République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université Mohammed Seddik Ben Yahia - Jijel

Faculté des Sciences Exactes et Informatique
Département d'Informatique

Mémoire de fin d'études pour l'obtention du diplôme de

Master en Informatique

Option : Réseaux et sécurité

Thème

Un système basé sur les certificats et les commentaires pour une gestion de confiance dynamique dans un environnement cloud multi-domaines.

Présenté par :

- Bouhariche Amine
- Bourouis Hicham

Encadré par :

- Lounis Newal

Année universitaire : 2020 - 2021

Dédicace

Je dédie ce travail à :

mon père, qui veillait sur notre confort et notre éducation, j'espère qu'Allah prolonge sa vie afin de qu'il se réjouisse avec plus de succès.

celle qui m'a transmis la vie, l'amour, le courage, à toi **chère mère** toutes mes joies, mon amour et ma reconnaissance.

mes chers frères et ma belle soeur.

Hicham pour son entente et son sympathie.

toute ma famille.

mes chers amis et mes collègues de promotion.

tous ceux ou celles qui me sont chers.

tous ceux qui ont participé à la réalisation de ce travail.

Amine

Dédicace

je dédie ce modeste travail à :

*** Ma chère mère ***

Quoi je fasse ou que je dise, je ne saurai point te remercier comme il se doit, ton affection me couvre ,ta bienveillance me guide et ta présence à mes cotés a toujours été mon source de force pour affronter les différents obstacles.

*** Mon chère père ***

Vous avez toujours été à mes cotés pour me soutenir et m'encourager pour que je puisse atteindre mes objectifs.

*** Mes belles sœurs ***

*** Mes très chères frères ***

Amine pour son entente et son sympathie.

*** Mes chères ami(e)s ***

*** Toute ma famille ***

Tous ceux que j'aime et ceux qui m'aiment.

Merci !

Hicham

Remerciements

Avant toute chose, nous rendons grâce à ***Allah*** *le tout puissant qui nous a fait ouvrir les portes du savoir, qui nous a donné le courage, la volonté, la force nécessaire durant tout notre cursus pédagogiques.*

Notre profonde gratitude à nos ***parents*** *pour leur soutien moral indéfectible.*

Nous tenons à remercie notre encadreur ***LOUNIS Nawel****, pour son aide, ses conseils, et ses orientations pour l'accomplissement de ce mémoire.*

Nous remercions également ***les membres du jury*** *qui nous ont honorés en acceptant l'invitation d'évaluer ce modeste travail.*

Enfin, nous tenons à exprimer notre reconnaissance à tous nos ***amis*** *et* ***collègues*** *pour le soutien moral et matériel.*

Résumé

La confiance est un facteur essentiel, en particulier pour les systèmes orientés services dans le domaine des technologies de l'information et de la sécurité. Plusieurs problèmes ont été soulevés par des entreprises et des particuliers concernant la fiabilité des ressources cloud. Dans le cloud computing, la confiance aide le consommateur à choisir le service d'un fournisseur de services cloud pour stocker et traiter ses informations sensibles.

Plusieurs modèles sont posé pour la gestion de confiance, certains de ces modèles se repose sur les SLA, les feedback, les domaines, la subjectivité,les certificats...

L'objectif de ce mémoire est de proposer et implémenter un système basé sur les certificats et les commentaires pour une gestion de confiance dynamique dans un environnement cloud multi-domaines. Nous avons proposé une architecture et un modèle d'évaluation de confiance hybride qui permet de calculer la valeur de confiance sur la base des notes associées aux : domaines de sécurité, les feedbacks des utilisateurs et au degré de confiance des autorités de certification.Notre système de confiance permet d'améliorer la sécurité des services cloud en appliquant plusieurs niveaux de sécurité : la gestion de confiance, l'authentification forte en combinant l'authentification par e-mail et par certificats et la gestion par certificat des droits d'accès aux ressources.

Mots-clés *: Cloud Computing, Gestion de Confiance, Certification, commentaire des utilisateurs , domaines de Sécurité, CA, les modèles de confiance.*

Abstract

Trust is an essential factor, especially for service oriented systems in the field of information technology and security. Several issues have been raised by businesses and individuals regarding the reliability of cloud resources. In cloud computing, trust helps the consumer choose the service of a cloud service provider to store and process their sensitive information.

Several models are posed for the management of trust ; some of these models are based on SLAs, on feedbacks, on domains, on subjectivity and some on the certificate.

The objective of this dissertation is to propose and implement a system based on certificates and comments for dynamic trust management in a multi-domain cloud environment. we have proposed a hybrid trust scoring architecture and model that calculates the trust value based on scores associated with : security domains, user feedback, and certification authority trust level. trust system improves the security of cloud services by applying several levels of security : trust management, strong authentication by combining authentication by e-mail and certificates and certificate management of access rights to resources.

Keywords : *Cloud Computing, Trust Management, Certification, user comments, Security areas, CA, trust models.*

TABLE DES MATIÈRES

TABLE DES FIGURES

LISTE DES TABLEAUX

LISTES DES ACRONYMES

AICPA	*American Institute of Certified Public Accountants.*
API	*Application Programming Interface.*
ASB	*Auditing Standards Board.*
CAIQ	*Consensus Assessments Initiative Questionnaire.*
CA	*Certificate Authority.*
CB	*Cloud Broker.*
CCM	*Cloud Controls Matrix.*
CRM	*Client Relation Management.*
CRTM	*la racine de confiance pour la mesure.*
CRL	*Certificates Revocation Lists.*
CSP	*Cloud Service Provider.*
CSS	*Cloud Storage Server.*
CSA	*Cloud Security Alliance.*
CTP	*Cloud Trust Pyramid.*
CTA	*Cloud Trust Authority.*
CTM	*Certification − based Trust Model.*
CTL	*Certificate Trust List.*
DO	*Data Owner.*
EC2	*Elastic Compute Cloud.*
IaaS	*Infrastructure as a Service.*
IBM	*International Business Machines.*
IP	*Internet Protocol.*
NIST	*National Institute of Standards and Technology.*
NWTM	*Novel Weighted Trust Model based on Cloud.*
PaaS	*Platform as a Service.*
PKI	*Public key Infrastructure.*
PLT	*Propositional logic Terms based trust model.*
QoS	*Quality of Service.*
RA	*Register Authority.*
RM	*Registration Manager.*

SaaS	*Software as a Service.*
SimpleDB4	*Simple Data Base* 4.
SLA	*Service Level Agreement.*
SOA	*Architectures Orientées Services.*
SQL	*Structured Query Language.*
STAR	*Security Trust Assurance Registry.*
S3	*Simple Storage Service.*
TaaS	*trust as a service*
TCG	*Trusted Computing Group.*
TCB	*la base informatique de confiance.*
TEK	*Les clés de chiffrement.*
TSE	*Trust Semantic Engine.*
TTs	*Trust Tickets.*
TTM	*Ticket Based Trust Model.*
TVEM	*Trusted Virtual Environment Module.*
VMM	*Moniteur de Machine Virtuelle.*
VTN	*Virtuel trust network.*

INTRODUCTION GÉNÉRALE

L'avancement rapide des technologies de l'information et de la communication a permis le développement de nouveaux paradigmes informatiques, où les techniques de traitement, de stockage, de communication, de partage et de diffusion de l'information ont radicalement changés. Les individus et les organisations font de plus en plus recours à des serveurs externes pour le stockage et la diffusion efficace et fiable d'informations.

Le Cloud Computing est une nouvelle technologie informatique apparue aux années 2008 qui permet le déplacement des traitements et fichiers informatiques d'un ordinateur local vers des serveurs virtuels distants. Elle consiste à proposer les services informatiques sous forme de services à la demande, accessibles de n'importe où, n'importe quand et par n'importe qui grâce à une connexion internet.

La réussite du cloud est liée principalement à l'utilisation et l'intégration de nombreuses technologies et la combinaison des avantages de cesdernières comme : la Virtualisation, l'internet, l'architecture orientée services (SOA), les grilles de calcul...Etc.

Avec l'émergence des services Cloud, plusieurs entreprises ont proposées leurs propres services. Pour les utilisateurs de cloud le choix de tel ou tel fournisseurs et selon quels critères (disponibilité, sécurité,. . .) est devenue une préoccupation essentielle.

La confiance dans le cloud est un axe très important dans le domaine flou de Cloud Computing. Le concept de la confiance permet de déterminer la relation entre les fournisseurs et les clients de cloud et qui permet aussi la sélection de fournisseur Cloud le plus fiable. Plusieurs modèles sont proposés pour la gestion, l'évaluation ou les échanges de la confiance dans le cloud comme les modèles basés sur la qualité de service, les modèles basés sur les commentaires des utilisateurs, les modèles basé sur les domaines, les modèles basés sur la sécurité..etc. Parmi les modèles basé sur la sécurité on site les modèles basé sur les certificats qui présente une partie très important des modèles de confiance qui fournit une confiance formel.

L'objectif principal de ce mémoire de master est de proposer et implémenter unsystème basé sur les certificats et les commentaires pour une gestion de confiance dynamique dans un environnement cloud multi-domainesoùnous avons proposé une architecture qui détail les composants du système de gestion de confiance et la relation entre ces composants dans un environnement cloud multi-domaines.En plus nous avons proposé notre modèlehybride d'évaluation de confiance qui permet de calculer la valeur de confiance sur la base des notes associées aux : différents domaines de sécurité, les feedbacks des utilisateurs et les degrés de confiance des autorités de certification.

Notre système de confiance permet d'améliorer la sécurité des services cloud, en appliquant plusieurs niveaux de sécurité :

- Une gestion de confiance dans des domaines de sécurité différents en se basant sur les commentaires des utilisateurs et le degré de confiance des autorités de certification.
- L'authentification forte des différentes entités en utilisant les deux méthodes d'authentification : l'authentification par email et l'authentification par certificats.
- Le contrôle d'accès aux ressources en se basant sur les certificats. la certification des diffèrent entités (utilisateur, fournisseur.)

Organisation de mémoire :

Notre mémoire est organisé en cinq chapitres

1. Le premier chapitre présente les notions fondamentales de cloud : l'historique, les origines, la définition, les caractéristiques, les modèles de déploiement,les modes de service et enfin les inconvénients et les limites.
2. Le deuxième chapitre consiste étudier le concept de la confiance dans le cloud, ou nous allons présenter une définition de ce concept, ses défis, ses types, ses caractéristiques, les différents mécanismes utilisé pour appliquer ce concept, ses modèles, des exemples sur ces modèles et une comparaison entre ces exemples.
3. Le troisième chapitre, est composé de deux partie la première représente le concept de certificats, sa définition et caractéristiques, ses modèle, ses architectures. Et la deuxième partie représente les modèles de confiance basé sur les certificats, les classe de ces modèles, des exemples sur ces classes et une comparaison et une discussion de ces exemples.
4. Le quatrième chapitre destiné à la présentation des détails de notre systèmeproposé basé sur les certificats et les commentaires pour une gestion de confiance dynamique dans un environnement cloud multi-domaines, l'architecture et modèle d'évaluation de confiance utilisé.
5. Le cinquième chapitre, dans ce chapitre nous avons présenté les outils utilisé dans l'implémentation de système proposé et l'implémentation de ce système.

Enfin, nous terminons par une conclusion générale dans laquelle nous dressons un bilan et une synthèse du travail effectué.

CHAPITRE 1

ENVIRONNEMENT CLOUD

1.1 Introduction

Le cloud computing est un terme qui fait référence aux ressources et aux systèmes informatiques disponible à la demande via Internet qui peut fournir un certain nombre de services informatiques sans se limiter aux ressources locales pour faciliter l'utilisation.

Nous ne réalisons peut-être pas que nous utilisons déjà certains services Cloud dans notre vie quotidienne ou sur notre lieu de travail. en fait, nous les utilisons à grande échelle avec de nombreux services sur internet tel que Gmail de Google ou Yahoo Mail et d'autres, les Applications de Google sur Google Apps, comme application qui comprend le traitement de texte en ligne, les calendriers, les feuilles de calcul Spreadsheets et les Application internet Microsoft Office Web Apps.

1.2 Historique

Le terme « Cloud », ou bien « nuage », a été utilisé historiquement comme une métaphore de l'Internet. À l'origine, un ordinateur central militaire qui a été développé en 1950 pour connecter des terminaux informatiques à travers une matrice interne [1].

Le terme « cloud computing » a été inventé en 1996 dans un document interne de Compaq. Le terme "cloud" était à l'origine lié au concept d'informatique distribuée, et qui est généralisé chez General Magic, créé par Apple au début des années 1990 [1].

Première utilisation d'un service de cloud est en 25 août 2006, où Amazon Web Services a lancé Elastic Compute Cloud (EC2), les premiers services web permettant aux utilisateurs de louer des ordinateurs virtuels et d'utiliser leurs propres programmes et applications en ligne [1].

L'émergence de cloud depuis l'année 2007, ou les compagnies IBM , Google et

un ensemble des universités fait un projet de recherche sur le terme Cloud Computing [1].

1.3 Facteurs importants dans le développement de cloud computing

Le Cloud est développé à partir des technologies et des approches commerciales qui ont émergé au fil des années, telles que les logiciels des normes d'interopérabilité, les technologies de Virtualisation, la communication à haut débit et Web 2.0 qui sont contribué à l'émergence du Cloud. La figure 1.2 montre les étapes de l'apparition de Cloud Computing [7].

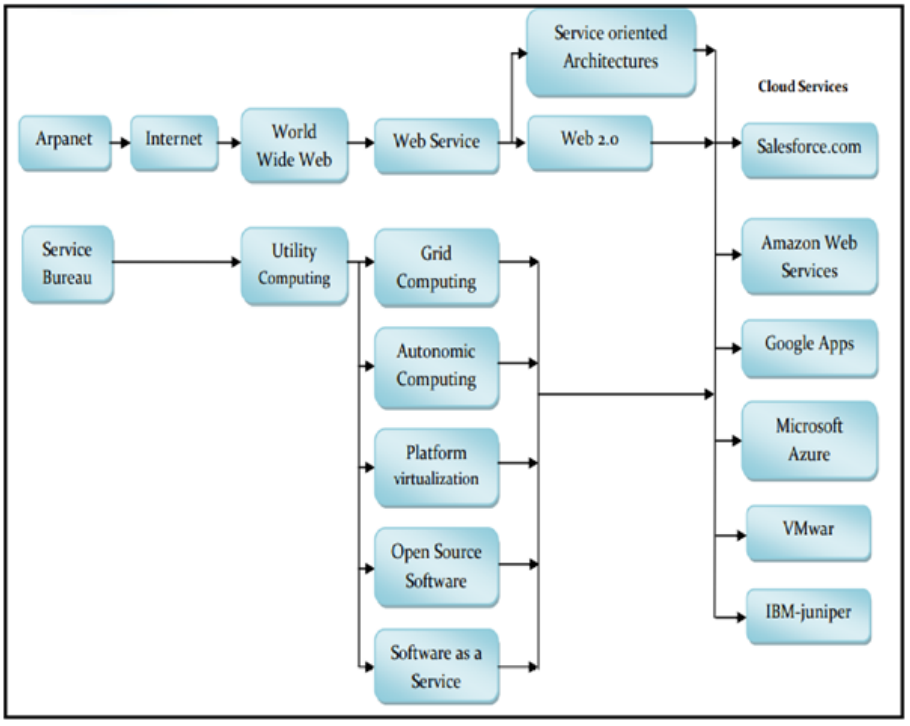

FIGURE 1.1 – Origines de l'informatique dans les nuages [8].

Les principaux éléments sont résumés dans les points suivants :

- **Informatique utilitaire « Computing Utility » :** l'Informatique utilitairepeut être définie comme la mise à disposition (packaging) de ressources informatique, telle que le calcul et le stockage, comme un service mesuré en cas de besoin. L'objectif est d'utiliser efficacement les services tout en réduisant les coûts associés [8]. Ce modèle a comme avantage un coût initial faible ou nul pour acquérir des ressources informatiques. Ce reconditionnement (repackaging) des services informatiques est devenu le fondement du passage à l'informatique «à la demande», logiciel en tant que service « SaaS » et le Cloud Computing qui ont, plus loin, propagé l'idée de l'informatique, application et réseau en tant que service.

- **Informatique en grille « Grid Computing » :** Contrairement aux réseaux Traditionnels qui mettent l'accent sur la communication entre les appareils, l'informatique en grille exploite les cycles de traitement inutilisés de tous les ordinateurs dans un réseau pour résoudre des problèmes trop intenses pour toute machine autonome. Dans l'informatique en grille , [8] les serveurs, le stockage et les réseaux sont combinés pour former des nœuds informatiques puissants qui peuvent être dynamiquement provisionnés selon les besoins.

- **Informatique autonome « Autonomic Computing » :** Se réfère aux caractéristiques d'autogestion (self-managing) des ressources informatiques distribuées, et l'adaptation aux changements imprévisibles, tout en cachant la complexité intrinsèque aux opérateurs et utilisateurs. L'informatique autonome, [8] est le fonctionnement d'un système informatique sans contrôle externe. L'objectif de l'informatique autonome, c'est d'avoir un ordinateur qui exécute des fonctions critiques et complexes, sans aucune intervention majeure par un utilisateur.

- **Platform Virtualisation :** C'est le partitionnement logique des ressources informatiques physiques dans des environnements d'exécution multiples, y compris les serveurs, les applications et systèmes d'exploitation. La Virtualisation est basée sur le concept d'une machine virtuelle s'exécutant sur une plate-forme informatique physique. La Virtualisation est commandée par un moniteur de machine virtuelle (VMM), connu sous le nom d'un Hyperviseur [8].

- **Logiciel en tant que service « SaaS : Software as a Service » :** C'est une distribution de logiciel et modèle de déploiement dans lequel les applications sont fournies aux clients sous forme de service. Les applications peuvent s'exécuter sur les systèmes informatiques des utilisateurs ou les serveurs Web du fournisseur (ex : le gestionnaire de relation client « CRM : Client Relation Management ») [8].

- **Architectures Orientées Services « SOA » :** C'est un ensemble de services qui communiquent les uns avec les autres, dont les interfaces sont connues et décrites, dont les fonctions sont faiblement couplés (le type d'interface n'est pas lié à la mise en œuvre), et dont l'utilisation peut être constituée par plusieurs organisations [8].

Les solutions Cloud reposent sur les technologies précédentes. Trois caractéristiques clés du Cloud le différencier des solutions traditionnelles :Services à la place de produits technologiques avec mise à jour en continu et automatiquement ; Self-service et paiement à l'usage (en fonction de ce que l'on consomme) ; Mutualisation et allocation dynamique de capacité (adaptation élastique aux pics de charge).

1.4 Cloud Computing

1.4.1 Définition

Le concept de Cloud Computing ou bien " l'informatique en nuage"en français n'a pas une définition exacte, ou de nombreuses définitions ont été proposées, en mettant l'accent sur les différents aspects qui caractérisent le paradigme parmi ces définition on cite :

La définition de Microsoft Azure :«le Cloud computing est la fourniture des services informatiques (notamment des services , du stockages ,des bases de données , la gestion réseaux , des logiciels , des outils d'analyses , l'intelligence Artificiel) via internet (le Cloud) dans le but d'offrir une innovation plus rapide , des ressources flexibles , et des économies d'échelle . En règle générale, vous payez uniquement les services Cloud que vous utilisez (réduisez les couts d'exploitation) gérez votre infrastructure plus efficacement et adaptez l'échelle des services en fonction des besoins de votre entreprise» [2].

Gartner est définit le Cloud « le Cloud computing est un style informatique évolutives dans lequel des capacités informatiques et élastiques sont fournies en tant que services à l'aide des technologies Internet » [3].

Pour Wikipédia « le Cloud computing correspond à l'accès à des services informatiques (serveurs, stockages, mise en réseaux, logiciels) via Internet a partir d'un fournisseur » [4].

IBM dit que « le Cloud computing est la fourniture des ressources informatique à la demande via Internet » [5].

Selon NIST (National Institute of Standards and Technology) « Le Cloud Computing est un modèle permettant un accès aisé, à la demande et au travers d'un réseau, à un ensemble partagé de ressources informatiques (par exemple des serveurs, des espaces de stockage, des applications) qui peuvent être rapidement mises en service avec un effort minimum de gestion et d'interaction avec le fournisseur de ce service.» [6].

La figure 1.2 présente une description générale du Cloud Computing selon NIST (National Institute of Standards and Technology) [7].

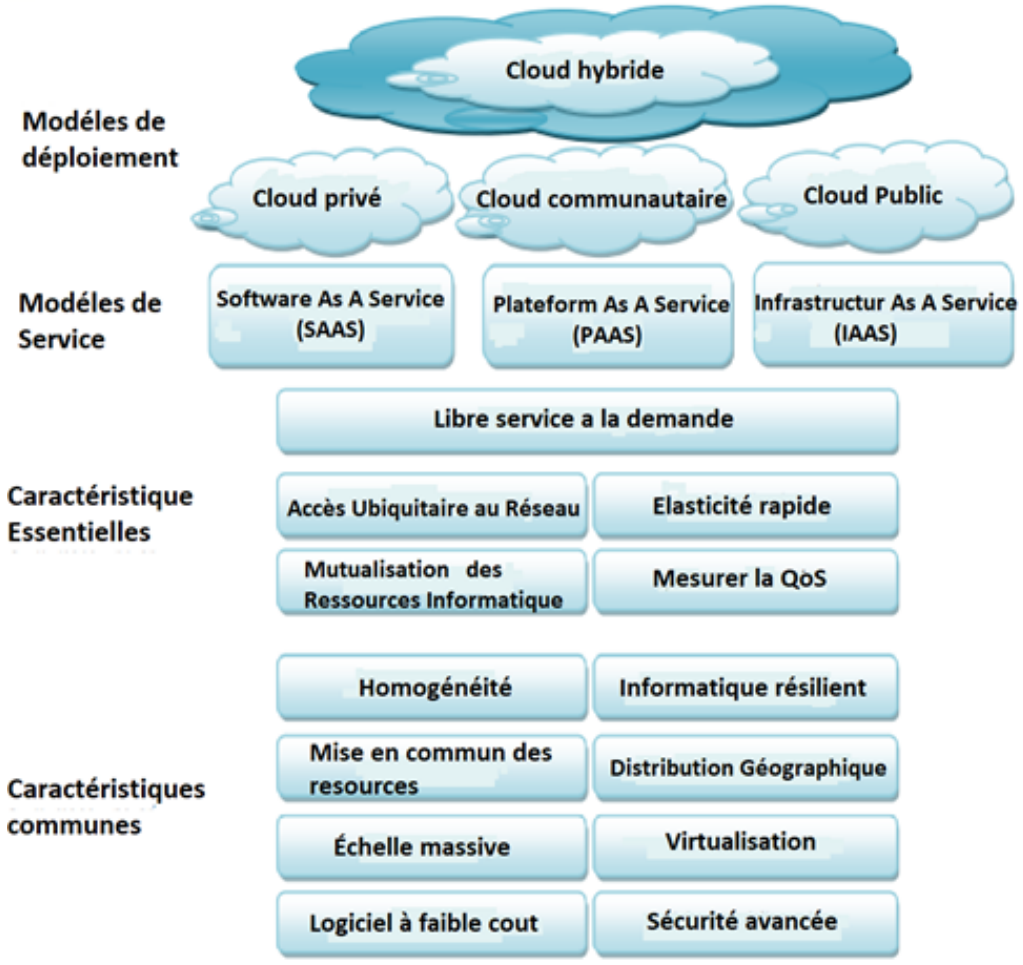

FIGURE 1.2 – Description du Cloud computing selon NIST [7].

Le Cloud computing a cinq caractéristiques qui le distinguent de l'hébergement traditionnel, que nous mentionnons ci-dessous :

1. **libre service à la demande (On-Demande self-service) :** Les consommateurs sont en mesure de s'aider eux-mêmes et de décider à quels services s'abonner et combien investir, le tout d'un simple glissement de carte de crédit ou à l'aide d'un système de paiement en ligne. Un service informatique peut désormais acheter rapidement plus de ressources à la demande pour faire face aux pics soudains de charge d'utilisateurs [9]

2. **Un accès ubiquitaire au réseau (Broad Network Access) :** les services de Cloud sont accessibles via le réseau, généralement Internet, en utilisant des mécanismes et des protocoles standards. Cet accès au Cloud est depuis n'importe où [8].

3. **la mutualisation des ressources informatiques (Resource Poolying) :** Les ressources informatiques du fournisseur sont regroupées pour servir les consommateurs multiples en utilisant un modèle multi-locataires, avec différentes ressources physiques et virtuelles affectées dynamiquement et réaffectées

en fonction de la demande des consommateurs. Le client n'a généralement aucun contrôle ou connaissances sur l'emplacement des ressources fournies, mais peut être en mesure de spécifier l'emplacement à un niveau supérieur d'abstraction (pays, ville, Datacenter). Des exemples de ressources incluant le stockage, le traitement, la mémoire et la bande passante [10].

4. **Mesure de la qualité de service (Measured service) :** Le système Cloud permet de contrôler et d'optimiser automatiquement l'utilisation des ressources en s'appuyant sur une capacité de comptage à un certain niveau d'abstraction approprié pour le type de service (comptes utilisateurs, traitement, bande passante et activité). L'utilisation des ressources peut être surveillée, contrôlée, rapportée, en assurant la transparence à la fois pour le fournisseur que pour le consommateur de service [10].

5. **Elasticité rapide (Rapide Elasticité) :** l'une des caractéristiques essentielles du cloud computing est l'élasticité des ressources. En fonction de la demande, les ressources peuvent être rapidement et automatiquement déployées et mises à l'échelle à n'importe quelle quantité et à tout moment [11]. Par exemple, la mise en ligne d'une nouvelle instance d'un serveur est réalisée en quelques minutes, alors que, l'arrêt et le redémarrage sont effectués en quelques secondes [11]. De plus, ces opérations vont s'effectuer automatiquement par des scripts [11, 12].

1.4.2 Les différentes entités qui collabore dans l'approvisionnement des services dans l'environnement de cloud computing

Plusieurs entités réagissent dans l'environnement de cloud computing, nous allons citer les entités les plus essentiel :

- **Le prestataire de service cloud ou Application (CSP pour Cloud Service Provider) :** : Il s'agit d'une entité qui gère le serveur de stockage cloud (CSS pour Cloud Storage Server), l'espace de stockage pour préserver les données des clients et la puissance de calcul élevée .

- **Le client/propriétaire ou plateforme (Cloud Client/Owner) :** Il s'agit d'une entité, qui a d'une grande quantité de fichiers de données à stocker dans le cloud et s'appuie sur ce dernier pour la gestion des données et du calcul, il peut être soit un consommateur individuel ou une organisation.

- **L'utilisateur (Cloud User) :** Il s'agit d'une unité, qui est inscrit sur le propriétaire et utilise les données de celui-ci stockées sur le cloud. L'utilisateur peut être un propriétaire lui-même.

- **Courtier ou infrastructure (CB ou Cloud Broker) :** deux types de

Brokers peuvent être distinguéesdans le cloud.

- Premièrement , les Brokers qui se concentrent sur la négociation des relations entre les consommateurs et les fournisseurs sans posséder ou gérer l'infrastructure cloud. Ils fournissent, par exemple, des services de conseil aux consommateurs de cloud pour déplacer leurs ressources informatiques dans un cloud approprié.
- Deuxièmement, les Brokers qui ajoutent des services supplémentaires sur le dessus de l'infrastructure / la plateforme / le logiciel d'un prestataire de cloud afin d'améliorer et sécurité de l'environnement Cloud pour les consommateurs. Par exemple, un Broker peut apporter au consommateur un service de gestion d'identité et d'accès au-dessus de service de base offert par le fournisseur cloud. À titre d'exemple, le Broker peut développer des API afin de rendre les services cloud interopérables et portable [13].

1.5 Modèles de déploiement de Cloud

En se basant sur la réponse aux deux questions essentielles : :

- Qui gère le cloud ?
- Qui est le client du service offert par le cloud ?

On peut classifier les clouds selon quatre modèles de déploiement : le cloud publique, le cloud privé, le cloud communautaire et le cloud hybride.

1.5.1 Cloud public « Public Cloud »

Un cloud public peut être consulté par tout abonné disposant d'une connexion Internet et un accès à l'espace nuage et est géré par une organisation. L'organisation peut être une entreprise (comme Google), un département académique ou gouvernemental. Le fournisseur de Cloud possède et gère l'infrastructure Cloud. Un nuage public ne signifie pas que les données d'un utilisateur est publiquement visible car les fournisseurs de Cloud public offrent généralement des mécanismes de contrôle d'accès pour les utilisateurs [15].

En général, le Cloud est exploité et géré dans un centre de données appartenant à un fournisseur de services qui héberge plusieurs clients et utilise le provisionnement dynamique. La mise en œuvre d'une plate-forme évolutive de services et la licence « pay-as-you-go » sont également des éléments attrayants de Cloud public. La Mise en œuvre du Cloud public peut être d'une grande aide à éliminer la charge paralysante de la maintenance des infrastructures sur les organisations informatiques [8].

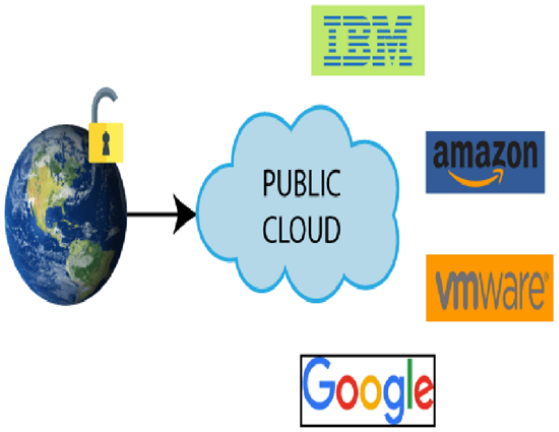

FIGURE 1.3 – Cloud Public [16].

1.5.2 Cloud privé « Private Cloud »

Dans un déploiement privé,l'infrastructure Cloud a uneutilisation privéeà l'intérieur d'une organisation. Cette infrastructure peut être placée et géré à l'intérieur de l'organisation elle-même ou bienplacéechez une tierce partie qui est responsable sur sa gestion.

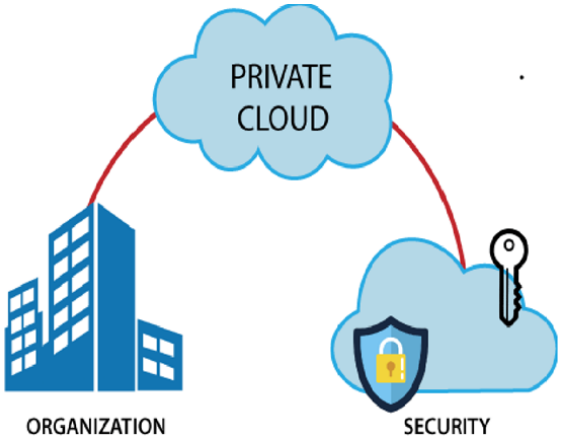

FIGURE 1.4 – Cloud Privé [16].

1.5.3 Cloud Communautaire « Community Cloud »

C'est un modèle de déploiement qui permet une mise en œuvre rapide. Sur le plan conceptuel, il réside quelque part entre un Cloud privé et un Cloud public. Un Cloud communautaire est partagé entre deux ou plusieurs organisations qui ont des exigences similaires dans le nuages, telles que des objectifs d'affaires non concurrentielles, ou un besoin de mutualiser les moyens de sécurité de haut niveau. Le Cloud est détenue et gérée par un ou plusieurs des collaborateurs dans la communauté. Un exemple de ce déploiement est Open Cirrus formé par HP, Intel, Yahoo, et autres [15, 17].

FIGURE 1.5 – Cloud Communautaire [16].

1.5.4 Cloud Hybride « Hybrid Cloud »

Un cloud hybride est essentiellement une combinaison d'au moins de deux nuages, où les nuages sont un mélange de clouds public, privé ou communautaire qui demeurent des entités uniques, mais sont liés entre eux par des technologies normalisées ou propriétaires qui permet la portabilité des applications.

Un exemple de déploiement de cloud hybride peut consister en une organisation qui déploie des applications de logiciels non critiques dans le Cloud public, tout en gardant les applications critiques ou sensibles dans un cloud privé. Les clouds hybrides combinent les deux modèles de cloud public et privé, et ils peuvent être particulièrement efficaces lorsque les deux types de nuages sont situés dans le même établissement [8].

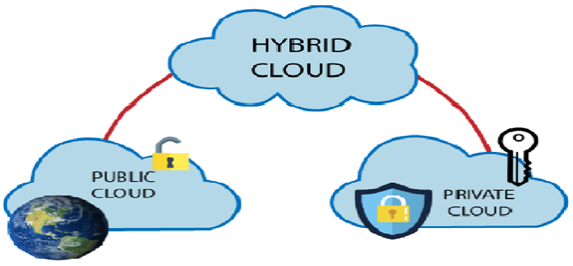

FIGURE 1.6 – Cloud Hybride [16].

1.5.5 Comparaison entre les types de Cloud

[H]

1.6 Les Différent couches du cloud computing

Les services de Cloud computing proposent des modèles de facturation à l'utilisation qui réduisent les dépenses et éliminent les taches de maintenance .Les fournisseurs Cloud hébergent différentes infrastructures, plateformes et offres logicielles sur site qu'ils "louent", ce qui permet à l'entreprise d'adapter à la hausse ou à la baisse des besoins les services de Cloud computing.

- **Logiciel en tant qu'un Service (SaaS pour Software as a Service) :** Ce modèle du service est caractérisé par l'utilisation d'une application parta-

Type / Paramètres	**Cloud Public**	**Cloud Privé**	**Cloud Communautaire**	**Cloud Hybride**
Description	Les services sont disponibles pour les utilisateurs publics	Est construit avec l'infrastructure privée existante. ce type de Cloud a des utilisateurs authentiques qui peuvent fournir dynamiquement les ressources.	Différent types de Cloud sont intégrés pour répondre à un besoin commun ou particulier de certain organisation.	Le système hétérogène de Cloud Hybride est le résultat d'un Cloud privé, qui incorpore différents types de services et de ressources distribué à partir de Clouds publics.
Scalabilité	Très élevé	Limité	Limité	Très élevé
Sécurité	Dépend totalement du fournisseur de service	Sécurité haut de gamme	Sécurisé	Sécurisé
Performance	Faible à Moyen	Bien	Très bien	Bien
Fiabilité	Moyen	Très élevé	Très élevé	Moyen à élevé
Cout	Moins cher	Très Couteuse	Couteuse	Couteuse
Exemple	Amazon, EC2,Google AppEngine ...	VMwar, Microsoft KVM Xer	SolaS Community Cloud , VMwar	IBM , HP ,VMware , vCloud Eucalvatus

FIGURE 1.7 – Comparaison entre les différents modèles de déploiement de cloud [19].

gée qui fonctionne sur une infrastructure Cloud [18]. Cette application prête à l'emploi ne nécessite pas de maintenance : les mises à jour, le déploiement, le stockage et la sauvegarde sont du ressort du fournisseur de services [12]. Un exemple courant d'application SaaS concerne les messageries Web (Gmail, Yahoo mail, etc.), dans lesquelles l'utilisateur peut envoyer et recevoir des e-mails sans avoir à gérer des fonctionnalités ou à effectuer la maintenance des serveurs et des systèmes d'exploitation sur lesquels elles s'exécutent.

- **Plateforme en tant qu'un Service (PaaS pour Platform as a Service) :** Ce modèle fournit comme service cloud une plateforme d'exécution, de déploiement et de développement des applications [18]. Elle permet d'exécuter des applications SaaS ou d'être mise à disposition des entreprises ou individus qui souhaitent faire héberger leurs propres applications. L'infrastructure cloud sous-jacente (réseaux, serveurs, stockage) est gérée par le fournisseur du service cloud. Hadoop 1 est un exemple de PaaS destiné aux applications distribuées et à la gestion intensive des quantités immenses de données.

- **Infrastructures en tant qu'un Service (SaaS pour Software as a Service) :** C'est un modèle de déploiement d'infrastructures qui fournit à la demande un ensemble de services de niveau bas (serveurs, réseaux, espace de stockage, bande passante etc.) [18]. Cela permet ainsi à une entreprise de pouvoir bénéficier de la puissance d'une infrastructure, ponctuellement, sans devoir investir beaucoup. Amazon EC2 (Amazon Elastic Compute Cloud 2) est un exemple d'IaaS qui permet de louer des machines virtuelles de tailles prédéfinies pour exécuter des applications. Elle fournit des services de calcul, du stockage tel que S3 (Simple Storage Service 3), et des bases de données en ligne tel que SimpleDB4 qui est un magasin de données No SQL.

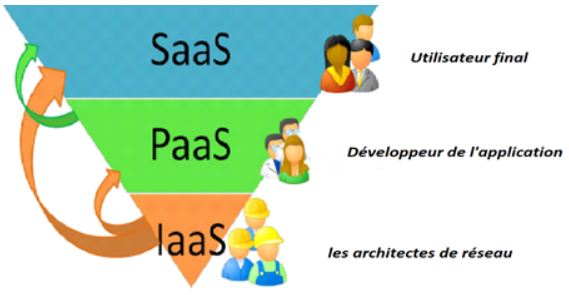

FIGURE 1.8 – Couches de Cloud Computing [19].

	Avantage	Inconvénient
SaaS	*Pas d'installation *Pas de licence *Migration *Accessible via abonnement	*Logiciel limité *Sécurité *dépendance des prestataires
IaaS	*Administration *Personnalisation *Flexibilité d'utilisation *Capacité de stockage infini	*Sécurité *Besoin d'un administrateur système *Demande très élevés
PaaS	*Pas d'infrastructure nécessaire *Pas d'installation *Environnement hétérogène	*Limitation de Langages *Pas de personnalisation dans la configuration des MV

FIGURE 1.9 – avantages et inconvénient des couches de Cloud [20].

1.7 Les Avantages et les inconvénients de cloud computing

1.7.1 Avantages

Parmi de nombreux avantages de Cloud on cite les suivants :

1.7.1.1 Avantages financiers :

sont, généralement pour les clouds publics, où les ressources informatiques sont acquises comme un service d'utilité à la demande auprès de fournisseurs externes.

- **Pay-as-You-Go :** Les coûts de l'utilisation de Cloud varient entre les trois principaux modèles de services : SaaS, IaaS et PaaS, mais le principe est le même. Les coûts SaaS dépendent de nombre d'utilisateur, les coûts PaaS augmentent en proportion avec l'utilisation et la taille des applications développées, et les coûts IaaS couvrent l'utilisation des serveurs et du stockage [20].

- **Les charges opérationnelles :** Traditionnellement, Construire une infrastructure informatique implique des coûts initiaux importants sur le matériel et le logiciel, entraînée par la planification à long terme, basée sur des prévisions de croissance de l'entreprise et les tendances du marché, tandis qu'un

système de Cloud évolue et, si nécessaire, se rétrécit. Avec le Cloud, les matériels et les licences logicielles ne sont pas laissés inutilisés lorsque l'entreprise réduit sa taille.

- **Réduire les coûts de gestion :** La gestion des infrastructures informatiques ou le déploiement des applications logicielles d'entreprise pour les postes de travail des employés posent une surcharge d'administration, qui est un facteur important dans le coût total de possession. Le Cloud permet de réduire cette surcharge en déchargeant les problèmes d'installation, de gestion et de maintenance du matériel (à travers IaaS), des systèmes d'exploitation de serveur (à travers PaaS), et de déploiement de l'application (à travers SaaS).

1.7.1.2 Avantages technologiques :

Les Clouds publics permettent un accès à la demande à un ensemble de ressources informatiques rapidement évolutives de n'importe où.

- **Évolutivité rapide à la demande :** Deux des cinq caractéristiques essentielles du Cloud sont : le libre-service à la demande et l'élasticité rapide, qui accélèrent tout à voir avec l'approvisionnement. Le Cloud peut fournir rapidement de nouveaux employés (temporaire ou permanente) avec des comptes utilisateur pour les applications SaaS, et ils peuvent utiliser n'importe quel ordinateur personnel pour y accéder. Le PaaS permet de développer de nouvelles applications logicielles commerciales basées sur le Web sans se soucier des serveurs, les pare-feux, la sécurité ou les systèmes d'exploitation. L'IaaS est utilisé pour obtenir un accès temporaire à une puissance de calcul apparemment illimitée et d e stockage de données au besoin .

- **Accès n'importe où :** Les services de Cloud sont basé sur le Web et ne dépend pas de l'ordinateur utilisé. Les documents et applications hébergés dans le Cloud sont accédés de n'importe où.

- **Aucun engagement à long terme :** Les ressources informatiques sont immédiatement disponibles et ils peuvent être utilisés aussi longtemps que nécessaire et se retira ensuite parce qu'ils sont acquis sur un mois en mois, voire de minute en minute.

- **Ressources informatiques pratiquement illimitées :** Ressources telles que la puissance de calcul et espace de stockage de données sont disponibles à la demande en fonction des besoins, ce qui permet un haut degré de flexibilité et d'évolutivité à répondre aux besoins changeants de l'entreprise. On oublie trop souvent la notion de saturation des machines et des processeurs.

- **L'épreuve du futur :** Avec SaaS et PaaS, l'obtention de la dernière version du logiciel « la mise à jour » est automatique. Il n'y a aucun frais pour

la mise à niveau vers la prochaine version des applications préférées ou de la plate-forme de développement et il est dans l'intérêt de fournisseur d'assurer que leurs systèmes améliorent et restent compétitifs. En outre, puisque les technologies (SaaS et PaaS) sont basées sur le Web, ils utilisent des protocoles de transfert d'information standard, qui facilitent les connexions avec d'autres logiciels sur le Web. Ces avantages ne s'appliquent pas à l'IaaS où toutes les applications logicielles d'entreprise sont gérées par les développeurs, mais les panneaux de contrôle du système et l'infrastructure sous-jacente seront tenus à jour.

1.7.1.3 Avantages environnementaux :

- **Partage des ressources :** quelques arguments, pour que le Cloud soit une solution informatique économe en énergie, sont les suivants :
  - Les clients partagent un ensemble de ressources informatiques.
  - Les fournisseurs utilisent des centres de données plus grande, plus moderne et plus éconergétique (économe en énergie).
  - L'utilisation accrue des serveurs en raison de la Virtualisation des serveurs.

- **Réduction des déplacements :** naturellement, le Cloud Computing signifie que les utilisateurs de Cloud n'ont plus à se rendre à un bureau pour faire le travail, ni les administrateurs système doivent rendre aux centres de données pour installer de nouveaux serveurs.

- **Collaboration de groupe plus facile :** pour de nombreux utilisateurs, c'est un avantage important du Cloud lorsque plusieurs utilisateurs peuvent facilement collaborer sur des documents et projets.

1.7.2 Inconvénients

- **Sécurité :** le problème de la sécurité et de la confidentialité des informations, certains utilisateurs craignent que d'autres personnes partagent leurs informations.

- **Confidentialité et propriétés des données :**le problème de la protection des droit de propriétés intellectuelle est l'un des problèmes qui soulève les inquiétudes des utilisateurs de ces services , il n'y'a aucun garantie que les droits des propriétés intellectuelle des utilisateurs ne seront pas violés.

- **Assurer le niveau de service :**le problème de la disponibilité d'internet est l'un des principaux problèmes , en particulier dans les pays en développement , ou le service nécessite une connexion internet permanente lors de l'utilisation de ce service.

- **Accès Physique :**L'accès physique d'une seule personne mal intentionnée qui possède une excellente connaissance de l'implémentation physique du Cloud et de ses points névralgiques peut suffire à mettre le Cloud hors service, provoquant une rupture dans la continuité du service et empêchant tout accès externe au Cloud.

- **Fonctionnalités peuvent être limitées :** Cette situation est destinée à changer, mais aujourd'hui de nombreuses applications basées sur le Web ne sont pas complètes comme leurs applications de bureau.

1.8 Les défis de cloud computing

En bref, le nouveau modèle de Cloud computing offre un certain nombre d'avantages par rapport aux modèles informatiques précédents, et de nombreuses organisations l'adoptent. Cependant, il existe encore un certain nombre de défis, qui sont actuellement relevés par les chercheurs et les praticiens sur le terrain. Voici un résumé de ces défis :

• **Performances :**Le plus gros problème de performances peut concerner certaines applications orientées transaction et d'autres applications gourmandes en données, et dans ce cas, le Cloud computing peut manquer de performances adéquates. En outre, les utilisateurs éloignés des fournisseurs de Cloud peuvent subir des retards et une latence élevée.

• **Sécurité et confidentialité :** Les entreprises sont toujours préoccupées par la sécurité lorsqu'elles utilisent le Cloud computing. Les clients sont préoccupés par l'exposition aux attaques lorsque des informations et des ressources informatiques importantes se trouvent hors du pare-feu. La résolution du problème de sécurité suppose que les fournisseurs de Cloud computing suivent les pratiques de sécurité standard. [29]

• **Disponibilité :**L'architecture de Cloud doit garantir un accès au service en très haute disponibilité avec des performances optimales. Une seule défaillance d'un équipement matériel peut engendrer une dégradation ou une coupure du service voire une perte de données.

• **Auto-guérison :** en cas d'échec d'application ou de stockage de données, il y aura toujours une sauvegarde en cours d'exécution sans retards importants, rendant le changement des ressources transparent pour l'utilisateur .

• **Gestion des données :** la distribution, le partitionnement, la sécurité et la synchronisation des données.

• **Contrôle :** certains services informatiques craignent que les fournisseurs de Cloud computing aient un contrôle total sur les plates-formes. Tout comme les four-

nisseurs de Cloud computing ne conçoivent généralement pas de plates-formes d'entreprise et de pratiques commerciales spécifiques.

- **Les coûts de transfert de données :** Avec le Cloud computing, les entreprises peuvent économiser de l'argent gaspillé sur le matériel et les logiciels, mais elles peuvent encourir des frais de bande passante réseau élevés. Le coût du débit de données peut être faible pour les petites applications Internet, qui ne sont pas gourmandes en données, mais peut augmenter considérablement pour les applications gourmandes en données qui sont précises et fiables.

- **Fiabilité :** Le Cloud computing n'offre toujours pas une fiabilité 24 heures sur 24. Il y a eu des cas où les services de Cloud computing ont subi des pannes pendant quelques heures. À l'avenir, nous nous attendons à voir plus de fournisseurs de Cloud computing, des services plus riches, des normes établies et de meilleures pratiques.

Dans le domaine de la recherche, HP Labs, Intel et Yahoo ont lancé un banc d'essai de recherche sur le Cloud distribué, avec un certain nombre d'installations en Asie, en Europe et en Amérique du Nord pour développer des innovations, notamment des puces informatiques spécifiques au Cloud. IBM a également lancé Cloud Computing Research, une suite de ressources informatiques disponibles pour un accès mondial à la demande et prenant en charge les processus métier.

1.9 Conclusion

Le Cloud computing est un paradigme qui partage l'infrastructure de calcul et de stockage sur un réseau évolutif de ressources. Dans le monde modern les données sont dispersées dans différents centres d données et les applications trouvent sur des serveurs distantes.

Afin de commercialiser la technologie Cloud, les utilisateurs doivent avoir la certitude que les fournisseurs de ressources terminent le travail soumis et que les informations sur les données traitées sont sécurisées.

Urquhart déclare que le plus gros problème de Cloud est la confiance .la confiance joue un rôle important dans tous les environnements de Cloud et la gestion de la confiance fait partie intégrante des aspects commerciaux de la technologie Cloud. Les fournisseurs de service Cloud offrent une infrastructure, une plateforme et de logiciels aux utilisateurs de manière économique et fiable.

Avec tous les avantages du paradigme de Cloud et son potentiel pour diminuer les coûts et réduire le temps nécessaire pour lancer de nouvelles initiatives, les ressources virtualités, les serveurs géographiquement dispersés et la co-implantation de traitement et de stockage posent des défis et opportunités, en même temps, pour les fournisseurs et utilisateurs de Cloud. Mais la sécurité du Cloud sera toujours une préoccupation majeure en raison de la nature ouverte et publique de Cloud. En effet,

l'intégrité, la confidentialité, la disponibilité sont encore des problèmes ouverts qui appellent des solutions efficaces et efficientes.

CHAPITRE 2

CONFIANCE DANS LE CLOUD

2.1 Introduction

La confiance dans le Cloud devient un problème complexe, des entreprises comme Google et Amazon ont mis en œuvredes systèmes de la gestion de confiance basé sur la réputation et aide les utilisateurs à localiser les fournisseurs de ressources dignes de confiance pour effectuer des transactions e-business de manière sécurisé et confiante. E-bay a un modèle de confiance centralisé intégré.

2.2 La Confiance

2.2.1 Définition

La confiance est un concept qui existe depuis assez longtemps. Elle est aussi ancienne que l'histoire de l'humanité et l'existence des interactions sociales humaines.

En psychologie sociale et en sociologie, la confiance est une hypothèse faite sur le futur comportement d'autrui. Il s'agit d'une conviction selon laquelle une personne serait capable d'agir d'une certaine manière face à une situation donnée : « Je vais tout raconter à mon père, j'ai confiance en ce [je suis convaincu(e)] qu'il me comprenne et m'aide » [21].

D'après Investopedia « la confiance est une relation fiduciaire dans laquelle une partie, connue sous le nom de trustor, donne à une autre partie, le trustee, le droit de détenir un titre de propriété ou d'actifs au profit d'un tiers, le beneficiary. Les fiducies sont établies pour fournir une protection juridique aux actifs du fiduciaire, pour s'assurer que ces actifs sont distribués selon les souhaits du fiduciaire et pour gagner du temps, réduire la paperasse et, dans certains cas, éviter ou réduire les droits de succession ou les droits de succession. En finance, une fiducie peut également être un type de fonds à capital fixe construit comme une société anonyme. » [22].

Lehmann est définit la confiance comme un « fait basique de la vie humain. » [23].

D'après Barber 1983 « La confiance se place dans une dimension sociale de la croyance, l'individu qui fait confiance espère que l'autre remplira des compétences techniques ainsi que des responsabilités et des obligations morales » [24].

Afin de définir le terme de confiance, Gambetta introduit la notion de probabilité subjective et de circonstances. «La confiance (ou symétriquement la défiance) est un niveau particulier de la probabilité subjective avec laquelle un agent accomplira une action spécifique, à la fois avant que nous ne puissions suivre chaque action (ou indépendamment de sa capacité de même pouvoir la tracer) et aussi dans un contexte dans lequel cela affecte notre propre action. »[[25].

Définition de J.A.Golbeck« la confiance c'est une relation entre deux ou plusieurs, de sorte qu'une personne ne doute pas des intentions et de la moralité de l'autre personne et elle attend de bonne intentions basées sur la connaissance que la personne a de l'autre partie, et c'est une question reportée afin que ses résultats apparaitra dans le future. » cette définition se rapproche de la définition de Gambetta où la confiance est un engagement à croire au bon déroulement des actions futures d'une autre entité [26].

D'après les définitions qui mentionnées précédemment nous concluons que « la confiance qu'une entité C (l'utilisateur) a dans une autre F (fournisseur) pour fournir un S (Service) est la probabilité que cette entité F satisfasse un requête de l'entité C pour le service S ».

Par conséquent, toutes les définitions sont presque dans le même sens, qui comprend la présence de trois éléments de base :

- **Trustor :** est un personne ou une organisation qui faisant la confiance.
- **Trustee :** est une personne ou un membre d'un conseil d'administration ayant le contrôle ou des pouvoirs d'administration de biens en fiducie avec une obligation légale de les administrer uniquement aux fins précisées.
- **Contexte :** ensemble des circonstances qui entoure la confiance [25].

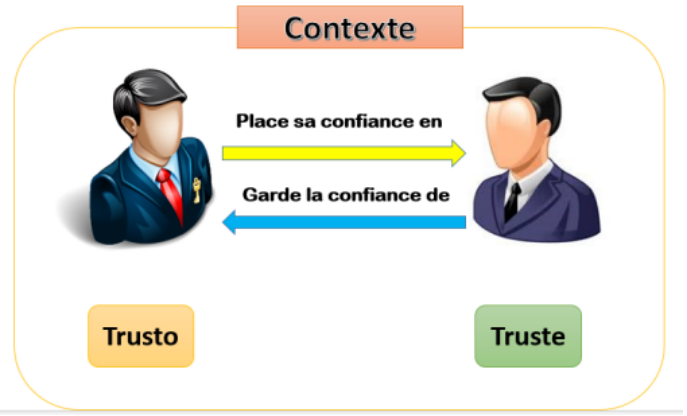

FIGURE 2.1 – les éléments de la confiance [25].

2.2.2 les types de la confiance

Deux types de confiances sont identifiés dans le Cloud computing ;la confiance direct et indirecte.

- **Confiance Directe (direct trust) :** la confiance directe entre en jeu lorsqu'une entité estime une autre sur la base d'expériences antérieures.
- **Confiance Indirecte (Indirect Trust) :** la confiance indirecte est la confiance dans laquelle une entité fait confiance à un autre fait confiance sur la base de la recommandation d'une troisième entité [27].

2.2.3 La nature de la confiance

La dynamique de la confiance est le plus grand défi de l'évaluation de la confiance et de la prédiction de la fiabilité. Elle est déterminée par les attributs naturels des entités dans la relation de confiance. Cette section résume la nature de la confiance comme suit [27] :

- **Incertitude subjective :** fait référence au fait que le trustee ne peut pas juger clairement le changement dynamique du trustor comme le contexte et le temps changent. La confiance ne peut être que évalué selon l'historique d'interaction précédent ; la confiance est le crédit.
La partie a un jugement subjectif sur le destinataire et différentes entités auront des critères différents. Même pour la même partie de confiance, le même contexte, la même période et le même comportement, la différence des créanciers, le jugement quantitatif donné est susceptible d'être différent. Dépendant du contexte : l'état de confiance spécifique est étroitement lié au contexte. Il est inutile de discuter de la question de la confiance à partir du contexte spécifique.

- **Asymétrie :** c'est-à-dire que la relation de confiance est à sens unique, A fait confiance à B et ne signifie pas que B fait également confiance à A.

- **Transitivité incomplète :** les relations de confiance ne sont généralement pas entièrement transitives, c'est-à-dire que A fait confiance à B, B fait confiance à C

et peut ne pas conclure que A fait confiance à C. Seulement sous certaines contraintes spécifiques, la confiance a un certain degré de transitivité. La recommandation est un moyen typique de communication de confiance, et c'est une incarnation du transfert de confiance. La littérature montre que la confiance de la capacité n'est pas transitive par la description formelle, alors que la confiance basée sur le concept est transitif.

- **Asynchronisme temporel :** cela signifie que le résultat de l'évaluation de la relation de confiance entre les entités est asynchrone temporelle. La solution au problème est de faire la moyenne de la tranche de temps ; la confiance se détériorera avec le temps, et la performance la plus directe est la suivante :
plus l'évaluation de la confiance est longue, moins elle est persuasive.

- **Multi-objectivité :** la confiance est souvent associée à plusieurs attributs de la partie de confiance et est influencée par plusieurs attributs. C'est un concept d'interaction multi-attributs. Prenant comme exemple les achats en ligne, l'évaluation du vendeur par le client peut inclure des évaluations de la qualité, du prix, de l'attitude du service et de la rapidité de la livraison.

2.2.4 Principes de Confiance

Pour garantir un niveau de confiance maximal, certains principes doivent être suivis :

- la transitivité de la confiance, si l'entité A fait confiance à l'entité B et l'entité B fait confiance à l'entité C, nous pouvons alors arriver à la conclusion que A peut faire confiance à l'entité C en se référant à la confiance de l'entité B.
- La confiance est fonction de la perception du risque, elle représente une croyance en une personne pour ses actions correctes. , La confiance doit également évaluer l'incertitude selon laquelle l'autre partie agit correctement et intégrer les risques associés.
- La confiance est déterminée par le temps, elle se construit au fil du temps sur la base des expériences passées.
- La confiance peut être mesurée, elle est mesurable par une valeur numérique, généralement dans l'intervalle [0 - 1].
- Des outils formels et sociaux sont nécessaires à l'évolution de la confiance, la confiance peut être modélisée selon différents modèles formels.

2.2.5 La confiance dans le cloud computing

L'informatique de confiance conduit le concept de confiance au domaine de l'informatique. Trusted Computing Group (TCG) définit la confiance comme : une entité qui peut toujours atteindre l'objectif souhaité de la manière attendue, alors l'entité est digne de confiance. Autrement dit, la confiance met l'accent sur l'attente du comportement de l'entité, tout en prêtant également attention à la sécurité et à la fiabilité du système [28, 29].

La confiance est une relation binaire correspondante. Cette relation peut être un-à-un, un-à-plusieurs ou plusieurs-à-un, plusieurs-à-plusieurs. Il existe plusieurs façons de gagner la confiance : la confiance directe, la confiance recommandée, la confiance de recommandation a plusieurs niveaux et la confiance hybride [29].

Dans les transactions en ligne (telles que les transactions de commerce électronique), la confiance est une partie qui croit que l'autre est fiable et capable de tenir sa promesse. Ce n'est que lorsque les deux parties se font confiance que la transaction se déroule sans heurts, la confiance est donc la prémisse et la coutume des activités commerciales.

Dans un environnement réseau complexe comme le Cloud, la confiance entre les entités peut être divisée en confiance directe et confiance indirecte. La confiance directe est une relation établie par deux entités sur la base de l'expérience passée. La confiance indirecte fait référence à la relation établie par la recommandation d'autres entités.

Par conséquent, la confiance présente les caractéristiques suivantes :

- Asymétrie (si l'entité A fait confiance à l'entité B mais n'a pas besoin que B rende A)
- Subjectivité (la confiance est le jugement subjectif de l'évaluateur sur l'objet d'évaluation),
- Dynamique (la confiance peut suivre un changement dans le temps, l'environnement ou d'autres facteurs (multi dimensionnalité)
- La confiance entre les entités est liée à plusieurs attributs, tels que la valeur de confiance historique, le statut social, le niveau de revenu, etc.)

2.2.6 Les défis de la confiance dans le cloud

Les entreprise d'aujourd'hui veulent développer, elles veulent des données plus sécurisées et accessibles partout et à quel moment quelque soit le support .et cela est possible pour le Cloud, mais il y'a des défis parmi ces défis on trouve la confiance qui rencontre un ensemble des défis sont les suivant [30] :

- Des politiques de sécurité différents : l'environnement Cloud se compose de plusieurs utilisateurs et distributeurs et chaqu'un s'utilise leur propre système de sécurité .donc comment réaliser la compatibilité entre ces systèmes de sécurités.

- Continuité et dépendance vis-à-vis des prestataires : la complexité des architectures et le manque de la transparence cause des risques pour la sécurité. la centralisation de la gestion et de contrôle introduit des échecs. Ça fait un risque aux les disponibilités des données d'utilisateurs du Cloud.

- Respect de la réglementation applicable et des bonnes pratiques : le Cloud détermine une loi applicable et chaque fournisseur doit respecter cet loi.

- L'amélioration de la confiance par le biais de mécanisme d'assurance : le Cloud ne peut garantir pas le control complet des utilisateurs, pour cela les utilisateurs doit s'assurer que les fournisseurs de Cloud respectent leur Obligations.

2.3 La sécurité et la confiance dans le Cloud

BearingPoint a développé la «Pyramide de confiance dans le Cloud» (Figure 2.2) en tant que cadre pour analyser les critères requis pour créer et gérer la confiance en tant que condition préalable au transfert de services vers le Cloud. Chaque couche capture des normes telles que les lois et les standards, ainsi que des facteurs non contraignants tels que les attitudes de confiance basées sur des valeurs culturelles. Le non-respect des critères de la pyramide de confiance peut entraîner une absence de confiance, et donc une probabilité moindre d'adoption de services Cloud, ainsi qu'une efficacité réduite en raison des frais généraux nécessaires pour examiner la prestation de services.

Comme le montre la figure, la confiance et les contrats fonctionnent comme un cercle vertueux. Avec des niveaux de confiance plus élevés, les organisations peuvent travailler selon l'esprit d'un accord sans avoir à recourir à des conditions contractuelles à chaque instant. Cependant, lorsqu'une relation méfiante existe, les clauses strictes d'un contrat jouent un rôle plus important.

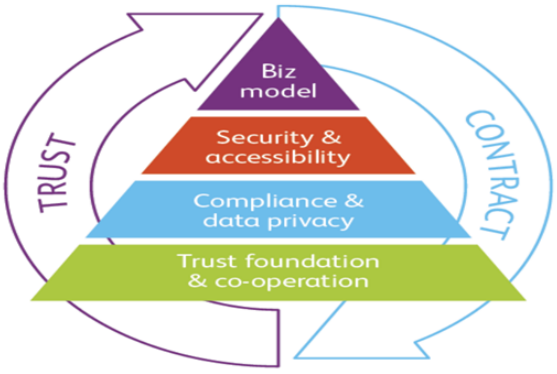

FIGURE 2.2 – Cloud Trust Pyramid [31].

2.4 Mécanismes de confiance dans le Cloud

Dans cette section, nous abordons les mécanismes de confiance existants dans le Cloud. À partir de la discussion, nous verrons que chacun des mécanismes aborde un aspect de la confiance mais pas d'autres.

1. Confiance basée sur la réputation :
La confiance et la réputation sont liées, mais différentes. Fondamentalement, la confiance est entre deux entités ; mais la réputation d'une entité est l'opinion agré-

gée d'une communauté à l'égard de cette entité. Habituellement, une entité qui jouit d'une grande réputation bénéficie de la confiance de nombreuses entités de cette communauté ; une entité, qui doit porter un jugement de confiance sur un fiduciaire, peut utiliser la réputation pour calculer ou estimer le niveau de confiance de ce trustor.

2. Le contrat ou niveau de Service (SLA) :
«Faire confiance, mais vérifier» [32]est un bon conseil pour gérer les relations entre les utilisateurs du Cloud et les fournisseurs de services Cloud. Après avoir établi la confiance initiale et utilisé un service Cloud, l'utilisateur du Cloud doit vérifier et réévaluer la confiance. Un Contrat de niveau de service (SLA) est un contrat juridique entre un utilisateur du Cloud et un fournisseur de services Cloud. Par conséquent, la surveillance de la qualité de service (QoS) et la vérification des SLA constituent une base importante de la gestion de la confiance pour le Cloud computing. Un certain nombre de modèles qui tirent confiance de la vérification des SLA ont été proposés [33, 34].
Un problème majeur est que le SLA se concentre sur les éléments «visibles» de la performance du service Cloud et ne traite pas des éléments «invisibles» tels que la sécurité et la confidentialité. Un autre problème est que de nombreux utilisateurs du Cloud n'ont pas la capacité d'effectuer eux-mêmes une surveillance fine de la qualité de service et une vérification des SLA, un tiers professionnel est nécessaire pour fournir ces services.

3. La Confiance en tant que Service (TaaS) :
Nous avons déjà noté la nécessité d'employer des professionnels tiers pour la surveillance de la qualité de service et la vérification des SLA. L'évaluation indépendante est également utile dans d'autres aspects du Cloud computing.

RSA a annoncé la Cloud Trust Authority (CTA) [35]en tant que service Cloud, appelé Trust as a Service (TaaS), pour fournir un point unique pour la configuration et la gestion de la sécurité des services Cloud de plusieurs fournisseurs. La version initiale du CTA comprend : un service d'identité, permettant une connexion unique entre plusieurs fournisseurs de Cloud, et un service de profilage de conformité, permettant à un utilisateur d'afficher les profils de sécurité de plusieurs fournisseurs de Cloud par rapport à un benchmark commun. Le CTA est un outil spécialisé dans la gestion de la confiance dans le Cloud et est développé à partir de la philosophie de RSA de «confiance = visibilité + contrôle» [36]. En tant qu'outil basé sur le Cloud, le CTA pourrait grandement simplifier la gestion de la confiance des utilisateurs du Cloud. Cependant, un utilisateur du Cloud doit toujours porter un jugement de confiance sur les assertions de service Cloud diffusées dans le CTA, car ces affirmations ont été faites par les fournisseurs de services Cloud eux-mêmes. Plus important encore, un utilisateur du Cloud doit juger de la fiabilité du CTA en tant qu'intermédiaire.

La question essentielle de tout mécanisme TaaS est de savoir quelle est la base de la relation de confiance entre les utilisateurs du Cloud et ces courtiers de confiance

commerciaux.

4. Mécanisme de la transparence de Cloud :
La transparence et la responsabilité sont une base reconnue pour gagner la confiance des fournisseurs de Cloud. Pour accroître la transparence du Cloud, la Cloud Security Alliance (CSA " Cloud Security Alliance ") a lancé le programme «Security, Trust & Assurance Registry (STAR)» [37], un registre gratuit accessible au public qui permet aux fournisseurs de services Coud de publier une auto-évaluation de leur sécurité contrôles, soit dans un «questionnaire de l'initiative d'évaluation du consensus (CAIQ "Consensus Assessments Initiative Questionnaire)» ou dans une «matrice de contrôles Cloud "Cloud Controls Matrix (CCM)"», qui incarnent les meilleures pratiques publiées par l'ASC. CAIQ contient plus de 140 questions que les utilisateurs du Cloud ou les auditeurs peuvent poser ; CCM est un cadre décrivant comment un fournisseur de Cloud s'aligne sur le guide de sécurité CSA [38].

Des exemples d'auto-évaluations des fournisseurs de Cloud sont disponibles sur le site Web de CSA STAR. STAR est une source utile pour les utilisateurs à la recherche de services Cloud. Cependant, les informations proposées sont une auto-évaluation du fournisseur de Cloud ; les utilisateurs du Cloud peuvent souhaiter des évaluations effectuées par des organisations professionnelles tierces indépendantes.

5. Accréditation formelle, audit et normes :
Étant donné que les exercices d'auto-évaluation peuvent être compromis par la malhonnêteté, certains soutiennent qu'une accréditation formelle d'une autorité indépendante de confiance est nécessaire pour un marché du Cloud sain ; d'autres soutiennent que l'accréditation formelle «étoufferait l'innovation de l'industrie» [39].

Des audits externes, des attestations ou des certifications à des fins plus générales (non spécifiques aux Clouds) ont été utilisés dans la pratique. Les exemples incluent : la série ISO / CEI 27000, qui sont des normes internationales de gestion de la sécurité de l'information, qui est une norme d'attestation pour les organisations de services, présentée par l'Auditing Standards Board (ASB) de l'American Institute of Certified Public Accountants (AICPA).

Spécifique au Cloud computing, en plus de CTP et STAR (pour l'auto-évaluation) [40], CSA a également lancé l'initiative Cloud Audit, qui fournit une interface et un espace de noms communs aux fournisseurs de Cloud pour produire des assertions d'audit, et permet aux utilisateurs du Cloud d'automatiser l'utilisation de ces données. Dans leurs propres processus d'audit. Cloud Audit pourrait faciliter l'audit automatisé du Cloud, mené par les fournisseurs de Cloud (pour l'auto-audit), les utilisateurs du Cloud (pour l'audit des utilisateurs du Cloud) et les auditeurs du Cloud (pour l'audit formel). Cloud Audit, CCM, CAIQ et CTP forment la pile de gouvernance, de gestion des risques et de conformité (GRC) CSA.

6. Les certificats en tant que mécanisme :
La confiance est L'un des principaux fondements de l'PKI. Par exemple, Alice doit

faire une confiance avec bob et cela se fait par le biais de certificats, de tickets de confiance (TTs) et de clés d'approbation, qui assure par l'autorité de certificat.

Une confiance fait référence au type de relation qui peut exister entre des individus ou des entités. Une confiance à un tiers fait référence à une situation dans laquelle deux entités se font confiance parce que chacune fait confiance à un tiers qui est le CA. L'infrastructure à clé publique prend en charge un certain nombre de services liés à la sécurité, notamment la confidentialité des données, l'intégrité des données et l'authentification de l'entité finale.

Fondamentalement, ces services sont basés sur des paires de clés publiques/privées. Le composant public de cette clé est émis sous la forme d'un certificat de clé publique et en association avec les algorithmes appropriés. Pour qu'une autorité puisse communiquer avec les principaux et les vérificateurs de manière rentable et fiable, il doit exister une relation étroite entre eux.

2.5 Modèle de confiance dans le Cloud

La confiance est l'un des facteurs essentiels pour l'établissement de la sécurité au sein de Cloud computing, plusieurs recherche ont été menées afin de réaliser un modèle de confiance qui rependre aux exigences de Cloud. La figure suivante représente une classification de ces travaux [64].

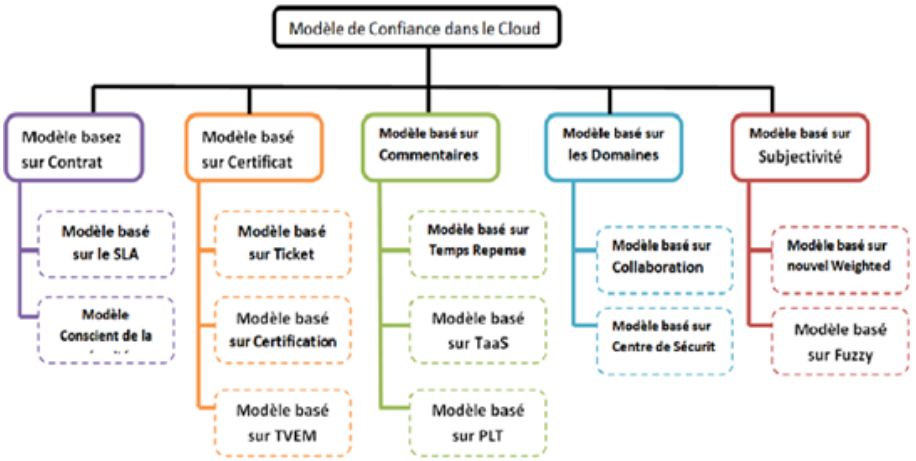

FIGURE 2.3 – modèles de confiance dans le cloud [44].

2.5.1 Modèle basé sur un Contrat (Agreement Based Model)

Dans cette catégorie, Les modèles de confiance sont créés sur les contrats et les accords entre le CSP et les utilisateurs du Cloud. Les contrats les plus fréquemment utilisés sont les SLA (accords de niveau de service (service level agreement) et les rapports de politique de service. Il contient plusieurs documents de sécurité et paramètres QoS pour établir la confiance entre deux parties. L'évaluation de la confiance

dans cette catégorie est illustrée à la figure 2.4.

Dans la première étape, l'utilisateur du Cloud donne ses exigences en matière de sécurité et de qualité de service au module d'évaluation de la confiance. Ce module est capable de créer et de négocier l'accord avec le fournisseur de services Cloud. En général, un tel accord est appelé un SLA ou une déclaration de pratique de service. Le module d'évaluation de la confiance dans sa prochaine étape, transmet une demande de négociation d'accord au fournisseur de Cloud avec les paramètres requis par l'utilisateur du Cloud. Enfin, le module de suivi des paramètres du contrat échange l'accord avec le consommateur pour l'établissement de la confiance entre les deux entités [45, 46].

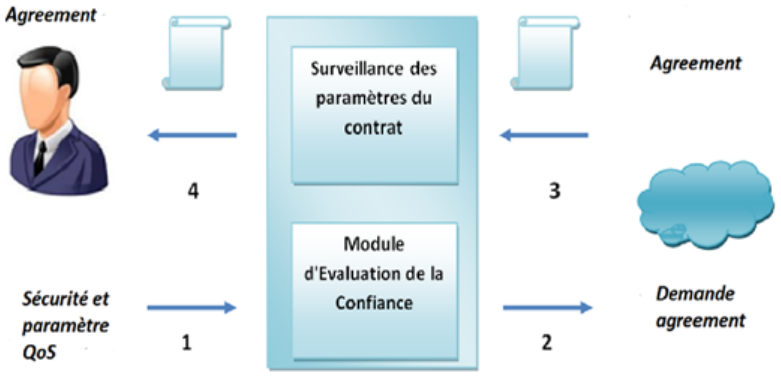

FIGURE 2.4 – Modèle de confiance basée sur les contrats [49].

Exemple : Modèle de Qualité de Service (QoS Quality of Service)

Ce modèle se repose sur l'utilisation du contrat de niveau de service (SLA) entre l'utilisateur et les fournisseurs de ressources cloud pour calculer la valeur de confiance. Ce modèle comprend trois éléments de base et chaque élément joue un rôle important dans le modèle.

1. **Un Administrateur System :** désigne la personne responsable des serveurs d'une organisation (entreprise, association, administration). Il travaille au sein d'une DSI (direction des systèmes d'information).
2. **Un Administrateur SLA :** qui assurer la communication entre un administrateur système et un administrateur de confiance et le client.
3. **Un Administrateur de confiance :** qui calcule la valeur de confiance.

- Comment Calculer la valeur de confiance

On calcule la confiance à partir des informations d'identification du fournisseur de ressources .on considère les attributs d'identifications tels que la disponibilité, la fiabilité, l'efficacité de turnaround et l'intégrité des données pour calculer la valeur de confiance.

- **Disponibilité (Dis) :**

La disponibilité est le degré auquel un système ou un composant est opérationnel et

accessible lorsqu'il est requis pour l'utilisation - IEEE90. En génie logiciel, la disponibilité est mesurée en termes de temps moyen entre les pannes et de temps moyen de réparation]. Lorsqu'un travail est soumis à une ressource Cloud, la ressource est dite indisponible dans l'une des situations suivantes :

1. La ressource est peut-être occupée à traiter la demande de travail.
2. En raison d'un problème de réseau.
3. La ressource ne fonctionne pas correctement ou est à l'arrêt.

Supposons que $R_i, R_i \ldots R_m$ sont les ressources Cloud. Pour chaque $i = 1, 2 \ldots m$, soit N_i le nombre de jobs soumis à la ressource Cloud R_i sur une période T. Sur N_i travailles soumis à R_i , soit A_i désigne le nombre de travailles acceptés par la ressource R_i sur la période T.

$$\text{La disponibilité de ressource } R_i(Dis) = A_i/N_i$$

- **Fiabilité (Fia) :**

La fiabilité est un élément important de la confiance [48]. Il est également appelé taux de réussite. La fiabilité est la capacité d'un système ou d'un composant à exécuter ses fonctions requises dans des conditions déterminées pendant une période de temps spécifiée - IEEE90. Une fois qu'une ressource Cloud accepte un travail, dans quelle mesure le travail est-il fiable ? La fiabilité d'une ressource Cloud est une mesure de la réussite des travaux acceptés par la ressource Cloud [48]. Parmi les travaux A_i acceptés par la ressourceR_i, laissez Ci désigner le nombre de travaux exécutés avec succès par la ressource R_i sur la période T.

$$\text{La fiabilité de ressource } R_i(Fia) = C_i/A_i$$

- **Intégrité des données (ID) :**

un problème clé qui nécessite une attention particulière dans les nuages est la sécurité. L'intégrité des données est un terme large et inclut la sécurité, la confidentialité et l'exactitude des données. La sécurité comprend la sécurité des données et l'exactitude inclut la précision des données. Une perte de données peut se produire en raison d'une faible latence du réseau. Une perte de précision peut survenir en raison d'une infrastructure informatique obsolète. Sur Ci travaux terminés avec succès par la ressource R_i , soit D_i le nombre d'intégrité des données des travaux préservés par la ressource R_i sur la période T.

$$\text{Intégrité des données } R_i(ID) = D_i/C_i$$

- **Efficacité de Turnaround (ET) :**

Le délai d'exécution réel est le temps exact entre la soumission d'un travail par un utilisateur et la livraison du travail terminé à l'utilisateur. Le délai d'exécution promis est le temps prévu par un fournisseur de ressources entre la soumission d'un travail et la livraison du travail terminé. Il est promis par le fournisseur de ressources à l'utilisateur dans le SLA. Ce délai d'exécution réel est normalement différent du délai d'exécution promis par le fournisseur de ressources dans le SLA.

- **Efficacité de turnaround pour un travaille d'un Ressource R_i = Délai d'exécution promis par R_i in SLA / Délai d'exécution réel par R_i pour Compléter le travaille :**

L'efficacité d'exécution est de 1 si le délai d'exécution promis est supérieur au délai d'exécution réel. L'efficacité de rotation d'une ressource R_i (ET) est la moyenne de l'efficacité de rotation sur tous les travaux soumis au cours de la période T. L'efficacité de rotation intègre la puissance de calcul et la vitesse de mise en réseau (en général, l'utilisation). De plus, il intègre également le débit qui correspond au nombre de transactions par seconde.

- **Valeur de confiance d'une ressource :**

Valeur de confiance d'une ressource $= W_1 * Dis + W_2 * Fia + W_3 * ID + W_4 * ET$. où $W_1, W_2, W_3 et W_4$ sont des poids positifs des paramètres de confiance tels que $W_1 + W_2 + W_3 + W_4 = 1$.
Les poids des attributs de confiance sont prédéterminés en fonction de leur priorité. Par exemple, $w_1 = 0,2, w_2 = 0,2, w_3 = 0,5, w_4 = 0,1$. Dans cet exemple, l'intégrité des données reçoit la priorité la plus élevée, tandis que l'efficacité de la rotation reçoit la priorité la plus basse.

2.5.2 Les modèles de confiance basée sur les certificats (Certificate based trust models)

Dans cette catégorie, l'établissement de la confiance se fait par le biais de certificats, de tickets de confiance (TTs) et de clés d'approbation émis par une autorité de certification (CA). Pour l'établissement de la confiance dans cette catégorie, les certificats de sécurité pour les logiciels, les plates-formes et les services d'infrastructure jouent un rôle important. Les tickets de confiance sont émis afin de respecter l'intégrité et la confidentialité des données sur le cloud et d'améliorer la confiance des clients [41]. Le contrôle des données qui sont transférées vers l'environnement cloud [42,43] aux clients Cloud est assuré à l'aide de divers certificats et clés secrètes utilisés dans le modèle de confiance. Comme le montre la figure 2.5 , cette classe comprend en outre les modèles de confiance basés sur les clés d'approbation du module de plateforme de confiance (TPM Trusted Plateforme Model) qui sont responsables du calcul des configurations et des mesures du Cloud pour l'établissement de la confiance.

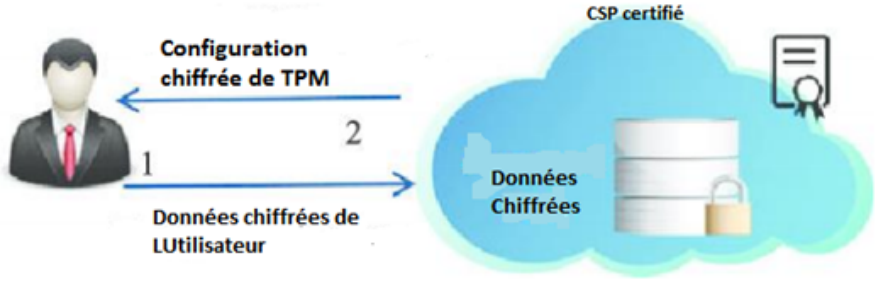

FIGURE 2.5 – modèle de confiance basé sur les Certificats [49].

On va présenter dans le chapitre suivant quelque exemple des modèles de confiance

basé sur les certificats.

2.5.3 Les modèles de confiance basée sur les commentaires (Feedback based trust models)

Ce modèle comprend des modèles de confiance qui recueillent des commentaires et des opinions d'autres consommateurs pour évaluer la confiance sur les fournisseurs de services de communication. En tant qu'étape initiale de l'évaluation de la confiance, divers CSP sont enregistrés avec le modèle de confiance via le module de registre de services [50]. Plus tard, le module de commentaires recueille et gère les commentaires des consommateurs concernant les différents paramètres de qualité de service et de sécurité proposés par les fournisseurs de Cloud enregistrés. Comme le montre la figure 2.7, le module d'évaluation de la confiance calcule le score de confiance des CSP pour les CSP sur la base des commentaires collectés. En outre, les utilisateurs du cloud peuvent envoyer une demande de score de confiance du fournisseur de services Cloud requis au module d'évaluation de la confiance et la même chose est renvoyée à l'utilisateur du Cloud.

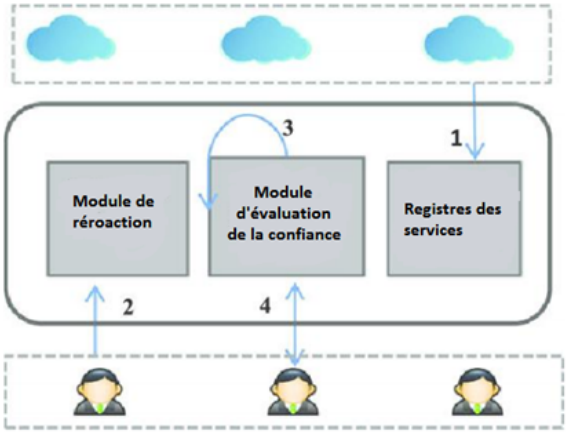

FIGURE 2.6 – modèle de confiance basé sur les commentaires [49].

Exemple : Modèle de confiance basé sur PLT (PLT-based trust model)s

Ce modèle d'évaluation de la confiance contient les modules suivants :

moteur de questionnaire de l'initiative d'évaluation par consensus (CAIQ consensus Assessments initiative questionnaire), gestionnaire d'enregistrement (RM) registration manager), moteur sémantique de confiance (TSE trust semantic engine), moteur de calcul de confiance (trust computation engine), gestionnaire de confiance (TMg Trust manager) et moteur de mise à jour de confiance (TUE trust update engine).

Le processus de formulation de la confiance se déroule en trois étapes principales :

1. Le module TMg fournit une interface qui est utilisée par les clients du Cloud pour spécifier leurs exigences en matière de sécurité et de QoS afin d'évaluer le score de confiance personnalisé pour les CSP.

2. Chaque valeur de confiance pour l'attribut individuel est combinée pour fournir un score de confiance personnalisé global au client.
3. Le TSE configure différentes formations du PLT qui représente le comportement de confiance du CSP en termes d'attributs spécifiques.
4. Enfin, l'AUT est utilisée pour mettre à jour les valeurs de confiance et recueillir les commentaires de diverses ressources sous la forme d'avis qui sont filtrés pour éliminer tout type de spam ou d'informations inutiles [51].

2.5.4 Les modèles de confiance basée sur les Domaines (Domain based trust models)

Les modèles de confiance basés sur le domaine, comme le montre la figure 2.8, sont principalement développés pour le calcul en grille, mais certains des modèles de confiance sélectifs ont été proposés dans cette catégorie pour l'environnement de Cloud computing. L'idée sous-jacente de cette catégorie est de diviser le Cloud en un certain nombre de domaines autonomes et de distinguer deux types de relations de confiance intra-domaine et inter-domaines qui sont respectivement extraites des tables de confiance directes et recommandées. Les valeurs d'approbation intra-domaine dépendent des transactions entre les entités qui sont dans le même domaine. Si une entité souhaite évaluer la valeur d'approbation d'une autre entité, elle vérifie d'abord la table d'approbation directe, si la valeur d'approbation directe (DTV) n'existe pas, puis elle recherche les valeurs d'approbation recommandées des autres entités. La valeur d'approbation inter domaine est une valeur complète basée sur les valeurs d'approbation directes et recommandées d'autres domaines [52, 53].

FIGURE 2.7 – Modèle de Confiance basé sur les Domaines [49].

Exemple : Modèle de confiance centré sur la sécurité et l'interopérabilité (Security and interoperability centered trust model)

Les deux rôles principaux, clients Cloud et CSPs où :

Chaque domaine inclut les ressources qui appartiennent au même fournisseur.

Les clients Cloud disposent de «tables de confiance des clients»

Les fournisseurs de services de communication gèrent des «tables de confiance de domaine» qui incluent le nom de domaine, le type de service, le degré de confiance

et le temps de génération.

Chaque domaine comprend un agent de confiance de domaine qui gère les tables de confiance pour stocker les attributs requis pour la coopération entre les fournisseurs de Cloud.

Au départ, lorsqu'un client souhaite évaluer la valeur d'approbation pour un certain CSP, il correspond au nom de domaine et au type de service requis dans la table d'approbation du client local.

Le client ne peut démarrer les transactions que si la valeur de confiance est supérieure au seuil défini, sinon le processus est suspendu. S'il n'y a aucune valeur dans la table de confiance directe, le score de confiance recommandé sera utilisé.

2.5.5 Les modèles de confiance Subjective (Subjective based trust models)

Les modèles de confiance subjectifs divisent la confiance en diverses sous-classes telles que la confiance d'autorité [54], la confiance de code [55] et la confiance d'exécution dans le Cloud. La théorie des ensembles de probabilités et la théorie des ensembles flous sont les principales techniques d'évaluation des informations de confiance sur un certain CSP et les services fournis. L'une ou l'autre des deux approches différentes, des algorithmes probabilistes ou de théorie floue, sont appliquées pour attribuer les poids et évaluer les sous-classes individuelles de confiance. Après avoir évalué les scores de confiance individuels pour chacune des sous-classes, une valeur de confiance finale est évaluée en agrégeant ces scores de confiance qui représentent la confiance globale du fournisseur de Cloud.

Exemple : nouveau modèle de confiance pondéré basé sur le Cloud (Novel Weighted trust model based on Cloud "NWTM")

Un NWTM Le modèle de confiance est basé sur le modèle de transformation Cloud qualitatif et quantitatif qui peut décrire précisément le caractère aléatoire et flou des valeurs de confiance. Le modèle peut utiliser l'algorithme de génération Cloud normal ou l'algorithme de génération Cloud arrière pour représenter les modèles Cloud. Le modèle de confiance pondéré basé sur le Cloud (CBWT) et l'algorithme de transfert d'informations de confiance pondéré (WTIT) sont utilisés pour l'établissement de la confiance. À l'étape initiale, le modèle CBWT calcule les valeurs Attente (Ex) et Entrée (En) pour les CSP. Différentes valeurs pour l'entropie sont combinées pour formuler l'hyper-entropie pour le CSP, qui représente le score de confiance initial. Après cela, l'algorithme WTIT est exécuté pour transférer les informations de confiance d'une entité à une autre en utilisant les valeurs de confiance recommandées.

2.6 Comparaison

Au niveau de cette section en essayer de faire une petite comparaison entreles cinq modèles étudiées précédemment :

Modèle	SLA	Certificat	feedback	Domaine	Subjective
Type de confiance	*Direct*	*Direct*	*Recommandé*	*Directe et Recommande*	*Recommandé*
Valeur de confiance	*Qualité de Service*	*Fiabilité des Cas*	*Evaluation des Interactions entre les entités*	*Intra domaine* *Inter domaine*	*La somme de confiance invalide*
Dynamique	*OUI*	*OUI*	*OUI*	*OUI*	*OUI*
Administrateur de Confiance	*Administrateur de système*	*Autorité de Certificat*	*Broker*	*Agent de domaine*	*Administrateur de système*
Cout	*Moyen*	*Couteuse*	*Couteuse*	*Moyen*	*Couteuse*

FIGURE 2.8 – Comparaison de modèles [54].

D'après le tableau précèdent :

- Les modèle de SLA et de Certificat ont le même type de confiance direct par contre les autres repose sur une confiance recommandé.
- La valeur de confiance en SLA se repose sur la qualité de service par contre dans les modèles subjective on fait la sommes des confiances invalide.
- Tous les modèles étudier fourni une confiance dynamique.
- Les couts de ces modèles sont entre Moyen et Couteuse.
- L'administrateur de confiance c'est l'Autorité de Certification dans les modèles à base Certificat, le Broker dans les modèles qui se base sur les feedbacks et l'Agent de domaine dans les modèles à base de domaines.

2.7 Conclusion

Dans ce chapitre, nous avons fait une petite introduction sur la confiance et sa nature, en plus nous avons présenté différents modèles d'évaluation de la confiance dans la littérature pour l'environnement de cloud computing.

Un aperçu de la gestion de la confiance, des types de confiance et des facteurs affectant la confiance ont été abordés.

Parallèlement à cela, Tous ces modèles de la littérature sont classés en cinq catégories, à savoir : les modèles de confiance basés sur des contrat/SLA, les modèles

de confiance basés sur des certificats / clés secrètes, des modèles de confiance basés sur le feedback, des modèles de confiance basés sur le domaine et les modèles de confiance subjective. Des explications détaillées sur chaque catégorie sont données ainsi que le travail de recherche effectué jusqu'à présent dans chaque classification.

En outre, nous avons discuté en détail de la classification des modèles d'évaluation de la confiance pour le Cloud.

CHAPITRE 3

LES CERTIFICATS ET LES MODÈLES DE CONFIANCE BASÉ SUR LES CERTIFICATS DANS LE CLOUD

3.1 Introduction

Les certifications en Cloud computing sont un problème pour le commerce électronique. Ce qui laisse penser qu'il va révolutionner toutes les formes de transactions électroniques. Mais avec de la patience, la demande de plus de systèmes PKI à traiter augmentera. Le plein potentiel des signatures électroniques ne peut être réalisé que si les grandes organisations qui émettent des certificats numériques, les autorités de certification (CA), sont opérationnelles.

Les formulaires de certification PKI font désormais l'objet de discussions et de recherches.

3.2 Notion de base de certificat

3.2.1 Définition de certificat

Une identité électronique qui est émise par une tierce partie de confiance pour une personne ou une entité réseau. Chaque certificat est signé avec la clé privée de signature d'une autorité de certification. Il garantit l'identité d'un individu, d'une entreprise ou d'une organisation. En particulier, il contient la clé publique de l'entité et des informations associées à cette entité.

3.2.2 Contenu du certificat

- ID
- Clé publique
- Signature

- Tiers de confiance

3.2.3 Cycle de d'un certificat

Les certificats ont un cycle de vie composé des phases suivantes :

1. Demande de certification.
2. Création et signature du certificat.
3. Remise au demandeur (publication).
4. Utilisation du certificat.
5. Suspension ou révocation du certificat.
6. Expiration du certificat (possible renouvellement).

FIGURE 3.1 – Cycle de vie d'un certificat [59].

3.3 Types de certificats

Les autorités de certification proposent une gamme de certificats. Vous pouvez utiliser un certificat à l'une des fins suivantes :

- Pour sécuriser les transactions Web entre les serveurs Web et les navigateurs Web.
- Pour sécuriser les règlements financiers en ligne et les Transactions Electroniques Sécurisées (SET).
- Pour sécuriser des réseaux, des réseaux privés virtuels (VPN), IP Security Protocol (IPSEC), IPv6 et des produits tels que Point-to-Point Tunneling Protocol (PPTP).
- Pour sécuriser les applications personnalisées.

Vous pouvez acheter différents types de certificats auprès d'une autorité de certification :

- Certificat racine.
- Certificat de serveur.

- Certificat personnel.
- Certificat d'éditeur de logiciel.
- Certificat de signature de contenu.

3.4 Les modèles de certificat

3.4.1 Les modèles de PKI

- PKI est un système de gestion de clés publiques qui vous permet de gérer des listes importantes .Clés publiques et assurer leur fiabilité, pour les entités en général du réseau.
- PKI ne distribue pas des clés mais des certificats Un certificat est valide par un tiers de confiance.
- PKI fournit 4 fonctions :
    - Confidentialité.
    - Authentification.
    - Non-répudiation [60].
    - Intégrité.

Et quatre services principaux suivants :

- Fabrication de bi-clés.
- Certification de clé publique et publication de certificats.
- Révocation de certification.
- Gestion la fonction de certification.

Les composants de PKI :L'infrastructure de gestion desclé publiques est constitué de plusieurs composants parmi les on cite :

- **L'autorité de certification (CA) :**

Elle est responsable de générer un certificat pour l'utilisateur. Le certificat contient des informations personnelles sur l'utilisateur mais surtouts clef publique et la date de validité de certificat. L'autorité de certification signera ce certificat avec sa clef privée.

- **L'autorité d'enregistrement (RA) :**

Le rôle de l'autorité d'enregistrement est de vérifier la demande d'enregistrement d'un nouvel utilisateur dans l'infrastructure. Les méthodes de vérification sont définies en fonction de la politique de certification choisie pour l'infrastructure. Si l'autorité d'enregistrement valide la demande d'enregistrement, Alors la requête de certificat peut être contenue dans l'autorité de certification.

- **Un annuaire :**

l'annuaire est indépendant de la PKI cependant la PKI en a besoin. L'esseules

contraintes de l'annuaire sont qu'il doit accepter le protocole X.509 pour le stockage des certificats révoqués et le protocole LDAP [61].

Les modèles PKI les plus populaires sont les suivants :

3.4.1.1 La certification croisée

Le terme de certification croisée désigne deux opérations :

- La première opération, est la mise en place d'un Relation de confiance entre deux AC via la signature de la clé publique d'une autre AC dans un certificat appelé "certificat croisé".
- La deuxième opération, exécutée fréquemment par l'application cliente, consiste à vérifier la fiabilité d'un certificat d'utilisateur signé par une autorité de certification au sein de votre réseau PKI. le opération est souvent appelée « marcher une chaîne de confiance ». La « chaîne » fait référence à une liste de validations de certificats croisés qui sont « parcourues » (ou tracées) à partir de la clé de l'autorité de certification racine ou « de confiance ancre » de l'utilisateur vérificateur à la clé CA nécessaire à la validation de l'autre utilisateur certificat.

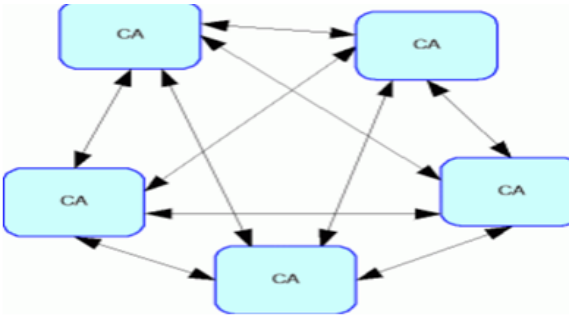

FIGURE 3.2 – La certification croisée [62].

3.4.1.2 Modèle de liste de confiance de certificat

Outre les certificats et les listes de révocation de certificats (CRL), le magasin de certificats prend en charge la liste de certificats de confiance (CTL). Un CTL est une liste prédéfinie d'éléments signés par une entité de confiance. Un CTL est une liste de hachages de certificats ou une liste de noms de fichiers. Tous les éléments de la liste sont authentifiés et approuvés par une entité de signature de confiance.

FIGURE 3.3 – Modèle de liste de confiance de certificat [62].

3.4.1.3 Chaînes de certificats

Une chaîne de certificats est une liste de certificats (commençant généralement par un certificat d'entité finale) suivi d'un ou plusieurs certificats CA (généralement le dernier étant un certificat auto-signé), avec les propriétés suivantes :

- L'émetteur de chaque certificat (sauf le dernier) correspond au sujet du certificat suivant dans la liste.
- Chaque certificat (sauf le dernier) est censé être signé par la clé secrète correspondant au certificat suivant de la chaîne (c'est-à-dire que la signature d'un certificat peut être vérifiée à l'aide de la clé publique contenue dans le certificat suivant).
- Le dernier certificat de la liste est une ancre de confiance : un certificat auquel vous faites confiance car il vous a été délivré par une procédure digne de confiance. Une ancre de confiance est un certificat CA (ou plus précisément, la clé de vérification publique d'une CA) utilisé par une partie de confiance comme point de départ pour la validation du chemin .

3.4.1.4 Le mécanisme hors-de-bande (OOB)

C'est un modèle de confiance qui permet de créer une empreinte de la clé d'une CA de manière sécurisée (à l'aide d'une fonction de hachage). Une fois créée, la clé peut être acheminée sur un réseau peu, voir non sécurisé. Le destinataire à qui on a au préalable fourni les informations concernant la fonction avec laquelle cette empreinte a été générée pourra comparer à la réception et verrier si les données n'ont pas été altérées an de pouvoir en récupérer de manière sûre la clé de la CA. Cette technique est communément utilisée pour sécuriser les protocoles sur les navigateurs et serveurs web.

3.4.1.5 Le message de demande de certificat

En premier lieu, l'utilisateur envoie sa clé publique vers une autorité, cette fois-ci, l'autorité d'enregistrement des certificats (RA), mais toujours à traversine liaison sécurisée.

La RA transfère un message signé au CA ; ce message inclut, en plus des informations concernant l'utilisateur, la clé publique de l'utilisateur : c'est ainsi qu'est émise la demande de certificat. L'utilisateur recevra alors de la part de l'autorité de certification, un certificat signé.

Enfin, après que le CA ait envoyé sa clé publique au système de vérification, l'utilisateur pourra transmettre les données qu'il devra signer et accompagner du certificat qui lui a été délivré afin que le système de vérification puisse confirmer leur authenticité.

3.4.1.6 Modèle de confiance de certificat (Certificat Trust Model)

La liste de confiance des certificats est une liste de certificats d'autorités de certification provenant d'une autorité de confiance. La liste elle-même est signée élec-

troniquement pour garantir son intégrité. Bien qu'ils soient simples, ils fournissent un appareil très utile pour communiquer la confiance et remplacer la nécessité du processus plus complexe de certification croisée. Elles sont employées dans un large éventail de structures administratives différentes, comme le modèle de reconnaissance croisée utilisé.

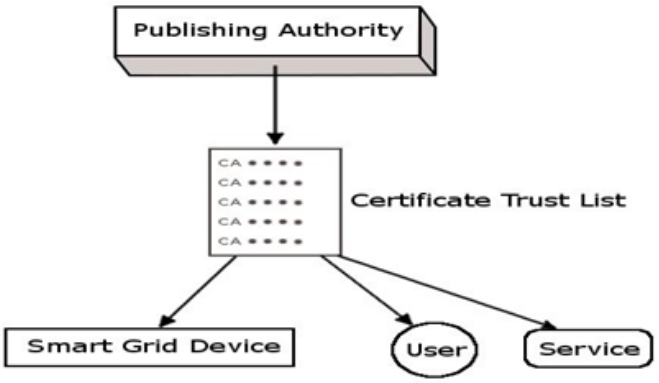

FIGURE 3.4 – Modèle de confiance de certificat [62].

3.5 Les architectures de certificat

3.5.1 Les architectures de PKI

Les architectures les plus couramment utilisées sont les suivantes :

3.5.1.1 L'architecture hiérarchique (racine)

L'architecture hiérarchique Le fonctionnement de cette architecture dans le cas de deux autorités de certification (CA1 et CA2) régies par une autorité de certification centrale ou (CAroot) est le suivant : CA1 et CA2 envoient leur clé publique au CA central qui génère un certificat pour chacun des deux CA. Au sein de cette architecture, le (CAroot) a le plus haut niveau d'autorité et possède donc un certificat auto signé. Aussi, cela implique que tous les composants de l'architecture placent leur confiance dans le CA central.

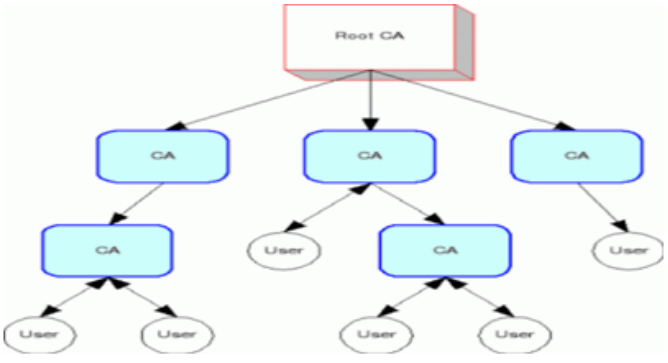

FIGURE 3.5 – L'architecture hiérarchique [62].

3.5.1.2 L'Architecture P2P (Peer-to-Peer)

Les différentes autorités sont en même niveau ou CA1 est capable de signer des certificats CA2 et vice versa.

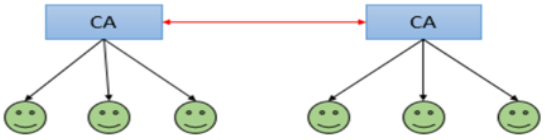

FIGURE 3.6 – L'architecture P2P [62].

3.5.1.3 L'architecture en pont (Bridge)

L'architecture en pont ou en Bridge estune association des deux architectures P2P ethiérarchique. Comme l'architecture hiérarchique a pour principales lacunes la disponibilité et la sécurité et que le modèle pair-à-pairest ralentit par la multitude d'échanges qui y sont générés, alors l'architecture en pont palieaux lacunes des deux architectures précédentes.

Son fonctionnement est similaire à celui du P2P à la différence que les échanges entre CA qui ralentissaient le P2P sont réduits dans la mesure où les CAs n'échangent leurs clés qu'avec l'autorité pont. On peut aussi définir cette architecture comme une architecture hiérarchique où le CAroot est au même niveau d'autorité que les autres CAs qui y sont affiliés.

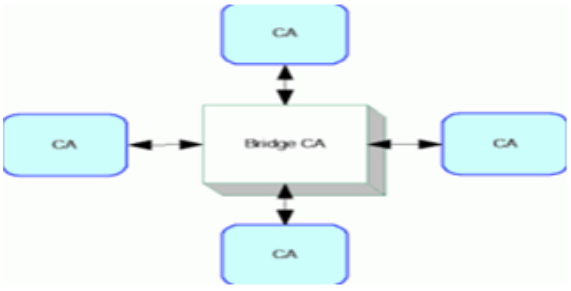

FIGURE 3.7 – L'architecture en pont(Bridge) [62].

3.6 Les modèles de confiance basée sur le certificat (Certificate based trust model)

Voici quelques modèles de confiance qui entrent dans la catégorie des modèles de confiance basés sur des certificats/clés.

3.6.1 Modèle de confiance basé sur les tickets (ticket based trust model(TTM))

Mahbub et al [56]. ont proposé un nouveau modèle TTM. Lorsque la date est partagée entre le propriétaire des données (DO) et les utilisateurs, les propriétaires

des données (DO) utilise des clés secrètes pour crypter les données. Ici, avec les données cryptées, une liste de référence est également partagée qui affiche l'identifiant de l'utilisateur, l'identifiant des données, les droits d'accès, etc. Un nouvel utilisateur est lui-même enregistré auprès de DO en fournissant des informations d'identification et une liste de référence est mise à jour en même temps. Après cela, tous les détails, y compris le délai d'expiration, les informations d'identification requises et la liste des capacités, sont ensuite transmis au nouvel utilisateur après l'enregistrement.

Dés que les DO envoient un ticket (un seul ticket) à l'utilisateur en suivant le mécanisme d'authentification suivant :

$$Trust\ Ticket_{UID}\{U_{PD}, U_{id}, D_{id}, AR, TT_{exp}\}SK_{PD,CSP}.$$

Ou :
U_{PD} : Identité des propriétaires des données.
U_{id} : Identité d'utilisateur.
D_{id} : Identité des données.
AR : Droits d'accès.
TT_{exp} : Date d'expiration de ticket de confiance.
$SK_{PD,CSP}$: Clé symétrique entre les PD et les fournisseurs de service.

Un nouvel utilisateur est lui-même enregistré auprès de DO en fournissant des informations d'identification et une liste de références est mise à jour en même temps.

Après cela, tous les détails, y compris l'heure d'expiration, les informations d'identification requises et la liste des capacités, sont ensuite transmis au nouvel utilisateur après l'enregistrement par le CSP.

Dans le protocole de déploiement de TT ; l'utilisateur envoie un TT au CSP pour accéder au données.

Le CSP envoie les données chiffrées à l'utilisateur après la vérification de ses informations comme dans la figure suivant [57].

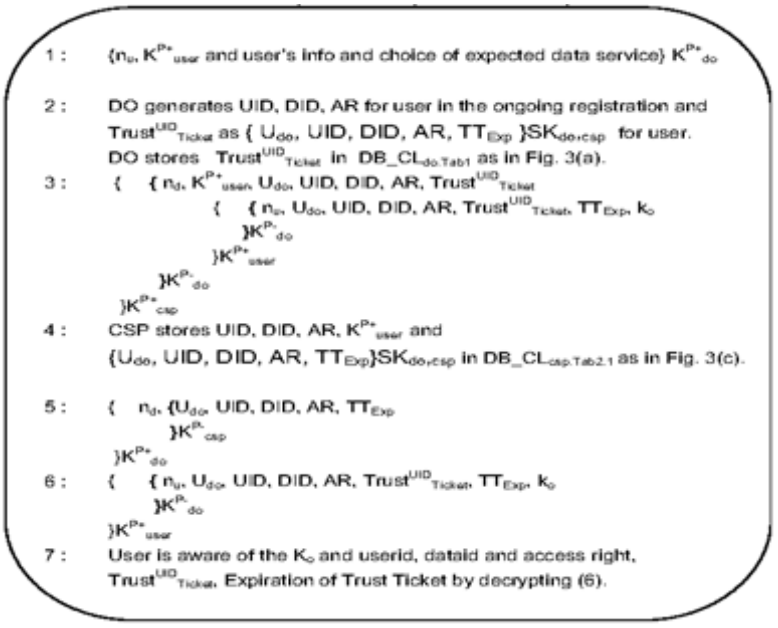

FIGURE 3.8 – Protocole Algorithmique pour le déploiement de Trust Ticket [57].

Ou :
- CSP, csp : fournisseur de service.
- CapList : Liste des Capacités (UID, DID, AR pour l'utilisateur) par DO .
- data, DhkID : data de DO, id de sauvegarder des données.
- K : clé de session générée par DO.
- KO : clé secret entre le DO et l'utilisateur enregistré.
- K^{p-}_{csp}, K^{p+}_{csp} Clé publique et secret pour le CSP.

Utilisateur K^{p+} utilisateur K^{p-} : clé publique et clé secret de l'utilisateur (User PK).
- K^{p+}_{do}, K^{p-}_{do} : clé publique et clé secret pour les DO (propriétaire de données).
- Loc : Localisation des données.
- n_x : nombres aléatoires uniques par x pour éviter une attaque par rejet.
- $SK_{do,esp}$: clé symétrique entre DO et CSP.
- TTicket : ticket de confiance.
- U/utilisateur, UDO : utilisateur enregistré, identité du Do d'un utilisateur enregistré .
- Uid, Did, AR : identité de l'utilisateur enregistré, identité des données, droits d'accès.
- yK_x : les données y sont cryptées avec la clé yK_x.

3.6.2 Modèle de confiance basé sur les certificats (Certification-based trust model (CTM))

Dans ce modèle, l'approche basée sur les certificats qui offre un « cadre de découverte » qui permet aux clients de spécifier les propriétés ou les problèmes de sécurité qui doivent être évalués dans un service cloud particulier.

La comparaison des certificats et la composition dynamique des services sont les deux fonctions principales assurées par le Framework de découverte. Les techniques

de raisonnement automatisé ont été utilisées pour comparer les certificats de divers services de sécurité proposés par différents fournisseurs de Cloud.

Une liste de tous les services certifiés est publiée par le cadre de découverte de telle sorte que si le cadre ne peut découvrir aucun service unique qui correspond aux exigences du client, une composition de services est fournie via une composition de service dynamique.

- **Analyse des caractéristiques non fonctionnelles :**

Le mécanisme de comparaison de certificats utilisé par ce modèle de confiance sélectionne le meilleur fournisseur Cloud certifié capable de mettre en œuvre les techniques de cryptage, assurant ainsi la confidentialité des données à un niveau moyen.

De même, le meilleur CSP certifié capable de créer et de définir les politiques de contrôle d'accès est sélectionné par le module de framework de découverte pour fournir l'assurance du contrôle et de la propriété des données.

La détection des comportements non fiables dans le Cloud est prise en charge par la vérification des certificats. D'autre part, le modèle ne fournit aucun mécanisme pour assurer le contrôle de l'exécution du processus et la transparence de la QoS. De plus, la composition dynamique des services introduit une grande complexité dans la mise en œuvre du cadre de découverte. Le nombre requis de services Cloud peut être examiné et validé à partir des certificats délivrés par les autorités d'accréditation, introduisant ainsi une grande flexibilité dans le modèle. De plus, le framework peut sélectionner le service Cloud accrédité par des tiers pour satisfaire la réplication des données qui assure la disponibilité des données.

- **Analyse des caractéristiques fonctionnelles :**

Le framework de découverte est responsable de l'évaluation des certificats émis par des tiers ainsi que de la vérification de ces certificats. De même, ce modèle de confiance est capable d'assurer la solidité de la liaison des certificats en soutenant la composition verticale des propriétés certifiées.

3.6.3 Modèle de confiance basé sur TVEM (TVEM based trust model (CTM))

Le modèle basé sur TVEM contient un module TVEM et un VTN. Initialement, l'usine TVEM (TF) gère la création du module TVEM avec la clé principale VTN racine, les certificats, les clés d'environnement de confiance (TEK) du côté du propriétaire des données. Après la création des clés, le TF gère le provisionnement de TVEM sur la plateforme du fournisseur de cloud hôte. Les données sont cryptées à l'aide du TEK et un VTN est établi entre le propriétaire des données et le CSP pour transférer ces données sur le Cloud. Plus tard, le TVEM mesure en continu la confiance dans le Cloud via la racine de confiance pour la mesure (CRTM) et la base

informatique de confiance (TCB) qui contient le BIOS et d'autres configurations de plate-forme attestées par le TPM sur le Cloud. Dans le même temps, le registre de configuration de l'environnement virtuel (VECR) est utilisé pour évaluer les politiques de l'Hyperviseur pour la double racine de confiance [28].

- **Analyse des caractéristiques non fonctionnelles :**

Les clés de chiffrement TEK et VTN sont utilisées pour assurer la confidentialité des données sur la plateforme Cloud. TCB mesure les configurations et VECR évalue les politiques de l'environnement virtuel, assurant ainsi la propriété des données sur le Cloud. Le VTN est fourni par le modèle pour contrôler à distance toutes les activités de calcul s'exécutant sur le Cloud et assurant le contrôle de l'exécution du processus. Les mesures et configurations du CRTM et du TCB aident à détecter les comportements non fiables ; cependant, le modèle n'offre pas l'assurance de la transparence de la QoS pour les consommateurs du Cloud.

La création, la gestion et la migration du TVEM, des certificats VTN et des TEK introduisent une complexité inapplicable du TF à la fin du DO. Cependant, le modèle est suffisamment flexible pour intégrer les algorithmes de sécurité souhaités compatibles avec le TPM installé sur la plateforme Cloud. Il ne prend en charge aucun mécanisme pour assurer la disponibilité des données.

- **Analyse des caractéristiques fonctionnelles :**

Le module TF côté consommateur est chargé de vérifier les clés. Le VTN qui est un lien de confiance et dédié entre la plate-forme Cloud et le consommateur est associé à une clé unique pour prendre en charge la liaison robuste des clés.

3.7 Analyses des caractéristiques fonctionnelles et caractéristiques non fonctionnelles de modèle de confiance basé sur le certificat

Nous avons essayé de présenter les différentes caractéristiques fonctionnelles et non fonctionnelles des modèles de confiances de certificats dans les deux tableaux suivants :

Caractéristique fonctionnelles	**TTM**	**CTM**	**TVEM**
Vérifications des certificats et Tickets	-	-	-

TABLE 3.1 – Analyses des caractéristiques fonctionnelles de modèle de certificat [57].

Caractéristique non fonctionnelles	TTM	CTM	TVEM
Confidentialité des données		-	-
Traiter contrôle d'exécution	-	-	-
Facilité d'application	-	-	-
La flexibilité	-	-	-
Disponibilité des données	-		-
Propriété des données	-	-	-
Transparence QoS			

TABLE 3.2 – Analyses des caractéristiques non fonctionnelles [57].

3.8 Comparaison entre les modèles de confiance basée sur les certificats

Le tableau suivant décrit une comparaison entre les modèles de confiance basé sur les certificats qui on a déjà explique.

Nom de modèle	*Processus impliqué*	*Défis*
TTM	Les données sont cryptées avec la clé secrète.	Manque de transparence de la Qos. Ne prend pas en charge la facilité d'application.
CTM	Des certificats sont émis qui évaluent les valeurs de confiance.	Manque de transparence de la QoS. Ne prend pas en charge la facilité d'application.
TVEM	Les données sont cryptées à l'aide de TEK et de VTN.	Les données ne sont pas disponibles tout le temps.

FIGURE 3.9 – Comparaison entre les modèles de confiance basée sur les certificats [60].

3.9 Conclusion

Ce troisième chapitre, est consacré à l'étude des certificats est les modèle de confiance basé sur les certificats. Premièrement nous avons présenté le concept de certificats, sa définition et caractéristiques, ses modèle, ses architectures. Après dans sa deuxième partie nous avons les modèles de confiance basée sur les certificats, les classe de ces modèles, des exemples sur ces classes et une comparaison et une discussion de ces exemples.

CHAPITRE 4

MODÈLE PROPOSÉ

4.1 Introduction

Dans les chapitres précédents, on a cité plusieurs modèles de confiance dans le cloud : les modèles de confiance basée sur les certificats, les domaines, les feedback, les SLAs et les modèles de confiances subjectives. Chacun de ces modèles a ses propres avantages et ses limites et aucun modèle de ces derniers n'offre une sécurité parfaite, d'où la naissance des modèles hybrides.

Dans ce mémoire de master, nous avons proposé un système de gestion de confiance dynamique ou nous avons proposé une architecture pour la gestion de confiance dans un environnement cloud multi-domaines en plus d'un modèle d'évaluation de confiance. Notre modèle d'évaluation est un modèle hybride qui permet de calculer la valeur de confiance sur la base des notes associées aux : différents domaines de sécurité, les feedbacks des utilisateurs et au degré de confiance des autorités de certification.

Notre système de confiance permet d'améliorer la sécurité des services cloud, en appliquant plusieurs niveaux de sécurité :

- Une gestion de confiance dans des domaines de sécurité différents en se basant sur les domaines différents de services, les commentaires des utilisateurs et le degré de confiance des autorité de certification.
- L'authentification forte des différentes entités en utilisant les deux méthodes d'authentification : l'authentification par email et l'authentification par certificats.
- Le contrôle d'accès aux ressources en se basant sur les certificats. la certification des diffèrent entités (utilisateur, fournisseur.)

4.2 Les notions de base du modèle proposé

Dans cette partie on a essayé de citer les composants qui constitué notre modèle proposé, les rôles de chacun de ces composants, les relations entre ces derniers.

4.2.1 Les composants de modèle proposé

Le modèle est constitué de quatre composant essentiel a savoir :

1. **L'utilisateur de cloud :** l'utilisateur de cloud c'est l'entité qui va consommer un service cloud. L'utilisateur cloud peut être une entité finale ou bien un fournisseur de cloud qui consomme des services appartient à d'autre fournisseur Cloud. Cette entité demande une recommandation du système de confiance afin de pouvoir trouver le service le plus crédible. L'utilisateur cloud et après la consommation du service cloud il commente le service et ce commentaire est envoyé au service de confiance.
2. **Le fournisseur de cloud :** Le fournisseur de cloud c'est l'entité qui fournisse des ressources informatiques sous forme de service. le but principal d'un fournisseur cloud est de rassemblent des ressources partageable sur le réseau.
3. **Système de confiance :** c'est l'entité qui assure la médiation entre les deux parties fournisseur et utilisateur de cloud. Le système de confiance et lors la réception d'une demande de recommandation d'un utilisateur cloudil aide ce dernier pour choisir son fournisseur le plus confiant en faisant des évaluations et donnant une note pour chaque fournisseur. Cette note est calculée sur la base de plusieurs critères qui sont : les commentaires des utilisateurs, les domaines de sécurité des fournisseurs et d'utilisateur, les caractéristiques des cloud et la réputation des autorités de certification. Le système de confiance à son tour est constitué de plusieurs composants :
   - **Le composant Classification :** qui faire la classification des caractéristiques des clouds, domaines, commentaires des utilisateurs et des autorités de certification. Le composant classification à son tour est composé de quatre modules :
     - **Classifier clouds :** lors le reçoit des caractéristiques des clouds par le service de confiance ce dernier enregistre ces caractéristiques dans l'annuaire des clouds.
     - **Classifier domaines :** la table de domaine est une table qui contienne les différents domaines.
     - **Classifier commentaires :** lors le reçoit des commentaires des utilisateurs le service de confiance enregistre ces derniers dans la table des commentaires.
     - **Classifier les autorités des certifications :** ce composant gère et classifier les différentes autorités de certification ou pour chaque autorité il calcule une note de confiance qui présent le degré de confiance de cette dernière. Les caractéristiques des autorités de certification sont enregistrées dans la table des autorités.

- **Le composant Evaluation de sécurité :** le rôle de cet composant est d'évaluer la confiance des différents clouds lors la réception d'une demande de recommandation d'un utilisateur. Cette évaluation se fait selon le modèle d'évaluation proposé. Après cette évaluation le composant Evaluation de sécurité envoi l'identifiant du cloud le plus confiant à l'adresse mail de l'utilisateur.

4. **Autorités de certification(CA) :** une autorité de certificat est une tierce partie de confiance permettant d'authentifier l'identité des correspondants. Une autorité de certification délivre des certificats décrivant des identités numériques et offre les moyens pour vérifier la validité de ses certificats. Notre système est un système multi- autorité ou un utilisateur peut avoir des certificats délivré par plusieurs autorités de certification.

4.2.2 Les relations entre les composants de modèle

Les relations entre les composants de notre modèle sont comme suit :

- **Le fournisseur de cloud /Autorité de certification :** le fournisseur demande un certificat au CA pour certifier ces ressources.
- **Autorité de certification /Le fournisseur de cloud :** le CA donner un certificat au fournisseur avec sa clé public et clé secret.
- **Le fournisseur de cloud / Système de confiance :** le fournisseur envoi eau service de confiance ses caractéristiques comme ID cloud, clé public de certificat de cloud , les domaines où il propose des services... le fournisseur cloud envoi aussi la réputation des autorité de certification au service de confiance.
- **Utilisateur de cloud / Système de confiance :** l'utilisateur cloud envoi ses exigence en qualité de service en plus de leur domaine (le choix de payé) et demande un service de recommandation. Et après la consommation du service, l'utilisateur commente le service consommé et envoi le feedback au service de confiance. L'utilisateur de cloud envoi aussi la réputation des autorités de certification utilisé au service de confiance.
- **Système de confiance / utilisateur de cloud :** aider l'utilisateur à choisir son cloud le plus confiant en lui transmis le fournisseur avec la note de confiance la plus haute.
- **Utilisateur de cloud / Fournisseur de cloud :** les utilisateurs négocient un contrat SLA avec le fournisseur et consomment les services des fournisseurs cloud.

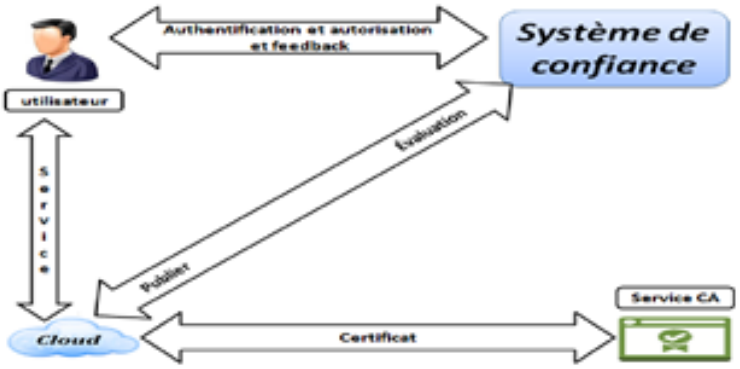

FIGURE 4.1 – Relation entre les composants de modèle proposé.

4.3 Architecture du modèle proposé

Dans cette partie nous avons présenté l'architecture globale de notre système de gestion de confiance.

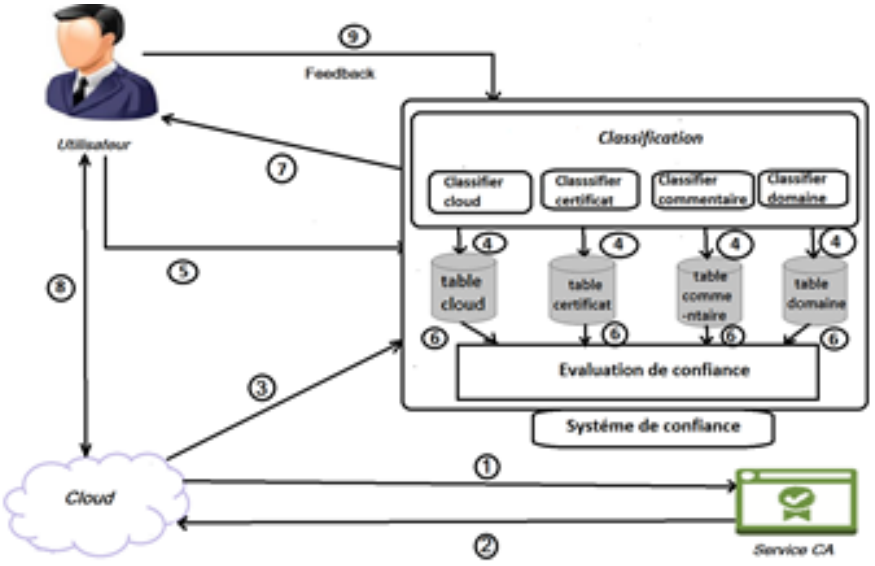

FIGURE 4.2 – Architecture globale de modèle proposé.

4.3.1 Les étapes de modèle proposé

1. Le cloud demande un certificat au service CA.
2. Le CA renvoie la réponse comme un certificat vers le cloud demandeur.
3. Les clouds certifiés envoient ses informations et caractéristique au service de confiance : le Id cloud, le nom de cloud, le certificat et ses domaines de cloud.
4. Le système de confiance faire une classification des clouds, des certificats, des domaines et des commentaires.
5. L'utilisateur envoie ces besoins au système de confiance avec leur authentification.

6. Le système de confiance récupère les informations nécessaires des bases de données : annuaire des cloud, table des commentaires, table des domaines et la table des certificats pour l'évaluation des valeurs de confiance des clouds. Cette évaluation se fait selon le modèle d'évaluation proposé.
7. Le système de confiance envoie à l'utilisateur un email contient l'identifiant du cloud qui à la plus grande valeur de confiance et si on a beaucoup de domaines il envoie ID de domaine de chaque cloud à la plus grande valeur de confiance.
8. L'utilisateur peut négocier une SLA avec le cloud recommandé. Après l'utilisateur doit se certifier (en cas des clients non certifié) pour qu'il s'authentifier et accéder au service cloud fourni.
9. L'utilisateur envoie un feedback qui contient une évaluation de cloud après la terminaison de la consommation de service.
10. Le système de confiance faire une mise à jour aux valeurs de confiances de ces cloud lors la réception de nouveaux commentaires des utilisateurs.

4.4 le modèle d'évaluation de confiance proposé

Dans notre modèle le système de confiance le choix du fournisseur le plus confiant est se fait selon quatre critères : les domaines de sécurité, les commentaires de clients et les réputations des certificats. Ou la valeur de confiance d'un cloud est calculée par la formule suivante :

$$Valeur\ de\ confiance = \frac{VCD + VCC + VS}{3} \tag{4.1}$$

Ou :
VCD : la valeur de confiance des domaines.
VCC : la valeur de confiance basée sur les commentaires des clients.
VS : la valeur de sécurité ou le degré de confiance de certificat.

4.4.1 la valeur de confiance des domaines

Dans notre système, un cloud peut fournir des services dans plusieurs domaines. Lorsqu'un utilisateur demande un service de recommandation. Le service de confiance récupère le domaine de l'utilisateur et essayer de recommander un service dans un domaine proche de celui de l'utilisateur en calculant la valeur de confiance des domaines par rapport au domaine de l'utilisateur. La valeur de confiance des domaines prend trois valeurs selon les trois niveaux : élevé, moyenne et faible avec les note respectivement (0.9 et 0.6 et 0.3). Cette valeur est calculée selon la proximité et la distance de l'emplacement géographique de service de fournisseur à celui de l'utilisateur.

Exemple :

Dans le cloud Amazon AWS qui situé à L'Amérique et qui propose plusieurs domaines de sécurité ou les centres de données appartient à ce cloud sont distribué dans des différents domaines géographique : l'Amérique, l'Europe, l'Asie et L'Afrique (Afrique de nord).
Si un utilisateur connecte on Afrique, le système de confiance donne les notes suivantes :

- AmazonAWS(Afrique)= 0.9,
- Amazon AWS(Amérique)= 0.3,
- Amazon AWS(Europe)= 0.6 et
- AmazonAWS(Asie)= 0.3.

Le service cloud ou bien le cloud en général qui est le plus proche géographiquement à la localisation de client prend la valeur confiance la plus haute.

4.4.2 la valeur de confiance basée sur les commentaires des clients

Les commentaires des utilisateurs est critère très important pour évaluer les services dans l'environnement cloud flou. La valeur de confiance basée sur les commentaires des clients est calculée par la façon suivante :

Lorsque les entités effectuent une deuxième transaction, la valeur VCC sera 0,5 car la confiance sera évaluée en tant que confiance directe après une transaction. La valeur de confiance des commentaires VCC est une combinaison du score d'évaluation de la transaction (ET) et du VCC. Un utilisateur peut commenter un service en lui donnant soit la note 0.1 si le service est fiable et -0.1 sinon.

La confiance d'un service en se basant sur les commentaires des utilisateurs est donné par l'équation suivant :

$$VCC = VCC + MOY(ET) \tag{4.2}$$

Tel que :

$$MOY(ET) = \frac{\sum notes\ de\ service\ données\ par\ les\ different\ utilisateurs}{le\ nbr\ totale\ des\ utilisateurs}$$

4.4.3 la valeur de sécurité

Afin de créer une confiance formelle dans notre système de confiance nous avions adapté la structure de clé publique (les certificats) en tant que mécanisme efficace pour créer et accroître la confiance entre l'utilisateur et le fournisseur dans le cloud.

Notre système de confiance se repose sur un modèle multi autorité ou un fournisseur ou bien un client de cloud peut avoir des certificats délivré par plusieurs autorités de certification.

Le service de confiance contient une liste des autorités de certification les plus confiants et chaque autorité avoir une note de confiance calcule par le service de confiance selon le prix et la date de validation de certification et le type de hachage et le degré de confiance de domaine de cloud. Selon la note de confiance les autorités de certification dans notre modèle appartient à trois niveaux de confiance :élevé, moyenne et faible. Le tableau 5.1 montre ces niveaux et note de chaque niveau.

Niveau	**Statuts**	**Prix**	**Duré de valide**	**Note**
Niveau 1	Elevé	700=< prix	Duré < 1ans	0,9
Niveau 2	Moyen	400=< p< 700	1ans =<D<2ans	0,6
Niveau 3	Faible	Prix < 400	2ans =< Duré	0,3

TABLE 4.1 – Classification des certificats.

4.5 Mécanisme de sécurité

Les aspects de sécurité ont un impact direct et très important sur la confiance comme nous l'avons déjà parlé dans le deuxième chapitre, la confiance est la base de tous autre mécanisme de sécurité (la pyramide mentionnée au chapitre précédent). Cette section est dédiée aux mécanismes utilisés pour sécuriser le service lors de son consommation. Nous pouvons résumer ces aspects dans le suivant :

Aspects	**Mécanisme**	**Proposition**
Authentification fort.	Offres une authentification avancée	Confirmé l'authentification par e-mail+ certificat.

FIGURE 4.3 – Différents Aspect de la sécurité.

4.6 Avantages de modèle proposé

Notre système de confiance permet :

- L'amélioration de la sécurité des services dans un environnement cloud multi-domaines , en appliquant plusieurs niveaux de sécurité : la gestion de confiance dans des domaines de sécurité différents en se basant sur ces domaines , les commentaires des utilisateurs et le degré de confiance des autorité de certification pour l'évaluation de la valeur finale de confiance. l'authentification forte (l'authentification par email et l'authentification par certificats) et la gestion par certificat des droits d'accès aux ressources.
- Fournit une confiance à cause de l'utilisation des certificats.
- Notre système permet la collaboration inter-clouds à travers plusieurs domaines de sécurité.
- Fournit une confiance dynamique ou la valeur finale de confiance est changé a chaque fois un utilisateur faire un commentaire sur le service.
- Enlever la responsabilité de chercher le cloud le plus confiant ou le service de confiance assume cette responsabilité.

4.7 Conclusion

Dans ce chapitre nous avions proposé notre système dynamique pour la gestion de confiance dans le cloud. Ou nous avons proposé une architecture pour la gestion de confiance dans un environnement cloud multi-domaines en plus d'un modèle d'évaluation de confiance. Ce modèle d'évaluation est un modèle hybride qui permet de calculer la valeur de confiance sur la base des notes associées aux : différents domaines de sécurité, les feedbacks des utilisateurs et les degrés de confiance des autorités de certification.

Notre modèle améliore la sécurité des services cloud en combinant plusieurs approches pour évaluer la confiance et en appliquant plusieurs niveaux de sécurité : la gestion de confiance, l'authentification forte et la gestion par certificat des droits d'accès aux ressources.

Dans ce chapitre, nous avions expliqué les principes de notre système en détail et dans le chapitre suivant nous avons présenté l'implémentation de ce système.

CHAPITRE 5

IMPLÉMENTATION

5.1 Introduction

Dans lechapitre précèdent nous avions présenté les détails de notresystème dynamique pour la gestion de confiance proposé ou nous avions détaillé notre architecture du système de gestion de confiance et le modèle d'évaluation hybride qui permet de calculer la valeur de confiance des différents clouds à travers plusieurs domaines de sécurité.

Au niveau de ce chapitre nous avons implémenté les différents composants de système proposé dans le chapitre précédent et la relation entre ces composants et aussi le déroulement ou bien les étapes d'une évaluation à travers un scénario d'exécution.

5.2 Les moyennes utilisées pour l'implémentation

Pour l'implémentation de notre système de confiance nous avons utilisé les deux outilsVisual Studio Code intégré de Python et DB Browser (SQL Lite) :

FIGURE 5.1 – Outiles d'implémentation.

5.2.1 Visual Studio Code intégré de Python

Visual Studio Code est un éditeur de code extensible développé par Microsoft pour Windows, Linux et macOS. C'est un éditeur de code source qui peut être utilisé

avec une variété de langages de programmation, notamment Python, Java, JavaScript, Go et C++. Il est basé sur le cadre Electron, qui est utilisé pour développer des applications Web [65].

Le code source de Visual Studio Code provient du projet logiciel libre et open source VSCode de Microsoft publié sous la licence MIT permissive, mais les binaires compilés sont des logiciels gratuits pour toute utilisation [66].

Dans cette implémentation nous avons utilisé le Python comme langage de programmation. LePython permet une souplesse et une rapidité dans le codage comme il permet d'intégrer les systèmes plus efficacement.

5.2.2 DB Browser (SQL Lite)

DB Browser for SQLite (DB4S) est un outil visuel open source de haute qualité pour créer, concevoir et éditer des fichiers de base de données compatibles avec SQLite.DB4S est destiné aux utilisateurs et aux développeurs qui souhaitent créer, rechercher et modifier des bases de données. DB4S utilise une interface familière semblable à une feuille de calcul et les commandes SQL complexes n'ont pas besoin d'être apprises [65].

5.3 Implémentation

5.3.1 Les interfaces principales

5.3.1.1 Page d'accueil

Lors le lancement de l'application (chez le service de confiance), la page d'accueil suivant est affiché.

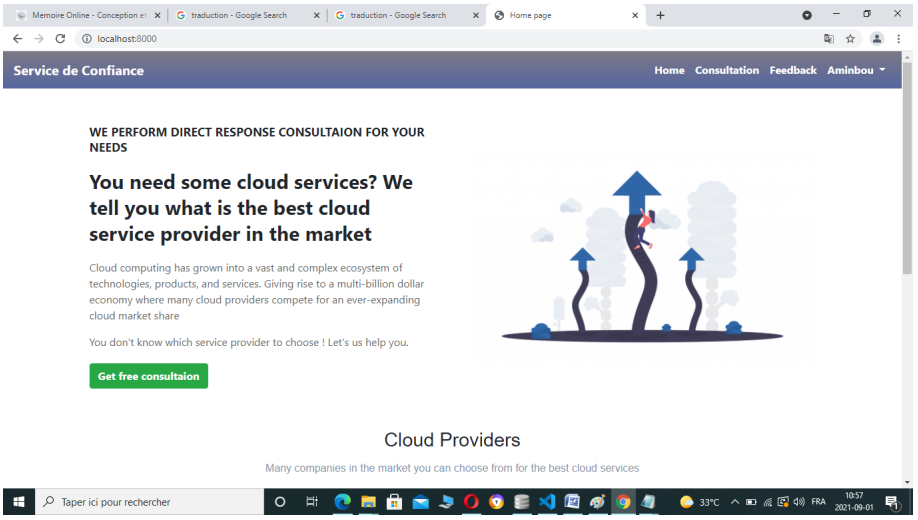

FIGURE 5.2 – page d'accueil.

Cette page d'accueil contient plusieurs liens vers d'autres pages. Les liens se trouver dans cette page sont les suivant : Home, Consultation, Feedback, login et

registrer et un bouton Get free consultation.

- **http ://localhost :8000/register**

Si l'utilisateur du service de confiance n'est pas enregistré, il doit d'abord s'enregistrer pour qu'il soit capable de se connecter au service de confiance. Pour s'enregistrer en clique le lien registrer et on introduit les informations suivants : (le nom, le email, mot de passe et la confirmation du mot de passe) et registrer par le bouton register.

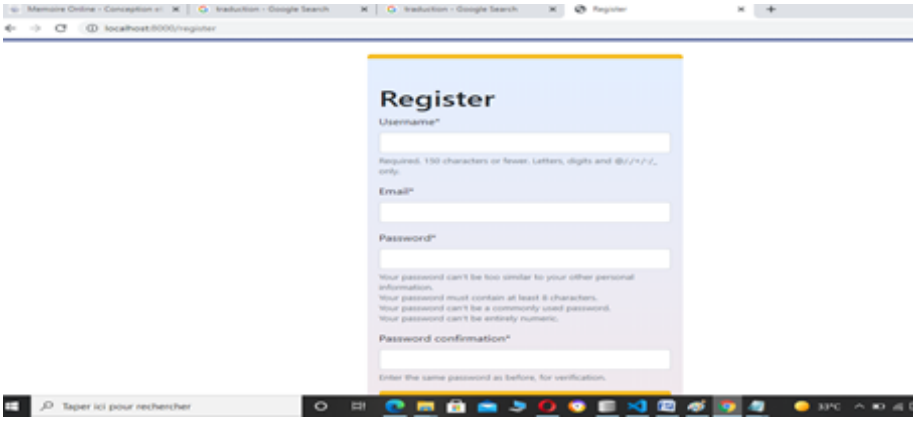

FIGURE 5.3 – Interface d'enregistrement .

- **http ://localhost :8000/login**

Si l'utilisateur du service de confiance est enregistré, il peut se connecter au service de confiance à travers le lien Login.

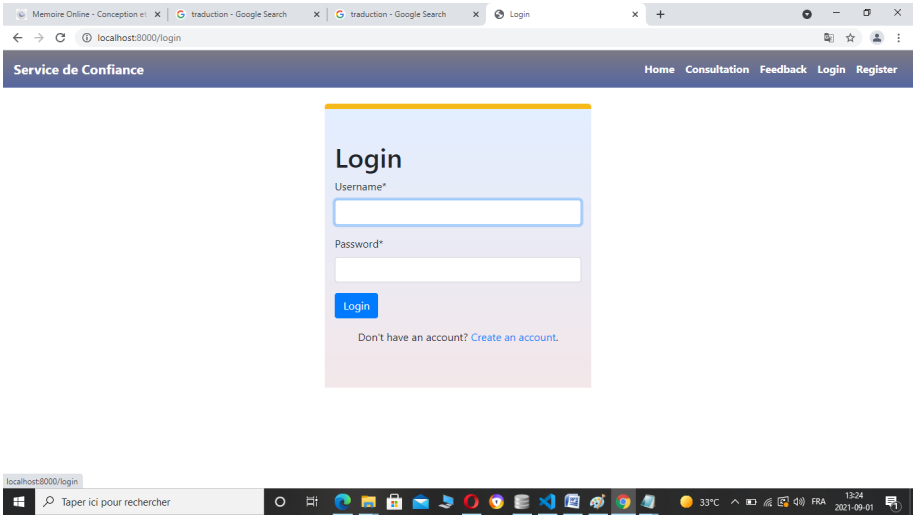

FIGURE 5.4 – Interface d'authentification.

- **http ://localhost :8000/login**

Les utilisateurs du service de confiance peuvent commenter les services recommander par le service de confiance à travers le lien Feedback en leurs donné soit la

note 0.1 lorsque le service est fiable ou bien -0.1 dans le cas échéant.

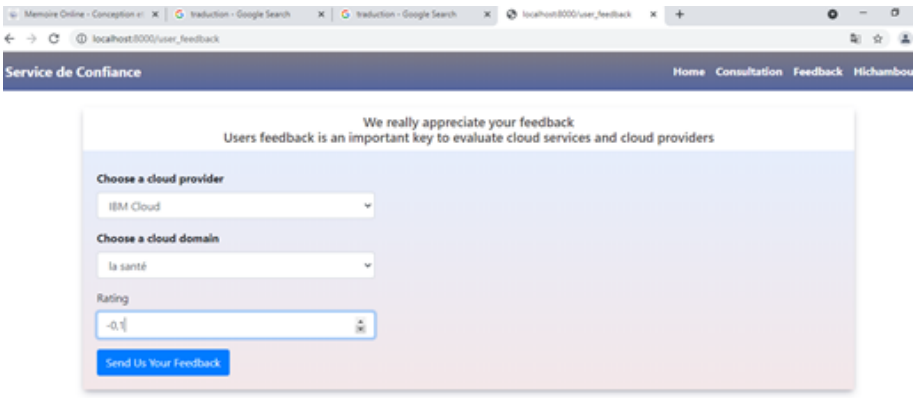

FIGURE 5.5 – Interface dédiée à la saisie du feedback utilisateur.

- **http ://localhost :8000/login ?consultaion=/consultaion**

Après la connexion au service de confiance, l'utilisateur peut faire une demande de recommandation en spécifiant d'abord un domaine de cloud.

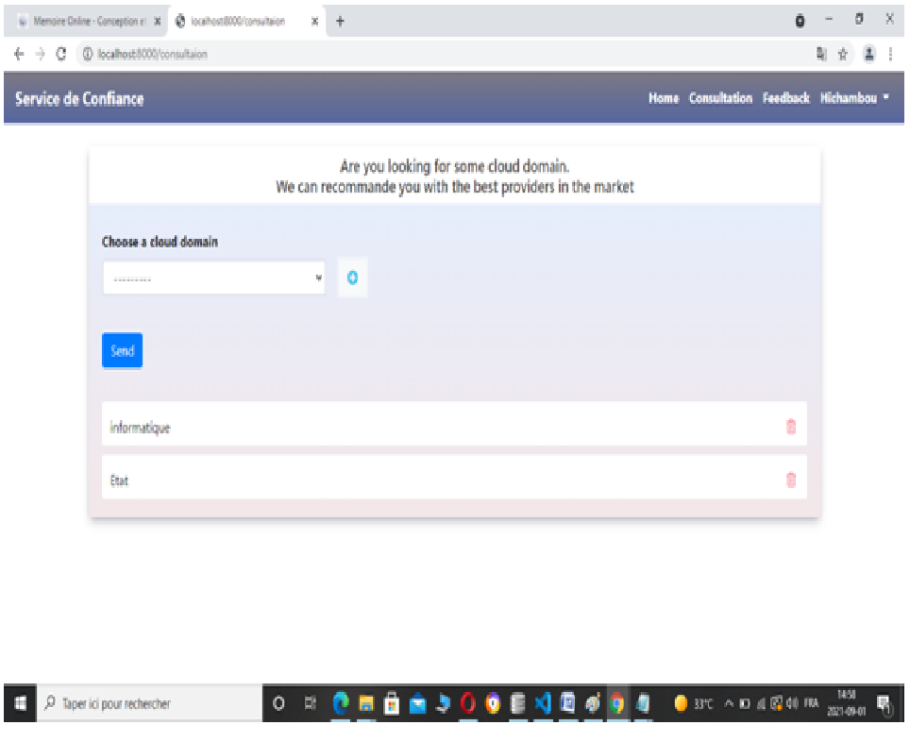

FIGURE 5.6 – Page de consultation.

5.3.1.2 Page Admin

La Page Admin contienne tous les liens de la page d'accueil et aussi le lien cloud providers. Et leur liens est http ://localhost :8000/admin/.

- **http ://localhost :8000/regions**

L'administrateur système peut gérer les domaines des clouds à travers le lien Cloud Domain.

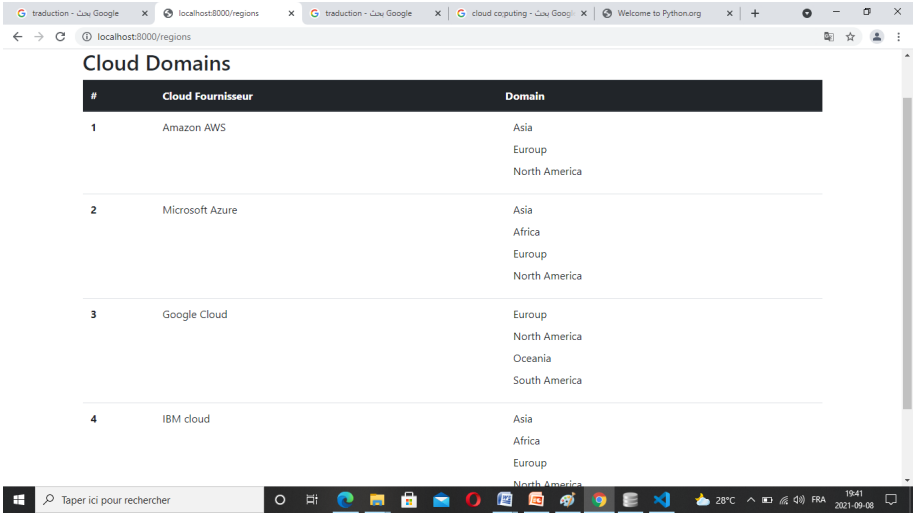

FIGURE 5.7 – Domaines du Cloud.

- **http ://localhost :8000/providers**

A travers le lien Cloud fournisseur, l'administrateur du système peut consulter les cloudset leurs caractéristiques (domaines, degré de confiance, moy des feedback et la note de recommandation).

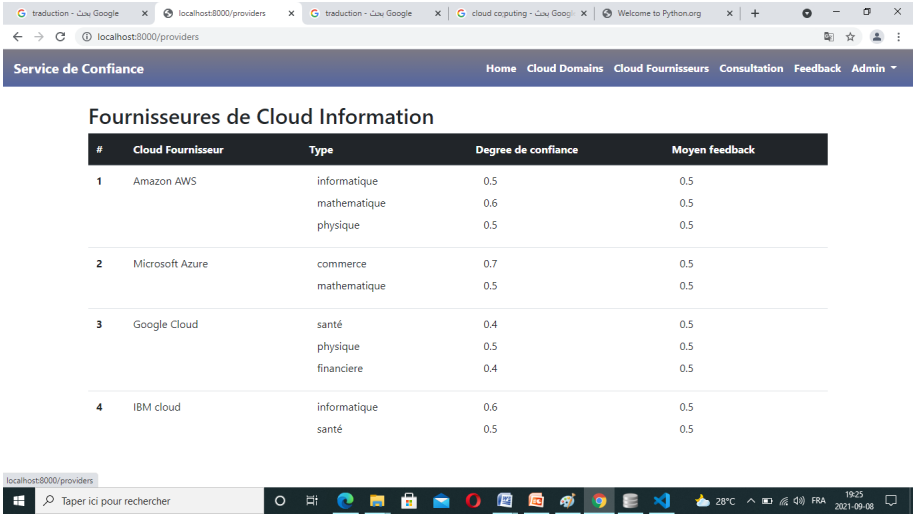

FIGURE 5.8 – Consultation de la liste des fournisseurs Cloud..

5.3.1.3 Page Django Administration

A travers cette page l'administrateur système peut accéder aux bases de données de l'application. Comme il est capable de les gérer à partir de cet interface ou il peut ajouter des domaines des clouds, des utilisateurs . . . , il est capable aussi de modifier leurs caractéristiques ou bien de les supprimer carrément.

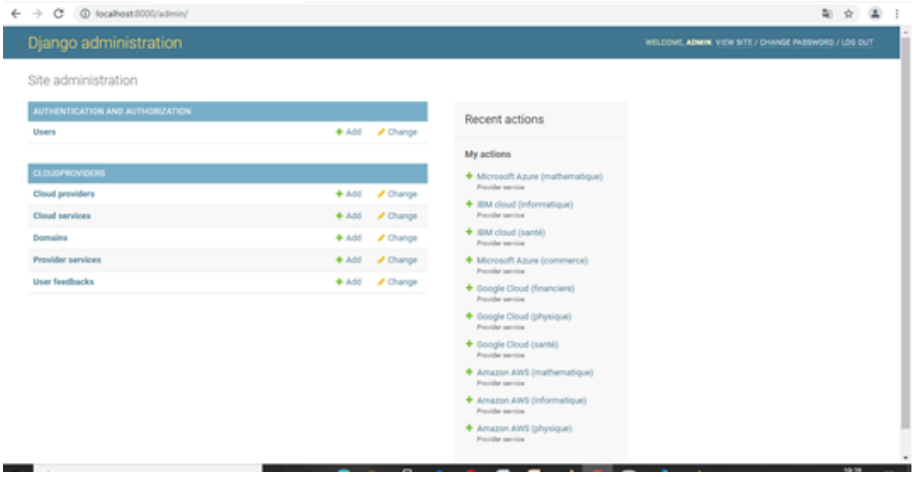

FIGURE 5.9 – Page Django administration.

5.4 Scénario d'exécution

Pour illustrer le déroulement de notre application nous avons présenté le scénario suivant :

1. Tout d'abord, l'administrateur se connecter au systèmeet gérer les cloud certifier et leurs domaines. A ce niveau, cinq clouds sont générer :

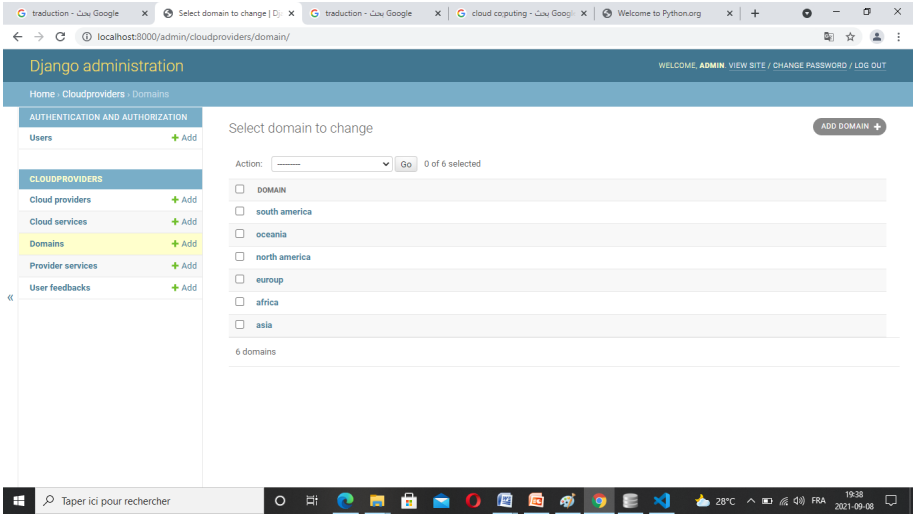

FIGURE 5.10 – créer la liste desclouds certifiés.

2. Pour chaque cloud en lui générant une liste des domaines où il offre ses services.

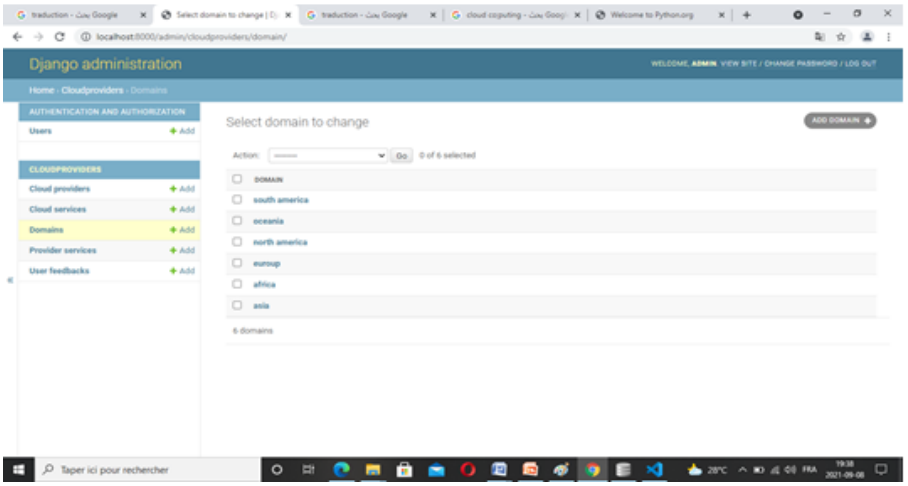

FIGURE 5.11 – créer les domaines pour les clouds.

3. Consulter les domaines de sécurité de chaque cloud.

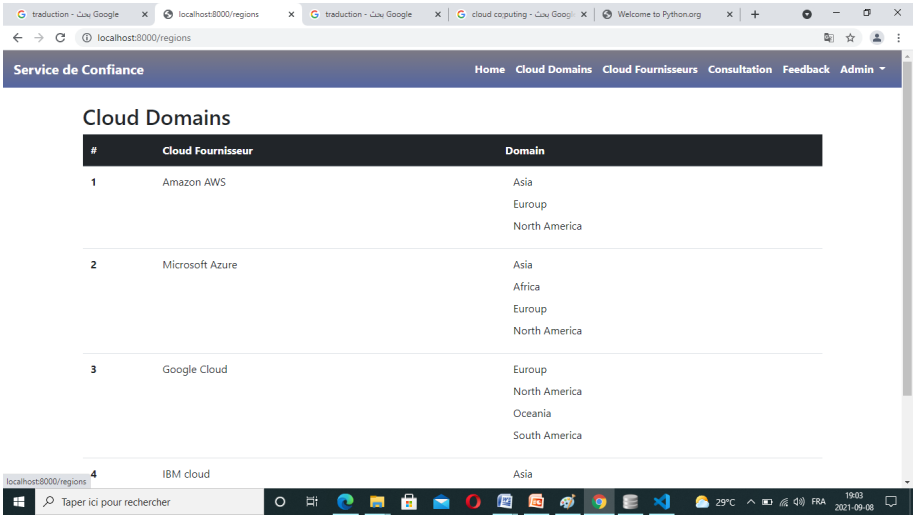

FIGURE 5.12 – liste des cloud avec leurs domaines de sécurité.

4. Utilisateur se registrer au niveau du service de confiance.

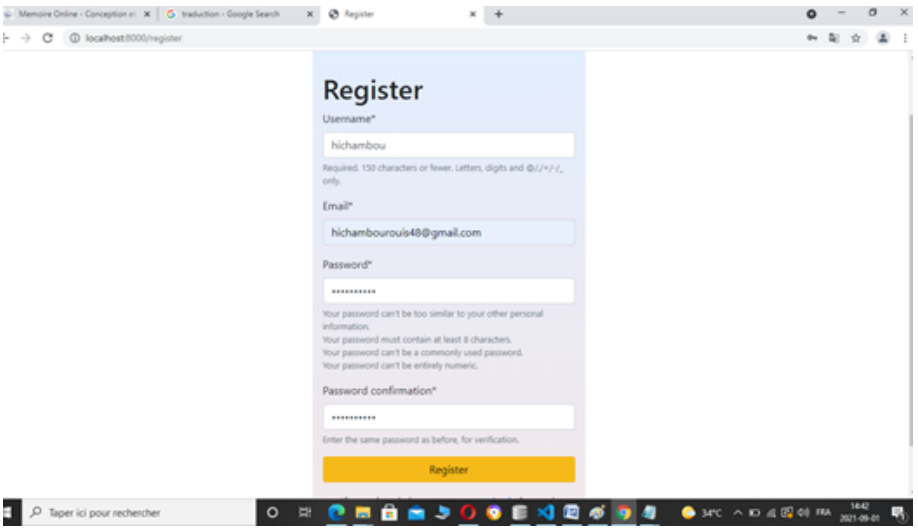

FIGURE 5.13 – L'enregistrement des informations de l'utilisateur.

- Après l'enregistrement, l'utilisateur peut accéder au service de confiance par le lien Login.

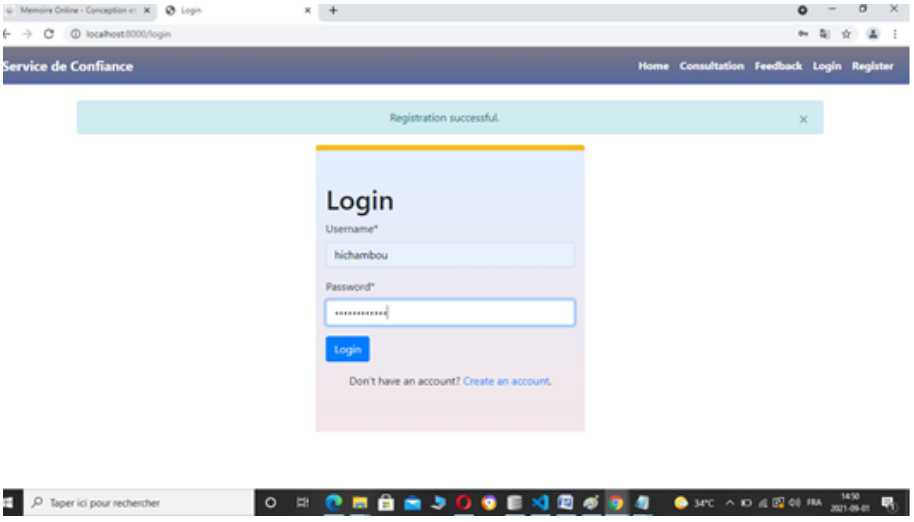

FIGURE 5.14 – Login au service de confiance.

- Si l'utilisateur se connecter avec succès la page suivante est affichée.

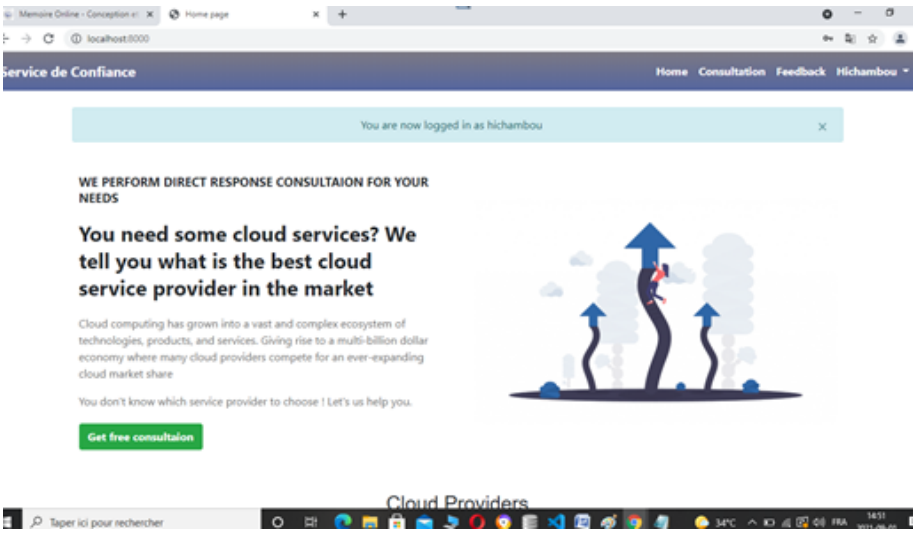

FIGURE 5.15 – Le succès de login.

5. Le service de confiance détermine la localisation de l'utilisateur.

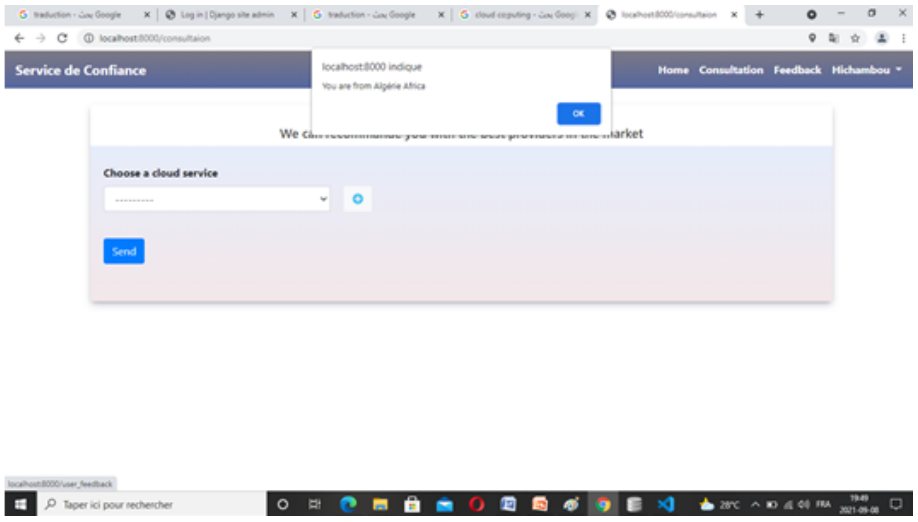

FIGURE 5.16 – Le service de confiance détermine la localisation de l'utilisateur.

6. Maintenant, l'utilisateur peut demander un service de recommandation en choisissant un domaine cloud.

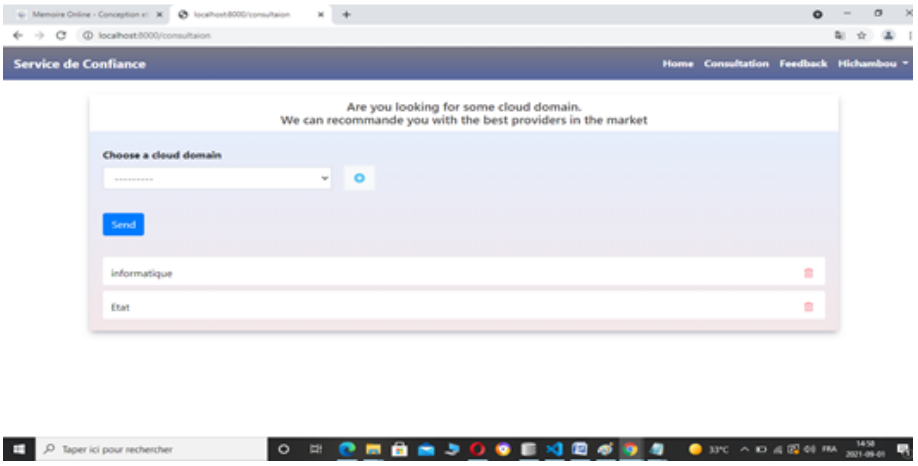

FIGURE 5.17 – L'envoie des besoins au système de confiance.

7. Après l'évaluation de la valeur de confiance. Les informations du cloud le plus confiant est envoyé à l'adresse mail de l'utilisateur.

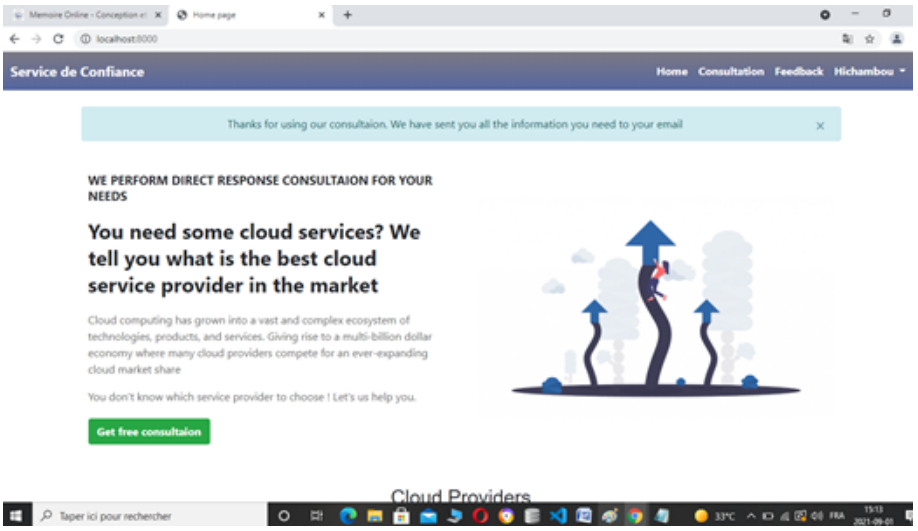

FIGURE 5.18 – L'envoie est réussi.

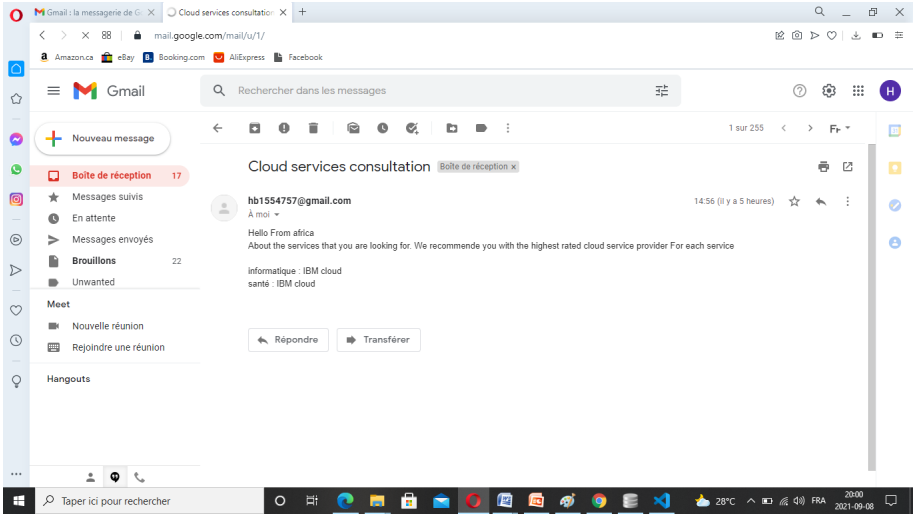

FIGURE 5.19 – la réception de mail.

8. L'utilisateur négocier en suite un contrat avec ce cloud le plus confiant.

10. Après la consommation du service par l'utilisateur, ce dernier peut se connecter au système de confiance et commenter le service utilisé.

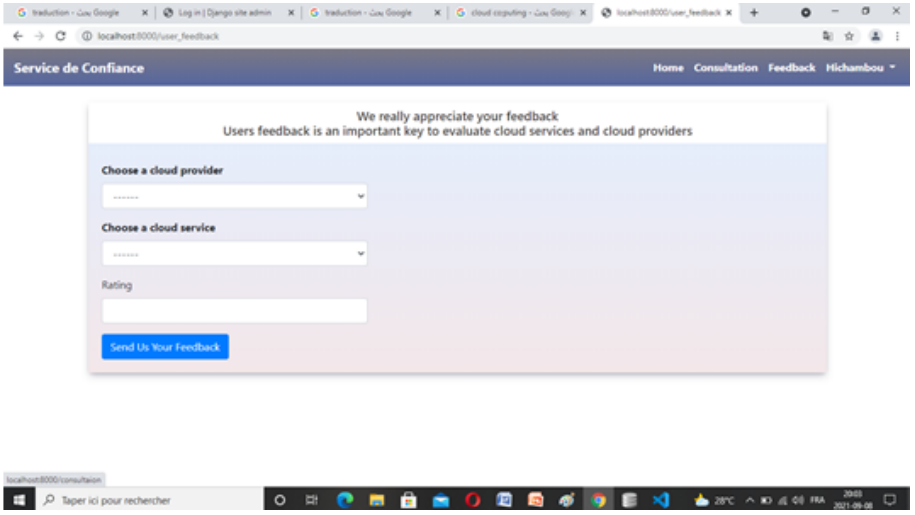

FIGURE 5.20 – L'envoie de Feedback.

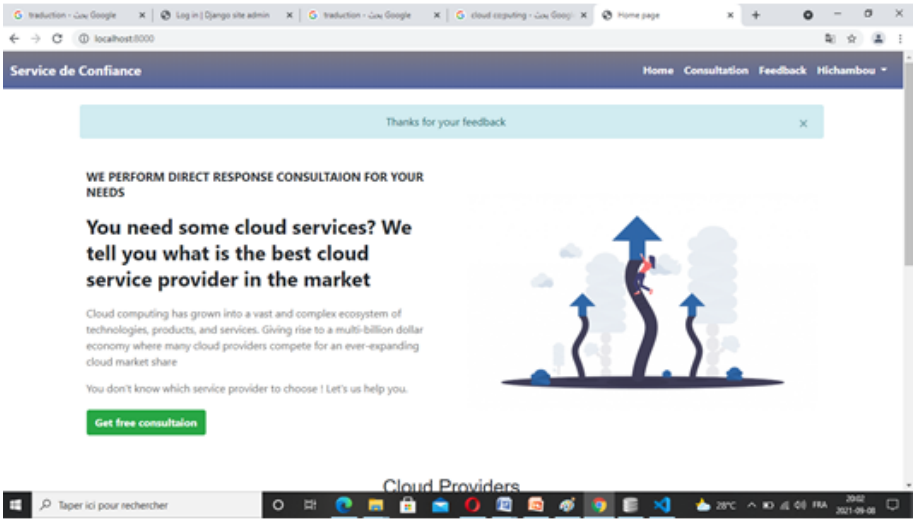

FIGURE 5.21 – L'envoie de Feedback avec succès.

5.5 Conclusion

Dans ce chapitre nous avions réalisé une implémentation de notre système de confiance on utilisant le Visual Studio Code comme éditeur de code, le Python comme langage de programmation et DB Browser (SQL Lite) comme un gestionnaire de base de données.

Ce chapitre est d'abord commencé par une présentation de l'environnement de travail en décrivons les composants logiciel utilisé dans l'implémentation, suivi par

une description des pages principal de notre application, et se termine par un scenario décri les étapes de notre modèle de confiance proposé.

CONCLUSION GÉNÉRALE

En conclusion, le travail de recherche effectuée dans lecadre de ce mastère aborde principalement sur le domaine de la sécurité dans le cloud computing est plus précisément sur le concept de la confiance.

L'objectif principal de ce travail de mémoire était de proposer et implémenter un système basé sur les certificats et les commentaires pour une gestion de confiance dynamique dans un environnement cloud multi-domaines, et de détailler l'architecture et modèle d'évaluation de confiance utilisé.

Nous avions commencé notre mémoire par un chapitre qui donne une présentation générale sur le concept de cloud : son historique, ses origines, sa définition, ses caractéristiques, ses modèles de déploiement, ses modes de service ainsi que ses avantages et ses inconvénients.

Nous avions exploré ensuite en détail dans lechapitre deux le concept de confiance ou nous avions entaméce concepts d'une façon générales comme nous avionsprésenté la relation entre la sécurité et la confiance, les mécanismes utiliser pour assurer le concept de la confiance, une classification des modèles de confiance dans le cloud et en termine par la présentation des exemplessur chaque classe du modèle.

En suite dans le troisième chapitre, nous avions parlé des certificats, ses modèles et ses architectures dans le cloud.Comme nous avions présenté quelque exemple de système de confiance basant sur les certificats et une discussion de ces travaux.

Notre contribution consiste à proposer et implémenter un système basé sur les certificats et les commentaires pour une gestion de confiance dynamique dans un environnement cloud multi-domaines.Ou nous avions proposé une architecture et un modèle d'évaluation de confiance dans un environnement cloud multi-domaines. Notre modèle d'évaluation est un modèle hybride qui permet de calculer la valeur de confiance sur la base des notes associées aux : domaines de sécurité, les feedbacks des utilisateurs et au degré de confiance des autorités de certification.

Notre système de confiancepermet d'améliorer la sécurité des services cloud on

combinant plusieurs approches pour l'évaluation de confiance et on appliquant plusieurs niveaux de sécurité : la gestion de confiance, l'authentification forte en combinant l'authentification par e-mail et par certificats et la gestion par certificat des droits d'accès aux ressources.

Dans les travaux ultérieurs nous comptant d'améliorer notre système de confiance en détaillant les composants de notre système, leurs rôles ainsi que l'amélioration du modèle d'évaluation de confiance utilisé. Comme nous comptant d'implémenter notre système dans une plateforme cloud réelle.

BIBLIOGRAPHIE

[1] https ://www.scality.com/solved/the-history-of-cloud-computing.

[2] https ://azure.microsoft.com/fr-fr/overview/what-is-cloud-computing/.

[3] https ://itrmanager.com/articles/112152/dossier-gartner-2e-partie-course-folle-externalisation-jusqu-emmenera.html.

[4] https ://fr.wikipedia.org/wiki/Cloud_computing.

[5] https ://www.ibm.com/fr-fr/cloud/learn/cloud-computing-gbl.

[6] https ://culture-informatique.net/cest-quoi-le-cloud.

[7] Timothy Grance, Peter Mell, *"The NIST definition of cloud computing"*, National Institute of Standards and Technology, Septembre 2011.

[8] Ronald L. Krutz,Russell Dean Vines, *"Cloud Security, A Comprehensive Guide to Secure Cloud Computing"*, WILEY 2010.

[9] https ://www.sciencedirect.com/topics/computer-science/on-demand-self-service.

[10] https ://core.ac.uk/download/pdf/20662836.pdf.

[11] Gong, J. Liu, Q. Zhang, H. Chen, and Z. Gong, emph "The characteristics of cloud computing", in 2010 39th International Conference on Parallel Processing Workshops,pp. 275–279, IEEE, 2010.

[12] S. Chhabra and V. S. Dixit, *"Cloud computing : State of the art and security issues"*, ACM SIGSOFT Software Engineering Notes, vol. 40, no. 2, pp. 1–11, 2015

[13] Sheikh Mahbub Habib, Sascha Hauke, Sebastian Ries, Max Muhlhauser. *"Trust as a facilitator in cloud computing : a survey. Journal of Cloud Computing : Advances, Systems and Applications"*, 2012.

[14] https ://www.lebigdata.fr/virtualisation-definition.

[15] Richard Hill, Peter Lake, Laurie Hirsch, Siavash Moshiri. *"Guide to Cloud Computing : Principles and Practice."*, Springer 2013.

[16] https ://www.javatpoint.com/public-cloud.

[17] Rajkumar Buyya, James Broberg, Aandrjez Goscinski. *" Cloud Computing : Principles and Paradigms"* WILEY 2011 ;

[18] P. M. Mell and T. Grance, *"Sp 800-145 : the nist definition of cloud computing"*, 2011.

[19] https ://www.memoireonline.com/07/15/9194/Etude-sur-la-securite-du-cloud-computing.html.

[20] http ://bib.univ-oeb.dz :8080/jspui/bitstream.

[21] https ://lesdefinitions.fr/confiance.

[22] https ://www.investopedia.com/terms/t/trust.asp.

[23] David H Mills. "The logic and limits of trust.", Business and Professional Ethics Journal,2(3) :7778, 1983.

[24] Chervany N.L Mcknight, D.H. PhD thesis, 1983.

[25] https ://hal.inria.fr/hal-00662479v1.

[26] NP.Kumarga and D.Sireesha. "Ensuring data integrity in cloud computing." internationneljournal of computer science and network security, 2014.

[27] M Grandison, T Solman. "Trust Management for Internet Application.", PhD thesis, University of London, 2003.

[28] Mei S, Wang Z, Cheng Y, Ren J, Wu J, Zhou J., 2012. "Trusted bytecode virtual machine module : a novel method for dynamic remoteattestation in cloud computing.", Int. J. Comput. Intell. Syst. 5, 924–932.

[29] Shanmugam U, Tamilselvan L., 2017. ″Trusted Computing Model with Attestation to Assure Security for Software Services in a Cloud Environment.", 10 (1).

[30] Rama Krishna Kalluri and CV Guru Rao. ″Addressing the security, privacy and trustchallenges of cloud computing.", International Journal of Computer Science and Information Technologies, 5(5) :60946097, 2014.

[31] https ://www.bearingpoint.com/en/our-success/thought-leadership/in-cloud-we-trust.

[32] https ://fr.wikipedia.org/wiki/Faites_confiance,_mais_v.

[33] Haq IU, Alnemr R, Paschke A, Schikuta E, Boley H, Meinel C (2010) Distributed trust management for validating sla choreographies. In : Wieder P, Yahyapour R, Ziegler W (eds). Grids and service-oriented architectures for service level agreements. Springer, US. pp 45–55.

[34] Pawar P, Rajarajan M, Nair S, Zisman A (2012) Trust model for optimized cloud services(Dimitrakos T, Moona R, Patel D, McKnight D, eds.). Springer, Berlin Heidelberg. pp 97–112.

[35] RSA (2011) RSA establishes cloud trust authority to accelerate cloudadoption. RSA.

[36] EMC (2011) Proof, not promises : Creating the trusted cloud. EMC.http ://www.emc.com/collateral/emc-perspective/11319-tvision-wp0211-ep.pdf

[37] CSA (2011) STAR (security , trust and assurance registry) program. CloudSecurity Alliance, 2012

[38] CSA (2011) Security guidance for critical areas of focus in cloudcomputing v3.0. Cloud Security Alliance.

[39] Everett C (2009) Cloud computing : A question of trust. Computer FraudSecurity 2009(6) : 5–7.

[40] ISO (2005) ISO/IEC 27001 :2005 information technology – securitytechniques – information security management systems – requirements.ISO.

[41] G. Spanoudakis, E. Damiani, and A. Mana., 2012, — Certifying Services in Cloud : The case for a hybrid, incremental and multi-layer approach‖, in Proc.

Of IEEE HASE'12, Omaha,NE,USA. Pp.102-122.

[42] A. Sunyaev and S. Schneider.,2013, Cloud services certification,Communications of the ACM, vol. 56, no. 2, pp.33–36.

[43] Sunyaev and S. Schneider.,2013,Cloud services certification,Communications of the ACM, vol. 56, no. 2, pp. 33–36.

[44] Ayesha Kanwal, Rahat Masood, Muhammad Awais Shibli, and Raa Mumtaz. Taxonomy for trust models in cloud computing. The Computer Journal, 58(4) :601626,2014.

[45] Pathan A.S.K, Mohammed M.M., 2015. Building Customer trust in cloud computing with an ICT-enabled global regulatory body. Wirel. Pers.Commun. 85, 77–99.

[46] Tang M, Dai X, Liu J, Chen J., 2017. Towards a trust evaluation middleware for cloud service selection. Future Gener. Comput. Syst. 74,302–312.

[47] Matin Chiregi and Nima Jafari Navimipour. A comprehensive study of the trust evaluation mechanisms in the cloud computing. Journal of Service Science Research, 9(1) :130,2017.

[48] Punit Gupta, Mayank Kumar Goyal, Prakash Kumar, and Alok Aggarwal, Trust and Reliability BasedScheduling Algorithm for Cloud IaaS, Proceedings of the Third International Conference on Trends in Information, Telecommunication and Computing, Lecture Notes in Electrical Engineering Volume 150, 2013, pp 603-607

[49] https ://www.researchgate.net/publication.

[50] Firdhous, M., Ghazali, O. and Hassan, S. (2011) A TrustComputing Mechanism for Cloud Computing. Proc. ITU, TheFully Networked Human ?-Innovations for Future Networks andServices (K-2011), Cape Town, December 12–14, pp. 1–7. IEEE,New York, USA.

[51] Habib, S.M., Ries, S. and Muhlhauser, M. (2011) Towards aTrust Management System for Cloud Computing. 10th Int. Conf.Trust, Security and Privacy in Computing and Communications(TrustCom), Changsha, November 16–18, pp. 933–939. IEEE,New York, USA.

[52] Huang, J. and Fox, M.S., 2006, An ontology of trust – formal semantics and transitivity, in Proceedings of the Eighth International Conference on Electronic

Commerce, ACM,pp.259–270.

[53] D Gunter, B Tierney, B Crowley, M Holding, J Lee.,2000, Netlogger : A toolkit for distributed system performance analysis, Proceedings 8th International Symposium on Modeling, Analysis and Simulation of Computer and Telecommunication Systems,pp.267-273.

[54] Zhaoxiong, Z., He, X. and Suoping, W. (2011) A novel weightedtrust model based on cloud. Adv. Inf. Sci. Serv. Sci., 3, 115–124.

[55] Li, W., Lingdi, P., Qinlong, Q. and Qifei, Z. (2012) Research ontrust management strategies in cloud computing environment.J. Comput. Inf. Syst., 8, 1757–1763.

[56] Ahmed, M. and Xiang, Y. (2011) Trust Ticket Deployment : A Notion of a Data Owner'S Trust in Cloud Computing. 10th Int. Conf. Trust, Security and Privacy in Computing and Communications (TrustCom), China, November 16–18, pp. 111–117.IEEE, New York, USA.

[57] Mahbub Ahmed and Yang Xiang. Trust ticket deployment : a notion of a data owner'strust in cloud computing. In 2011IEEE 10th International Conference on Trust, Securityand Privacy in Computing and Communications, pages 111117. IEEE, 2011.

[58] Li, W. and Ping, L. (2009) Trust Model to Enhance Security and Interoperability of Cloud Environment. 1st Int. Conf. Cloud Computing (CloudCom), China, December 1–4, pp. 69–79. Springer, Berlin.

[59] https ://moodle.utc.fr/pluginfile.php.

[60] http ://securiteinfo.com/cryptographie/pki.shtml.

[61] https ://fr.slideshare.net/aliarousyoucef/mise-en-place-dune-autorit-decertificationpki-sous-windows-server-2008.

[62] SAIDOU DIOP. Une infrastructure a cles publiques (pki) pour securiser les messages dans un reseau v2g, 2018.

[63] https ://www.venafi.com/fr/blog/comment-fonctionnent-les-chaines-de-certificats.

[64] Taxonomy for Trust Models in Cloud Computing.

[65] Visual Studio Code — Wikipédia (wikipedia.org).

[66] DB Browser for SQLite (sqlitebrowser.org).