage area network), des serveurs de fichiers sous forme de bases de données, des entrepôts de données, des sauvegardes hors site, etc. En plus du cryptage, des stratégies de contrôle d'accès fortes et une fédération des données doivent être utilisées pour contrecarrer les attaques.

- **Les données en cours d'utilisation :** Il fait référence aux données dynamiques qui sont stockées dans un état non persistant, par exemple des clés de données ou de chiffrement dans le cache, la mémoire principale, des transactions dans une file d'attente de messages, des données actuellement traitées par une application. Ces données sont généralement en clair pour exécuter des fonctions à valeur ajoutée telles que la recherche et la récupération des données, mais l'alliance pour la sécurité dans le Cloud recommande désormais le cryptage des données en cours d'utilisation pour une sécurité accrue.

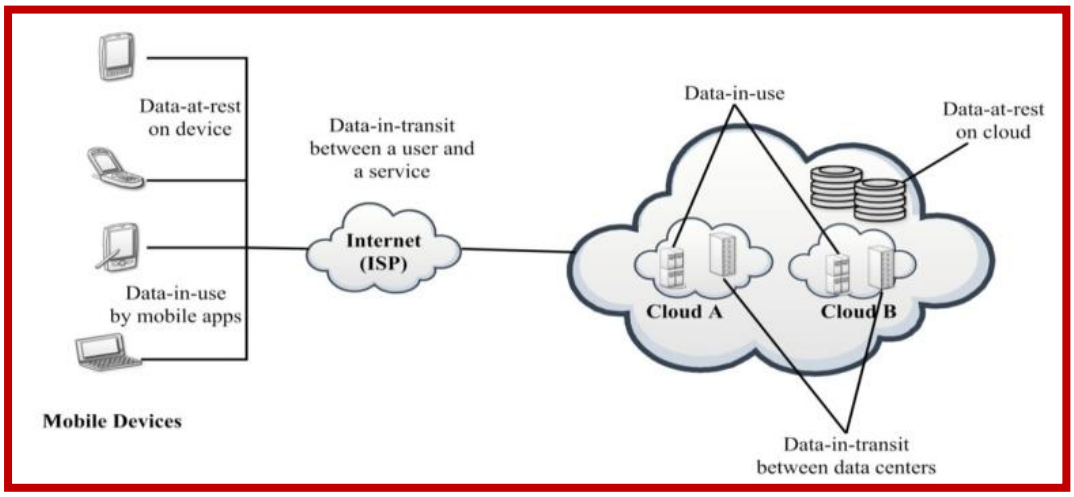

Figure 19: les états possibles de données [12]

Avec l'utilisation sophistiquée d'outils de piratage, les données stockées dans le Cloud présentent un risque accru d'attaque malveillante. Ainsi, il devrait également exister des schémas d'authentification robustes pour le Cloud computing afin de garantir l'accès aux données uniquement aux utilisateurs légitimes et autorisés. Les fournisseurs SaaS doivent vérifier l'identité de chaque utilisateur essayant d'accéder au système Cloud. Les systèmes de sécurité des données dans MCC sont classés comme suit [12]:

6.1. Solution basés-mot-de-passe:

La plupart des systèmes actuels ont adapté l'authentification basée sur un mot de passe dans laquelle le serveur Cloud maintient la base de données des mots de passe ou leurs valeurs de hachage.ces systèmes sont souvent vulnérables car l'attaquant peut facilement voler, deviner ou modifier les mots de passe stockés sur le serveur. Un schéma de contrôle d'accès a été proposé par Ren et al.2016 (F2AC: lightweight, fine-grained and flexible Access control), ce schéma prenait en charge des opérations dynamiques telles que l'ajout ou la suppression d'utilisateurs au sein d'un groupe ad hoc, autoriser ou révoquer les privilèges des membres de manière transitoire et séparer l'authentification d'accès de l'authentification système. Il est vulnérable à l'usurpation, à deviner le mot de passe et à l'attaque par rejeu (Replay attack). Les problèmes de mots de passe soulignent la nécessité d'un autre système d'identification de l'utilisateur.

6.2. Basé sur la Cryptographie:

C'est un moyen classique de préserver la confidentialité des données et d'authentifier les utilisateurs sur des réseaux non sécurisés. L'individu ou le groupe d'utilisateurs possédant la clé cryptographique correcte ont accès aux données cryptées. Il est important de payer attention aux états possibles des données: les données en transit, les données statiques et les données en cours d'utilisation. Le cryptage des données statiques est différent de l'utilisation de la cryptographie pour protéger les données en transit.la particularité est que les clés de cryptage doivent être temporaires, tandis que pour les données statiques, les clés peuvent être conservées aussi longtemps que les données stockées sont conservées cryptées. [3][12]

Le moyen le plus courant de protéger les données en mouvement consiste à utiliser le chiffrement associé à l'authentification pour créer un canal permettant la transmission sécurisée de données en provenance ou à destination du Cloud. Le cryptage permet de garantir la confidentialité des données en cas de violation de l'intégrité de la communication entre les deux parties. L'authentification est utilisée pour s'assurer que les parties qui s'envoient des données sont authentiques. Le transfert de données via des moyens programmatiques, par transfert manuel de fichiers ou via un navigateur utilisant les protocoles HTTPS, TLS ou SSL sont des protocoles sécurisés utilisés pour ce type de problème. Une clé PKI (Public Key infrastructure) est utilisée pour authentifier la transaction et les algorithmes de chiffrement sont utilisés pour protéger les données réelles. [3]

Il existe plusieurs variantes de schémas et de techniques basés sur la cryptographie dans un environnement de Cloud mobile. Ces schémas diffèrent par l'utilisation de l'algorithme cryptographique suivant :

6.2.1. Cryptographie symétrique :

Il a été développé dans les années 1970 dans lequel le cryptage et le décryptage sont effectués par clé partagée commune [51].

Ali et al. 2015 ont proposé une méthodologie de partage sécurisé des données dans le Cloud (SeDaSC : Secure data sharing in Cloud) [53] applicable à la fois dans les environnements conventionnels et MCC basés sur le cryptage symétrique. Il fournit la confidentialité, l'intégrité, le contrôle d'accès .Il implique trois entités, propriétaire de données, tiers de confiance connu sous le nom de serveur cryptographique sur le Cloud (CS : Cryptographic server) et le Cloud pour le stockage. Le propriétaire des données envoie le fichier de données, la liste des utilisateurs partageant le fichier de données et les paramètres requis pour générer une liste de contrôle d'accès au CS. CS est responsable du chiffrement, du déchiffrement, de la gestion des clés et de la maintenance des listes de contrôle d'accès. CS génère la clé symétrique et chiffre les données avant de les stocker dans le Cloud. CS divise la clé symétrique en deux parts de clé pour chaque utilisateur: une part est transmise à l'utilisateur et une autre part de clé est stockée dans la liste de contrôle d'accès (ACL) associée au fichier de données. Chaque fois qu'une personne quitte un groupe, CS supprime ses enregistrements des ACL des fichiers associés sans rechiffrer les fichiers. Étant donné que la clé n'est pas en sa possession, le membre ne peut déchiffrer aucun fichier de données. CS ne partage pas l'intégralité

de la clé avec les membres du groupe afin de contrecarrer les attaques d'initiés afin d'empêcher tout utilisateur malveillant appartenant à un groupe de déchiffrer, modifier et rechiffrer les données. il est vulnérable aux problèmes liées au données en transit, car le propriétaire des données transfère le fichier non chiffré à CS. Le fonctionnement de la méthodologie SeDaSC est présenté dans figure (21) :

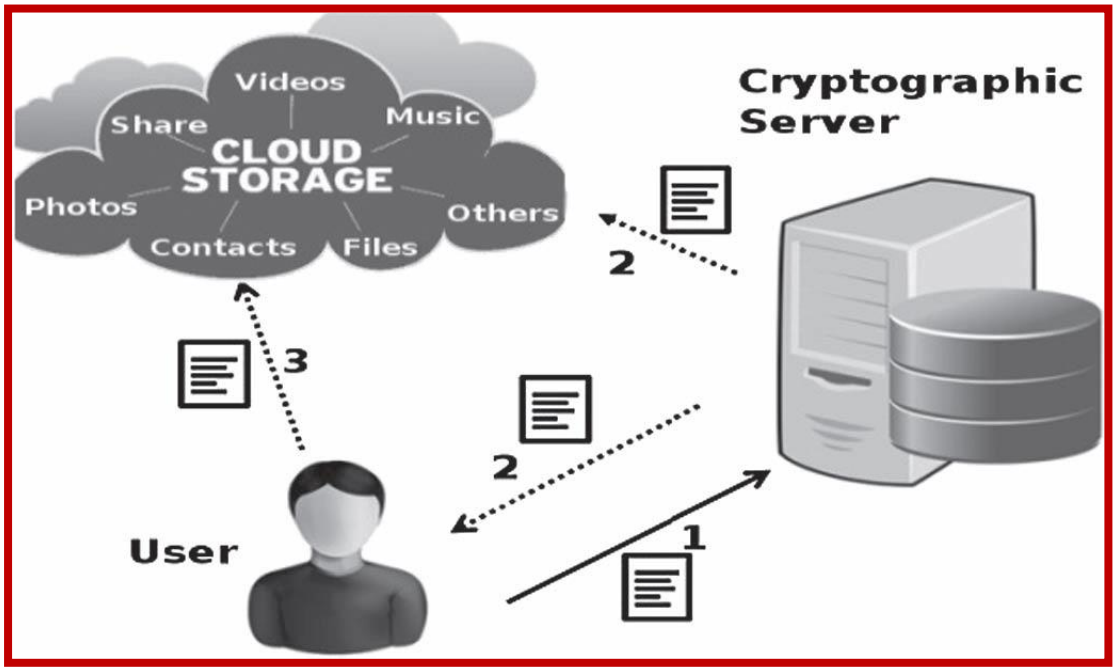

Figure 20 : Idée de base pour la méthodologie SeDaSC [53]

6.2.2. Cryptographie Asymétrique : il a été introduit par Diffie et Hellman en 1976 [54].

Les deux clés différentes sont impliquées, une clé publique connue de tous utilisée pour le chiffrement et la vérification des signatures numériques et la clé privée correspondante appartenant au destinataire utilisée uniquement pour le déchiffrement et la signature numérique du message.

Zhou et Huang 2011 [59] ont proposé (PP-CP-ABE : privacy-preserving cipher policy attribute-based encryption) et (ABDS : attribute-based data storage) pour un stockage efficace des données dans l'environnement MCC. Dans PP-CP-ABE, les opérations de cryptage et de décryptage gourmands en calculs sont externalisées vers les Fournisseurs Cloud sans compromettre le niveau de sécurité par rapport au CP-ABE traditionnel dans lequel les opérations sont effectuées localement.

Comme montré dans la figure (21) le framework se compose du propriétaire de données (DO : data owner), du demandeur de données (DR : data requester), du fournisseur de service de cryptage (ESP : encryption service provider), du fournisseur de service de décryptage (DSP : decryption service provider), du fournisseur de service de stockage (SSP : storage service provider) et de l'autorité de confiance (TA : trused

authority). PP-CP-ABE fournit des services de chiffrement et de déchiffrement aux DO et aux DR, respectivement, par l'intermédiaire de tiers (ESP et DSP) avec stockage des données chiffrées dans SSP sans

révéler le contenu des données et les clés secrètes. ABDS permet aux appareils mobiles légers et aux ressources limitées d'accéder et de gérer les données cryptées stockées dans le Cloud par le biais de fréquents téléchargements, chargement et mises à jour. Cette solution ne fournit pas l'intégrité des données.

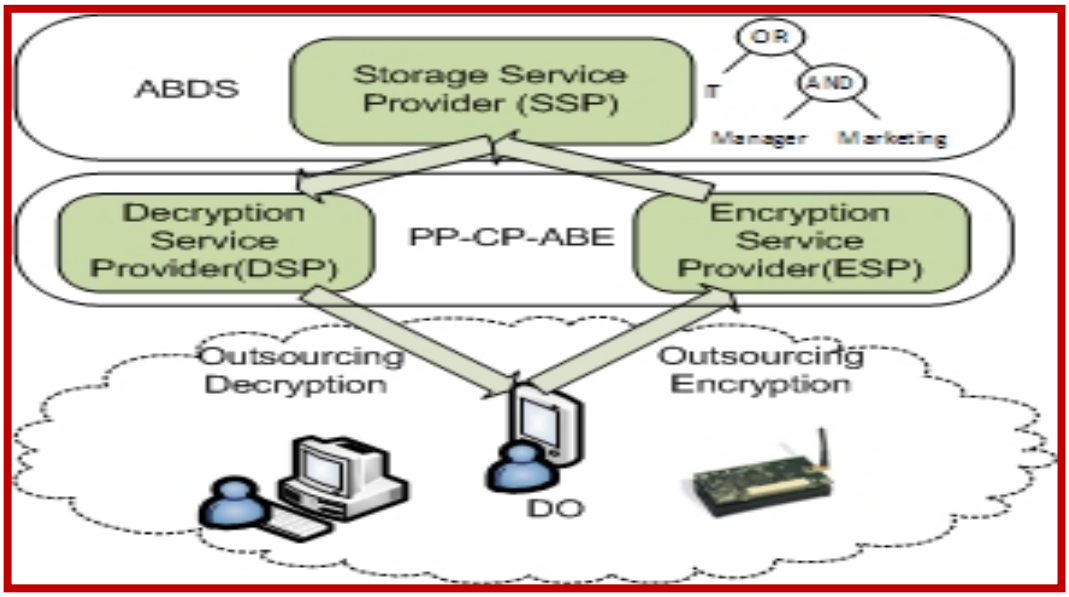

Figure 21 : Architecture système du Framework proposé [59]

6.3. Basés sur la biométrie:

Dans les schémas ou systèmes basés sur la cryptographie, un attaquant peut obtenir des clés de manière illégale et se faire passer pour un véritable utilisateur. Une solution très fiable et naturelle pour prévenir de telles attaques consiste à utiliser des traits biométriques, qui reconnaissent les utilisateurs par leurs caractéristiques physiologiques et comportementales. Vos doigts, vos yeux et votre voix sont toujours avec vous et ne peuvent être imités ni possédés par d'autres. Mais il est possible que des modèles biométriques tels que des empreintes digitales soient acquis furtivement et utilisés par un utilisateur malveillant. Il existe plusieurs solutions de reconnaissance biométrique basées sur le Cloud disponibles sur le marché, telles qu'Eyeprint ID, etc.

Les attaques dans un système biométrique peuvent être classées comme des attaques au niveau de l'interface utilisateur telles que l'usurpation d'identité, attaques à l'interface entre les modules, telles que les attaques par rejeu (Replay attack) ou par force brute, et sur la base de données de modèles, telle que la modification de modèles stockés. Les attaques peuvent se produire dans un système de reconnaissance biométrique à plusieurs endroits, comme illustré à la Figure ci-dessous :

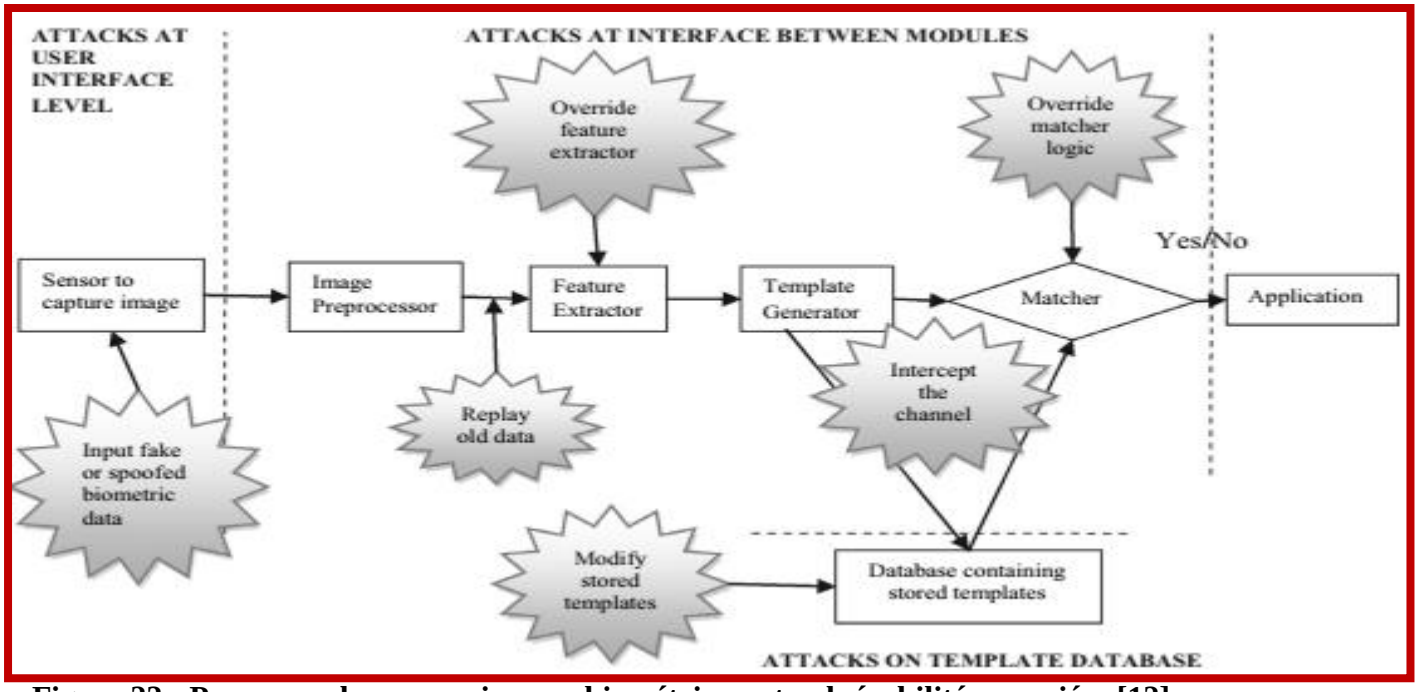

Figure 22 : Processus de reconnaissance biométrique et vulnérabilités associées [12]

- Présentation de biométrie fausse ou usurpée au capteur, par exemple un faux doigt ou un masque facial.
- Un système biométrique faible peut permettre à un intrus de prendre le contrôle de modèles en lançant une attaque per rejeu.
- Les caractéristiques extraites de l'image source peuvent être remplacées par un ensemble de caractéristiques frauduleuses,
- Le canal de communication entre la base de données et le matcher sur lequel le modèle stocké est envoyé peut être intercepté et modifié.
- Le matcher peut également être compromis et corrompu pour produire de faux scores de match.
- Les modèles stockés dans la base de données peuvent également être falsifiés localement ou à distance.

Les divers systèmes de sécurité basés sur la biométrie ont été conçus par divers chercheurs autour de caractéristiques uniques d'individus. La probabilité que deux personnes partagent le même trait biométrique est pratiquement négligeable. Pawle et Pawar 2013 [55] ont proposé le système de reconnaissance faciale (FRS) qui comprend deux phases, L'une d'entre elles est la phase d'enregistrement d'un nouvel utilisateur, au cours de laquelle l'utilisateur remplit le formulaire d'inscription avec les détails nécessaires lorsqu'il souhaite accéder au cloud.FRS vérifie si le nom d'utilisateur est disponible, le mot de passe est créé en capturant une image du visage via une caméra Web ou mobile. La prochaine étape est la détection de visage qui identifie le visage dans l'image capturée en éliminant les autres parties. L'image capturée doit être alignée pour pouvoir être reconnue et ses caractéristiques sont extraites pour créer un modèle de visage qui est stocké dans une base de données. Une fois le processus d'enregistrement

terminé, l'utilisateur enregistré se connecte au serveur Cloud en saisissant le nom d'utilisateur et l'image faciale est à nouveau capturée et comparée au modèle stocké. Si une correspondance est trouvée, l'accès est donné. Sinon, un message d'erreur est affiché.la figure ci-dessous illustre l'architecture FRS :

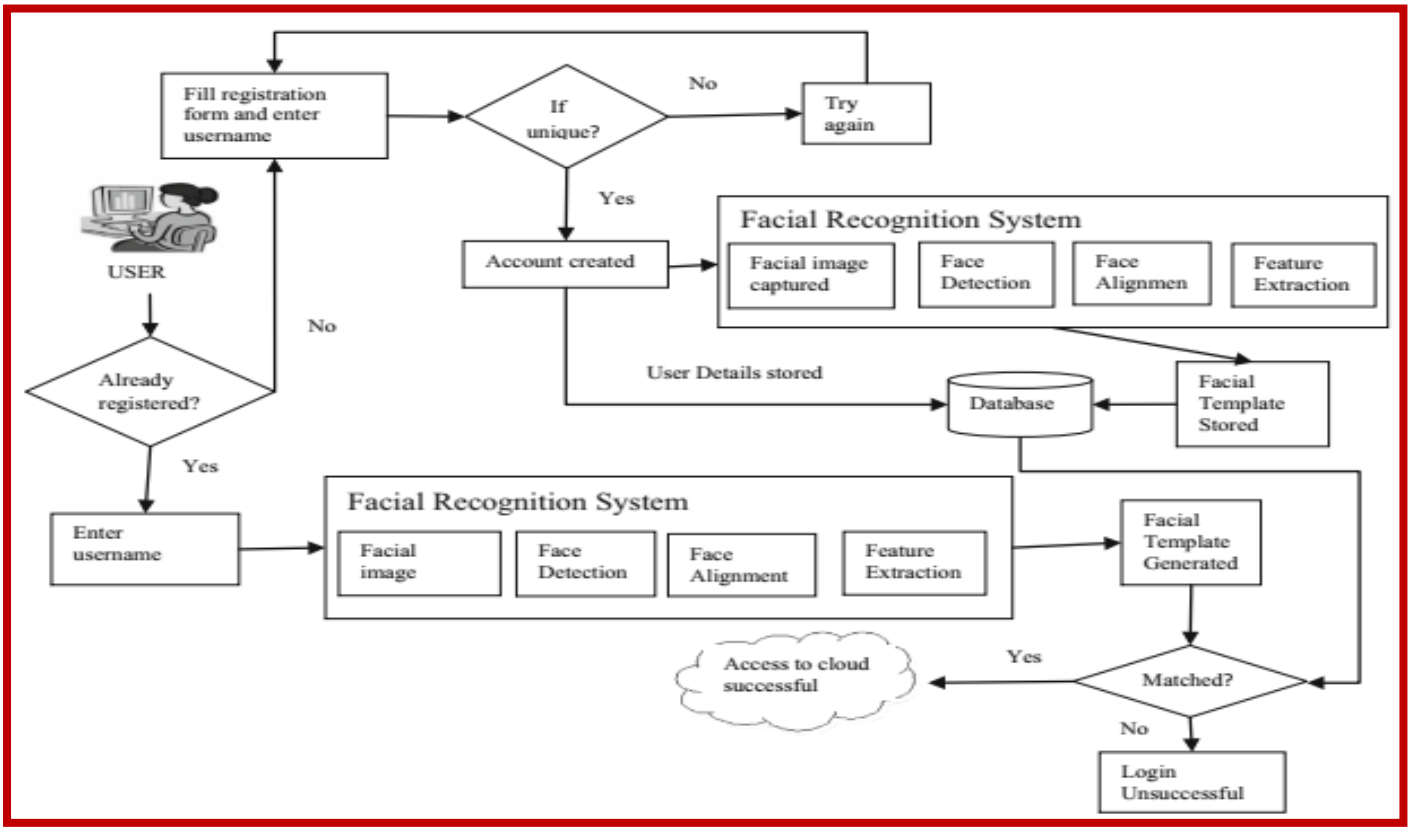

Figure 23 : Architecture FRS [12].

6.4. Basé sur l'authentification multifactorielle:

Ils combinent deux ou plusieurs schémas afin de fournir des schémas d'authentification et de sécurité des données plus efficaces. Il existe toujours un risque de déchiffrement du mot de passe, même si les informations biométriques sont protégées à l'aide d'un mot de passe dans certains schémas d'authentification multifactorielle. Il est possible d'intégrer la biométrie à l'infrastructure cryptographique. L'authentification biométrique, qui semble être une solution plus fiable que les autres mesures d'authentification traditionnelles, est également vulnérable aux attaques en matière d'authentification à distance sur des réseaux ouverts.

6.5. Basé sur la détection d'intrusion:

Un mécanisme de détection d'intrusion efficace devrait enregistrer toutes les signatures de programmes malveillants dans le téléphone, mais il nécessitera d'importantes ressources de calcul et de mémoire des périphériques mobiles.

Zonouz et al. [16] ont développé Secloud, une solution de sécurité légère pour Smartphones basée sur le Cloud. Il émule un Smartphone dans un nuage et le maintient synchronisé en envoyant les entrées de l'appareil et les connexions réseau en continu au nuage. Il se compose de 3 entités principales: l'agent client, un logiciel léger fonctionnant sur les Smartphones pour collecter les entrées utilisateur et capteur de l'appareil et passer à une réplique émulée sur le Cloud; serveur proxy pour la mise en miroir du trafic réseau entre les Smartphones et le réplique de Secloud; et un émulateur dans le Cloud exécutant diverses solutions de sécurité basées sur l'hôte et sur le réseau, telles que des analyseurs de virus, un vérificateur d'intégrité des fichiers, un IDS basé sur le réseau, Snort. Il effectue une analyse de sécurité à l'aide de techniques de détection d'intrusion sur une réplique émulée plutôt que sur le périphérique lui-même, réduisant ainsi les besoins en énergie et en puissance de traitement des périphériques mobiles.

Khoi Khac Nguyen et al. [57] Ont proposé un Framework avec un mécanisme de détection d'intrusion avancé basé sur l'apprentissage en profondeur qui permet de détecter diverses attaques avec une grande précision. L'idée principale de la méthode d'apprentissage en profondeur consiste à utiliser une base de données d'apprentissage pour former le réseau de neurones préétabli en mode hors connexion dans le but d'ajuster les poids du réseau de neurones. Ensuite, le réseau de neurones sera utilisé pour détecter les cybers attaques dans le système Cloud en mode en ligne.

La figure (24) montre comment le système fonctionne. Lorsqu'une demande, c'est-à-dire un paquet, d'un utilisateur mobile est envoyé au système, il sera transmis au module de détection d'attaque. Ce module remplit trois fonctions principales:

- **collecte et prétraitement des données** : qui est responsable de la collecte des données et du prétraitement de la demande pour correspondre au modèle d'apprentissage en profondeur.
- **reconnaissance des attaques :** qui est utilisé pour classifier les demandes entrantes en fonction du modèle d'apprentissage en profondeur formé.
- **traitement des requêtes :** qui détermine si la demande est normale ou suspecte ,Si la demande est normale, elle sera servie par les ressources Cloud disponibles. Sinon, la demande sera signalée au module de contrôle de sécurité.

  Lorsqu'une requête suspecte est envoyée au module de contrôle de la sécurité, la fonction de vérification de la requête est activée. En particulier, la demande sera vérifiée avec soin en comparant avec la base de données actuelle et / ou en envoyant aux fournisseurs de services de sécurité une double vérification. Si la demande est identifiée comme étant sans danger, elle sera traitée comme d'habitude. D'autre part, la demande sera traitée comme une demande malveillante et la fonction de défense d'attaque sera activée pour mettre en œuvre des politiques de sécurité rapides afin d'empêcher la propagation ainsi que les impacts de cette attaque.

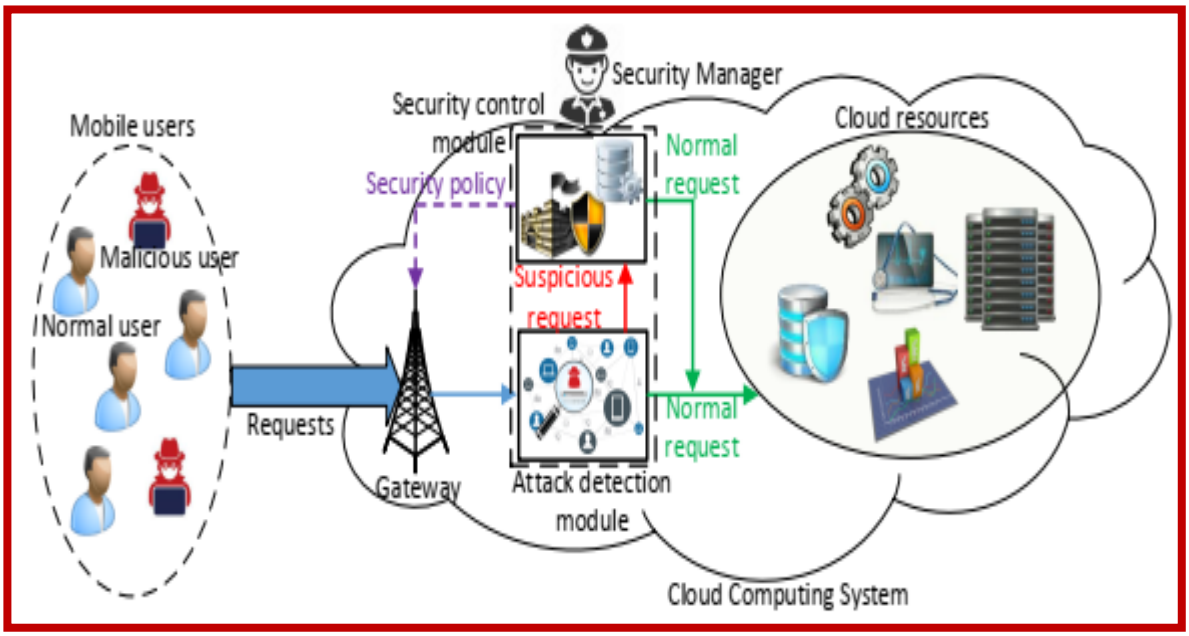

Figure 24 : système de détection de cyber attaques dans le Cloud computing [57]

7. Conclusion :

Dans ce chapitre, nous avons présenté une étude structurée de diverse attaques et problèmes de sécurité liés au déploiement d'applications mobiles sur le Cloud, ainsi que des enquêtes critiques sur les Frameworks de sécurité existantes proposées pour résoudre ces problèmes de sécurité. L'analyse comparative basée sur la force et la faiblesse des solutions prédominantes existantes suggère le besoin de mécanismes de sécurité futuristes pour exploiter de manière efficace des ressources de Cloud computing hétérogènes et des capacités d'appareils mobiles.

Chapitre 3

Authentification des utilisateurs et sécurisation des données dans le cloud

1. Introduction

Comme nous l'avons annoncé dans les chapitres précédents le Cloud computing mobile pose de nombreux problèmes de sécurité et de nombreuses solutions ont été proposées. L'un des aspects les plus importants sur lequel nous allons nous concentrer est l'autorisation et l'authentification avec la sécurisation des données.

L'authentification biométrique est devenue très populaire de nos jours dans les applications de préservation de la sécurité et de la confidentialité, telles que le contrôle d'accès, le système de surveillance, le traitement des visas, la vérification des frontières, etc. L'authentification biométrique est une technique qui s'appuie sur les caractéristiques biométriques uniques des individus pour vérifier l'identité de l'utilisateur afin de sécuriser l'accès aux dispositifs ou systèmes électroniques [1]. Les caractéristiques biométriques, telles que empreinte digitale, visage, composants faciaux, empreinte palmaire, géométrie de la main, iris, rétine, démarche et voix sont des formes communes d'attributs clés en authentification biométrique [2]. Ces dernières années, les visages humains sont largement utilisés en tant qu'attributs clés les plus distinctifs de l'authentification biométrique en raison de leurs caractéristiques uniques, robustesse, disponibilité, accessibilité et acceptabilité.

dans ce chapitre, nous proposons un framework de sécurité efficace combinant deux techniques de sécurité qui sont jeton homomorphique avec vérification distribuée des données codées par effacement et reconnaissance des visages pour authentifier les utilisateurs dans le cloud.

2. Architecture global du System proposé

Nous proposons un Framework de sécurité garantissant l'authentification et l'autorisation des utilisateurs, ainsi que la sécurité et l'exactitude du stockage des données dans le Cloud. Pour le serveur d'authentification, il repose sur la reconnaissance faciale et la vérification des utilisateurs, basées sur des réseaux de neurones à convolution et des réseaux d'inception. En ce qui concerne la sécurisation de la partie des données, nous nous sommes basés sur le jeton homomorphique et le code de correction de l'effacement (en englais : erasure correcting code) lors de la préparation de la distribution des fichiers pour assurer les redondances et garantir la fiabilité des données. La figure ci-dessous montre l'architecture globale du système Cloud :

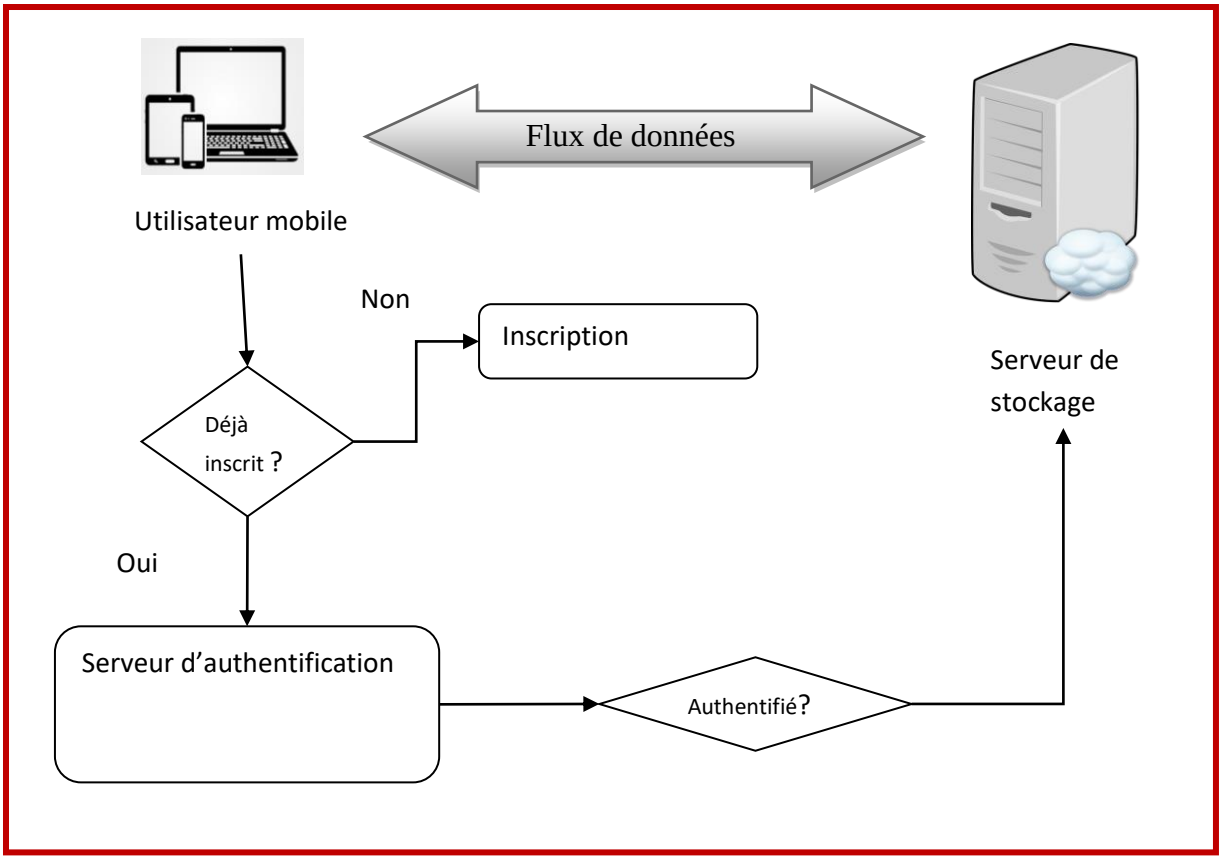

Figure 25 : Architecture globale du système proposé.

3. Les modules de Système proposé

➢ utilisateur

Les utilisateurs, dont les données doivent être stockées dans le Cloud et qui l'utilisent pour le calcul des données, comprennent à la fois des consommateurs individuels et des organisations.

➢ Fournisseur de services Cloud (CSP):

Un CSP, qui possède des ressources et une expertise importantes dans la création et la gestion de serveurs de stockage en Cloud distribués, possède et exploite des systèmes de Cloud computing en direct.

➢ Module de stockage de données en Cloud :

Stockage de données en Cloud, un utilisateur stocke ses données via un CSP dans un ensemble de serveurs en Cloud, qui s'exécutent simultanément, l'utilisateur interagit avec les serveurs en nuage via le CSP pour accéder à ses données ou les récupérer. Dans certains cas, l'utilisateur peut avoir besoin d'effectuer des opérations au niveau du bloc sur ses données. Les utilisateurs doivent être équipés de moyens de sécurité afin de pouvoir

assurer en permanence l'exactitude des données stockées, même en l'absence de copies locales. Au cas où les utilisateurs n'auraient pas nécessairement le temps, de faisabilité ou de ressources pour surveiller leurs données, ils peuvent déléguer les tâches à un TPA approuvé facultatif de leurs choix respectifs. Dans notre modèle, nous supposons que les canaux de communication point à point entre chaque serveur de Cloud et l'utilisateur sont authentifiés et fiables, ce qui peut être réalisé dans la pratique avec un minimum de temps système.

- **Serveur d'authentification en Cloud**

Le serveur d'authentification de notre modèle comporte une étape de reconnaissance faciale et de vérification. Après avoir renseigné toutes les informations nécessaires, y compris une photo prise pour l'utilisateur au cours de l'étape d'inscription, l'utilisateur doit passer par une étape qui consiste à reconnaître et à vérifier le visage.

4. Architecture de serveur d'authentification

L'architecture générale du serveur d'authentification proposé est illustrée à la figure. Elle comprend les étapes suivantes: capture d'image, détection de visage, extraction des caractéristiques, classification

- **Capture d'image** il s'agit de l'étape où l'image de la personne est capturée et visible sur son visage

- **Détection de visage**

Pour créer un détecteur de visage, nous avons utilisé OpenCV. Cette bibliothèque nous fournit un excellent algorithme de détection de visage en temps réel utilisant Haar Cascades. Open CV for JAVA a une classe appelée Cascade Classifier qui implémente l'algorithme. Au moment de la création de l'objet de la classe, vous devez indiquer l'emplacement du fichier xml nécessaire à CascadeClassifier pour détecter les visages sur l'image. Le fichier xml que j'utilise réellement est un fichier préformé qui est envoyé avec OpenCV. Le fichier s'appelle «haarcascade_frontalface_alt.xml»

- **Extraction des caractéristiques**

Afin de reconnaître les visages, nous aurions besoin d'extraire les caractéristiques de visage d'une image donnée. Nous pouvons soit former notre propre réseau de neurones pour obtenir des traits de bonne qualité, soit utiliser un réseau préformé. Dans ce projet nous avons utilisé le modèle FaceNet préformé. Le réseau préformé est juste un modèle qui a déjà été formé et qui en a calculé les poids.

- **Classification**

Dans la classification, nous nous sommes basés sur les réseaux siamois, nous allons continuer à utiliser l'architecture convolutifs, mais avec de nombreuses couches convolutives et couches connectées, à l'exception du fait que la dernière couche de prédiction (couche soft max) ne sera pas utilisée. Nous allons donc utiliser une fonction de similarité d qui mesure la similitude ou la différence entre deux images Si la fonction renvoie une valeur inférieure à une constante γ ou à un seuil, nous savons que les images sont assez similaires, sinon nous savons qu'elles sont différentes, donc pas le même visage ou le même personnage.la fonction Maintenant, le réseau de neurones pour chaque itération (par pas en avant et par propagation inverse) apprendra la fonction d comme indiqué :

$$\boldsymbol{d = \left(F(x^1) - F(x^2)\right)^2}$$

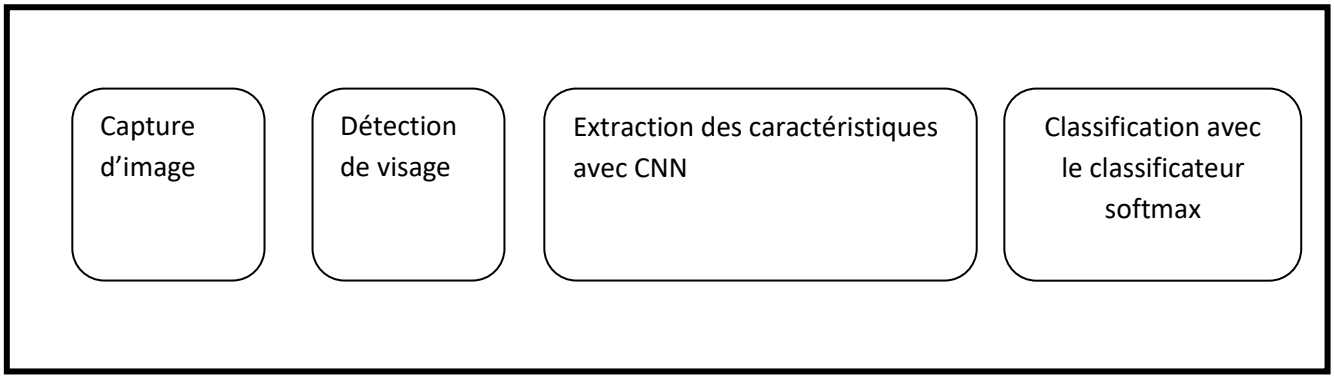

Figure 26 : Architecture de serveur d'authentification.

5. L'Apprentissage en profondeur et la reconnaissance faciale

5.1. la reconnaissance faciale

Le visage humain joue un rôle important dans la reconnaissance de la personne dans le système de surveillance basé sur la vision. La reconnaissance faciale est une technique permettant d'identifier ou de vérifier automatiquement une personne à partir d'une image ou d'une image vidéo. Comparée à d'autres systèmes biométriques, la reconnaissance faciale a le potentiel de reconnaître des sujets non coopératifs dans un environnement non intrusif. Manière.

Il est maintenant devenu le moyen d'identification biométrique le plus répandu et le plus utilisé [64]. La technologie de reconnaissance faciale a été développée sur la base de deux arrangements: métrique faciale et (Eigenfaces) [65]. Les mesures faciales reposent sur la

mesure des caractéristiques faciales telles que les yeux, le nez et la bouche. Eigenfaces fait référence à une approche de reconnaissance des visages basée sur l'apparence, qui cherche à capturer les variations dans une collection d'images de visages et à utiliser cette information pour coder et comparer des images de visages individuels de manière holistique (par opposition à des caractéristiques.

5.2. L'apprentissage en profondeur

L'apprentissage en profondeur est un domaine très riche, les réseaux de neurone sont la meilleure méthode pour l'adresser. Il existe de nombreuses architectures d'apprentissage en profondeur utilisées telles que: réseaux de neurones convolutionnel, réseaux de Boltzmann restreints (RBM), réseaux de croyances profondes (DBN), réseaux de neurones récurrents (RNN), autoencoders, etc., toutes ces architectures sont choisi sur la base des données ou de l'objectif d'apprentissage [66]. Le modèle choisi dans notre système est CNN, c'est le meilleur modèle utilisé pour le traitement de l'image et très efficace.

6. Le principe de réseau nuerons convolutionne l (CNN)

6.1. Les réseaux de nuerons convolutionne l (CNN)

Un réseau de neurones est un système de «neurones» artificiels interconnectés qui échangent des messages entre eux. Les connexions ont des pondérations numériques qui sont réglées pendant le processus de formation, de sorte qu'un réseau correctement formé répondra correctement lorsqu'il sera présenté avec une image ou un motif à reconnaître. Le réseau est constitué de plusieurs couches de «neurones» à détection de caractéristiques. Chaque couche contient de nombreux neurones qui répondent à différentes combinaisons d'entrées provenant des couches précédentes. Comme le montre la figure 1, les couches sont construites de sorte que la première couche détecte un ensemble de motifs primitifs dans l'entrée. la deuxième couche détecte des motifs de motifs, la troisième couche détecte des motifs de ces motifs, etc. Les CNN typiques utilisent 5 à 25 couches distinctes de reconnaissance de motif .[73]

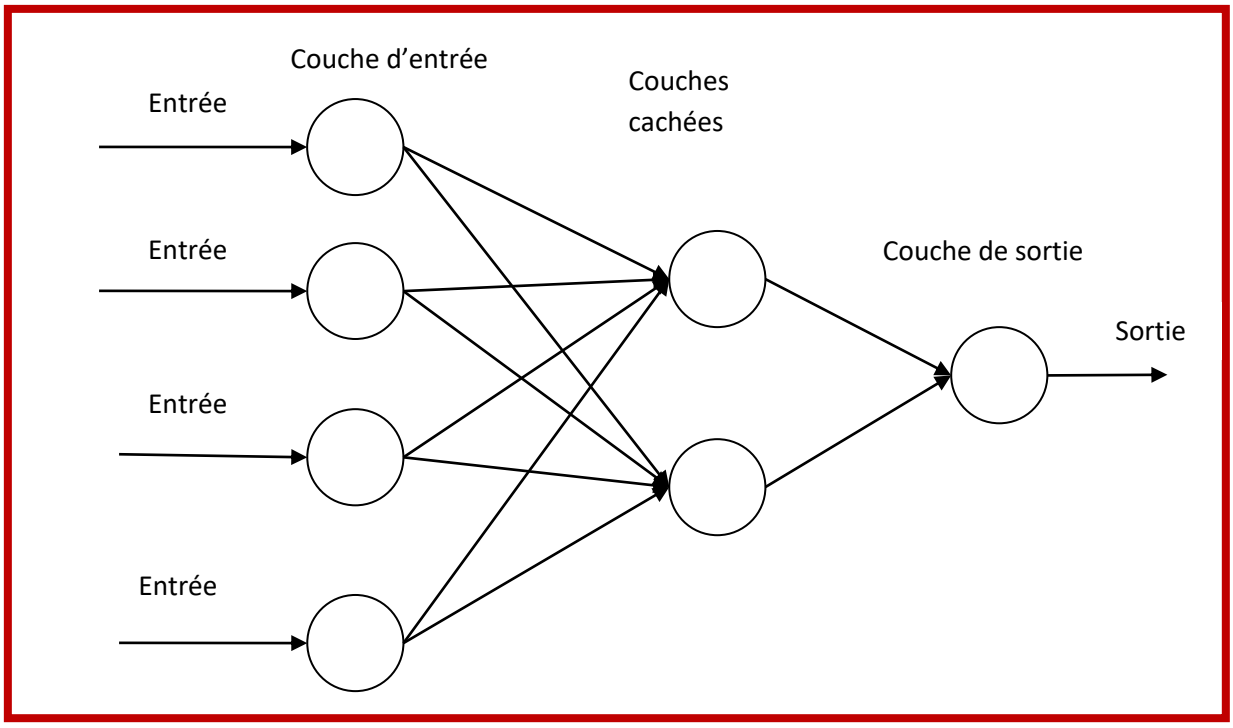

Figure 27 : Un simple réseau de neurones feedforward (FNN) à trois couches.

Des vecteurs d'image bruts d'entrée à la sortie finale du score de la classe, l'ensemble du réseau exprimera toujours une seule fonction de score perceptif (le poids). La dernière couche contiendra les fonctions de perte (Loss function) associées aux classes, et tous les conseils et astuces développés pour les ANN (artificial neural network) traditionnels s'appliquent toujours. La seule différence notable entre les CNN et les ANN traditionnels est que les CNN sont principalement utilisés dans le domaine de la reconnaissance de formes au sein d'images. Cela nous permet de coder des caractéristiques spécifiques à l'image dans l'architecture, ce qui rend le réseau plus adapté aux tâches axées sur l'image, tout en réduisant davantage les paramètres nécessaires à la configuration du modèle.

6.2. Architecture globale de CNN

Les CNN sont constitués de trois types de couches. Ce sont des couches convolutives (convolutional layers), des couches de mise en commun (Pooling layers) et des couches entièrement connectées (fully connected layers). Lorsque ces couches sont empilées, une architecture CNN a été formée. Une architecture CNN simplifiée pour la classification est illustrée à la figure :

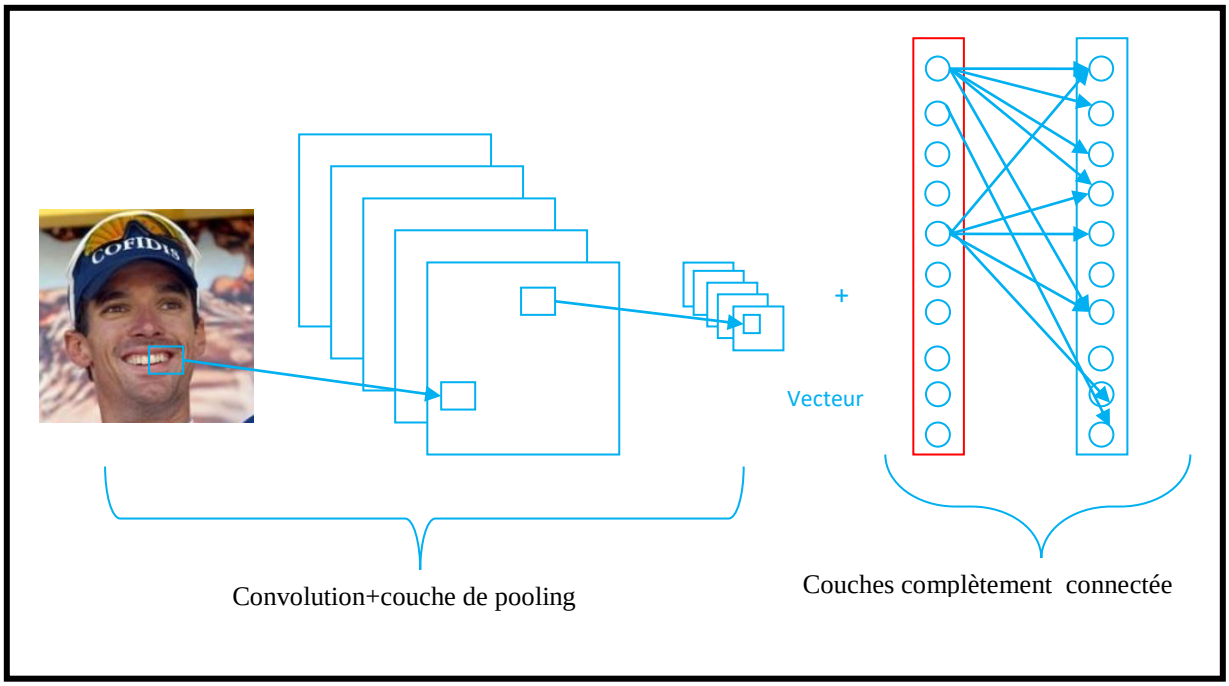

Figure 28: Une conception traditionnelle de réseaux de neurones convolutifs.

6.2.1. la Couche de convolution

L'entrée de chaque couche de convolution, comme le réseau de neurones traditionnel, est la sortie de la couche supérieure et est convolutée par plusieurs noyaux (Kernal) de convolution [72]. Les noyaux de convolution sont utilisés de manière répétée dans chaque champ sensoriel de la région entière et le résultat de la convolution constitue une carte des caractéristiques (features Map) de l'image d'entrée. Et les noyaux de convolution sont les contenus à apprendre de la couche de convolution, y compris la matrice de pondération w et le bias b. [72]

6.2.2. la Couche de Pooling

Les cartes de caractéristiques (feature Map en englais) de sortie obtenues après le calcul de la couche de convolution ne sont généralement pas beaucoup réduites en dimension. Si la dimension ne change pas, il faudra beaucoup de calculs et le processus d'apprentissage en réseau deviendra très difficile, ce qui donnera plus de chances d'obtenir un résultat raisonnable.[72]

La couche de pooling est généralement une couche destinée à réduire la dimension de la carte de caractéristiques et constitue une méthode de sous-échantillonnage non linéaire.

Dans le réseau, chaque carte de caractéristiques insérée dans la couche de pooling est

échantillonnée et le nombre de cartes de caractéristiques en sortie reste inchangé, mais la taille de chaque carte de caractéristiques sera plus petite. Ainsi, l'objectif de réduire la quantité de calcul et de résister au changement de micro déplacement est atteint. [72]

6.2.3. La Couche complètement connectée

Pour le réseau, après plusieurs piles continues de couches de convolution et de couches de regroupement, il y aura généralement plusieurs couches entièrement connectées à proximité de la couche de sortie. Et ces couches entièrement connectées forment un perceptron multicouche (MLP) jouant le rôle de classificateur.[72]

6.2.4. La Couche de régression Softmax

Comme les caractéristiques de visage sont plus complexes et que la catégorie de visage est plus importante et qu'il n'ya pas de modèle uniforme, le classifier softmax, qui possède une forte capacité de classification non linéaire, est utilisé à la dernière couche du réseau. Le classificateur Softmax est un multi-classificateur, qui peut non seulement compléter la tâche de dichotomie, mais également les multiples (plus de 2) tâche.[72]

6.3. Architecture de model de réseau convolutionnel proposé

Le schéma de principe de l'algorithme de reconnaissance CNN proposé est présenté à la figure (29) L'algorithme est principalement exécuté en trois étapes, comme ci-dessous:

1) Redimensionnez les images d'entrée au format 16x16x1, 16x16x3, 32x32x1, 32x32x3, 64x64x1 et 64x64x1.
2) Construisez une structure CNN avec quinze couches composées Ces quinze couches contiennent respectivement trois couches de convolution, trois couches de batch_normalization (bn), deux couches de mise en commun (max pooling), trois couches d'activation Relu, et des couches convolutives respectivement.
3) Après avoir extrait toutes les caractéristiques, utilisez le classifieur Softmax pour la classification.

Nous avons utilisé, l'algorithme de descente de gradient stochastique pour entraîner l'extracteur de caractéristiques et le classificateur, qui peuvent extraire les caractéristiques du visage et les classer automatiquement.

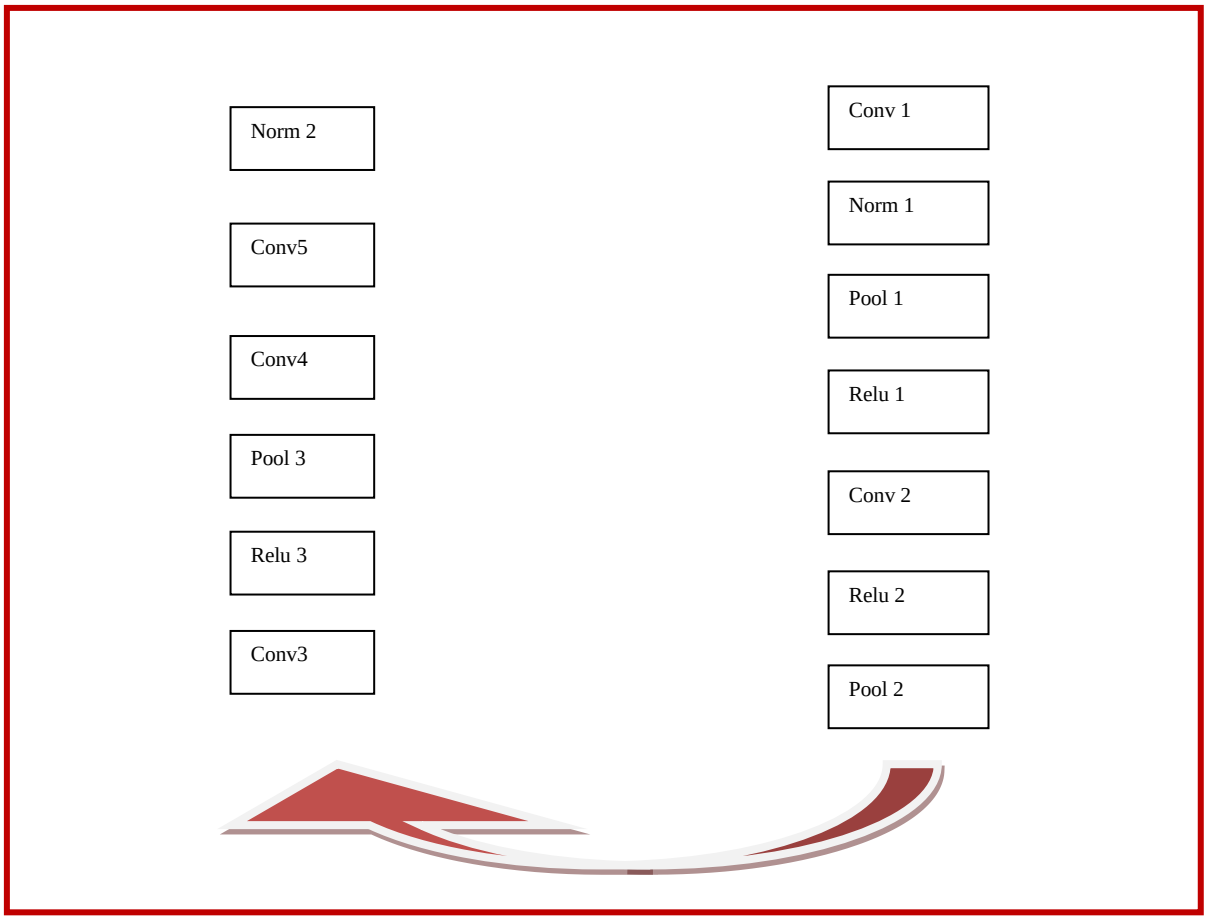

Figure 29 : La structure du bloc d'extraction de caractéristiques du CNN proposé.

6.4. Construction l'architecture de réseau neuronal

Dans un premier temps, nous devons construire l'architecture de réseau neuronal basée sur Inception Networks (première construction de GoogLeNet).

```
buildBlock3a(graph);
 buildBlock3b(graph);
 buildBlock3c(graph);

 buildBlock4a(graph);
 buildBlock4e(graph);

 buildBlock5a(graph);
 buildBlock5b(graph);

 graph.addLayer("avgpool",
         new SubsamplingLayer.Builder(SubsamplingLayer.PoolingType.AVG, new int[]{3, 3},
                 new int[]{1, 1})
                 .convolutionMode(ConvolutionMode.Truncate)
                 .build(),
         "inception_5b")
         .addLayer("dense", new DenseLayer.Builder().nIn(736).nOut(encodings)
                 .activation(Activation.IDENTITY).build(), "avgpool")
         .addVertex("encodings", new L2NormalizeVertex(new int[]{}, 1e-12), "dense")
         .setInputTypes(InputType.convolutional(96, 96, inputShape[0])).pretrain(true);

/* Uncomment in case of training the network, graph.setOutputs should be lossLayer then
 .addLayer("lossLayer", new CenterLossOutputLayer.Builder()
                 .lossFunction(LossFunctions.LossFunction.SQUARED_LOSS)
                 .activation(Activation.SOFTMAX).nIn(128).nOut(numClasses).lambda(1e-
4).alpha(0.9)

.gradientNormalization(GradientNormalization.RenormalizeL2PerLayer).build(),
         "embeddings")*/
 graph.setOutputs("encodings");
```

Figure 30 : code de creation de l'architecture CNN.

6.5. La phase d'Apprentissage

La formation de réseaux de neurones est particulièrement couteuse en termes de calcul et nécessite en même temps beaucoup d'efforts en raison d'une sélection de triplets effectuée avec soin. Grâce à l'apprentissage par transfert, nous pouvons utiliser les poids de réseau neuronal déjà formés, même à partir d'autres langages et structures. De cette manière, nous pouvons utiliser toutes les connaissances en détection de visage de ces réseaux de neurones acquises pendant l'apprentissage. Les poids sont lus à partir de fichiers Excel trouvés à

l'origine dans Keras Open Face, puis copiés dans le code java. Des efforts sont nécessaires pour adapter les poids de Keras à deeplearning4j.

```
buildBlock3a(graph);
 buildBlock3b(graph);
 buildBlock3c(graph);

 buildBlock4a(graph);
 buildBlock4e(graph);

 buildBlock5a(graph);
 buildBlock5b(graph);

 graph.addLayer("avgpool",
         new SubsamplingLayer.Builder(SubsamplingLayer.PoolingType.AVG, new
int[]{3, 3},
                 new int[]{1, 1})
                 .convolutionMode(ConvolutionMode.Truncate)
                 .build(),
         "inception_5b")
         .addLayer("dense", new DenseLayer.Builder().nIn(736).nOut(encodings)
                 .activation(Activation.IDENTITY).build(), "avgpool")
         .addVertex("encodings", new L2NormalizeVertex(new int[]{}, 1e-12),
"dense")
         .setInputTypes(InputType.convolutional(96, 96,
inputShape[0])).pretrain(true);

/* Uncomment in case of training the network, graph.setOutputs should be
lossLayer then
 .addLayer("lossLayer", new CenterLossOutputLayer.Builder()
                 .lossFunction(LossFunctions.LossFunction.SQUARED_LOSS)

.activation(Activation.SOFTMAX).nIn(128).nOut(numClasses).lambda(1e-
4).alpha(0.9)

.gradientNormalization(GradientNormalization.RenormalizeL2PerLayer).build(),
         "embeddings")*/
 graph.setOutputs("encodings");
```

Figure 31 : code la phase d'apprentissage.

6.6. La phase de test

A fin de tester l'architecture Cnn proposé on a divisé la base donnée LFW en deux partie la première utilisé pour le test est la deuxième utilisé pour l'apprentissage

7. évaluation

Précision (Accuracy) : pour chaque image du fichier LFW non aligné, dans un fichier csv, nous l'avons téléchargée (data.csv). Nous avons ensuite utilisé le modèle FaceNet que nous avons utilisé lors du training pour tester le modèle de reconnaissance faciale. Nous avons utilisé la configuration avec image restreinte pour tester ce modèle sur la base du fichier [pairs.txt], Nombre de faces: 13075, Nombre de tests: 6000, Accuracy: 98,4.

8. Interfaces d'application

8.1. Login administrateur

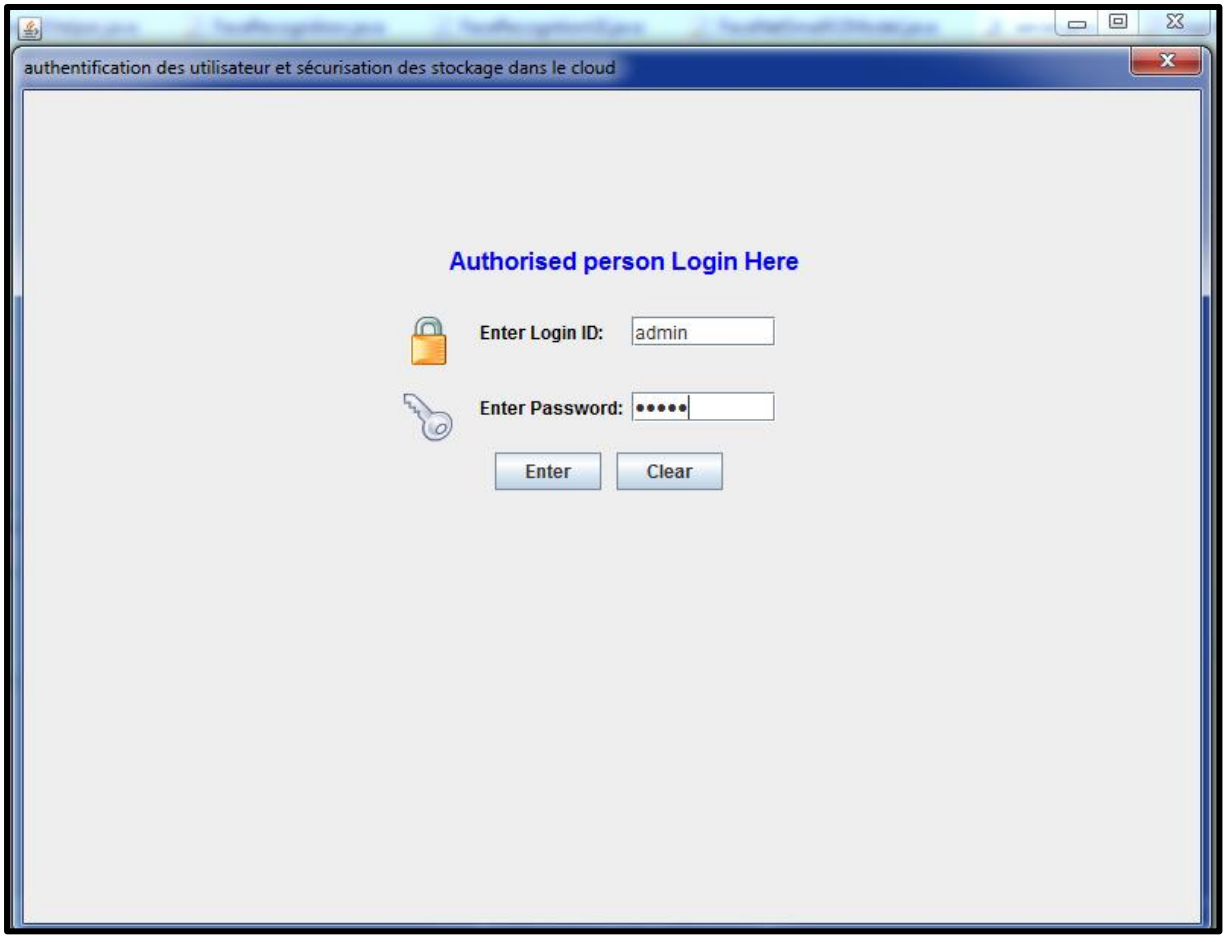

Figure 32 : Login administrateur.

8.2. Serveur d'authentification

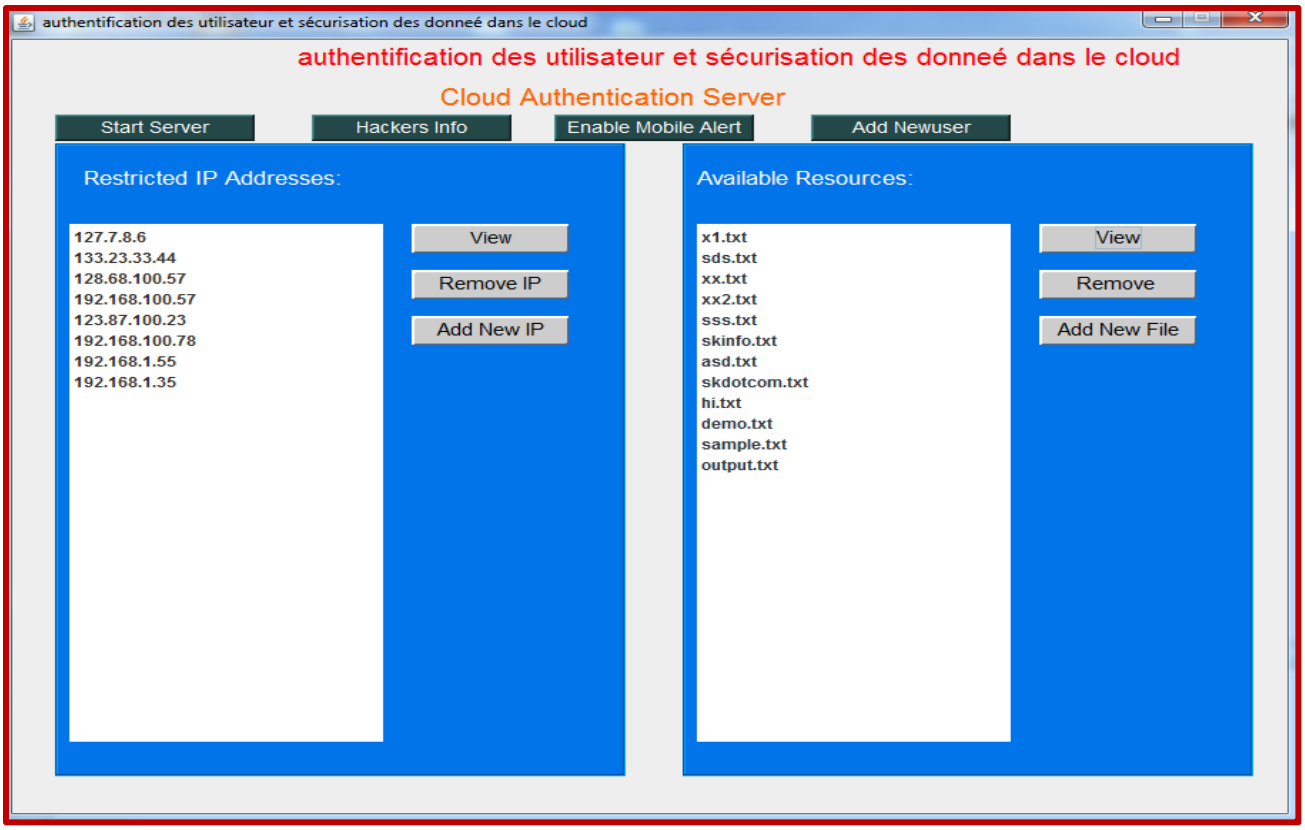

Figure 33 : serveur d'authentification.

8.3. Interface de la reconnaissance faciale

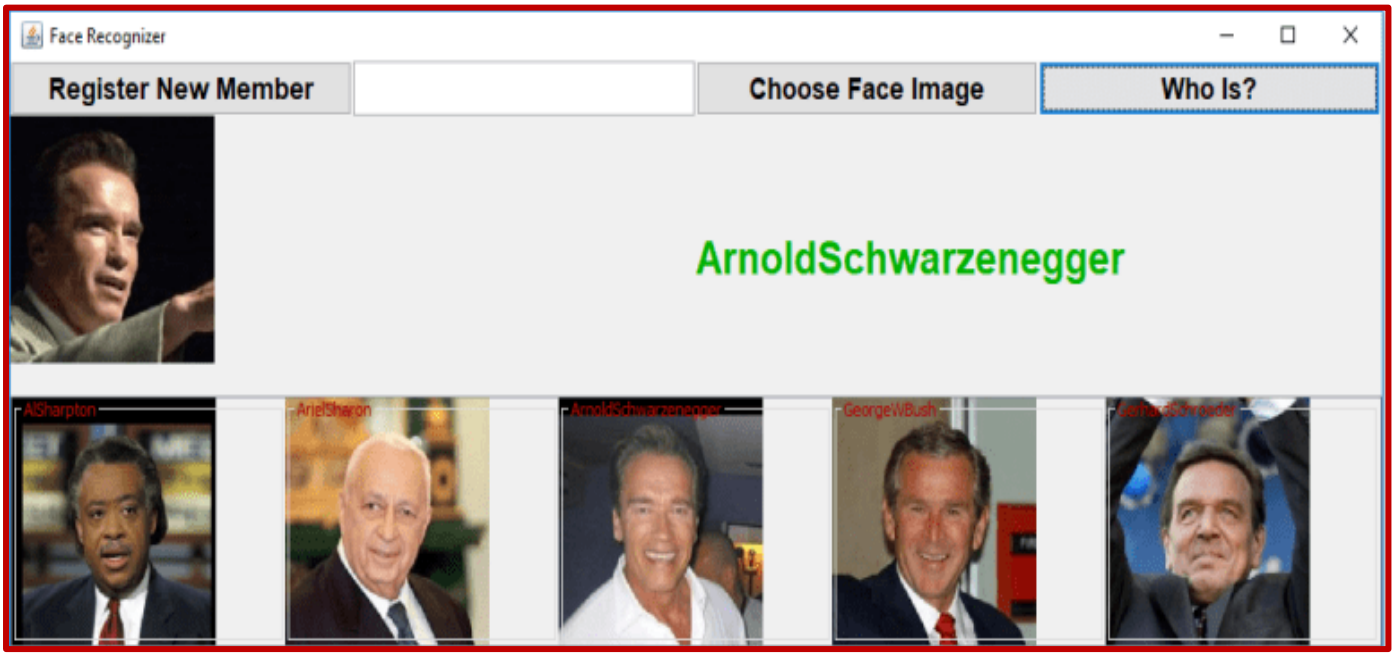

Figure 34 : reconnaissance facial des utilisateurs.

9. Outils / Bibliothèques utilisées

- Java, Swing, RMI,
- OpenCV
- Keras,DL4J
- Eclipse

10. Conclusion

Dans ce chapitre, nous avons proposé un framework de sécurité efficace et robuste assurant la sécurité des données et fournissant un schéma d'authentification biométrique basé sur la reconnaissance faciale. Le schéma utilise un réseau de neurones convolutionnel avec un algorithme de propagation en arrière pour reconnaître le visage de l'utilisateur et utilise un jeton homomorphique avec une vérification distribuée des données codées par effacement. Le système authentifie un utilisateur sur la base de la correspondance correcte de son visage avec une base de données de visages.

Conclusion Générale

Les problèmes de sécurité représentent un problème majeur pour les systèmes d'information adoptés, en particulier dans les environnements de cloud computing, dans lesquels les applications et les données sensibles sont transférées dans les datacenters en cloud. Le cloud computing pose de nombreuses nouvelles vulnérabilités telles que le contrôle des accès, les vulnérabilités de virtualisation, les vulnérabilités de données et les vulnérabilités de logiciels. En outre, avec l'évolution des technologies de cloud computing et le nombre croissant d'utilisateurs du cloud, les dimensions de la sécurité ne cesseront de croître.

Les services de cloud computing sont basés sur le partage. Le cloud computing fournit une variété de services tels qu'IaaS, SaaS et PaaS. Ces services étant des services payants, la sécurité est une préoccupation majeure pour identifier un utilisateur autorisé dans le cloud computing. Pour fournir des services de cloud uniquement à l'utilisateur autorisé, une authentification sécurisée est nécessaire dans le cloud computing. Il y a tellement de techniques d'authentification telles que mot de passe, reconnaissance vocale, reconnaissance de doigt, reconnaissance de la paume, etc., mais elle présente néanmoins certains inconvénients: parfois, les techniques de mot de passe ne sont pas réalisables. L'utilisateur peut oublier ce mot de passe, etc. Il est donc préférable d'utiliser le système de reconnaissance faciale plutôt que les techniques d'authentification traditionnelles ou biométriques. Le système de reconnaissance faciale améliore considérablement le niveau de sécurité du fournisseur de cloud en termes d'authentification sécurisée.

Le framework que nous proposons vise à sécuriser l'accès au cloud via la reconnaissance facial. Le framework assure également la sécurité et l'exactitude du stockage des données. Les caractéristiques les plus importantes de notre framework sont la combinaison des techniques puissantes et efficaces, telles que le codage de l'effacement (erasor coding)et la reconnaissance des visages, afin de fournir un haut niveau de sécurité. Bien qu'il présente certaines limites, car le réseau de neurones que nous avons utilisé pour le système de reconnaissance des visages doit encore être amélioré, mais toujours il a donné une performance satisfaisante

Bibliography:

[1] Aery, Manish. (2016). Mobile Cloud Computing: Security Issues and Challenges. International Journal of Advanced Computer Research. 7.

[2] https://cloud-computing.developpez.com/actu/97105 .mars 2016

[3] El Alloussi, Hassan & Laila, Fetjah & Sekkaki, Abderrahim. (2012). L'état de l'art de la sécurité dans le Cloud Computing.

[4] Toumi, Hicham & Eddaoui, A & Talea, Mohamed & Benlahmar, EL Habib. (2014). VERS UNE ARCHITECTURE DE SÉCURITÉ DE CLOUD COMPUTING.

[5] Modares, Hero & Lloret, Jaime & Moravejosharieh, Amir & Salleh, Rosli. (2014). Security in mobile cloud computing. 3. 1548-1560. 10.4018/978-1-4666-6539-2.ch072.

[6] Fernando, Niroshinie, Loke, Seng W. and Rahayu, Wenny 2013, Mobile cloud computing: a survey, Future generation computer systems, vol. 29, no. 1, pp. 84-106, doi: 10.1016/j.future.2012.05.023.

[7] Suhas, Anirudh. (2015). Mobile Cloud Computing: architecture, applications and as a next generation of cloud computing. 10.13140/RG.2.1.4436.6563.

[8] M. Padma et al,International Journal of Computer Science and Mobile Computing, Vol.3 Issue.5, May-2014, pg. 972-97

[9] Sulami, Noha & Monowar, Muhammad Mostafa. (2015). Data Confidentiality and Integrity in Mobile Cloud Computing. Journal of Emerging Trends in Computing and Information Sciences. 6. 6.

[10] Dr. Stefan Hüsemann. (2012). Les enjeux du Cloud Computing en enterprise :L'intégration dans le Cloud.

[11] Ahmin,A. (2014) systéme de détection d'intrusion Adaptatif et distribué.

[12] Bhatia, T. & Verma, A.K. J Supercomput (2017) 73: 2558. https://doi.org/10.1007/s11227-016-1945-y

[13]. Ren W, Zeng L, Liu R, Cheng C (2016) F2AC: a lightweight, fine-grained, and flexible access control scheme for file storage in mobile cloud computing. Mob Inf Syst 2016:1–9. doi:10.1155/2016/5232846

[14]Khan AN, Kiah MLM, Khan SU, Madani SA (2013) Towards secure mobile cloud computing: a survey. Future Gener Comput Syst 29(5):1278–1299

[15] Rajkumer, B. et al. (2013, Mai). "Mastering Cloud Computing: Foundations and Applications Programming". Publier par: Morgan Kaufmann. (pp.3-14), 468p.

[16] Zonouz S et al (2013) Secloud: a cloud based comprehensive and lightweight security solution for smartphones. Comput Secur 37(9):215–227

[17] http://www.omnisecu.com/ccna-security/different-classes-of-network-attacks-and-how-to-defend-them.php

[18] T.Swathi et al., International Journal of Computer Science and Mobile Computing, Vol.3 Issue.5, May- 2014, pg. 540-546

[19] White Paper, "Mobile Cloud Computing Solution Brief," AEPONA, November 2010.

[20] Hoang T. Dinh et al., A Survey of Mobile Cloud Computing: Architecture, Applications, and Approaches.

[21] X. Chen, J. Liu*, J. Han, and H. Xu, " Primary Exploration of Mobile Learning Mode under a Cloud Computing Environment," in Proceedings of the International Conference on E-Health Networking, Digital Ecosystems and Technologies (EDT), vol. 2, pp. 484 - 487, June 2010.

[22] H. Gao and Y. Zhai, "System Design of Cloud Computing Based on Mobile Learning," in Proceedings of the 3rd International Symposium on Knowledge Acquisition and Modeling (KAM), pp. 293 - 242, November 2010.

[23] Jian Li, "Study on the Development of Mobile Learning Promoted by Cloud Computing," in Proceedings of the 2nd International Conference on Information Engineering and Computer Science (ICIECS), pp. 1, December 2010.

[24] L. T. Kohn, J. M. Corrigan, and S. Donaldson, "To Err Is Human: Building a Safer Health System," NATIONAL ACADEMY PRESS Washington, 1999.

[25] D. Kopec, M. H. Kabir, D. Reinharth, O. Rothschild, and J. A. Castiglione, "Human Errors in Medical Practice: Systematic Classification and Reduction with Automated Information Systems," Journal of Medical Systems, vol. 27, no. 4, pp. 297 - 313, August 2003.

[26] https://www.devteam.space/blog/virtualization-techniques-in-cloud-computing/.

[27] Thinh Le Vinh. Security and Trust in Mobile Cloud Computing. Cryptography and Security [cs.CR]. Conservatoire national des arts et metiers - CNAM, 2017. English.

[28] K.Kavitha, Study on Cloud Computing Model and its Benefits, challenges International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization) Vol. 2, Issue 1, January 2014

[29] Asha Mathew,"security and privacy issues of cloud computing; solutions and secure framework,"InternationalJournal of Multidisciplinary Research", Vol.2 Issue 4, April 2012, ISSN 2231 5780.

[30] NikhileshBarik, "Benefits and Challenges in Cloud Computing", "International Journal of Network Security & Its Applications (IJNSA)", Vol.4,No.1,2012.

[31]https://searchservervirtualization.techtarget.com/definition/hardware-assisted-virtualization

[32] Peter Mell (NIST), Tim Grance (NIST) ,The NIST Definition of Cloud Computing ,National Institute of Standards and Technology Special Publication 800-1457 pages (September 2011).

[33] Robert Brennan Hart and Edward Wilson-Smythe,The new realities of cloud computing in 2018.

[34] https://medium.com/@Unfoldlabs/8-trends-in-cloud-computing-for-2018-d893be2d8989.

[35] https://timesofcloud.com/cloud-tutorial/history-and-vision-of-cloud-computing/

[36] https://blog.3li.com/cloud-les-modeles-de-deploiement/.

[37] Mohamed Shameem, P & Shaji, R.S.. (2013). A Methodological Survey on Load Balancing Techniques in Cloud Computing. Asian Journal of Information Technology. 12. 160-169. 10.3923/ajit.2013.160.169.

[38] http://tech.gaeatimes.com/index.php/archive/top-10-cloud-computing-service-providers-in-2010/

[39] https://www.sam-solutions.com/blog/best-cloud-computing-service-providers/

[40] Mr. C.Arun, Dr. K.Prabu, ADVANTAGES OF MOBILE CLOUD COMPUTING, International Research Journal of Engineering and Technology (IRJET) ,Volume: 05 Issue: 03 ,Mar-2018.

[41] https://negosentro.com/what-are-the-advantages-and-disadvantages-of-mobile-cloud-computing/ ,December 7, 2016 .

[42] Surabhi S.Golechha et al, Mobile Cloud Computing: World's Leading Technology for Mobile Devices / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (2) , 2014

[43] https://searchservervirtualization.techtarget.com/definition/hypervisor

[44] https://www.cloudworldwideservices.com/en/cloud-adoption-statistics-cloud-future/

[45] P. Ravi Kumar et al. 6th International Conference on Smart Computing and Communications, ICSCC 2017, 7-8 December 2017, Kurukshetra, India Exploring Data Security Issues and Solutions in Cloud Computing.

[46] (Liorens et al, 2006) Liorens, C., Levier, L., Valois, D. (2006), Tableaux de bord de la sécurité réseau, éditions eyrolles, ISBN: 2-212-11973-9.

[47] Salifu Abdul-Mumin , DETECTION OF MAN-IN-THE-MIDDLE ATTACK IN IEEE 802.11 NETWORKS MAY, 2011

[48] Pareek, Shilpa & Gautam, Ashutosh & Dey, Ratul. (2017). Different Type Network Security Threats and Solutions, A Review. IPASJ International Journal of Computer Science (IIJCS) ISSN 2321-5992. 5. 001-010.

[49] https://security.stackexchange.com/questions/183723/i-started-to-learn-about-mitm-attacks-and-i-cant-figure-out-few-things

[50] https://www.cse.wustl.edu/~jain/cse571-11/ftp/virtual/index.html

[51] Simmons GJ (1979) Symmetric and asymmetric encryption. ACM Comput Surv (CSUR) 11(4):305–330

[52] Stallings W (2006) Cryptography and network security: principles and practice. Prentice Hall, Upper Saddle River

[53] Ali M et al (2015) SeDaSC: secure data sharing in clouds. IEEE Syst J PP(99):1–10. doi:10.1109/JSYST.2014.2379646

[54]Diffie W, Hellman ME (1976) New directions in cryptography. IEEE Trans Inf Theory 22(6):644–654

[55] Pawle A, Pawar P (2013) Face recognition system (FRS) on cloud computing for user authentication. Int J Soft Comput Eng 3(4):189–192

[56] Sabiyyah Sabir, Security Issues in Cloud Computing and theirSolutions: A Review, (IJACSA) International Journal of Advanced Computer Science and Applications,Vol. 9, No. 11, 2018

[57] Khoi Khac Nguyen et al. Cyberattack Detection in Mobile Cloud Computing: A Deep Learning Approach ,16 Dec 2017.

[58] Inderjeet Kaur Detection and prevention of ARP cache poisoning June 2013

[59] Zhou Z, Huang D (2011) Efficient and secure data storage operations for mobile cloud computing. In:Proceedings of the 8th International Conference on Network and Service Management. Laxenburg, Austria, pp 37–45

[60] Dijiang Huang and Huijun Wu, Mobile Cloud Computing Foundations and Service Models,2018.

[61]BENDIAB GUELTOUM ,2015, Sécurité des applications métiers au niveau du Cloud Computing : Contrôle d'accès au niveau des APIs du Cloud Computing

[62] Arnold, J. et al. (2011, Août). "Guide for Security-Focused Configuration Management of Information Systems". Rapport consulté le 15 avril, 2014, sur NIST Special Publication 800-128: http://csrc.nist.gov/ publications/PubsSPs.html.

[63] Mozammel Chowdhury , Junbin Gao, and Rafiqul Islam School of Computing & Mathematics, Charles Sturt University, Bathurst, Australia.

[64] Gopalan, R., Jacobs, D.: Comparing and combining lighting insensitive approaches for face recognition. Comput. Vis. Image Underst. 114(1), 135–145 (2010).

[65] Turk, M.A., Pentland, A.P.: Face recognition using eigenfaces. In: Proceedings of the IEEE, pp. 586–591 (1991)

[66] Deep Learning for Biometrics: A Survey KALAIVANI SUNDARARAJAN and DAMON L. WOODARD, University of Florida

[67]Ali, Mazhar & U. Khan, Samee & Vasilakos, Athanasios. (2015). Security in Cloud Computing: Opportunities and Challenges. Information Sciences. 305. 10.1016/j.ins.2015.01.025.

[68]M. Sadiku, S. Musa, O. Momoh, Cloud computing: opportunities and challenges, IEEE Potentials 33 (1) (2014) 34–36.

[69]M. Aslam, C. Gehrmann, M. Bjorkman, Security and trust preserving VM migrations in public clouds, in: IEEE 11th International Conference on Trust,Security and Privacy in Computing and Communications (TrustCom), 2012, pp. 869–876

[70] R. Latif, H. Abbas, S. Assar, Q. Ali, Cloud computing risk assessment: a systematic literature review, in: Future Information Technology, Springer,
Berlin, Heidelberg, 2014, pp. 285–295.

[71] Chris Kanich. 2018. DeepAuth: A Framework for Continuous User Reauthentication in Mobile Apps. In The 27th ACM International Conference on Information and Knowledge Management (CIKM'18), October 22–26, 2018, Torino,Italy. ACM, New York, NY, USA, 9 pages.

[72] Kewen Yan et al, Face Recognition Based on Convolution Neural Network, Proceedings of the 36th Chinese Control Conference July 26-28, 2017, Dalian, China

[73] Samer Hijazi, Rishi Kumar, and Chris Rowen, IP Group, Cadence ,Using Convolutional Neural Networks for Image Recognition.