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

Université SAAD DAHLAB-BLIDA
USDB

Faculté des Sciences
Département informatique

Mémoire pour l'obtention du diplôme de master en informatique

Option : Ingénierie du logiciel

THEME

Protection de l'accès aux données Par le modèle RBAC pour le Cloud privé

Promotrice :
Mme :Oukid
Co-promotrice :
Mme Ghebghoub

Réalisé par :
Nessah Hadjer
Dahmane saoussen

Organisme d'accueil : Université Saad Dahlab Blida

Soutenue le 24/09/2013, devant le jury composé de :

Président :Mr Cherif Zahar.
Examinateur :Mme Ameur.
Examinateur :Mme Attaf.

Promotion 2012/2013

Remerciement

Tous d'abord ; nous remercions ***Dieu***, notre guide, notre force, notre bonheur, et la raison de notre existence. C'est lui qui nous a fait comprendre le bute de cette vie, et qui nous a donné le pouvoir d'aimer les gents et d'apprécier les choses. Merci d'être la dans les moments les plus difficiles.

Nous souhaitons remercier notre promotrice ***Madame OUKID*** de nous avoir accueillies parmi ses étudiants, et d'avoir ainsi bien voulu partager avec nous sa passion pour la recherche, La rigueur du raisonnement, le refuse de toute idée préconçue, la remise en question perpétuelle même de ce qui semble établi, demeure a nous yeux les point fort de son enseignement et de ses direction de recherche.

Nous exprimons nos sincère remerciements et notre grande gratitude a notre co-promotrice Madame GHABGHOUB Yasmin, d'avoir accepté guider notre travail et nous faire le plaisir de profiter de leurs expériences et de ces compétences.

Merci à Monsieur le chef de département ***MASSIED Mohamed*** qui nous honore de le voir a l'université.

Nous remercions aussi tous ***les professeurs*** qui nous ont soutenu durant notre formation a l'université, et tous ceux qui nous ont aidé a l'élaboration de se mémoire.

Dédicace

Je dédie ce mémoire de fin d'études
A

A mes très chers parents qui m'ont toujours soutenu particulièrement durant toutes mes années d'études,

A mon cher frère et mes chères sœurs,

A mon binôme Saoussen et à toute ma famille,

A tous les enseignants et étudiants du département Informatique de l'Université de Blida, en particulier ceux de la promotion 2012-2013

Hadjer

Chapitre 02: Sécurité

Chapitre 05 Implémentation

Liste des tableaux :

Résumé

Avec la grande tendance du Cloud computing, aujourd'hui le stockage de données dans le Cloud est devenue l'une des solutions de stockage le plus populaire pour l'informatique de l'entreprise. Le déplacement des données vers le Cloud peut soulager l'entreprise de la charge de stockage des données locales et ces entretient. Malgré ces avantages, la sécurité reste l'un des grands défis du fait que les données des clients ne résident plus dans leur possession physique mais sur des serveurs externes. Pour cette raison, le contrôle d'accès est essentiel dans tous systèmes où les données sont partagées entre plusieurs utilisateurs avec différents niveaux de confiance.

Le but de ce travail est de mettre en œuvre un système de gestion des accès solide aux sources des données stockées dans un Cloud privé, et nous avons choisi pour réaliser notre solution la politique de contrôle d'accès RBAC (Role Base Access Control).

Mot-clé : contrôle d'accès, RBAC, Cloud computing.

Abstract

In front of the big trend of cloud computing these days, the data storage in the cloud is getting to be the most important solution for business's information technology by moving data to the cloud, the company can benefits of its many advantages(it declines local storage charges) ,But when your things are out of your keep, you have to be concerned for its safety, which is the main challenge of the cloud computing, consequently of, client's data are not in their physical own ship, but in external servers, for these reasons, access control is essential for all systems where data are shared between many users and with different levels of confidence

The aim of this work is to set to work, is to precede our solution, we adopt RBAC(Role Base Access Control).

introduction généraie :

Avec la généralisation d'internet, le développement des réseaux hauts débit, la location d'application et le paiement à l'usage résultent de l'apparition d'un nouveau concept « Le Cloud Computing ». Celui-ci consiste en une interconnexion et une coopération de ressource informatique, située dans diverses structures interne, externe ou mixtes et dont le mode d'accès est basé sur les protocoles et standards internet, le Cloud computing est devenu ainsi le sujet le plus débattu aujourd'hui dans le secteur des technologie de l'information, le consensus qui dégage est que le cloud computing jouera un rôle de plus important dans les opération informatique des entreprises au cour des années a venir, c'est pour cela Le Cloud computing pose de nouveaux défis aux professionnels de la sécurité, de la conformité et de l'audit des systèmes d'information qui sont chargés de protéger les données de l'entreprise ainsi que les ressources informatiques tout en s'assurant de la conformité des mesures de sécurité. Le Cloud bouleverse la prédictibilité associée aux architectures informatiques, aux contrôles de sécurité et aux procédures d'audit traditionnels et oblige les abonnés aux services Cloud à déléguer deux ressources essentielles aux fournisseurs de services Cloud : Le contrôle des données, des applications et des actions et la visibilité du statut des données et de l'utilisation des applications.

I. Présentation de sujet

Le Cloud computing à été développé pour fournir des services informatiques à la demande aux organisations comme aux utilisateurs individuels, cette technologie est encore à ces premiers stades de développement car elle souffre de différentes menaces de sécurité qui empêchent les utilisateurs de lui fait confiance.

1. Problématique

En complément des problèmes habituels de sécurisation des systèmes informatiques, le Cloud Computing présente un facteur de risque supplémentaire du fait de l'externalisation de services stratégiques auprès d'un fournisseur externe. Il est en effet plus difficile, avec cette dimension d'externalisation, d'assurer l'intégrité et la confidentialité des informations, la disponibilité des données et des services, et l'établissement de la conformité à une politique ou réglementation.

Donc on se trouve face à un problème de gestion et de contrôle des accès aux données sensibles ou relatives stockets dans le Cloud Computing.

2. Objectif

Après avoir pris connaissance des principaux problèmes, Nos objectifs sont :

- Contrôler l'accès des utilisateurs des ressources selon les rôles.
- Augmenter la confiance entre propriétaire de Cloud et fournisseur.
- Gagner le temps en gérant les utilisateurs par rôle.
- Permettre au propriétaire de données de gérer ces données.

Chapitre 1
Cloud Computing

I. Introduction

Une nouvelle génération de technologies révolutionne actuellement le monde de l'informatique. Le stockage de données et les services sur Internet, connus sous le nom de « Cloud computing », sont en plein essor et viennent compléter le modèle traditionnel des logiciels et des données reposant sur des PC et des serveurs de bureau. En d'autres termes, le Cloud computing est une approche visant à optimiser la convivialité de l'informatique. Les utilisateurs peuvent ainsi accéder aux applications et aux données logicielles stockées sur des centres de données hors site, et non plus sur leur périphérique, leur PC ou le centre de données interne d'une entreprise.

Dans l'effervescence qui accompagne toute grande nouveauté dans le monde de l'informatique, le Cloud Computing est apparu pour certains comme une révolution et pour d'autres comme un simple terme Marketing qui ne fait que rassembler des services et des technologies qui existent depuis longtemps.
En effet l'année 2008 a vu l'émergence du terme « Cloud Computing » dans les journaux spécialisés, et les annonces de nouvelles solutions chez tous les grands acteurs de l'informatique: Microsoft, Google, Amazon, IBM, Dell, Oracle... [3]

Pour vulgariser, le Cloud Computing peut être perçu comme un système d'exploitation distribué sur des milliers de machines. Cet OS distribué, que l'on représente par ce fameux nuage, assure l'abstraction de l'infrastructure (matérielle, réseau, etc.) et a pour rôle d'héberger et d'exécuter des applications ou des services mais aussi de stocker des données.

L'idée de mettre ses applications et données dans un nuage unique, accessible par tout le monde et réparti sur des milliers de machines « abstraites » peut faire peur. Comme nous le verrons, les avancées en terme de sécurité, tant sur le plan technologique qu'intellectuel, nous permettent d'assurer une confiance optimale.

On peut en fait diviser le Cloud computing en deux catégories bien distinctes (même si un fournisseur peut proposer les deux) :

1. Stockage

Les données du client sont sauvegardées sur plusieurs serveurs, par exemple Amazon Simple Storage Service (ou Amazon S3), souvent accompagné de copies de sauvegardes Ce type de Cloud permet, si l'on a stocké des applications sur le serveur d'y accéder et de les exécuter, et ressemble alors à un système de fichier partagé de type AFS(*), accessible depuis son explorateur internet. [1]

Figure I.1 : Quelques serveurs du site Nancy [2]

2. Logiciels

Sur ce point, le Cloud computing est similaire au Software as a Service si ce n'est que le propriétaire du logiciel n'est pas forcément le propriétaire du matériel. On peut distinguer alors deux philosophies. Amazon vend du temps sur une machine virtuelle, avec ses offres Elastic Compute Cloud (Amazon EC2) et Simple Storage Service (S3), alors que Microsoft, avec Microsoft Azure, et Google, avec Google App Engine, proposent l'utilisation de leurs Langages et de leurs bibliothèques, ce qui rend la maintenance plus aisée (elle ne dépend plus des besoins du client), mais beaucoup moins flexible pour le client. [2]

Ainsi le développement remarquable du *Cloud Computing*, ces dernières années, suscite de plus en plus l'intérêt des différents utilisateurs de l'internet et de l'informatique qui cherchent à profiter au mieux des services et des applications disponibles en ligne à travers le web en mode services à la demande et facturation à l'usage tel que l'accès de n'importe où, n'importe quand et par n'importe qui à des données et services sur un serveur distant .

Ce modèle leur épargne les coûts de gestion interne, puisque les ressources informatiques sont administrées au niveau du fournisseur du *Cloud Computing*.

La disponibilité des services en ligne donne aussi la possibilité de ne plus s'approprier d'équipements informatiques mais de payer les frais en fonction de l'utilisation des ressources. Ce modèle attire déjà un grand nombre d'entreprises notamment les petites et moyennes entreprises (PME) et les très petites entreprises (TPE).
Le *Cloud Computing* offre également la modularité des ressources informatiques (*hard* et *soft*) et leur disponibilité, en terme de volume et dans le temps, selon les besoins du client et à sa demande.

Les capacités informatiques concernées par le Cloud Computing sont variées : capacité de calcul, espace de stockage, bande passante ou encore logiciels de messagerie et de collaboration, environnements de développement et logiciels spéciaux tels que la gestion des relations avec la clientèle.

II. Qu'es-ce-que le Cloud computing

1. Définition

Selon une définition donnée par le NIST (US National Institute of Standards and Technology) le Cloud computing est un modèle permettent un accès aisé, à la demande et au travers d'un réseau, à un ensemble partagé de ressource informatique (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. [4]

2. Historique

2.1. L'informatique utilitaire de JOHN MCCARTHY

Cette notion de consommation a été proposée en 1961, lors d'une conférence au MIT (Massachusetts Institute of Technologie), par John McCarthy aussi connu comme l'un des pionniers de l'intelligence artificielle (dont il proposa le nom en 1955) et pour avoir inventé du LISP en 1958.

Lors de ce discours, John McCarthy suggéra que la technologie informatique partagée (« time-sharing ») pouvait construire un bel avenir dans lequel la puissance de calcul et même les applications spécifiques pouvaient être vendues comme un service public.

Cette idée, très populaire dans les années 60, disparu au milieu des années 70 : à l'époque, les technologies matérielles, logicielles et réseaux n'étaient tout simplement pas prêtes. [5]

Le Cloud Computing met en œuvre l'idée d'informatique utilitaire du type service public, proposée par John McCarthy. Il peut aussi être comparé au cluster de calcul dans lequel un groupe d'ordinateurs se relient pour former un ordinateur virtuel unique permettant le calcul de haute performance (HPC), mais aussi à l'informatique en grille (Gri Computing) où des ordinateurs reliés et répartis géographiquement permettent la résolution d'un problème commun.[5]

2.2. Les services bureau

C'est dans cette philosophie, que depuis les années 70, on inventa la notion de « service bureau » pour qualifier une entreprise louant des lignes téléphoniques, répondeuses, services informatiques etc. Généralement, les clients des « services bureau » n'ont ni l'ampleur ni l'expertise pour intégrer en interne ces services, c'est pourquoi ils passent par un prestataire. La combinaison de technologies, processus et expertise dans le domaine des entreprises est la valeur ajoutée des « services bureau », comme modèle économique basé sur leur capacité à produire des services et à les déployer en volume. IBM lui-même était un « service bureau » en proposant la notion de « on-demande ».

À l'époque, le coût d'achat et d'exploitation de mainframes IBM était hors de prix. C'est pourquoi, des solutions permettant aux entreprises de pouvoir exploiter ces technologies à moindre frais avec la notion de « paiement à la consommation » furent proposées. [5]

2. 3. Les applications providers

Les ASP, « Application Service Provider » ont aussi leur part dans l'historique du Cloud Computing. Une ASP désigne une application fournie comme un service, c'est ce que l'on nomme maintenant SaaS pour « Software as a Service » dans la terminologie actuelle du Cloud Computing. Plutôt que d'installer le logiciel sur le poste client en ayant à assurer les phases d'installations et de maintenance sur chaque poste, les applications ASP sont hébergées et centralisées sur un serveur unique et accessible par les clients au travers de protocole standard. C'est par exemple le cas avec des applications Web accessibles par http : il n'y a alors plus de déploiement ou de maintenance à effectuer sur le poste utilisateur, celui-ci n'a alors besoin que d'un simple navigateur Internet. Le déploiement, la configuration, la

maintenance, la sauvegarde, etc. sont désormais de la responsabilité du fournisseur du service, le client est alors consommateur. [5][

2. 4. La virtualisation

La virtualisation a été la première pierre vers l'ère du Cloud Computing. Tel que joue un rôle décisif de catalyseur pour ce nouveau paradigme. En effet, cette notion permet une gestion optimisée des ressources matérielles dans le but de pouvoir y exécuter plusieurs systèmes « virtuels » sur une seule ressource physique et fournir une couche supplémentaire d'abstraction du matériel.

Nous en concluons que la virtualisation est le concept qui permet au « Cloud Computing » d'offrir à un moindre coût tous les types de machines : petite ou puissante ; sur Linux, Windows ou Unix ; etc.

2. 5.Les centres de données

Un centre de données ou centre de traitement de données en français est une salle informatique où sont stockés les serveurs. Ces centres de données (*Data center* en anglais) regroupent une multitude de machines. Les données mises en place sur les serveurs doivent être accessibles à tout moment et protégées des risques extérieurs, par conséquent les data center se doivent d'être protégés des principaux risques de coupure électrique, d'intrusion ou d'attaques. Il y a ainsi des protections contre les coupures électriques, les risques d'incendie et l'accès de personnes malveillantes. [6]

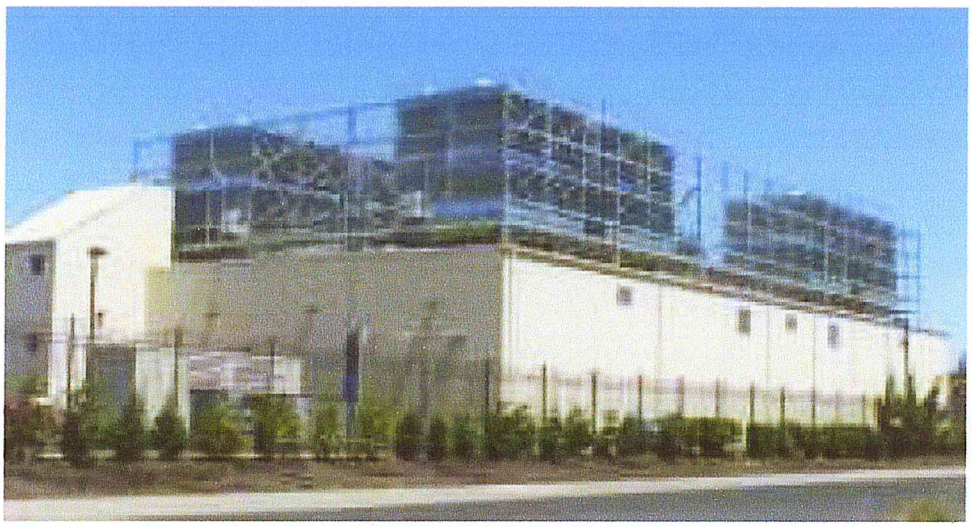


Figure I.2 : centres de données Google [6]

III. Fonctionnement de Cloud computing

Le Cloud (figure I.2) permet donc de fournir un ensemble d'applications sans utiliser la mémoire, la puissance de calcul et la capacité de stockage d'un seul serveur. Le visiteur se connecte sur le site du client des services de Cloud, utilise les applications qui lui sont proposées sans avoir conscience qu'il accède a des machines différentes (virtuelles ou non), et utilisent les applications proposées pour éventuellement stocker des données personnelles sur des serveurs distants. De plus, le client n'a pas d'accès direct a ses données. [1]

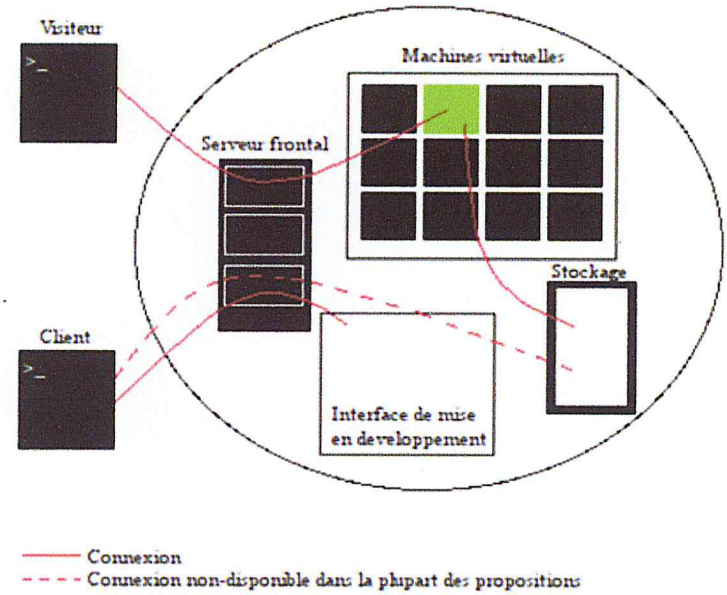


Figure I.3 : Fonctionnement de Cloud computing [1]

IV. Les composants du Cloud computing

Le Cloud dépend des composants suivants :

- **Client** : Logiciel permettant à un internaute de se connecter au Cloud. Généralement, un explorateur internet suffit, mais d'autres moyens peuvent être utilises suivant les services proposes par l'hébergeur ou par l'acheteur du service de Cloud.

- **Service** : Protocoles proposes par l'hébergeur ou par le client (paiement, mapping, chat, mail, ...)

- **Application** : Les applications sont soit proposées de base par l'hébergeur, soit développées par le client. Chacune d'elles dispose d'une ou plusieurs machines virtuelles.

- **Plate-forme** : Système d'hébergement des applications.

- **Stockage** : Moyen de stockage mis à disposition du client. La plupart des hébergeurs proposent une base de données SQL ou système de stockage sur laquelle le client n'a pas d'accès direct, ce qui peut être changé (avec un gain considérable de liberté). Il est aussi envisageable de lui fournir un système de stockage classique (système de fichier accessible en FTP par exemple).

- **Infrastructure** : Il s'agit du serveur frontal (Gère les requêtes en lançant des machines virtuelles adéquates ou en communiquant avec des machines virtuelles adéquates déjà lancées.).[1]

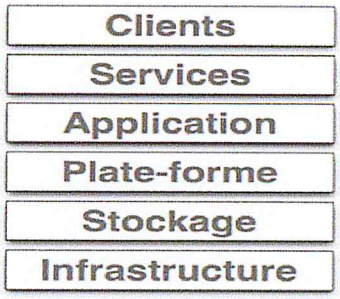


Figure I.4 : l'architecture du Cloud computing. [7]

Plus précisément, nous distinguons trois couches de Cloud Computing:

- ✓ Infrastructure : qui est le support de la plate-forme, tel que l'utilisateur peut installer son OS et/ou ses logiciels

  Ex : Machine virtuelle, Réseau VPN virtuel, etc.

- ✓ Plateforme : qui exécute l'application, tel que l'utilisateur peut paramétrer des logiciels

  Ex : Gestionnaire de Site Web, Gestionnaire de messagerie, etc.

- ✓ Applicative : qui est en contact avec le client, tel que l'utilisateur peut installer son OS et/ou ses logiciels

  Ex : application bureautique, BAL de messagerie, Site Web, etc.

V. Les différentes couches du Cloud

Le Cloud computing comprend trois modèles qu'il est important de différencier car le service fourni n'est pas le même et ils ne s'adressent pas au même public. Il existe en effet trois façons principales d'aller vers le Cloud, pour lesquelles le transfert de responsabilités diffère complètement :
Nous allons définir les trois couches

1. L'infrastructure comme un service (IaaS)

Capacité à fournir une puissance de traitement, un espace de stockage, des infrastructures de réseaux ainsi que d'autres ressources informatiques, en permettant au client de déployer et d'exécuter des applications de son choix. Le client n'a pas à gérer l'infrastructure « Cloud » sous-jacente. En revanche, il conserve le contrôle des systèmes d'exploitation, des espaces de stockage, des applications déployées et dans une certaine mesure de certains composants réseau. [8]

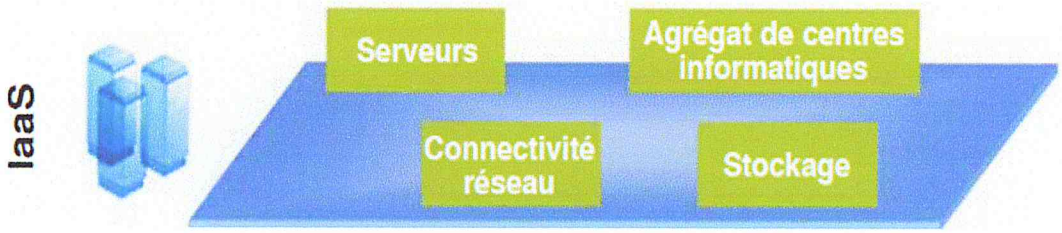


Figure I.5 : L'infrastructure comme un service (IaaS) [9]

2. La plateforme comme un service (PaaS)

Capacité à déployer sur une infrastructure Cloud des applications développées ou acquises par le client, et programmées avec des langages et outils pris en charge par un prestataire externe. Le client n'a pas à gérer l'infrastructure Cloud sous-jacente (réseau, serveurs, systèmes d'exploitation, stockage).En revanche, il conserve le contrôle des applications ainsi déployées et éventuellement des configurations de leur environnement. [8]

Figure I.6 : L'infrastructure comme un service (PaaS) [9]

3. Le logiciel comme un service (SaaS) :

Il s'agit de la mise à disposition d'un logiciel non pas sous la forme d'un produit que le client installe en interne sur ses serveurs, mais en tant qu'application accessible à distance comme un service, par le biais d'Internet et du Web. Les clients ne payent pas pour posséder le logiciel en lui-même mais plutôt pour l'utiliser. Ils l'utilisent soit directement via l'interface disponible, soit via des API fournies (souvent réalisées grâce aux Web Services ou à l'architecture REST (Representational state transfer)).

L'utilisation reste transparente pour les utilisateurs, qui ne ce soucient ni de la plateforme, ni du matériel qui sont mutualisés avec d'autres entreprises.
Deux principales différences avec l'ASP traditionnel sont qu'une simple interface web est utilisée côté client dans tous les cas (pas de client lourd), et que le SaaS propose une seule instance de logiciel qui évolue indépendamment des clients. [10]

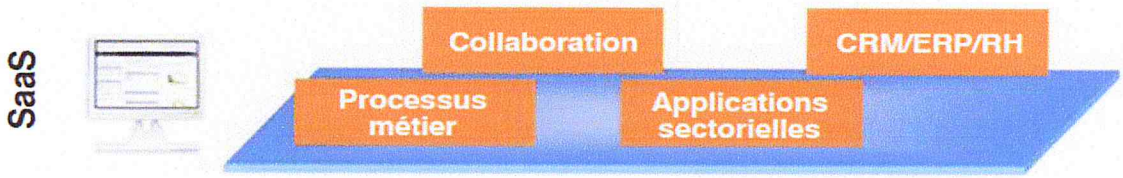


Figure I.7: L'infrastructure comme un service (SaaS) [9]

VI. Les architectures modèles du Cloud

L'environnement Cloud comprend des Cloud privés, publics, hybrides et communautaires.

1. Cloud privé

L'infrastructure du Cloud est réservée à l'usage exclusif d'une seule organisation. Elle peut être possédée, gérée et opérée par cette organisation, un intervenant extérieur ou une combinaison des deux. Elle est située dans les locaux de l'organisation ou dans ceux d'un hébergeur externe. [8]

2. Cloud public

L'infrastructure du Cloud est destinée à un usage public. Elle peut être possédée, gérée et opérée par un organisme privé, public, académique ou une combinaison de ceux-ci. Elle est située chez un hébergeur. [8]

3. Cloud hybride

L'infrastructure du Cloud est composée d'au moins deux infrastructures différentes (privée, publique ou communautaire) qui conservent leur autonomie mais qui sont liées entre elles par des technologies (propriétaires ou non) assurant la portabilité des données et des applications. [8]

4. Cloud communautaire

L'infrastructure du Cloud est réservée à l'usage d'une communauté spécifique de consommateurs partageant des intérêts communs : missions, exigences de sécurité, partage d'informations et ou d'applications,... Elle peut être possédée, gérée et opérée par un ou plusieurs organismes participant à la communauté, un intervenant extérieur ou une combinaison d'entre eux. Elle est située dans les locaux de l'organisation ou dans ceux d'un hébergeur externe. [8]

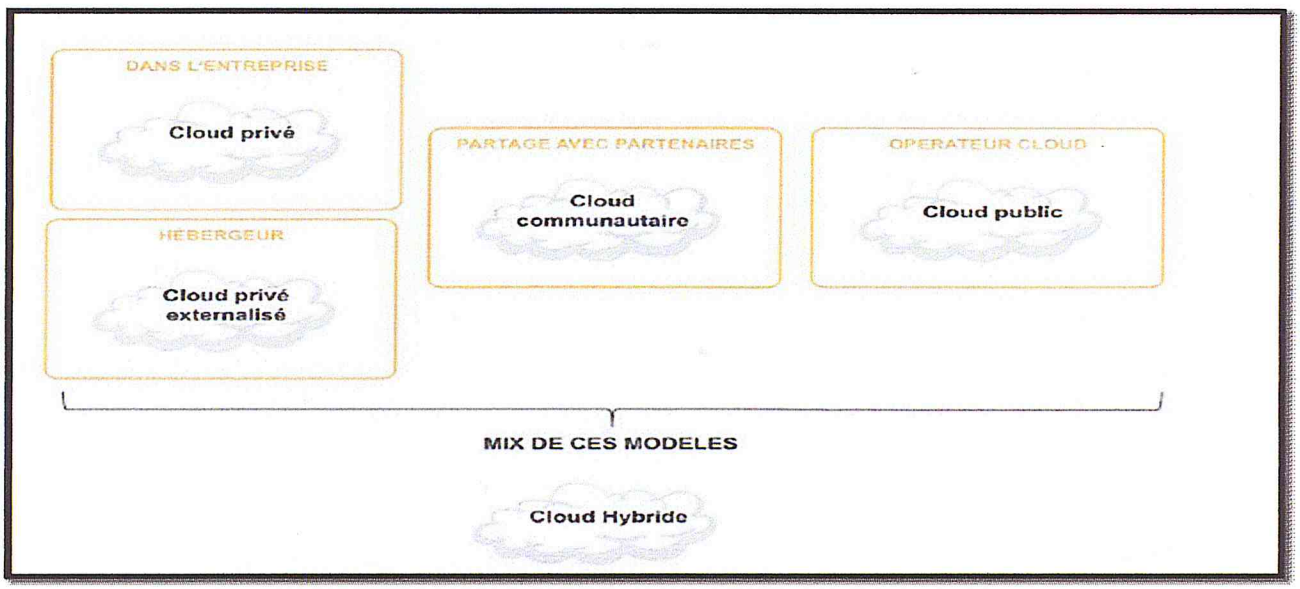


Figure I.8 : Les différents modèles de déploiement d'un Cloud

VII. Les caractéristiques du Cloud computing

Service à la demande, les clients d'un Cloud peuvent gérer leurs ressources sans interaction avec le fournisseur de service.

- Service accessible par réseau : les ressources sont accessibles depuis tout périphérique réseau (PC, tablette, clients lourds ou légers).
- Transparence : Les clients n'ont aucun contrôle ni même connaissance de l'emplacement exact, y compris géographiquement, des ressources qui leur rendent le service demandé.
- Elasticité : Les ressources sont allouées et recyclées en fonction des besoins et sont perçues comme illimitées par le client.
- Service de qualité : le Cloud contrôle et optimise ses ressources tout en fournissant des métriques à ses clients pour contrôler la qualité de service fournie.

VIII. Les Avantages du Cloud computing

- ✓ La réduction des coûts d'infrastructure informatique et de logiciels.
- ✓ La mise à jour des logiciels sur demande.
- ✓ Une plus grande capacité de calcul.
- ✓ Un espace de stockage des données dynamique (la mémoire louée dans le nuage augmente ou se réduit en fonction des données qui y sont enregistrées).
- ✓ La mobilité.
- ✓ La simplicité et la rapidité de l'accès aux données.
- ✓ L'extensibilité du système et, dans certains cas
- ✓ L'amélioration de la sécurité.

IX. Les inconvénients du Cloud computing

✓ **La bande passante peut faire exploser votre budget :**

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

✓ **La fiabilité du Cloud :**

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

✓ **Taille de l'entreprise :**

Si votre entreprise est grande alors vos ressources sont grandes, ce qui inclut une grande consommation du cloud. Vous trouverez peut être plus d'intérêt à mettre au point votre propre Cloud plutôt que d'en utiliser un externalisé. Les gains sont bien plus importants quand on passe d'une petite consommation de ressources à une consommation plus importante.

X. Conclusion

Nous venons de voir dans ce chapitre les concepts liés au Cloud computing, son architecture, ses services et leurs modèles de déploiement.

Chapitre 2
La sécurité

I. Introduction

Avec le développement de l'utilisation d'internet, de plus en plus d'entreprises ouvrent leur système d'information a leurs partenaires ou leurs fournisseurs, il est donc essentiel de connaitre les ressources de l'entreprise a protéger et de maitriser le contrôle d'accès et les droits des utilisateur du système d'information.

Par ailleurs, avec le nomadisme, consistant à permettre aux personnels de se connecter au système d'information a partir de n'importe quel endroit, les personnels sont menés a transporter une partie du système d'information de l'entreprise hors de l'infrastructure sécurisé de l'entreprise.

Dans ce chapitre nous allons nous intéresser plus particulièrement à la gestion du contrôle d'accès avec le modèle de sécurité RBAC.

II. Sécurité informatique

La sécurité informatique est l'ensemble des techniques, organisationnels, juridiques et humains nécessaire et mis en place pour conserver, rétablir, et garantir la sécurité des systèmes liée a la sécurité de l'information et des systèmes d'information.

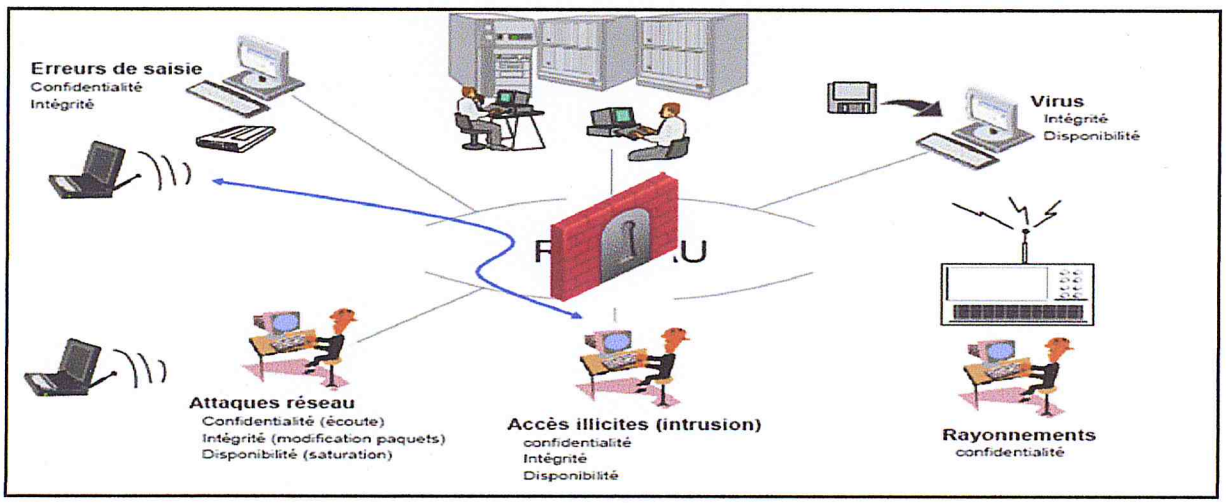


Figure II.1 : La sécurité des systèmes informatiques [12]

a. Les principales causes de l'insécurité informatique

❖ Un utilisateur du système

L'énorme majorité des problèmes liés à la sécurité d'un système d'information a pour origine un utilisateur, généralement insouciant. Il n'a pas le désir de porter atteinte à l'intégrité du système sur lequel il travaille, mais son comportement favorise le danger.

❖ Une personne malveillante

Une personne parvient à s'introduire sur le système, légitimement ou non, et à accéder ensuite à des données ou à des programmes auxquels elle n'est pas censée avoir accès. Le cas fréquent est de passer par des logiciels utilisés au sein du système, mais mal sécurisés.

❖ Un programme malveillant

Un logiciel destiné à nuire ou à abuser des ressources du système est installé (par mégarde ou par malveillance) sur le système, ouvrant la porte à des intrusions ou modifiant les données. Des données confidentielles peuvent être collectées à l'insu de l'utilisateur et être réutilisées à des fins malveillantes.

❖ Un sinistre (vol, incendie, dégât des eaux)

Une mauvaise manipulation ou une malveillance entraînant une perte de matériel et/ou de donnée

❖ Écoute passive :

Écoute :Elle consiste à se placer sur un réseau informatique ou de télécommunication pour collecter et analyser les informations ou les trames qui y circulent

Interception de signaux compromettants : l'attaquant tente de récupérer un signal électromagnétique pour l'interpréter et en déduire des informations utilisables.

Cryptanalyse : L'attaque de données cryptées est réalisée par interception et analyse des cryptogrammes circulant lors d'une communication ou obtenus par une source quelconque.

b. Les moyens techniques de la sécurité informatique

De nombreux moyens techniques peuvent être mis en œuvre pour assurer une sécurité du système d'information. Il convient de choisir les moyens nécessaires, suffisants, et justes. Voici une liste non exhaustive de moyens techniques pouvant répondre à certains besoins en termes de sécurité du système d'information :

1. Contrôle des accès au système d'information

Le contrôle d'accès consiste à vérifier si une entité (une personne, un ordinateur, ...) demandant d'accéder à une ressource a les droits nécessaires pour le faire. (On va détaillé plus tard).

2. Surveillance du réseau

La surveillance du réseau est la supervision d'un réseau de communication actif afin de diagnostiquer les problèmes et de recueillir des statistique d'administration et d'ajustement.

Quelques moyens pour surveiller un réseau

- **Analyseur de paquet (sniffer)**

  C'est un logiciel pouvant lire ou enregistrer des données transitant par le biais d'un réseau local non-commuté. Il permet de capturer chaque paquet du flux de données en traversant le réseau, voire, décoder les paquets de données bruts, afficher les valeurs de divers champs du paquet et analyser leur contenue conformément aux spécifications.

- **Système de détection d'intrusion (IDS)**

  Un système de détection d'intrusion est un mécanisme destiné à repérer des activités anormales ou suspectes sur la cible analysé (un réseau ou un hôte).Il permet ainsi d'avoir une connaissance sur les tentatives réussies comme échouées des intrusions.

3. Sécurité applicative

La sécurité applicative est la sécurisation technique de tout type d'application (application métier, web, commerciale, etc.)

Quelques moyens de la sécurité applicative :

❖ **Séparation des privilèges**

La séparation des privilèges est un principe qui dicte que chaque fonctionnalité ne doit posséder que les privilèges et ressources nécessaire à son exécution, et rien de plus. Ainsi en cas de défaillance grave du système, les dommages ne peuvent pas dépasser ce qui est autorisé par les privilèges et les ressource utilisés, ces derniers étant eux-mêmes limités par la séparation de privilège.

❖ **Audit de code**

En programmation informatique, l'audit de code est une pratique consiste à parcourir le code source d'un logiciel afin de s'assurer du respect de règles précises.

4. Cryptographie

La cryptographie est une des disciplines de la cryptologie s'attachant à protéger des messages (assurant confidentialité, authenticité et intégrité) en s'aidant souvent de secret ou clé.

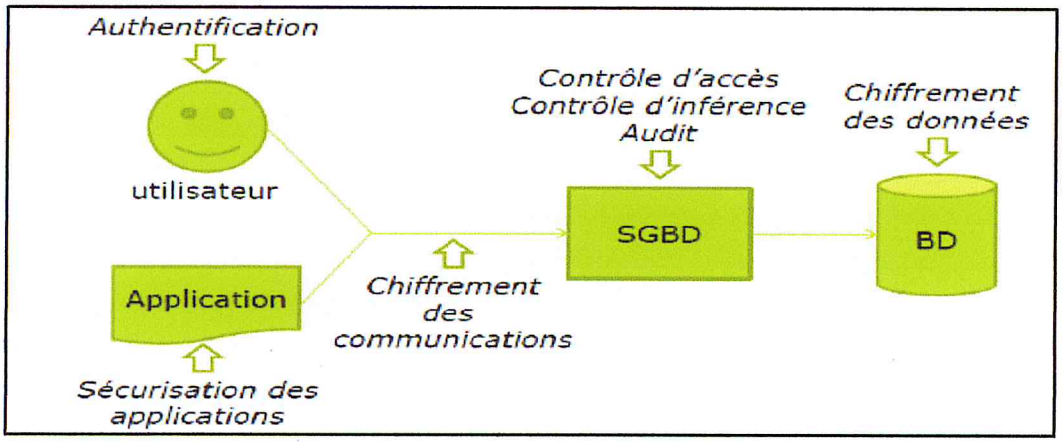


Figure II.2: Protections contre les attaques. [13]

III. Sécurité de l'informatique dans les nuages

Le Cloud Computing est un procédé qui consiste à transférer sur des serveurs distants les calculs informatiques et les capacités de stockage, traditionnellement localisés sur le poste informatique de l'utilisateur.

Les utilisateurs ou les entreprises peuvent ainsi accéder virtuellement et de manière évolutive à de nombreux services en ligne. Les applications et les données ne sont plus hébergées sur l'ordinateur local, mais dans un nuage ("Cloud") composé d'un certain nombre de serveurs distants interconnectés au moyen d'une excellente bande passante indispensable à la fluidité du système.

Malgré les avantages multiples que présente le Cloud Computing, la sécurité reste le grand défi qui confronte cette nouvelle technologie. En complément des problèmes habituels de sécurisation des systèmes informatiques, le Cloud Computing présente un facteur de risque supplémentaire du fait de l'externalisation de services stratégiques auprès d'un fournisseur externe. Il est en effet plus difficile, avec cette dimension d'externalisation, d'assurer l'intégrité et la confidentialité des informations, la disponibilité des données et des services [9]

De manière générale la mise en place d'application Cloud permet aux services informatiques de l'entreprise (SI et SSI) de repenser le schéma de sécurité et d'appréhender les nouvelles problématiques [4] :

- ✓ Confidentialité de la donnée, localisée hors de l'entreprise
- ✓ Le transport de la donnée vers le terminal de l'utilisateur
- ✓ La sécurité du terminal de l'utilisateur
- ✓ L'authentification de l'utilisateur

a. Confidentialité de la donnée, localisée hors de l'entreprise

Lors de la mise en place d'une application Cloud, un des impacts majeur sur la sécurité est la localisation de la donnée hors de l'entreprise. Cette localisation hors murs fait peser un risque physique sur celle-ci. [4]

b. Transport des données

Le transport des données est le second problème des applications Cloud : si la donnée est en sécurité dans les Datacenter (quelle que soit la méthode), il faut qu'elle le soit aussi pendant son transport jusqu'au terminal de l'utilisateur.la plupart du temps, les données transitent sur un réseau non sécurisé tel qu''internet.

Le risque principal dans ce cas l'écoute sur le réseau à des fins d'espionnage. Pour lever ce risque, la seule solution est le chiffrement des communications entre l'application et le terminal de l'utilisateur. [4]

c. La sécurité du terminal de l'utilisateur

La sécurité du terminal de l'utilisateur est l'aspect le plus difficilement appréhendable.

En effet la sécurité du terminal n'est pas directement liée à l'approche Cloud, mais elle peut directement impacter la sécurité de l'application Cloud.

La sécurité du poste de travail de l'utilisateur, moins maitrisée et plus nomade, devient donc un enjeu important car ce poste directement connecté à l'application Cloud : il en est une porte d'entrée. Le risque principal est l'introduction d'un attaquant sur le réseau de l'application Cloud à des fins malicieuses, via le poste de l'utilisateur.[4]

d. L'authentification de l'utilisateur

Consiste à assurer que seules les personnes autorisées aient accès aux ressources échangées

IV. Comment mettre en œuvre un Cloud sécurisé

- ✓ **Assurer la protection des données confidentielles**

Consiste au chiffrement de la donnée . [9]

- ✓ **Mettre en œuvre une solide gestion des accès et des identités**

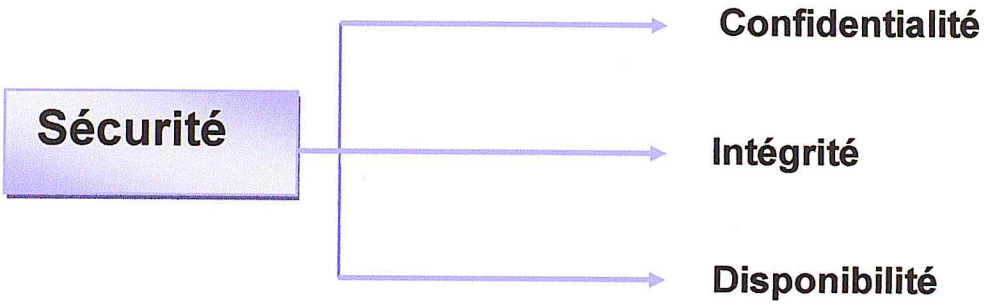
La gestion des accès et des identités est cruciale pour la sécurité du Cloud. Elle permet de limiter l'accès aux données et aux applications aux seuls utilisateurs autorisés. [9]

- ✓ **Mettre en place un programme de gestion des failles et des intrusions**

Dans un environnement Cloud de confiance, vous devez mettre en œuvre un programme et des mécanismes rigoureux de gestion des failles, notamment des systèmes de détection et de prévention des intrusions, pour que les ressources informatiques (serveurs, réseau, composantes de l'infrastructure et points de terminaison) soient sous surveillance permanente. [9]

V. Objectifs de la sécurité informatique

Les principes fondamentaux de la sécurité confidentialité, intégrité et disponibilité s'appliquent à la plupart des systèmes.



1. La confidentialité

Mécanisme pour transmettre les données d'un client et assure que ne soient accessibles que par les entités autorisées (seul le destinataire autorisé puisse les lire).Les différentes solutions de Cloud Computing comportent des mécanismes de confidentialité comme la gestion des identités et des accès. [5]

2. L'intégrité

Mécanisme pour garantir que les données protégées n'ont pas été modifiées durant la transmission par une personne non autorisée. [5]

Exemple :

Les clients qui cherchent à externaliser leurs données peuvent évidemment s'attendre à être protégés contre les modifications non autorisées. Les systèmes dans les nuages fournissent un certain nombre de mécanismes de protection de l'intégrité des données.

Dans le cas de Windows, des mécanismes assurent l'intégrité des données dans la conception de la machine virtuelle elle-même.

Pour le service de stockage de Windows Azure, l'intégrité est définie par les applications utilisant le modèle de contrôle d'accès. Chaque compte de stockage a deux clés qui sont utilisées pour contrôler l'accès à toutes les données dans ce compte de stockage.[3]

3. La Disponibilité

Les données doivent rester accessibles aux utilisateurs (une attaque de type DoS, par exemple, vise à empêcher les utilisateurs normaux d'un service d'y accéder). [5]

Exemple :

L'un des principaux avantages fournis par des plates-formes de Cloud Computing est la disponibilité robuste basée sur la redondance réalisée avec des technologies de virtualisation. Windows Azure par exemple offre de nombreux niveaux de redondance fournissant une disponibilité maximale des données et des applications. Les données sont répliquées au sein de Windows Azure sur trois nœuds distincts pour minimiser l'impact des pannes matérielles. Les clients peuvent exploiter la nature géographique de l'infrastructure Windows Azure en creusant un deuxième

compte de stockage fournissant des capacités de basculement à chaud. Dans de tels scénarios, les clients peuvent créer des rôles personnalisés à répliquer et synchroniser les données entre les installations de Microsoft. Ils peuvent également créer des rôles personnalisés pour écrire des données de stockage pour des sauvegardes sur site privé.

Les agents tournant sur les machines virtuelles invitées surveillent la santé de ladite machine. Si l'agent ne répond plus, le contrôleur redémarre la machine virtuelle. Les clients pourront éventuellement choisir d'exécuter des processus de suivi de santé plus sophistiqués et adaptés à leur politique de continuité.

En cas de défaillance du matériel, le contrôleur déplace l'instance du rôle vers un nouveau nœud et reprogramme la configuration réseau pour les instances de ce rôle afin de rétablir la disponibilité totale du service.
Les contrôleurs adhèrent au même principe de disponibilité grâce à la redondance et à un basculement automatique assurant la disponibilité continue des capacités de gestion des contrôleurs. [5]

VI. Contrôle d'accès aux systèmes d'informatique dans les nuages

1 .Les politiques de sécurité

Une politique de contrôle d'accès dans les nuages peut être définie comme une exigence de sécurité de Cloud qui spécifie comment et quand un utilisateur peut accéder à une ressource spécifique. Une telle politique peut être exécutée dans un système Cloud grâce à un mécanisme de contrôle d'accès. Ce dernier est responsable de l'octroi ou le refus de l'accès d'utilisateur à une ressource.

La plupart des politiques de sécurité reposent sur les notion de sujet ,d'objet et de droit d'accès .Un sujet est une entité active, correspondant à un processus qui s'exécute pour compte d'un utilisateur .Dans ce contexte, un utilisateur est soit une personne physique connue du système informatique et enregistrée comme

utilisateur ,soit un serveur (personne morale) représentant des fonctions des services automatiques, tel que le serveur d'impression, le serveur de base de données, le serveur de messagerie, etc. .

Un objet est une entité considérée comme « passive« qui contient ou reçoit des informations.

A un instant donné, un sujet à un droit d'accès sur un objet si et seulement si le processus correspondant au sujet est autorisé à exécuter l'opération correspondante à ce type d'accès sur cet objet. [14]

En ce qui concerne les politiques de contrôle d'accès, plusieurs d'entre eux ont été introduites au cours de la dernière décennies, à savoir les politiques de contrôle d'accès obligatoire (MAC), le contrôle d'accès discrétionnaire (DAC) et le contrôle d'accès à base de rôles (RBAC).

Chacun d'eux a des exigences de sécurité spécifiques dans différents environnements de travail.

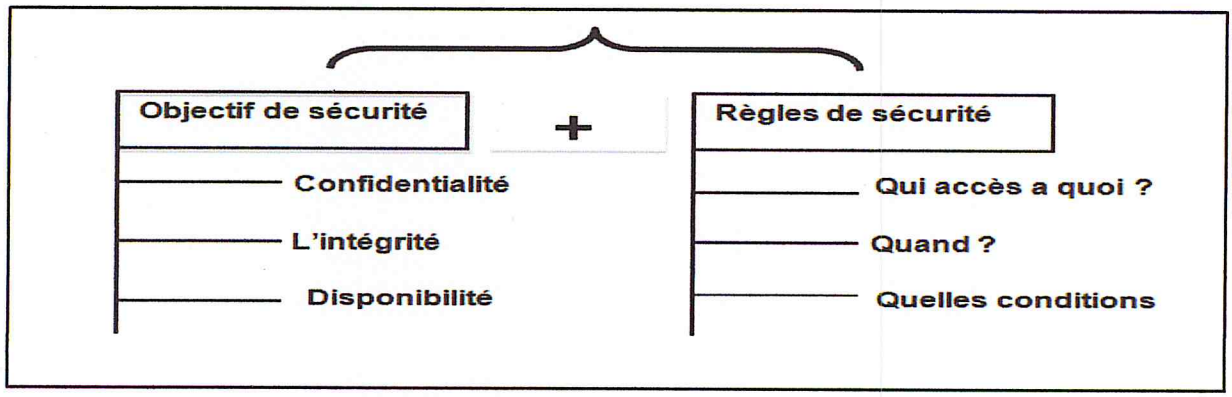


Figure II.3 : Qu'est ce que c'est les politique de sécurité

2. Contrôle d'accès

Le contrôle d'accès est un mécanisme par lequel un système autorise ou interdit le droit à des entités actives (sujet : personnes, processus, machines, etc.) d'accéder et d'effectuer des opérations sur des entités passive (objet : fichier, dossier, etc.).Les

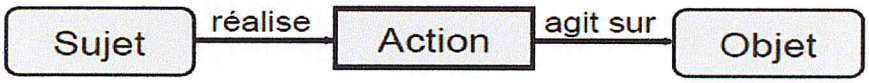
Mécanisme de contrôle d'accès au niveau des applications expriment des politiques de sécurité. [15]

3.Rôle de contrôle d'accès dans le Cloud computing

Le contrôle d'accès est d'une importance vitale dans un environnement Cloud car elle se préoccupe de contrôler et de limiter les actions ou opérations dans les systèmes de Cloud qui sont effectuées par un utilisateur sur un ensemble de ressources Cloud.

4.Concepts de bases de contrôle d'accès

- Sujets = entités actives du SI
  - Utilisateurs, processus travaillant pour le compte d'utilisateurs
- Objets = entités passives du SI
  - Contiennent les informations à protéger (fichiers, relations dans une BD relationnelle, ...)
- Actions (ou Opérations) = permettent aux sujets de manipuler les objets
  - Lecture d'un fichier, requête dans une BD .16]



- Les sujets ont des permissions de réaliser des actions sur des objets

5.Modèle de sécurité

Un modèle de contrôle d'accès peut être défini comme un conteneur abstrait d'un ensemble de mises en œuvre du mécanisme de contrôle d'accès, qui est capable de préserver soutenir la motivation des politiques du système par le biais d'un cadre conceptuel. Le modèle de contrôle comble le fossé existant entre l'abstraction et le mécanisme de la politique dans un système.

Les politiques d'autorisation les plus citées dans la littérature sont généralement Associées à un modèle de sécurité. D'une manière générale, un modèle peut être défini comme un formalisme (souvent mathématique) qui offre une vue subjective mais pertinente de la réalité .On modélise pour mieux comprendre le système qu'on développe, c'est –à-dire pour visualiser ses propriétés, spécifier sa structure ou son comportement, documenter et guider sa construction, etc. A partir de là, un modèle de sécurité peut être défini comme un formalisme permettent de représenter, de façon claire et non-ambiguë, la politique de sécurité. Il aide à l'abstraire (afin de réduire sa complexité) et à faciliter sa compréhension, comme il peut servir à vérifier que cette politique est complète (tout est protégé) et cohérente, et que la mise en œuvre par le système de protection est complète (tout est protégé) et cohérente, et que la mise en œuvre par le système de protection est conforme aux propriétés attendues du système. [14]

6.Les types de contrôle d'accès

La technologie de contrôle d'accès a évolué grâce aux efforts de développement et de recherche supportés par le département de défense.

Ces recherches ont données naissance à deux types fondamentaux de contrôle d'accès.

1. Contrôle d'accès discrétionnaire.
2. Contrôle d'accès obligatoire

Plusieurs modèles de contrôle d'accès ont été développés par la suite.

a.Les contrôles d'aces discrétionnaires (DAC)

Dans le cas d'une politique discrétionnaire, les droit d'accès à chaque information sont manipulés librement par le responsable de l'information (généralement propriétaire), qui les affecte.les droits peuvent être accordés par se responsable à chaque utilisateur, à des groupes d'utilisateurs, ou bien aux deux. Ceci peut parfois amener le système dans un état d'insécurité (c'est-à-dire contraire aux objectifs de sécurité qui ont été choisis) [14].

Les politiques de contrôle d'accès discrétionnaires s'appuient sur les notions de propriété (tout sujet est propriétaire d'un ensemble d'objets) et de droit d'accès (lecture, écriture, etc.).

> Le contrôle d'accès est dit discrétionnaire lorsque la technique de restriction d'accès aux objets est basée sur l'identité des sujets et/ou des groupes auxquelles ils appartiennent. Le contrôle est discrétionnaire dans le sens où un sujet possédant un certain droit d'accès est capable de conférer ce droit à tout autre utilisateur.

Un sujet peut lui même accepter ou refuser l'accès à un objet qu'il possède

- Les permissions d'accès peuvent être assignées, supprimées, modifiées, ou transmises à la discrétion du propriétaire de l'objet.
- Basé sur l'identité des sujets et des permissions d'accès sur les objets
- L'organisation délègue une partie de ses droits à chaque utilisateur (la façon dont un utilisateur délègue ses droits peut être réglementée)
- Exemple : contrôle d'accès aux fichiers dans Unix

Contrôle d'accès discrétionnaire

- ✓ Suppose que l'on puisse définir un propriétaire pour chaque ressource

Ne satisfait pas le « *principe du moindre privilège* » : un utilisateur peut transmettre plus de droits que nécessaire à un autre utilisateur

- ✓ Un droit d'accès peut être transmis sans que son propriétaire soit informé : Adonne un droit en lecture à B sur un de ses fichiers, B copie ce fichier, B étant propriétaire de la copie, transmet son droit de lecture à C
  → A doit faire confiance à B

- ✓ La confiance ne suffit pas :
  - A possède un fichier sensible, B n'est pas autorisé à le lire
  - B implémente un cheval de Troie, et réussit à convaincre A de l'utiliser
  - Si A exécute le programme, le programme acquiert les droits de A le temps de l'exécution, et peut copier le fichier sensible dans un fichier auquel B a accès

- ✓ En résumé, le contrôle d'accès discrétionnaire
  - Permet de limiter l'accès d'utilisateurs honnêtes et d'éviter l'altération d'information
  - N'est pas adapté au contexte où l'information est très sensible

b.Les contrôles d'accès obligatoires (MAC)

Une politique de sécurité d'autorisation obligatoire(ou MAC de l'anglai « Mandatory Access control ») impose des règles d'autorisation incontournables qui s'ajoutent aux règles discrétionnaires.une politique obligatoire suppose que les utilisateurs et objets aient été étiquetés. [14]

Classiquement ,les objets se voient attribuer une classification ,tandis que les utilisateurs possèdent une habilitation.les règles qui régissent les autorisations d'accès sont basées sur une comparaison de l'habilitation de l'utilisateur et de la classification de l'objet.ces règles incontournables assurent que le système vérifie des propriétés générales de confidentialité ou d'intégrité par exemple.ces règles sont souvent utilisées conjointement aux règles d'une politique discrétionnaire car leur pouvoir d'expression est en général relativement faible.

Par exemple, un utilisateur sera autorisé à manipuler une information dans le système si l'utilisateur en question possède le droit de lecteur sur l'information (contrôle discrétionnaire) et s'il est habilité à manipuler cette information (contrôle obligatoire). [17]

- ➢ Exemple : modèle de Bell La padula (non discrétionnaire)

c.Le contrôle d'accès *basé sur les rôles (RBAC)*

Une politique de contrôle d'accès à base de rôle (RBAC pour Rôle-Based Accès Contrôle) se base sur la description des fonctions qu'un utilisateur a le droit d'accomplir au sein d'une organisation pour établir les règles d'accès aux informations .[18]

Le contrôle d'accès basé sur (RBAC) est une méthode de régulation de l'accès aux ressources informatiques ou de réseau basé sur les rôles des utilisateurs individuels au sein d'une entreprise. Dans ce contexte, l'accès est la capacité d'un utilisateur à exécuter une tâche spécifique, comme afficher, créer ou modifier un fichier.

Le contrôle d'accès basé sur le rôle (RBAC) est une technologie qui a pris beaucoup d'attention, en particulier, dans le domaine des applications commerciales grâce à son potentiel de réduire la complexité et le cout de la gestion de sécurité réseau, car l'un des problèmes les plus difficiles à gérer de grands réseaux, c'est la complexité de l'administration de la sécurité. Sous RBAC, la gestion de la sécurité est simplifiée par l'utilisation des rôles, par la hiérarchie et les contraintes pour organiser les privilèges d'accès

Avec RBAC, le concept central des politiques d'accès est le rôle. Les permissions sont affectées à des rôles et les rôles sont affectés à des utilisateurs.

Eléments du modèle

- U : ensemble d'utilisateurs
- R : rôles (fonctionnel, organisationnel)
- P : permissions
- AU : affectation des utilisateurs aux rôles (relation plusieurs-à plusieurs)
- AP : affection des permissions aux rôles (relation plusieurs-à-plusieurs)

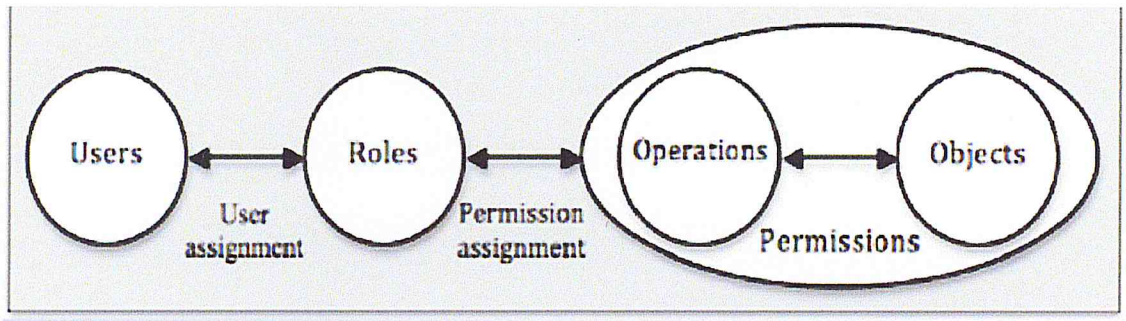


Figure II.4: Modèle RBAC. [16]

VII. Conclusion

Dans ce chapitre nous avons vu la sécurité informatique en générale avec ses différents aspects. Tel qu' il est important de bien comprendre toutes les concepts de cet dernière avant de passer au sécurité dans un environnement Cloud computing plus précisément le contrôle d' accès en utilisant un politique de sécurité très importants : La politique basé sur le rôle (RBAC) que nous avons décrit dans ce chapitre, ceci nous permettra de répondre de manière appropriée de notre objectif.

Chapitre 3

Les solutions existantes de Cloud Privé

I. Introductions

Le Cloud Computing se développe à une vitesse extraordinaire, et tous les grands acteurs du web y lancent des offres.

II. Les acteurs du Cloud

Le marché du Cloud Computing est partagé entre plusieurs acteurs : les éditeurs, les fournisseurs, etc.

1. Editeurs

Les éditeurs fournissent une technologie de Cloud Computing qui peut être hébergée sur les infrastructures physiques d'une société de services et être proposée comme un Cloud public, ou bien directement installée sur les infrastructures internes d'une entreprise laissant place à un Cloud privé.[5]

Exemple

✓ **VMware**

Est un éditeur de produits de virtualisation. Comme beaucoup d'autres éditeurs, VMware s'est lancé depuis 2008 à la conquête du Cloud Computing. Aujourd'hui, il édite des produits pour la couche IaaS comme « vSphere » et « vCloud Director », « vFabric » .

✓ **Microsoft**

Fourni des produits de Cloud Computing comme « Windows Azure Appliance », dont la sortie est prévue en 2011. « Windows Azure Appliance » est la version produit de Windows Azure que l'on va pouvoir installer directement sur les infrastructures d'une entreprise.

2. Fournisseur

Les fournisseurs de services de Cloud Computing sont des hébergeurs tels que l'on a l'habitude de les retrouver depuis plusieurs années sur Internet

Ils mettent à disposition des infrastructures physiques proposant une plateforme de Cloud.[5]

Exemple :

- ✓ **Microsoft :** avec sa plate-forme d'IaaS, de PaaS et de SaaS au travers de « Windows Azure » et « Office 365 »
- ✓ **Google :** avec son service SaaS « Google App » et son PaaS « Google App Engine ».
- ✓ **Amazon :** avec ses services de IaaS et PaaS comme « Elastic Compute Cloud (EC2) », « Elastic MapReduce » ou encore « Simple Storage Service (S3) ».

III. Les solutions existantes

Dans cette partie, nous présentons 2 solutions apportées par les acteurs: Amazon et Microsoft.

a. Microsoft Windows Azure Platform

Lors de la PDC « *Professionnal Developper Conference* » de Novembre 2008, Microsoft annonçait l'arrivée de sa propre solution de Cloud Computing nommée Windows Azure.

Cette dernière a été rendue commerciale en janvier 2010 et ne cesse de se développer au regard des annonces faites par Microsoft lors de la PDC du 28 octobre 2010

Cette nouvelle mouture ne correspond en rien à une nouvelle version du système d'exploitation mais plus à une prolongation de celui-ci vers l'industrialisation de l'hébergement d'applications exploitant d'une manière ou d'une autre le Web, permettant d'aboutir à terme au fameux adage « Tout et toujours connecté ».

Windows Azure relève bien de système d'exploitation serveurs et non de système d'exploitation Client. Celui-ci évolue dans l'univers du Cloud en proposant ainsi une industrialisation de vos hébergements applicatifs web avec un système d'exploitation dédié et une ingénierie correspondante au travers d'une toute nouvelle plateforme de Cloud Services. [19]

1. Présentation de la solution *Paas*: Windows azure Platform

Windows Azure est une plateforme dédiée à l'hébergement cloud proposé par Microsoft. Rassemble plusieurs services pouvant travailler ensemble ou indépendamment, chacun ayant un rôle précis :

- **Windows Azure :** principal composant de la plateforme Azure, il s'agit en fait d'un système d'exploitation, adapté au cloud et installé sur les serveurs de Microsoft. [21]
- **SQL Azure :** il s'agit de la version cloud du SGBD de Microsoft, SQL Server. [21]
- **Azure AppFabric :** permet d'interconnecter des services hébergés sur le « Cloud » avec des applications existantes. [20]

1.1. Windows Azure :

Windows Azure = OS on the Cloud. [19]

Windows Azure est un Cloud OS permettant l'hébergement d'applications sur une plateforme Windows basée sur la technologie de virtualisation Hyper-V.

Comme tout système d'exploitation, il permet d'utiliser le matériel mis à disposition sans avoir à se préoccuper des caractéristiques techniques ni de l'infrastructure. Il fournit ce qu'on appelle une « abstraction » de l'infrastructure. Le rôle de Windows Azure est de gérer un système pouvant s'étendre à plusieurs serveurs fonctionnant ensemble, c'est ce qu'on appelle le Cloud, afin de :

- ✓ Stocker des données
- ✓ Exécuter des applications

Ce système fournit deux services principaux, indépendants l'un de l'autre : Compute et Storage.

a. Compute : service d'exécution

Ce service se base sur des rôles. Les rôles sont en quelque sorte des applications que l'on va créer sur notre plateforme Azure. Il existe deux types de rôles :

- ✓ **Web Role** : comme leur nom l'indique, ce sont des applications de type web accessible directement par un navigateur web à travers un Internet Information Services (IIS). Hébergé dans Azure. [Tekigo, chpelle] Dont le but est d'interagir avec des utilisateurs via le web.

Par exemple, un site internet, une boutique en ligne ou une interface utilisateur sont des « Web Role ». [21]

- ✓ **Worker Roles** : ceux- la ne sont pas faits pour être en interaction avec l'utilisateur, mais plutôt permettant d'héberger n'importe quel type d'application. [21]

Comme par exemple de la manipulation de fichiers.

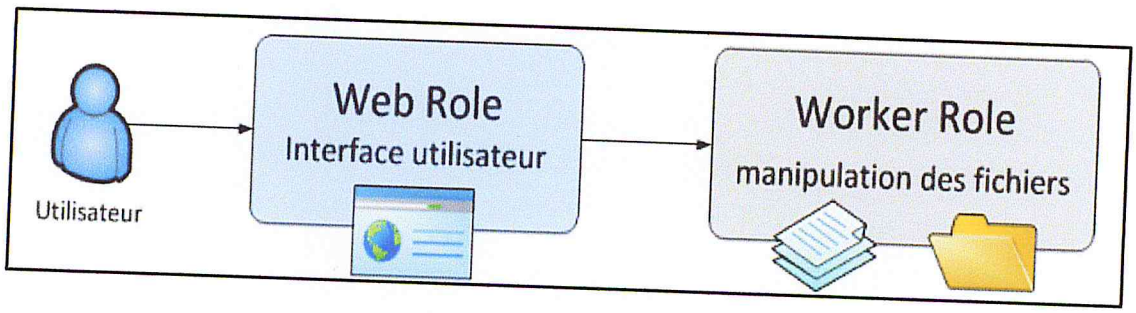


Figure III.1 : Exemple d'une application web destinée à gérer des fichiers à distance, via une interface sur le navigateur. [21]

Ainsi un Service Azure que vous développerez pourra être un simple Web rôle, un simple Worker role ou une combinaison des deux. [21]

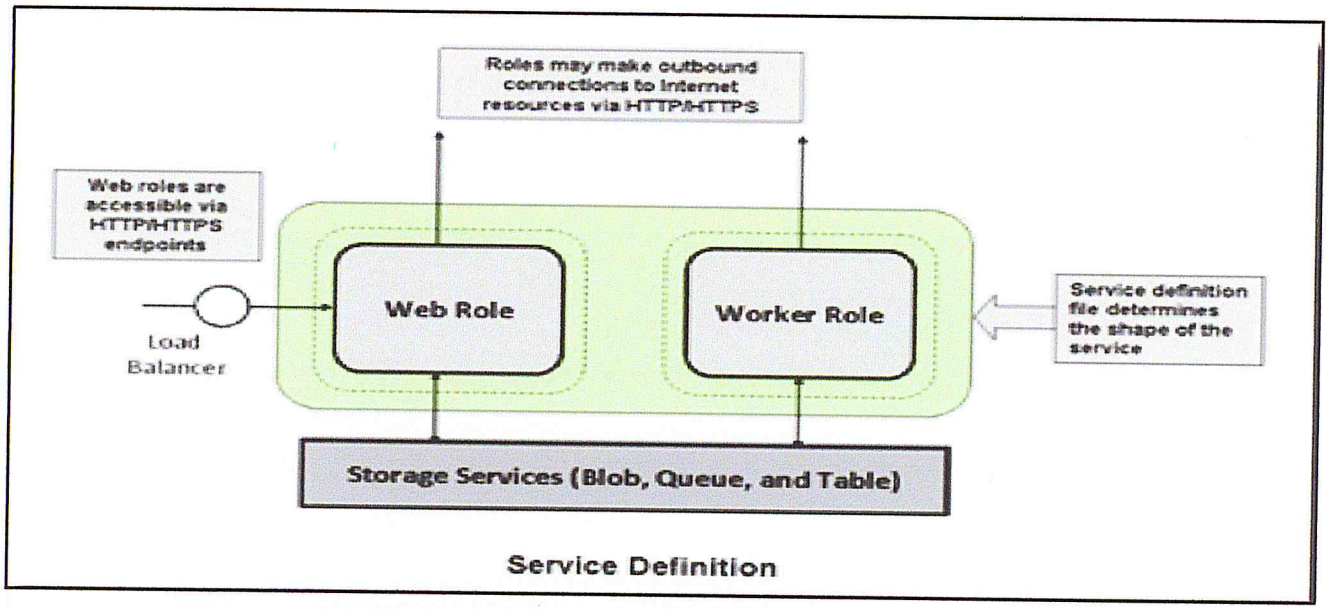


Figure III.2: Notions des rôles sur Windows azure. [21]

b. Storage : service de stockage de données

Le service de Storage est donc la partie du système Windows Azure qui va s'occuper de stocker des données. Il fonctionne via plusieurs outils, adaptés aux différents types de données que l'on peut manipuler :

- **Blobs :** stockage de fichiers.
- **Tables :** enregistrement de données sous la forme nom / valeur.
- **Queues** : transmission d'informations entre rôles (ex : instructions données à un *worker role* par un *web role*).

Ces trois méthodes de stockage sont également accessibles aux applications qui ne sont pas exécutées dans Windows Azure (c'est-à-dire au sein du service de traitement Windows Azure). Par exemple, une application sur site ou hébergée peut choisir de stocker des fichiers vidéo lourds en tant que blobs Windows Azure. [21]

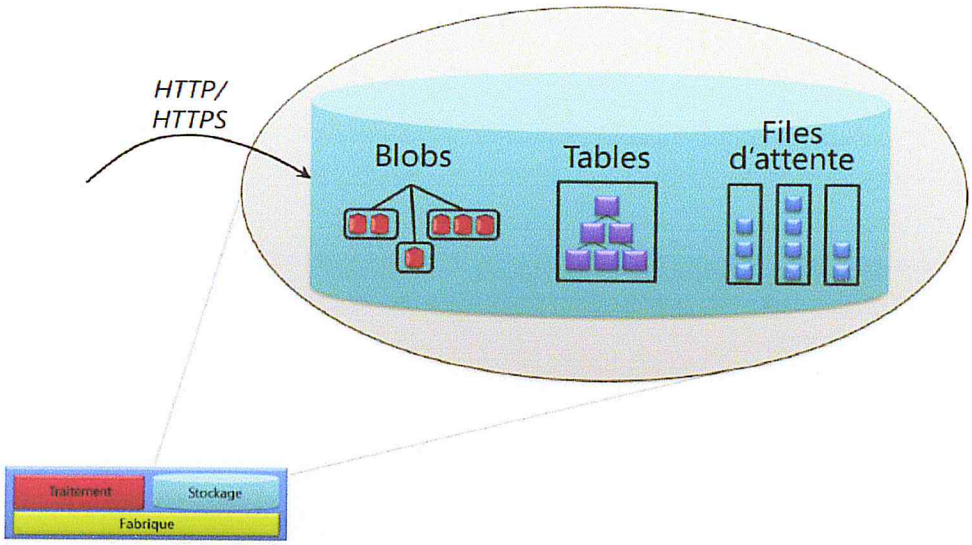


Figure III.3 : Le service de stockage Windows Azure est accessible via des applications Windows Azure ou des applications externes. [22]

1.2. SQL Azure

Un service de bases de données relationnelles, basé sur le produit serveur « Microsoft SQL Server ». Depuis une simple interface d'administration, il est possible de créer, de manière instantanée, une base de données SQL Server sur une infrastructure fiable et garantissant une disponibilité de plus de 99,95 %.[23]

1.3.Azure AppFabric

Un service de bus applicatif (ServiceBus) ou encore un service de contrôle d'accès (compatible avec différents fournisseurs d'identité comme Google Account, OpenID, LiveId, Active Directory, etc.).[23]

IV. Découverte de la plateforme Windows Azure

La plateforme va vous permettre de gérer votre compte ainsi que les différents projets que vous hébergerez sur Azure.

1. Inscription sur Windows Azure

✓ Premièrement il faut Créer un compte sur la plateforme Azure :

Afin de pouvoir déployer vos projets sur le cloud Azure, il vous faudra un compte. Il en existe deux types : payant, ou gratuit pour 30 jours.

2. Comptes Azure gratuits 30 jours

Afin de vous permettre de tester Windows Azure, Microsoft a mis en place des comptes gratuits pour une durée de 30 jours, sans carte bleue nécessaire

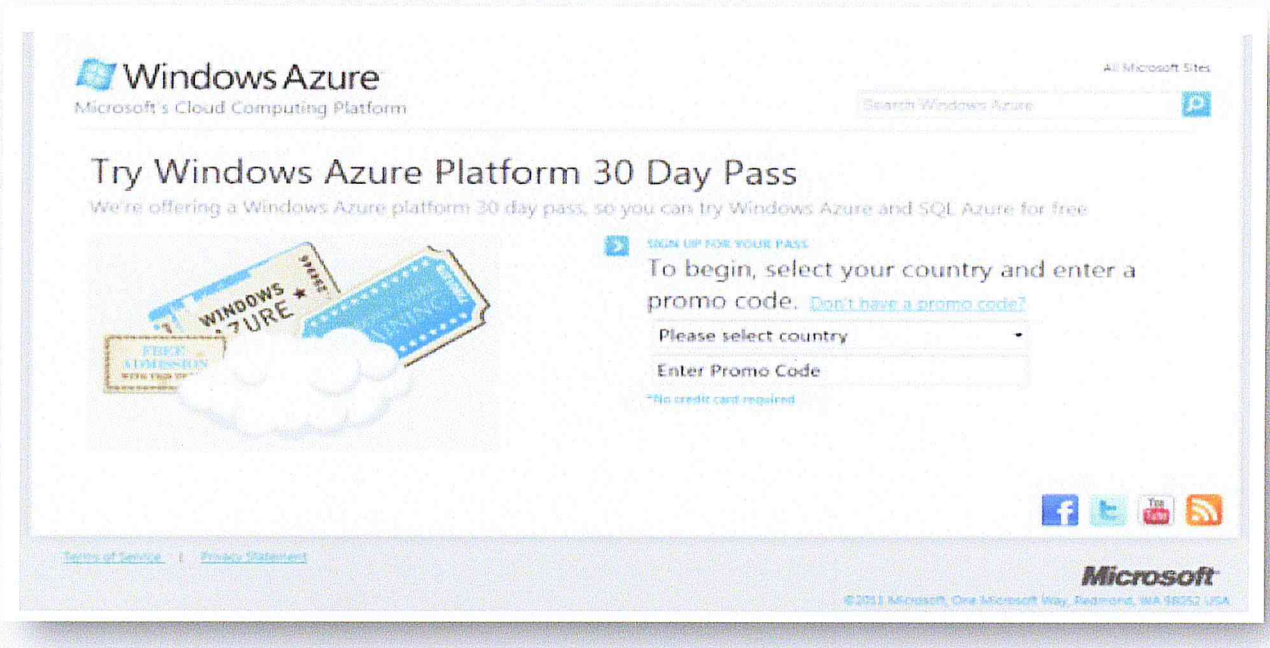


Figure III.4 : Comptes Azure gratuits 30 jours [21]

Le site vous demande votre pays, ainsi qu'un code promo. Saisissez le code **MSCLOUD** et validez le formulaire.

Il vous faut ensuite vous connecter avec un compte Windows Live ID. Si vous avez déjà un compte Hotmail, Messenger ou autre service Microsoft, vous pouvez vous identifier avec. Dans le cas contraire il va vous falloir créer un compte. Utilisez pour cela le bouton **Sign Up**.

Vous devrez ensuite entrer vos coordonnées, et accepter les conditions d'utilisations de la plateforme Windows Azure

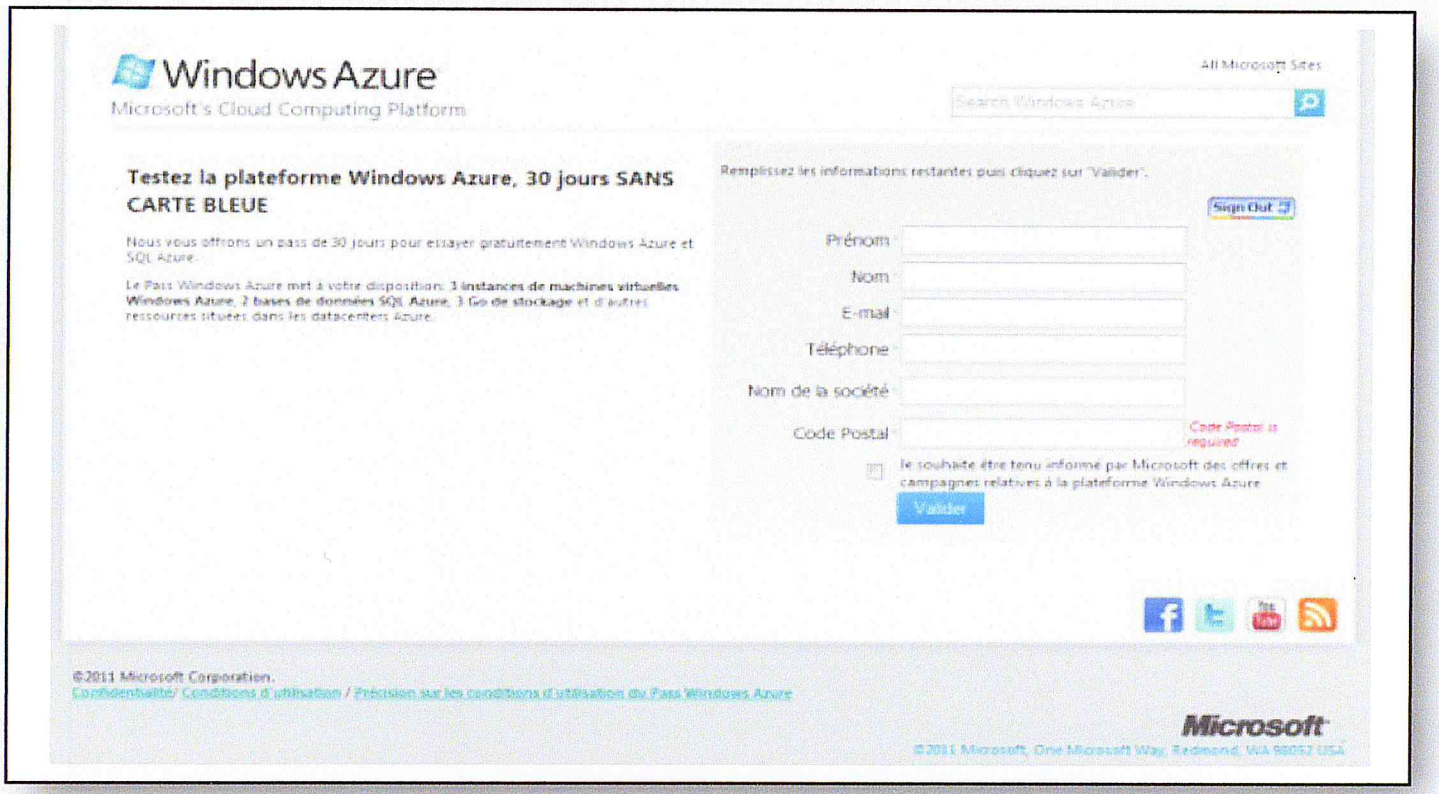
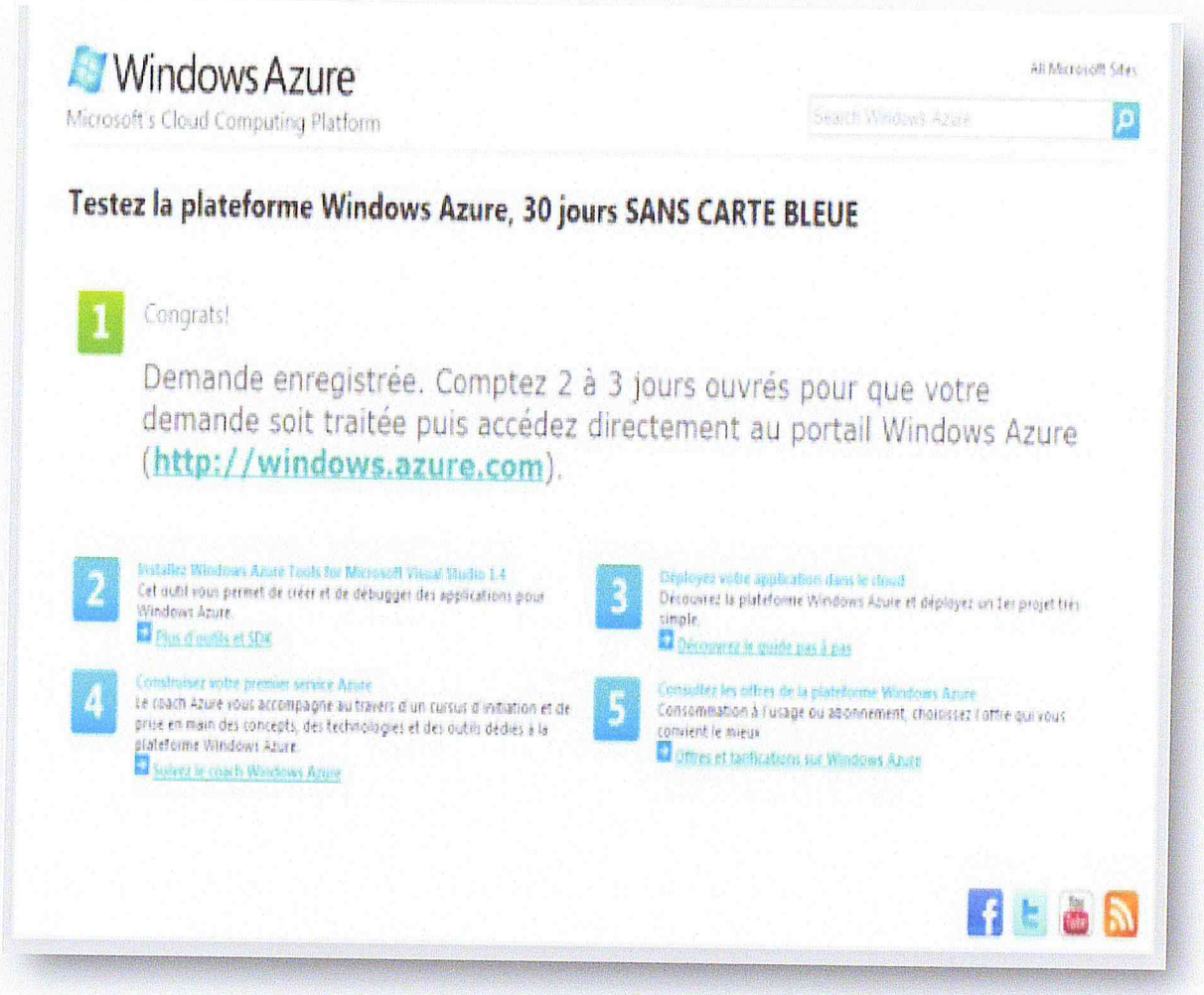


Figure III.5 : remplir le formulaire de validation. [21]

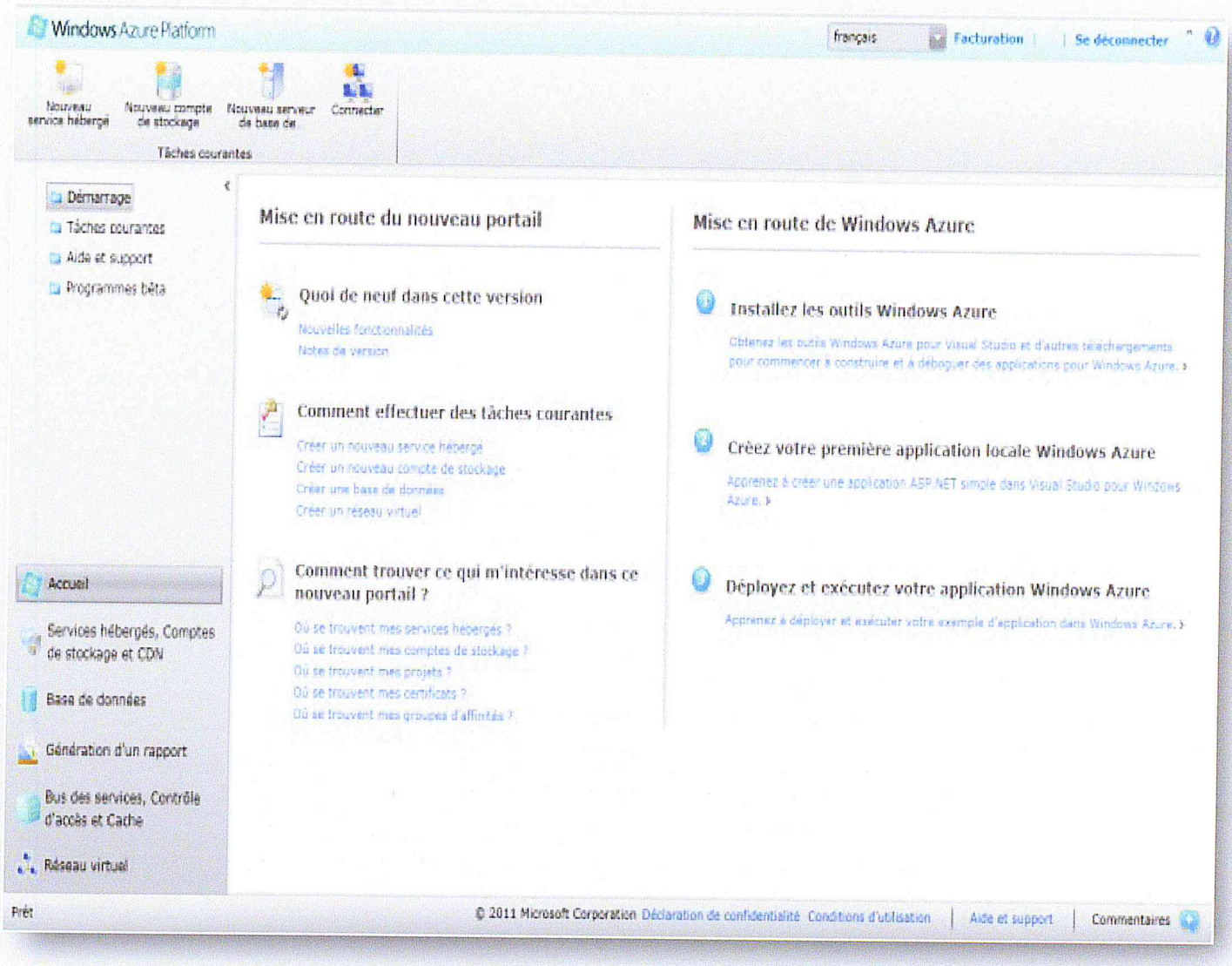


FigureIII.6: page de confirmation.[21]

Une fois que vous avez envoyé vos coordonnées et validé, une dernière page vous confirme que votre demande a bien été enregistrée. Il ne vous reste plus qu'à attendre que votre compte soit activé, ce qui peut prendre jusqu'à trois jours d'après Microsoft. En pratique, cela est souvent réalisé plus rapidement.

3. L'interface de la plateforme

Nous allons découvrir l'interface de cette plateforme



FigureIII.7: Interface Windows azure.[21]

Nous allons maintenant pouvoir passer en revue les parties principales de l'interface :

❖ **La barre d'outils :**

Située tout en haut, elle vous permet d'accéder rapidement aux fonctionnalités principales, selon la page sur laquelle vous vous trouvez. Remarquez également le lien **Billing** en haut à droite, qui vous permet d'accéder à l'espace facturation.

❖ **La barre latérale :**

Elle affiche dans sa partie supérieure un menu différent selon la page sur laquelle vous vous trouvez, et dans sa partie inférieure le menu principal, qui vous permet de naviguer entre les différentes zones d'administration proposées par la plateforme :

- *Accueil :* Retour à l'accueil de la plateforme
- *Services hébergés, Comptes de stockage et CDN :* État du compte et gestion des services hébergés. C'est cette section que vous utiliserez le plus souvent.
- *Base de données :* Gestion des bases de données SQL Azure.
- *Génération d'un rapport :* Fournit des rapports sur les bugs et l'utilisation des applications et données hébergées sur votre compte Azure.
- *Bus des services, Contrôle d'accès et Cache :* Permet d'utiliser les différentes fonctionnalités de Azure AppFabric.
- *Réseau virtuel :* Permet d'utiliser plusieurs fonctionnalités réseau comme *Windows Azure Connect*, qui permet de créer une connexion réseau entre vos Web Roles Azure et un serveur situé en dehors du cloud.

❖ **La zone de travail :**

Sur chaque page, elle affichera les informations principales.

4. La page d'accueil de la plateforme

La page d'accueil met en avant les différentes rubriques d'aide qui vous sont proposées. Le but est de vous accompagner au maximum dans votre utilisation de Windows Azure. Certaines pages d'aides sont directement listées au centre de la fenêtre, dans la zone de travail. D'autres sont regroupées au sein de thématiques que vous pourrez parcourir à l'aide du menu de la barre latérale. La barre d'outils vous propose plusieurs options :

- **Nouveau service hébergé :** Héberger un nouveau projet sur votre compte Azure.
- **Nouveau compte de stockage :** Nouveau compte de stockage, vous permettant d'utiliser les fonctionnalités du service *Azure Storage*.
- **Nouveau serveur de base de données :** Création d'une nouvelle base de données.
- **Connecter :** Nouvelle connexion *Azure Connect*.

5. Services hébergés, Comptes de stockage et CDN

Cette partie vous permet d'accéder aux fonctionnalités qui composent le système d'exploitation **Windows Azure**. C'est-à-dire principalement les services *Compute* et *Storage*.

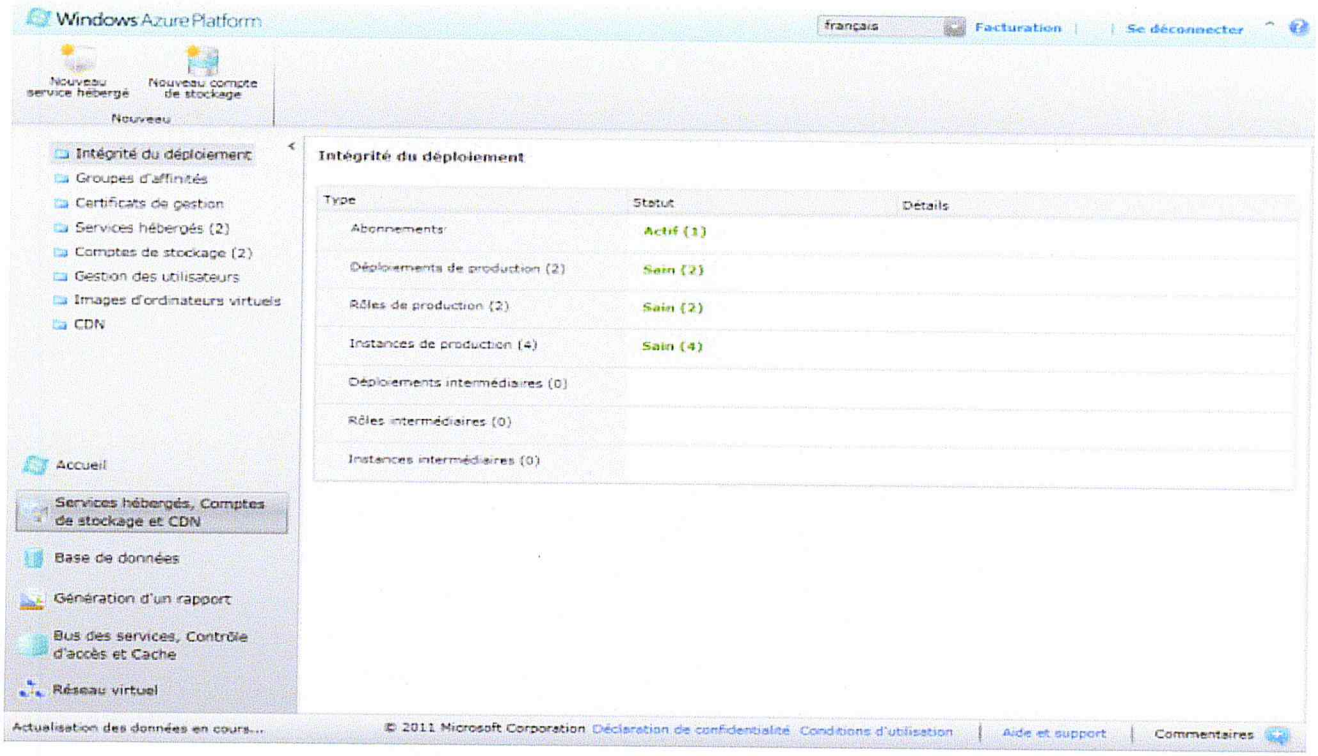


Figure III.8 : Interface de services hébergés, Comptes de stockage et CDN. [21]

Voici les différentes sections auxquelles vous avez accès dans cette partie :

- **Intégrité du déploiement :** État de santé de votre compte Azure et des applications hébergées.
- **Groupes d'affinités :** Permet de créer des groupes pour rassembler différentes applications travaillant ensemble.
- **Services hébergés :** Gestion des différents projets hébergés sur votre compte Azure.
- **Comptes de stockage :** Gestion des comptes Azure Storage.
- **Gestion des utilisateurs :** Permet de donner l'accès à votre compte à plusieurs utilisateurs.

6. Base de données

Cette section vous permet de gérer vos bases de données **SQL Azure** . Pour créer une ou plusieurs bases de données, il vous faut d'abord créer un serveur de bases de données. Basiquement, cela revient à installer SQL Azure sur une machine virtuelle qui sera chargée d'héberger vos bases de données. Pour chaque serveur, vous devrez préciser un nom et un mot de passe pour l'administrateur. Vous pourrez également choisir où vous souhaitez héberger votre base de données, c'est-à-dire dans quel Datacenter.

Pour chaque base de données, vous devrez choisir un nom et une taille, adaptée à ce que vous souhaitez stocker dessus.

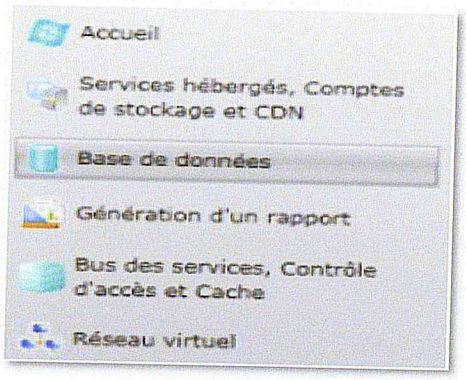


Figure III.9 : création de la base de données. [21]

V. Où est hébergé Windows Azure

Windows Azure est une infrastructure hébergée dans les data centres Microsoft dans un premier temps localisés aux US et rapidement à l'échelle mondiale :[21]

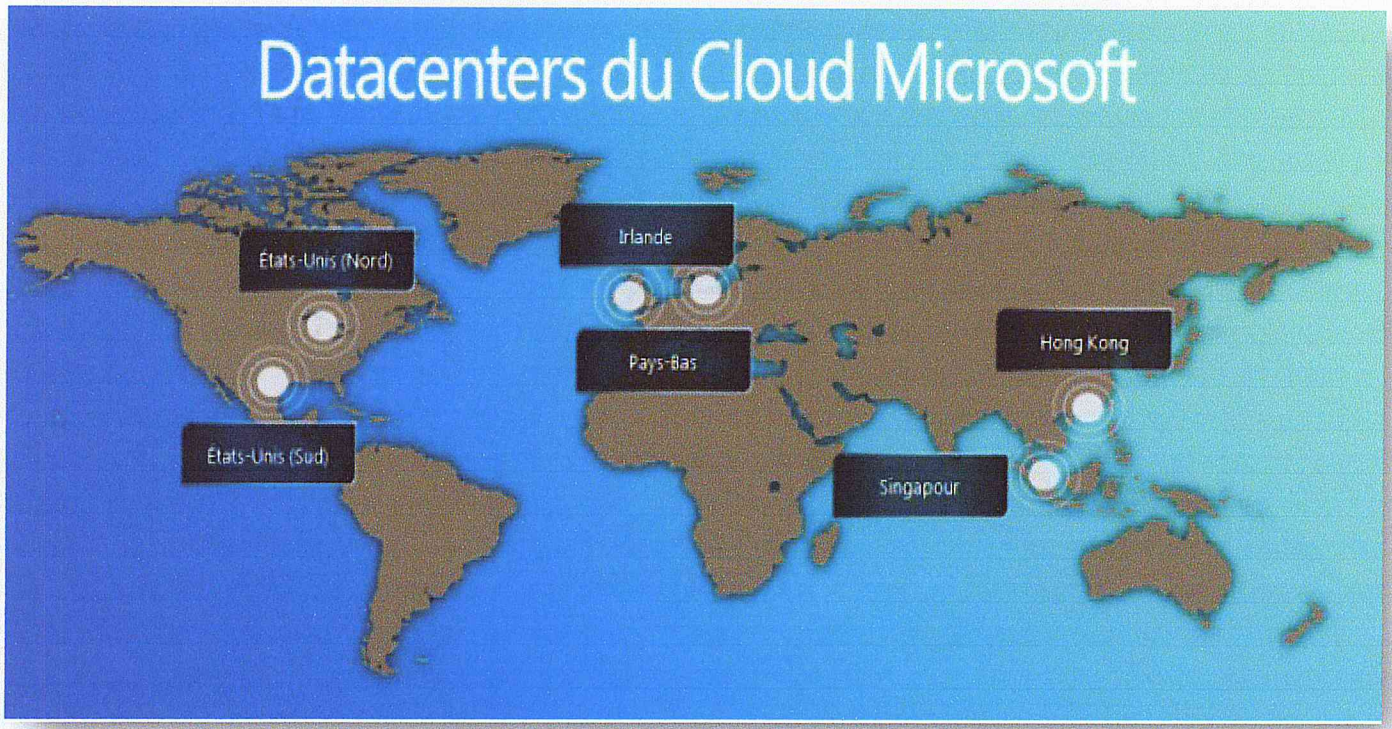


Figure III.10: ***Les Datacenter Windows Azure*** **[21]**

VI. Amazon Web Services :

« Amazon Web Services » (AWS) met à disposition un cloud public depuis 2006. Au départ le but d'Amazon était de rentabiliser ses énormes infrastructures requises pour assumer les montées en charge pendant la période de Noël sur leur boutique en ligne. Aujourd'hui Amazon propose de nombreux services en ligne, à commencer par l'IaaS le plus connu : Elastic Compute Cloud (EC2).

1. Présentation de la solution IaaS : Amazon EC2

EC2 est une des solutions pionnières en matière de « Cloud Computing ».
Basé sur les produits de virtualisation XEN qui permet à ses clients de louer à l'heure des machines virtuelles Linux ou Windows nommé « instance ». [20,23]

a. C'est quoi Une instance EC2

Une instance EC2 est un serveur virtuel d'une capacité donnée,
Permettent d'exécuter des applications comme MySQL Enterprise, Oracle Database 11g, Hadoop, Apache HTTP ou IBM WebSphere Portal Server. Sur ces serveurs virtuels les clients d'Amazon peuvent aussi exécuter des centaines d'autres applications ou leurs propres applications.

Tel qu'une instance EC2 possède un disque dur, ou du moins un espace de stockage équivalent à un disque dur. Mais ce stockage n'est pas pérenne, il a la même durée de vie que l'instance. [23]

En termes de capacité matérielle, il existe différents types d'instances EC2, distinguées par leur puissance CPU et d'autres caractéristiques. [23]

Amazon met à disposition un catalogue de machines virtuelles prêtes à l'emploi, nommées les « Amazon Machine Images » (AMI). [5]

b. C'est quoi AMI

Une *Amazon Machine Image* (AMI) est le regroupement, au sein d'une même unité, d'un système d'exploitation, des logiciels applicatifs, et des paramètres de configuration associés. [24]
Un grand nombre d'AMI sont déjà préconfigurée et prêtes à l'emploi avec différents systèmes d'exploitations disponibles dont Windows Server, Ubuntu, RedHat, OpenSolaris, Oracle Enterprise Linux... Avec chaque AMI des logiciels sont présent pour la gestion d'une base de données (IBM DB2,

MySQL ...) , l'hébergement web, le développement d'applications, l'encodage et la diffusion en continu de vidéos etc.[27]

Il existe des API permettant de configurer et de superviser les ressources EC2 depuis des logiciels de management tiers ou bien directement depuis la console de management Web d'Amazon : la « AWS Management Console ». AWS management Console (Figure 1). [5]

Pour utiliser Amazon EC2, il suffit de :

- ✓ Sélectionner une image préconfigurée, avec un modèle afin de démarrer immédiatement. Ou créer une Amazon Machine Image (AMI) contenant votre application, vos bibliothèques et données, et vos paramètres de configuration associés.
- ✓ Configurer la sécurité et l'accès au réseau sur votre instance Amazon EC2.
- ✓ Choisir quel(s) type(s) d'instances et quel système d'exploitation vous voulez, puis démarrer, arrêter et surveiller autant d'instances de votre AMI que nécessaires, à l'aide des API (Application Programming Interface) de service Web ou la variété d'outils de gestion proposés.
- ✓ Déterminer si vous voulez exécuter dans plusieurs emplacements, utiliser des points de terminaison d'IP statique, ou annexer du stockage persistant par bloc à vos instances.
- ✓ Payer seulement les ressources que vous consommez, comme les heures-instance ou le transfert de données. » [25]

Avec EC2 Amazon offre un certain nombre d'autres services à ses clients pour construire une solution capable de monter en charge et d'éviter les pannes.

• **« Amazon Elastic Block Store »**

Permet de conserver un espace de stockage indépendant des instances serveurs. Cet espace disque est partagé entre toutes les instances actives.[29]

- **« Multiple Locations »**

Permet de choisir le lieu d'hébergement de ses instances parmi trois zones (États-Unis côte Est et côte Ouest ou Europe). [29]

Ce service permet d'éviter les pannes liées à un data centre particulier et de réduire le temps de latence réseau pour le client. [29]

- **« Amazon Virtual Private Cloud » (VPC)**

Permet d'accéder à ses instances au travers d'un VPN et offre par conséquent une solution de « Private Cloud . [29]

- **« Elastic Load Balancing »**

Permet de répartir la charge entre les instances d'un même client. [29]

VII. Découvert l'interface d'Amazon

Dans cette partie nous allons présenter quelques interfaces d'Amazon aws

1. Création d'un compte

Avant de pouvoir profiter des services web Amazon, vous devez tout d'abord créer un compte sur **http://aws.amazon.com**.[28]

Cet unique compte vous permettra d'accéder à l'ensemble des services, avec un niveau administrateur sur chacun d'entre eux.

Sur une page intitulée **Sing In or Create an AWS Account**.

Entrez votre adresse mail dans le champ **My e-mail address is** et sélectionnez **I am a new user**. [28]

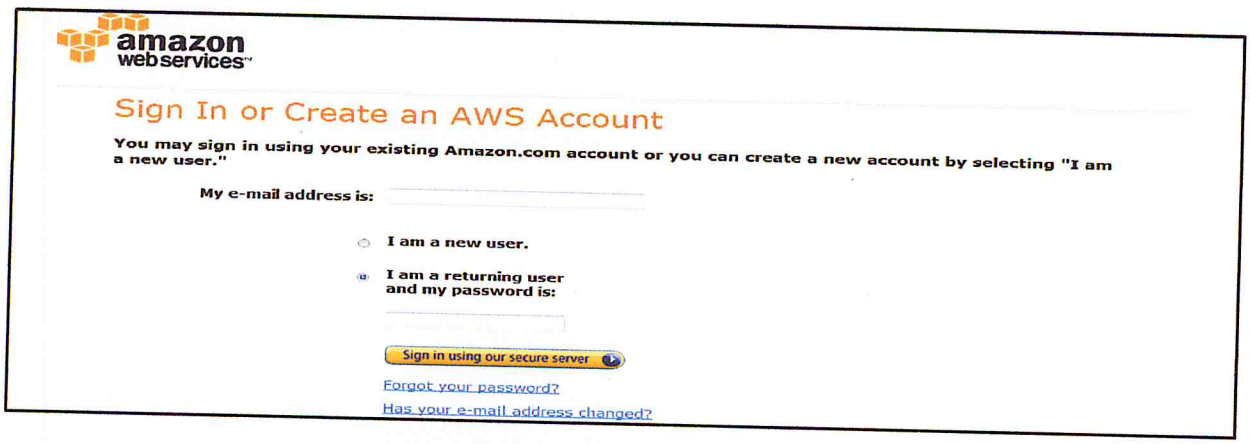


Figure III.11: créer un compte sur AWS. [28]

Lorsque votre compte sera créé, vous pourrez utiliser cette page pour vous identifier en sélection **I am a returning user and my password is** et en entrant votre mot de passe dans le champ correspondant . [28]

Un formulaire en anglais vous invitera à saisir :

- votre nom ;
- votre adresse e-mail ;
- une confirmation de votre adresse e-mail ;
- votre mot de passe ;
- une confirmation de votre mot de passe.

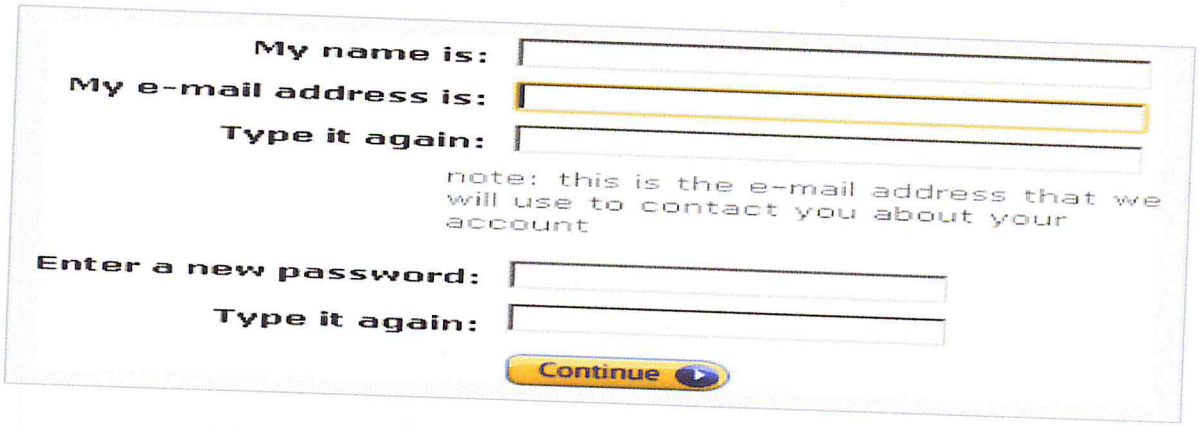


Figure III.12: formulaire d'identifications. [28]

2. Console de management

La console de management est le cœur de l'interface d'administration des services AW

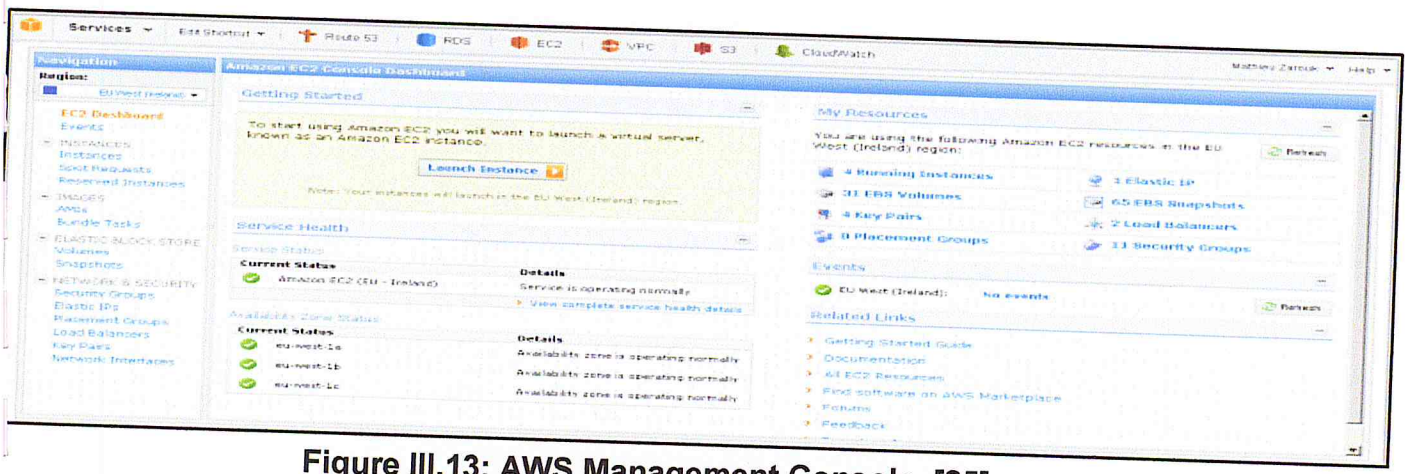


Figure III.13: AWS Management Console. [25]

Cette console peut être décomposée en trois parties :

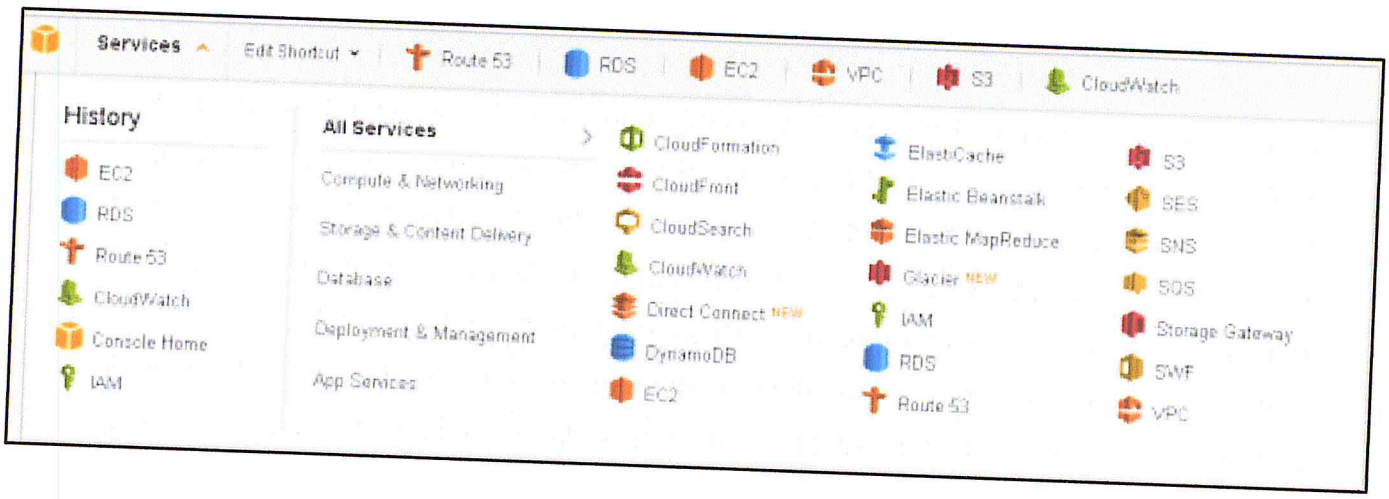


Figure III.14: un bandeau supérieur vous permettant de naviguer entre les différents services AWS. [25]

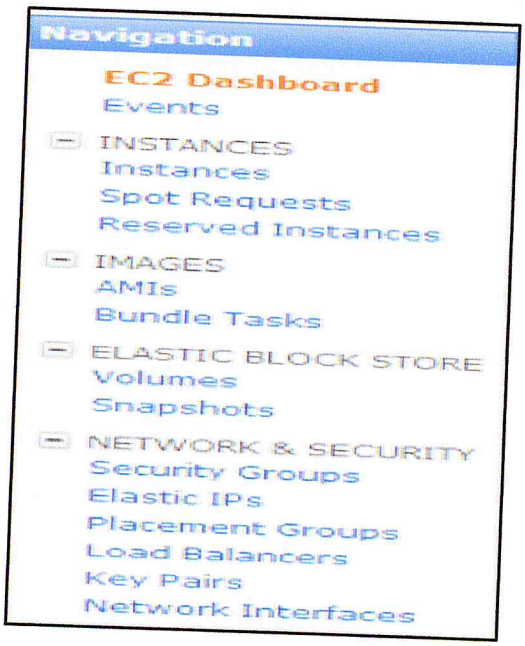


Figure III.15: un panneau latéral gauche permet de naviguer entre les différents panneaux de configuration du service sélectionné. [25]

Figure III.16: menus déroulants permet de sélectionner la région dans laquelle vous travaillez et d'accéder à l'aide en ligne ou l'administration de votre compte. [25]

3. Fonctionnalités d'Amazon EC2

Avec AWS Management Console, les développeurs peuvent commencer et arrêter les instances EC2, afficher et réaliser des actions sur des instances en cours, et gérer des stockages Elastic Block Store d'un simple clic. **[25]**

a. Instances et AMI

Lancez et gérez les instances Amazon EC2. Trouvez, gérez et créez des images machine Amazon (AMI). **[25]**

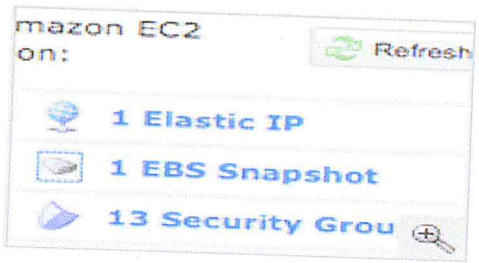


Figure III.17: Instances et AMI. [25]

b. Elastic Block Store

Créez, gérez et effacez des captures d'écran et des stockages EBS. Attachez et détachez des stockages vers les instances Amazon EC2. **[25]**

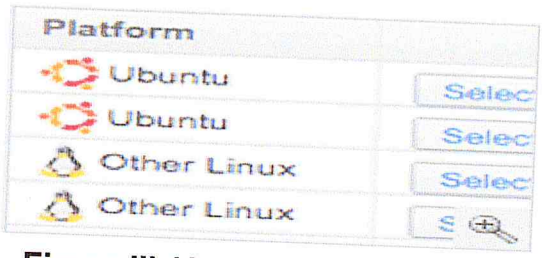


Figure III.18: Elastic Block Store. [25]

c. Contrôler les instances

Autorisez et désactivez les contrôles pour les instances Amazon EC2 et affichez les mesures en temps réel. **[25]**

Figure III.19: Contrôler les instances [25]

d. Instances réservées

Affichez les instances réservées disponibles et achetez-les directement à partir de la console. **[25]**

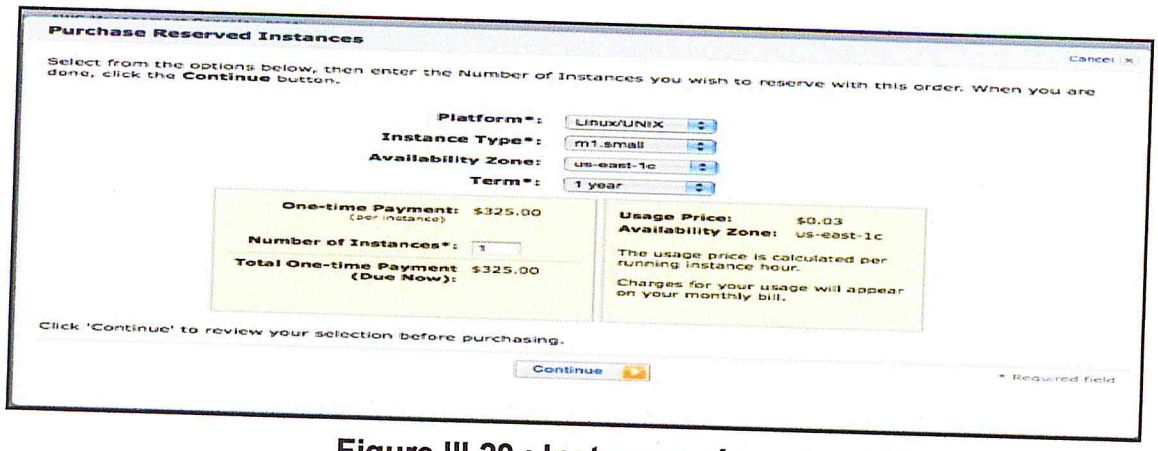


Figure III.20 : Instances réservées. [25]

Pour une utilisation optimale de cette console, Amazon recommande l'utilisation de Mozilla Firefox, Apple Safari, Google Chrome ou Internet Explorer dans ses versions 9 ou supérieures.

VIII. Où est hébergé Elastic Compute Cloud

Les serveurs virtuels constituant Amazon Elastic Compute Cloud sont au cœur des Amazon Web Services. [24]

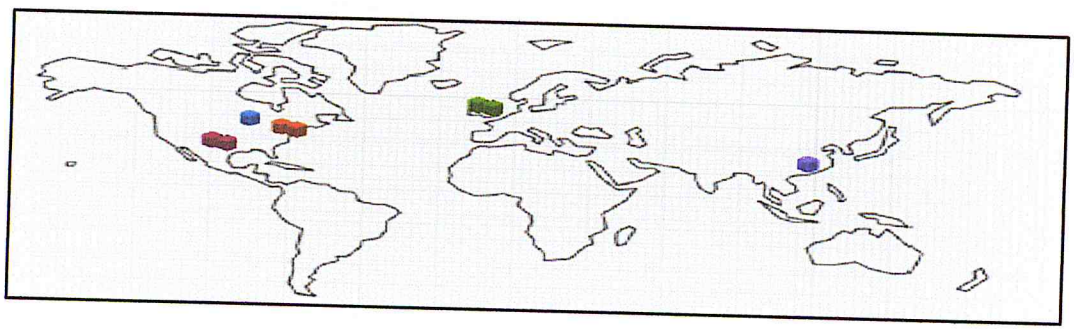


Figure III.21: *Les Datacenter Amazon aws* [26]

Enfin, le Tableau 1 présente un tableau comparatif des 2, en termes de type de service, les principales caractéristiques et les technologies d'infrastructure.

Solutions	Services	Description	Infrastructure
Amazon EC2	IaaS	Intégration de machines virtuelles, existantes ou nouvellement créées via AWS	Xen hyperviseur
Microsoft Windows Azure	PaaS	Est un « SE »dans le cloud plateforme de développement mais aussi et surtout plateforme d'hébergement.	Hyper-V

Tableau .1 : Comparaison entre les solutions de Cloud

XI. Conclusion

Il existe plusieurs solutions pour le Cloud computing. Chacune d'elle présente une vision différente sur l'architecture du Cloud et la mise en œuvre.

Amazon EC2 est une solution robuste qui offre à leur utilisateur, cette flexibilité de configuration. A l'autre extrême, une solution comme Windows Azure, facilite le développement à leur utilisateur.

Chapitre 4
Analyse et conception

I. Introduction

Avec la grande tendance du Cloud computing, aujourd'hui le stockage de données dans le Cloud est devenue l'une des solutions de stockage le plus populaire pour l'informatique d'entreprise.

Le déplacement des données vers le Cloud peut soulager l'entreprise de la charge de stockage des données locales et ces entretient. Malgré ces avantages, la sécurité reste l'un des grands défis du fait que les données des clients ne résident plus dans leur possession physique mais sur des serveurs externes.

Ces données peuvent contenir des informations sensibles qui ne doivent pas être voir par les utilisateurs non autorisées.

Pour cette raison, le contrôle d'accès est essentiel dans tous les systèmes où les données sont partagées entre plusieurs utilisateurs avec différents niveaux de confiance.

Différents modèles de contrôle d'accès sont utilisés, y compris le contrôle le plus commun obligatoire d'accès (MAC), contrôle d'accès discrétionnaire (DAC), et le Contrôle d'accès basé sur les rôles (RBAC).

II. Proposition de la solution

Notre solution vise à mettre en œuvre un système de gestion solide des accès aux sources de données stockées dans un Cloud privé, et nous avons choisi pour réaliser notre solution la politique de contrôle d'accès RBAC (Role Base Access Control).

Notre solution permet de contrôler les utilisateurs grâce à une formule booléenne donnée par le propriétaire de données (*figure IV.4*).tel que cette formule nous définit que seuls les utilisateurs autorisés qui ont l'autorisation d'accéder aux sources de données voulues après le décryptage des données, car les données vont être crypter en attribuant a chaque ressource une clé secrète.

III. Représentation de RBAC

RBAC utilise les rôles tels que décrits précédemment pour gérer les autorisations. Pour cela, les utilisateurs d'un système sont associés à un ou plusieurs rôles définis à l'avance. Lorsque ceux-ci souhaitent effectuer une opération, ils vont activer un ou plusieurs rôles pour ouvrir une session. Ils pourront alors effectuer toutes les opérations permises par les rôles de cette session, grâce aux privilèges auxquels ils sont associés. Cette gestion a de nombreux avantages, puisqu'elle ajoute une couche d'abstraction pour l'affectation des utilisateurs aux privilèges sur les ressources. [30]

Le modèle RBAC définit un ensemble des concepts basiques

- **Rôle (R) :** Un rôle représente de façon abstraite une fonction identifiée dans l'organisation (par exemple, chef de service, ingénieur d'étude, etc.) [31]
- **Permission (P) :** est un ensemble de droits correspondant aux tâches qui peuvent être effectuées par un rôle [31]
- **Utilisateur (U) :** est une personne ou entité autorisée à interagir avec le système à travers un ou plusieurs rôles affectés.
- **Objet (o):** Les objets désignent les données informatiques à protéger. [32]
- **Opération :** les opérations sont les actions à réaliser sur les objets. [32]

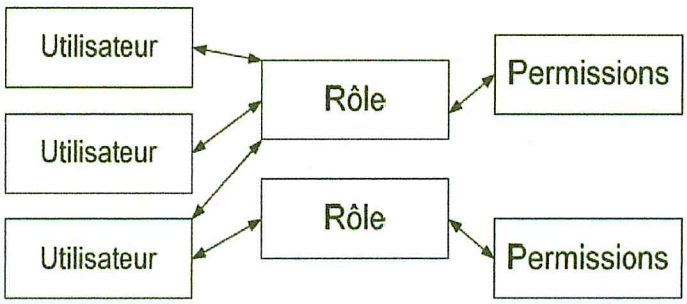


Figure IV .1 : Positionnement de la notion de rôle dans le fonctionnement de RBAC. [31]

Des associations impliquent ces concepts :

- l'affectation des utilisateurs aux rôles (UA)
- les permissions aux rôles (PA).
- Les utilisateurs obtiennent les permissions accordées aux rôles qu'ils jouent. [32]

Le modèle entité-association décrit par la Figure VI.2 présente deux relations, « *détient* (*rôle, permission*) » et « *joue* (*sujet, rôle*) », qui définissent précisément les permissions accordées à chaque sujet.

Un rôle peut détenir plusieurs permissions et une même permission peut être détenue par plusieurs rôles.

De même, un sujet peut jouer plusieurs rôles et, inversement, un rôle peut être joué par plusieurs sujets.

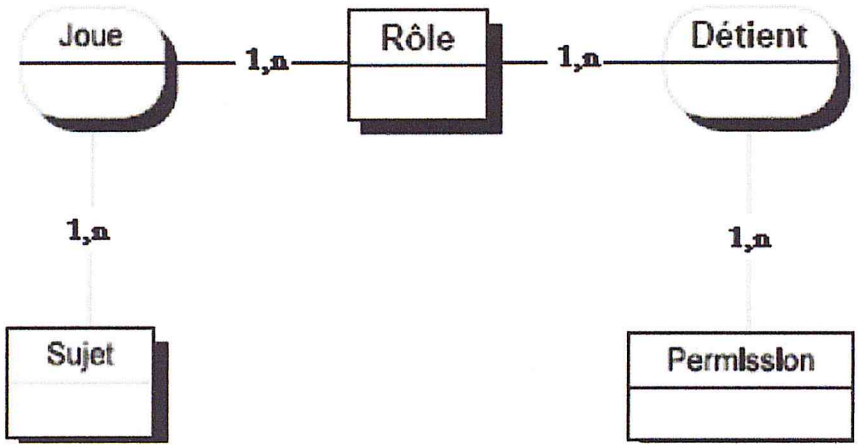


Figure IV.2 : La relation « détient » et la relation « joue » [31]

IV. Contrainte

Ce modèle met en place des contraintes pour éviter le conflit d'intérêts.

Par exemple, un utilisateur n'a pas le droit de jouer le rôle de l'enseignant et d'étudiant lors d'une opération.

V. Description formel de RBAC

Modèle comporte les éléments suivants:

- u, r, p, des utilisateurs, des rôles, des permissions respectivement.

➢ Pour chaque utilisateur, le rôle actif est celui que l'utilisateur utilise actuellement:[33]

AR (u: utilisateur) = {le rôle actif pour u}

➢ Un ou plusieurs autorisations peuvent être attribuées à chaque rôle:
PA (r: rôle) = {autorisations attribuées à r}

➢ Un ou plusieurs rôles peuvent être affectés à chaque utilisateur:
RA (u: utilisateur) = {rôles assignés à u}

➢ Le prédicat permettre (u, p) est utilisé pour indiquer si l'utilisateur u a l'autorisation p:

Permis (u: utilisateur, p: permission) = vrai ssi u a p.

Permis de prédicat (u, p) est utilisé pour indiquer si l'utilisateur dispose de l'autorisation u p:

Trois règles de base sont nécessaires:

1) L'utilisateur doit sélectionner un rôle avant de recevoir l'autorisation:
   ∀ u: utilisateur, p: autorisation (permis (u, p) ⇒ AR (u) ≠ φ)

2) un utilisateur peut seulement activer un rôle qui est affecté à lui
   ∀ u: user, (AR (u) ⊆ RA (u))

3) Un utilisateur a une autorisation que si la permission est autorisée pour le rôle actif de l'utilisateur

   ∀ u: utilisateur, p: autorisation (permis (u, p) ⇒ p ∈ PA (AR (u))).

VI. Les règles de contrôle d'accès

L'application des règles de contrôle d'accès permet d'assurer que les sujets possèdent uniquement les droits d'accès qui leur ont été octroyés sur les objets. [34]

Dans une règle de contrôle d'accès nous trouvons les paramètres suivants :

- ✓ Le *sujet* qui peut être un utilisateur, une machine, un processus, un programme, etc.
- ✓ L'objet qui peut être un fichier, une base de données, une machine, un programme, etc.
- ✓ le *droit d'accès* qui désigne l'effet recherché lorsqu'un sujet accède à un objet (lire, écrire, modifier, etc.). [34]

Le système de contrôle d'accès doit évaluer ces paramètres et selon l'évaluation générer une décision. Cette décision peut être positive pour permettre l'accès à l'objet ou négative pour y refuser l'accès.

VII. Le stockage des données dans un Cloud privé

1. Les étapes de stockage des données dans le Cloud privé

Il ya trois étapes :

1) L'externalisation des données
2) Le stockage des données
3) La récupération des données

2. Architecture de base

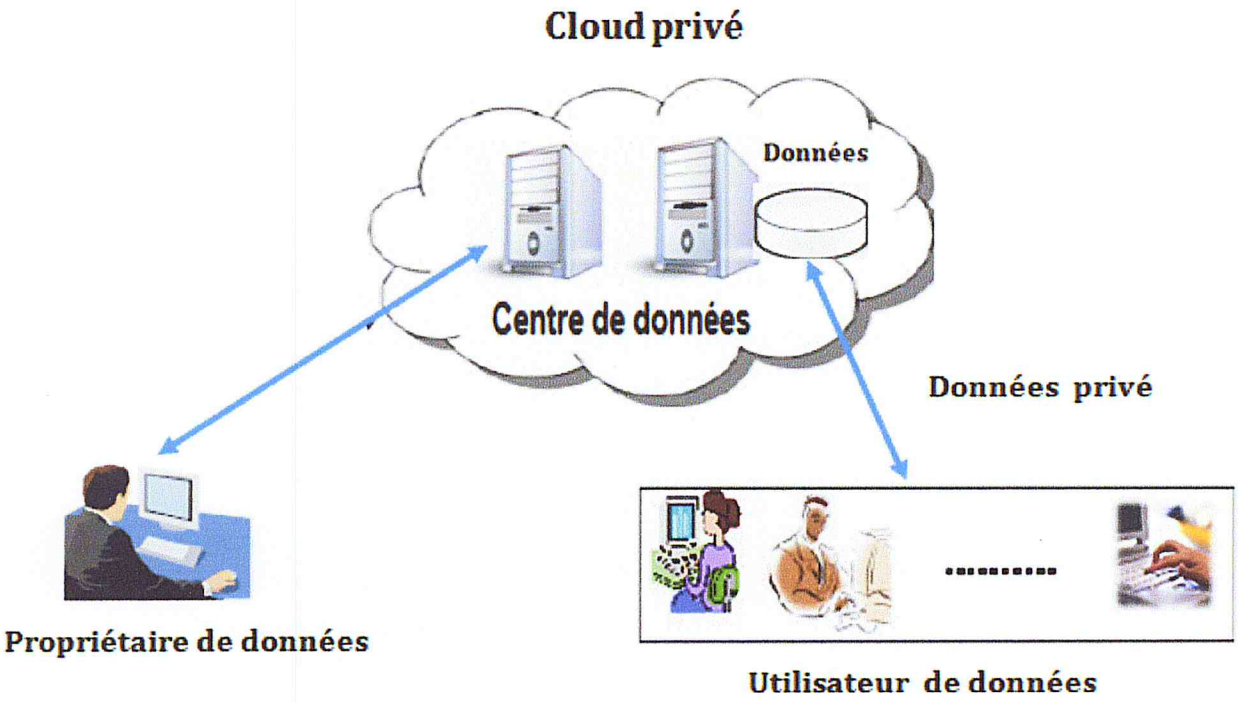


Figure IV.3 : Architecture de stockage de données dans un Cloud privé

L'architecture de base se compose des acteurs suivants :

- **Cloud privé :** Il stocke les données qui peuvent accéder que par des utilisateurs autorisés.

- **Données privé :** Désignent les données à protéger.

- **Centre de données :** Un espace de stockage (serveurs de stockage en nuage) important, qui est géré par le fournisseur de services Cloud.

- **Propriétaire de données :** Est une entité qui stocke leur donnée dans le Cloud, a tous les droits d'autoriser l'utilisateur et lui donner des droits d'accès en fonction de la politique de contrôle d'accès.

- **Utilisateur de données:** Est une entité qui utilise les données stockée par le propriétaire de données. Ils devraient avoir l'autorisation d'accès. Et les autorisations sont fixées par le propriétaire des données lors du stockage de données en utilisant RBAC dans notre solution proposé.

VIII. Schématisation de la solution proposé

Le schéma suivant illustre l'architecture de notre solution

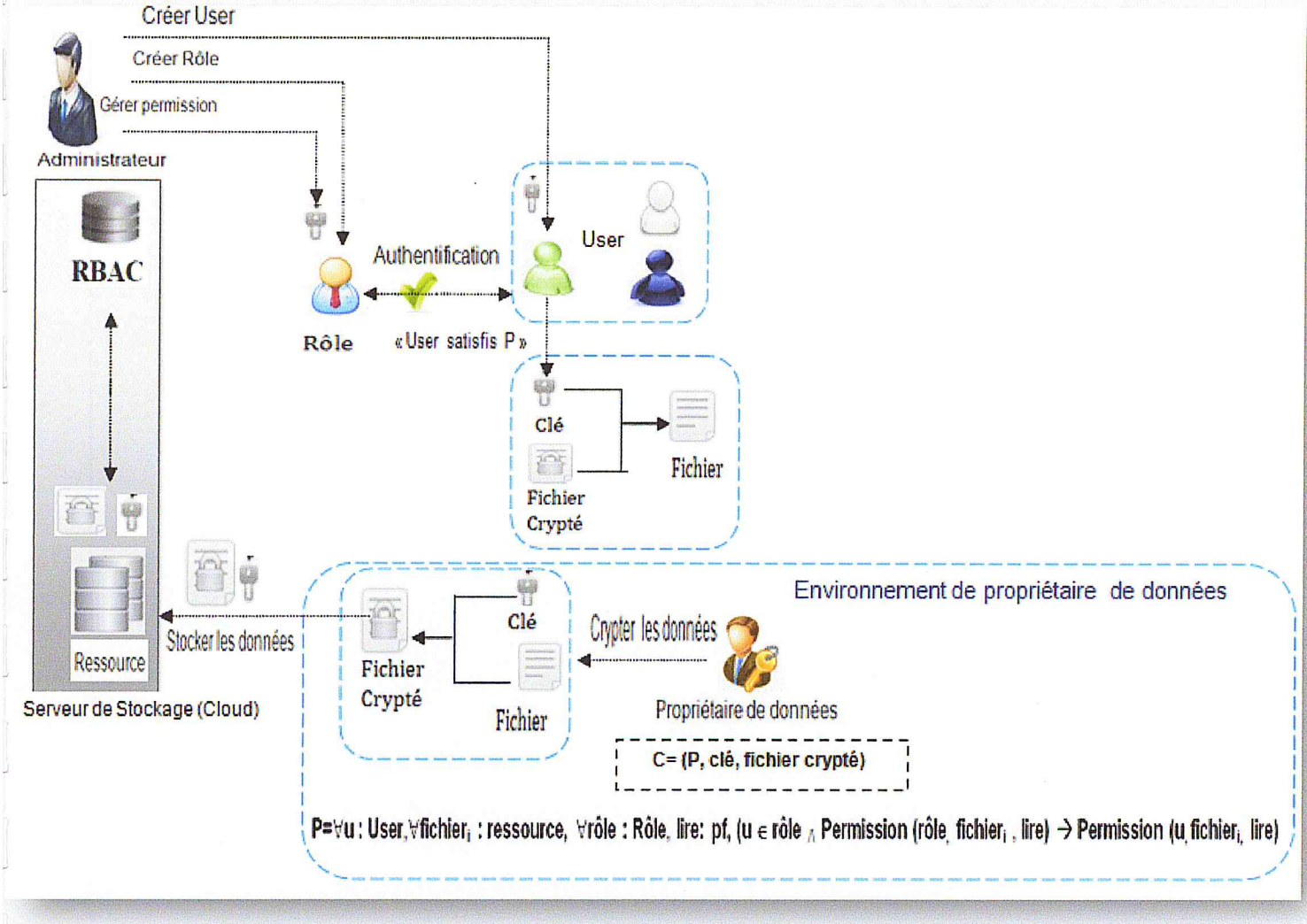


Figure IV.4: Système de sécurité

Toutes les actions pour la gestion des rôles, ne s'appliquent pas au propriétaire de données.

Les règles suivantes doivent être remplies:

Regle1 : Un ou plusieurs rôles peuvent être affectés à chaque utilisateur:
RA (u: utilisateur) = {rôles assignés à u}

Regle2 : L'utilisateur doit sélectionner un rôle avant de recevoir l'autorisation:
∀ u: utilisateur, p: autorisation (permis (u, p) ⇒ AR (u) ≠ φ)

Regle3 : Un utilisateur a une autorisation que si la permission
est autorisée pour le rôle actif de l'utilisateur

∀ u: utilisateur, p: autorisation (permis (u, p) ⇒ p ∈ PA (AR (u))).

Le schéma proposé spécifie un système de contrôle d'accès, mettre en œuvre la plupart des fonctionnalités de RBAC. Notre système permet au propriétaire de données à stocker sous forme cryptée dans le nuage et d'accorder l'accès à ces données pour les utilisateurs ayant des rôles spécifiques.

Le système proposé comprend les parties suivantes :

- ✓ **Administrateur** : A tous les droits d'autoriser l'utilisateur et de lui donner les droits d'accès en fonction de la politique et maintient sa renseignements confidentiels d'autres utilisateurs non autorisés.
- ✓ **Propriétaire de données :** Qui stocke leur donnée dans le Cloud
- ✓ **User :** Représente l'ensemble des utilisateurs de système.
- ✓ **Rôle** : Un ensemble des rôles que ces utilisateurs peuvent avoir.
- ✓ **Ressource:** Un ensemble des données qui doivent être partagés avec les autres utilisateurs de notre système.
- ✓ **P :** Représente la formule d'accès proposé par le propriétaire de données.
- ✓ **Permission:** Il s'agit de deux types de permission dans notre proposition:
  a) La capacité de lire des fichiers.
  b) La capacité écrire des fichiers.

Nous allons utiliser :

« **Permission F** » pour indiquer la permission de lecture sur le fichier **F**.

« **Permission E** » pour indiquer la permission de l'écriture sur le fichier **F**.

Nous supposons que les permissions d'écriture sont données au propriétaire de données, et les autres utilisateurs que le propriétaire de données devrait recevoir l'autorisation de lecture seulement.

IX .Etude conceptuelle

Afin d'effectuer la conception de notre système, nous avons opté pour une démarche orientée OBJET « UML » (Unified Modelling Langage) et Le processus que nous vous proposons de suivre pour le développement est UP (Unified Process).

1. UML :

UML se définit comme un langage de modélisation graphique et textuel destiné à comprendre et décrire des besoins, spécifier et documenter des systèmes, indiquer des architectures logicielles, concevoir des solutions et communiquer des points de vue.[8]

2. Processus unifié UP :

Le processus que nous allons suivre pour le la conception de notre solution est UP (Unified Process), il regroupe les activités amené pour transformer les besoins d'un utilisateur en système logiciel.

a. Caractéristiques essentielles du processus unifié

- Le processus unifié est à base de composants
- Le processus unifié utilise le langage UML (ensemble d'outils et de diagramme),
- Le processus unifié est piloté par les cas d'utilisation
- Centré sur l'architecture
- Itératif et incrémental

b. Les principes fondamentaux du Processus Unifié (UP)

Le Processus Unifié (UP, pour Unified Process) est un processus de développement logiciel «itératif et incrémental, centré sur l'architecture, conduit par les cas d'utilisation et piloté par les risques»:

- **Itératif et incrémental:** le projet est découpé en itérations de courte durée (environ 1mois) qui aident à mieux suivre l'avancement global. À la fin de chaque itération, une partie exécutable du système final est produite, de façon incrémentale.

• **Centré sur l'architecture:** tout système complexe doit être décomposé en parties modulaires afin de garantir une maintenance et une évolution facilitées. Cette architecture (fonctionnelle, logique, matérielle, etc.) doit être modélisée en UML et pas seulement documentée en texte.

•**Piloté par les risques:** les risques majeurs du projet doivent être identifiés au plus tôt, mais surtout levés le plus rapidement possible. Les mesures à prendre dans ce cadre déterminent l'ordre des itérations.

•**Conduit par les cas d'utilisation**: le projet est mené en tenant compte des besoins et des exigences des utilisateurs. Les cas d'utilisation du futur système sont identifiés, décrits avec précision et priorisés.

c. Le cycle de vie du processus unifié

La gestion d'un tel processus est organisée suivant les quatre phases suivantes: initialisation, élaboration, construction et transition.

✓ **La phase d'initialisation :**

Conduit à définir la «vision» du projet, sa portée, sa faisabilité, son business case, afin de pouvoir décider au mieux de sa poursuite ou de son arrêt.

✓ **La phase d'élaboration :**

Poursuit trois objectifs principaux en parallèle:

•identifier et décrire la majeure partie des besoins des utilisateurs,

•construire (et pas seulement décrire dans un document!) l'architecture de base du système,

•lever les risques majeurs du projet.

✓ **La phase de construction :**

Consiste surtout à concevoir et implémenter l'ensemble des éléments opérationnels (autres que ceux de l'architecture de base). C'est la phase la plus consommatrice en ressources et en effort.

✓ **La phase de transition :**

Permet de faire passer le système informatique des mains des développeurs à celles des utilisateurs finaux.

d. Présentation du cycle de vie d'UP

Le processus unifié répète un certain nombre de fois une série de cycles.

Chaque cycle se traduit par une nouvelle version du système. Ce produit se compose d'un corps de code source réparti sur plusieurs composants pouvant être compilés et exécutés, il s'accompagne de manuels et de produits associés. Pour mener efficacement le cycle, les développeurs ont besoin de construire toutes les représentations du produit logiciel :

Modèle des cas d'utilisations	Expose les cas d'utilisations et leurs relations avec les utilisateurs.
Modèle d'analyse	Détaille les cas d'utilisations et procède à une première répartition du comportement du système entre divers objets.
Modèle de conception	Définie la structure statique du système sous forme de sous systèmes, classes et interfaces. Définie les cas d'utilisations réalisés sous forme de collaboration entre les sous systèmes, les classes et les interfaces.
Modèle de déploiement	Définit les nœuds physiques des ordinateurs et l'affectation de ces composants sur ces nœuds.
Modèle d'implémentation	Intègre les composants (code source) et la correspondance entre les classes et les composants.
Modèle de test	Décrit les cas de tests vérifiant les cas d'utilisations.
Représentation de l'architecture	Description de l'architecture.

Tableau 2: Présentation de cycle de vie de l'UP

X. Spécification des besoins

Cette partie consiste à répondre à la question **« que doit faire le système »** et pour cela UML offre des moyens qui représentent une formalisation très riche :

1. Diagramme de cas d'utilisation

Le Diagramme de Cas d'Utilisation a pour objectif de représenter le système du point de vue utilisateur. *[35]*

On trouve dans le diagramme de cas d'utilisation : les utilisateurs sont appelés acteurs, qu'ils interagissent avec les cas d'utilisation.

Acteur :

Un acteur représente un rôle joué par une personne ou une chose qui interagit avec le système. (la même personne physique peut donc être représentée par plusieurs acteurs en fonction des rôles qu'elle joue). [36]

La Représentation: Il est représenté par un bonhomme

Le nom

- Les acteurs de notre système sont listés ci-dessous :

- **Propriétaire de donnés :** Est une entité chargé de stocker les données dans le Cloud et gérer les formules d'accès en fonction de rôle des utilisateurs.

- **Utilisateur :** Pouvant être n'importe quelle entité ayant un accès au système voulant consulter les données stockée par le propriétaire de données.
- **Administrateur :** Est une entité chargé de gérer l'accès aux données en fonction de rôle affecté aux utilisateurs

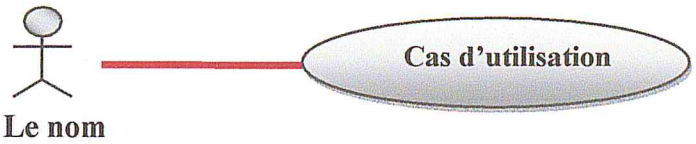
Un cas d'utilisation :

Le cas d'utilisation (ou use case) correspond à un objectif du système, motivé par un besoin d'un ou plusieurs acteurs. L'ensemble des use cases décrit les objectifs (le but) du système. [36]

La Représentation : Il est représenté par

La relation

Elle exprime l'interaction existant entre un acteur et un cas d'utilisation. [36]

La Représentation : Il est représenté par 

Il existe 3 types de relations entre cas d'utilisation :

- ✓ **La relation de généralisation** :

Dans une relation de généralisation entre 2 cas d'utilisation, le cas d'utilisation enfant est une spécialisation du cas d'utilisation parent. [36]

- ✓ **La relation d'extension :**

On dit qu'un cas d'utilisation A étend un cas d'utilisation B lorsque A peut être appelé au cours de l'exécution de B. [37]

- ✓ **la relation d'inclusion :**

Un cas A inclut un cas B si le comportement décrit par A inclut le comportement de B : le cas A dépend de B. [37]

a. Représentation des diagrammes de Cas d'Utilisation de système :

1. Diagramme de cas d'utilisation de propriétaire de données

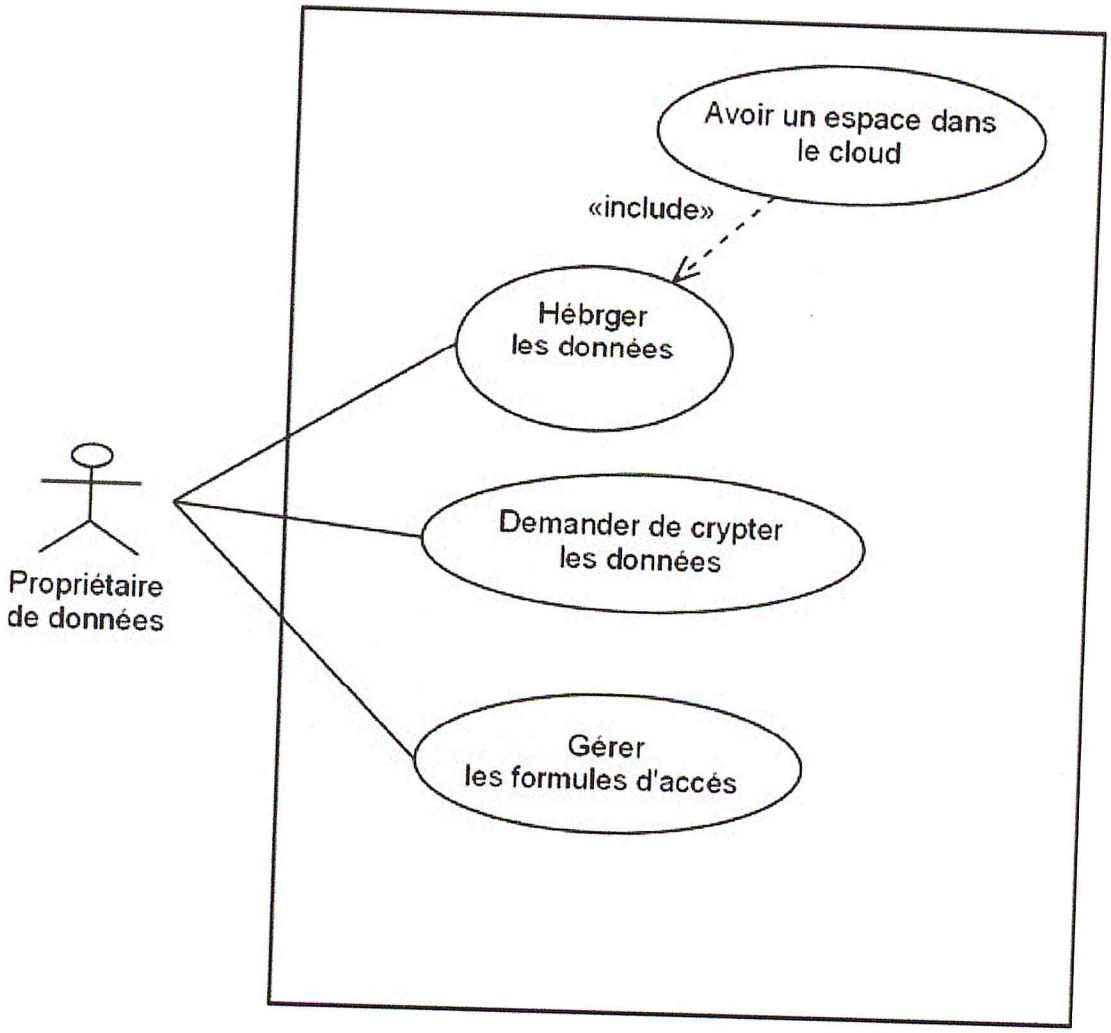


Figure IV.5 : Diagramme de cas d'utilisation de propriétaire de donnés

2. Diagramme de cas d'utilisation d'utilisateur

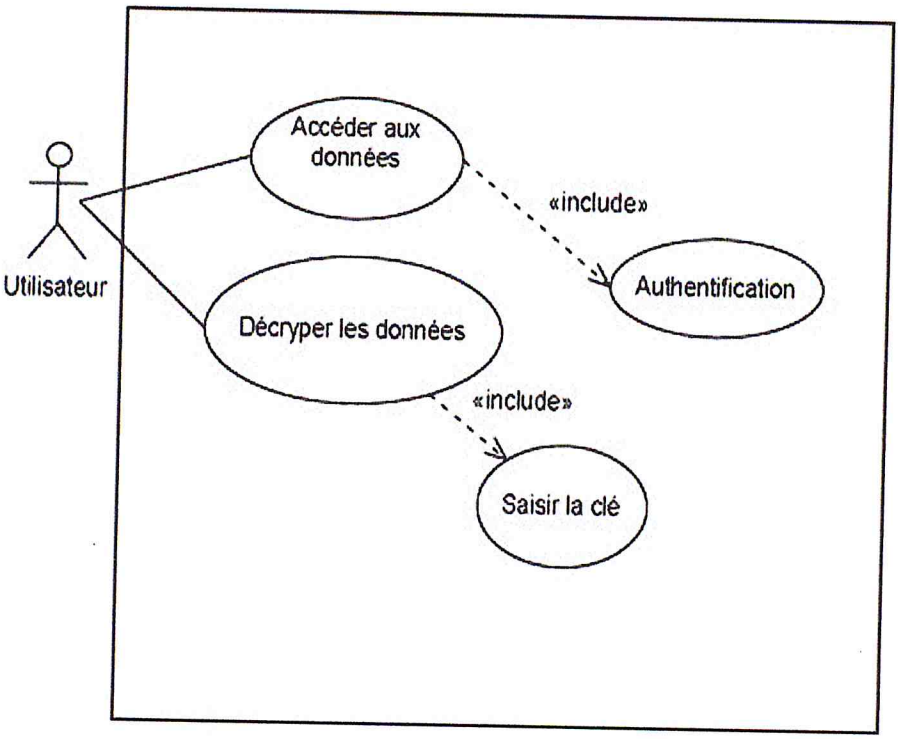


Figure IV.6 : Diagramme de cas d'utilisation d'utilisateur

3. Diagramme de cas d'utilisation d'authentification

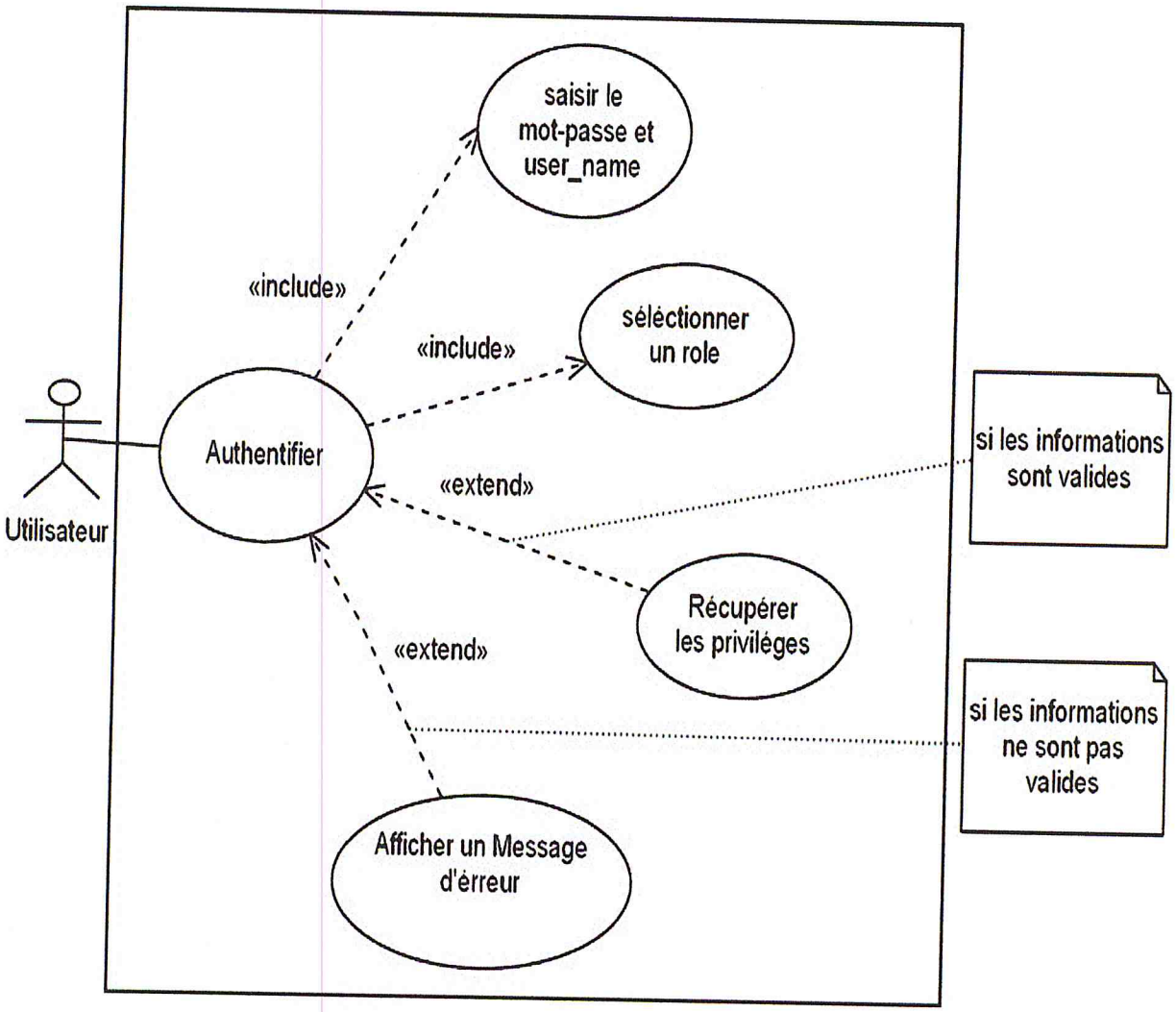


Figure IV.7 : Diagramme de cas d'utilisation d'authentification

4. Diagramme de cas d'utilisation d'administrateur

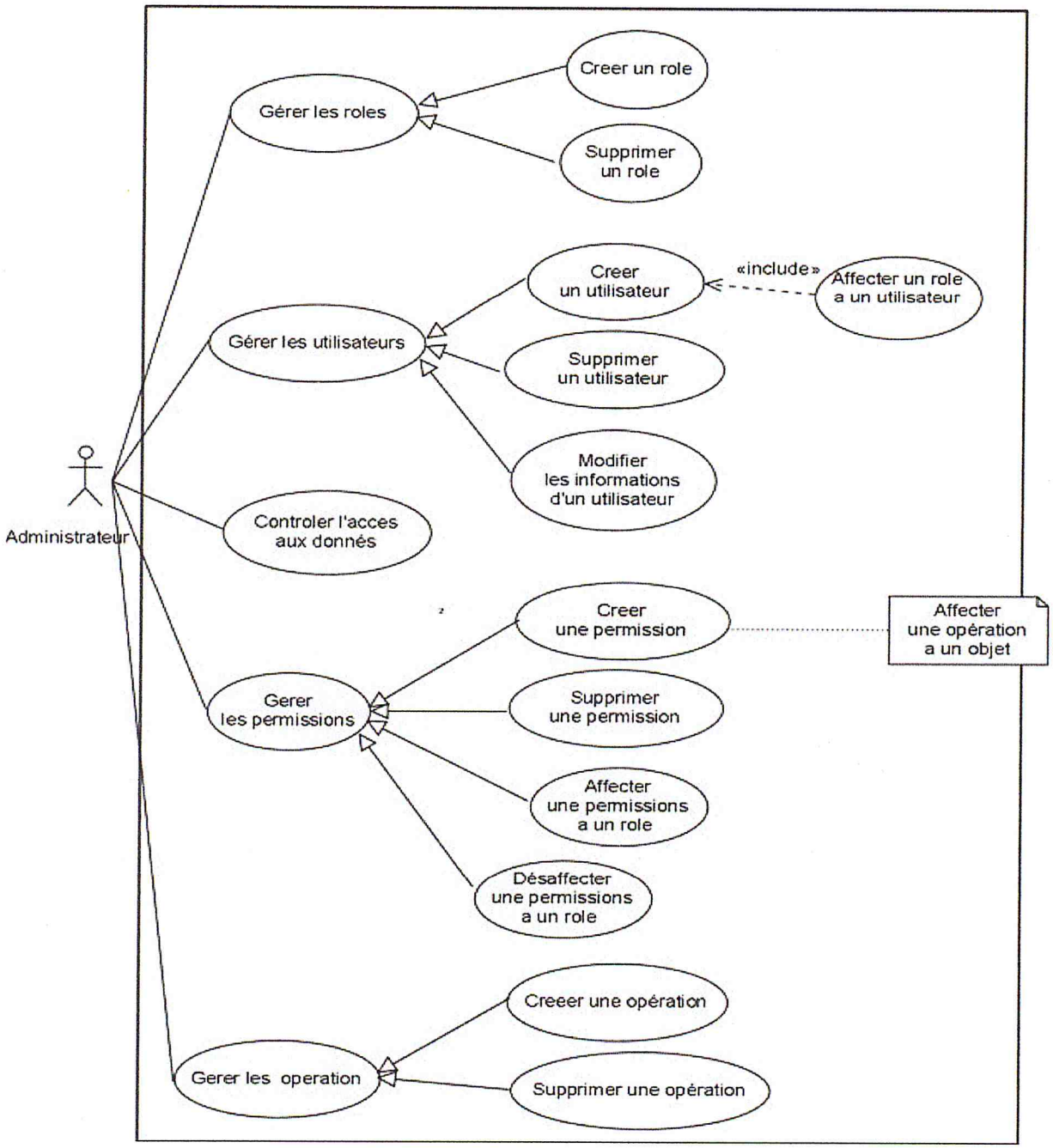


Figure IV.8 : Diagramme de cas d'utilisation d'administrateur

XI. *Analyse des* besoins

Cette partie de modélisation s'agit de spécifier le « quoi ». L'analyse tend à modéliser le comportement dynamique du système en utilisant le diagramme de séquence

1. Diagramme de séquence

Les diagrammes de séquence qui sont une représentation temporelle des objets et de leurs interactions. [35]

Un scénario est une instance d'un cas d'utilisation, autrement dit, à chaque fois qu'une instance d'un acteur déclenche un cas d'utilisation, un scénario est créé.

Symbolique	Signification
	Acteur
Message 	Message
	ligne de vie
	Activation

Table .3: Symbole utilisés dans le diagramme de séquence.

a. Représentation des diagrammes de séquence de système :

1. Diagramme de séquence d'authentification

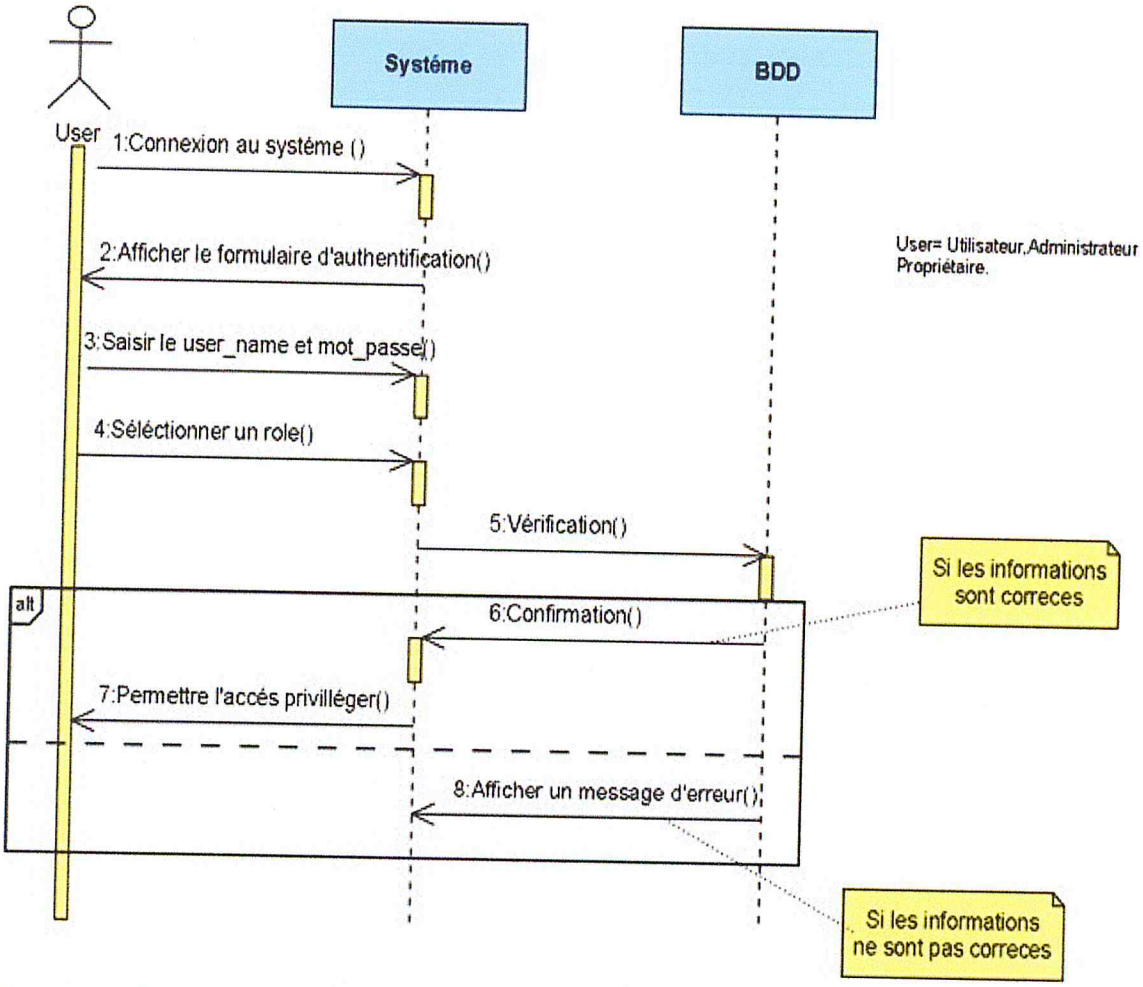


Figure IV .9 : *Diagramme de séquence* d'authentification

Nous donnons ci-dessous la description textuelle détaillée de ce cas d'utilisation :

- **Description du scenario**

1 .L'utilisateur connecte au système.

2. Le système lui affiche un formulaire d'authentification.

3. L'utilisateur saisit son user-name et son mot-passe.

4. l'utilisateur sélectionne un rôle.

5 : Le système vérifie les informations entrées par l'utilisateur.

6 : La confirmation des informations.

7 : Le système permet l'accès de l'utilisateur selon leur privilège.

8 : Sinon si les informations sont erronées le système affiche un message d'erreur.

2. Diagramme de séquence de création d'un rôle

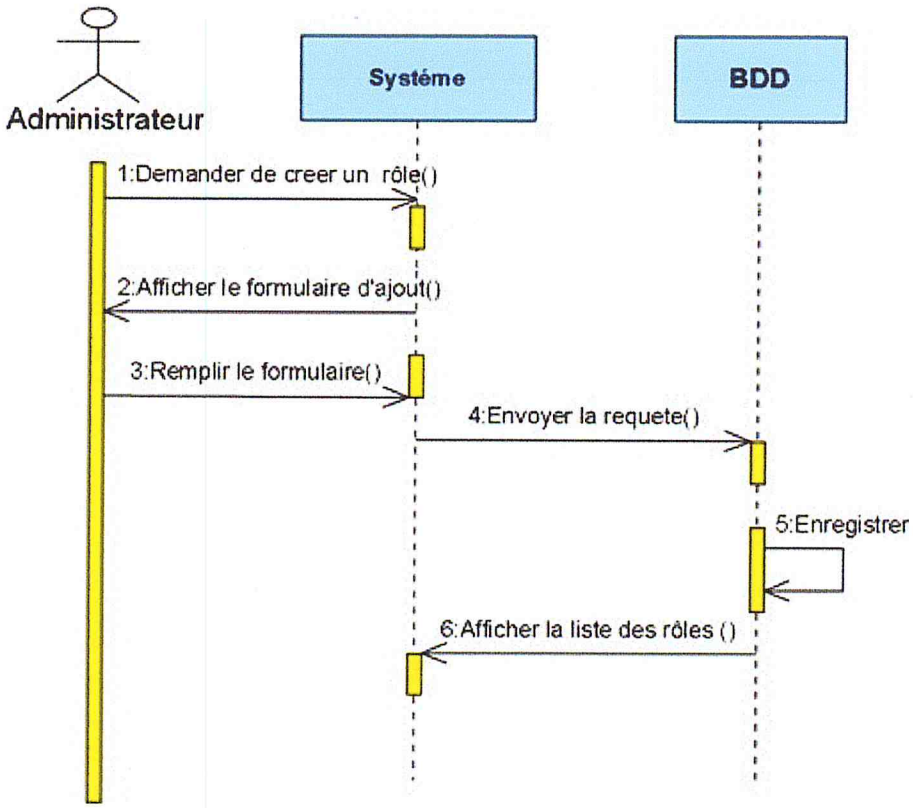


Figure IV .10 : *Diagramme de séquence* de création d'un rôle

Nous donnons ci-dessous la description textuelle détaillée de ce cas d'utilisation :

- **Description du scenario**

1. L'administrateur demande au système de créer un rôle.
2. Le système affiche le formulaire d'ajout.
3. L'administrateur remplie le formulaire d'ajout.
4. Le système envoie une requête au BDD.
5. La BDD enregistre les informations.
6. La BDD affiche la nouvelle liste des rôles.

3. Diagramme de séquence d'affecter d'un rôle à un utilisateur

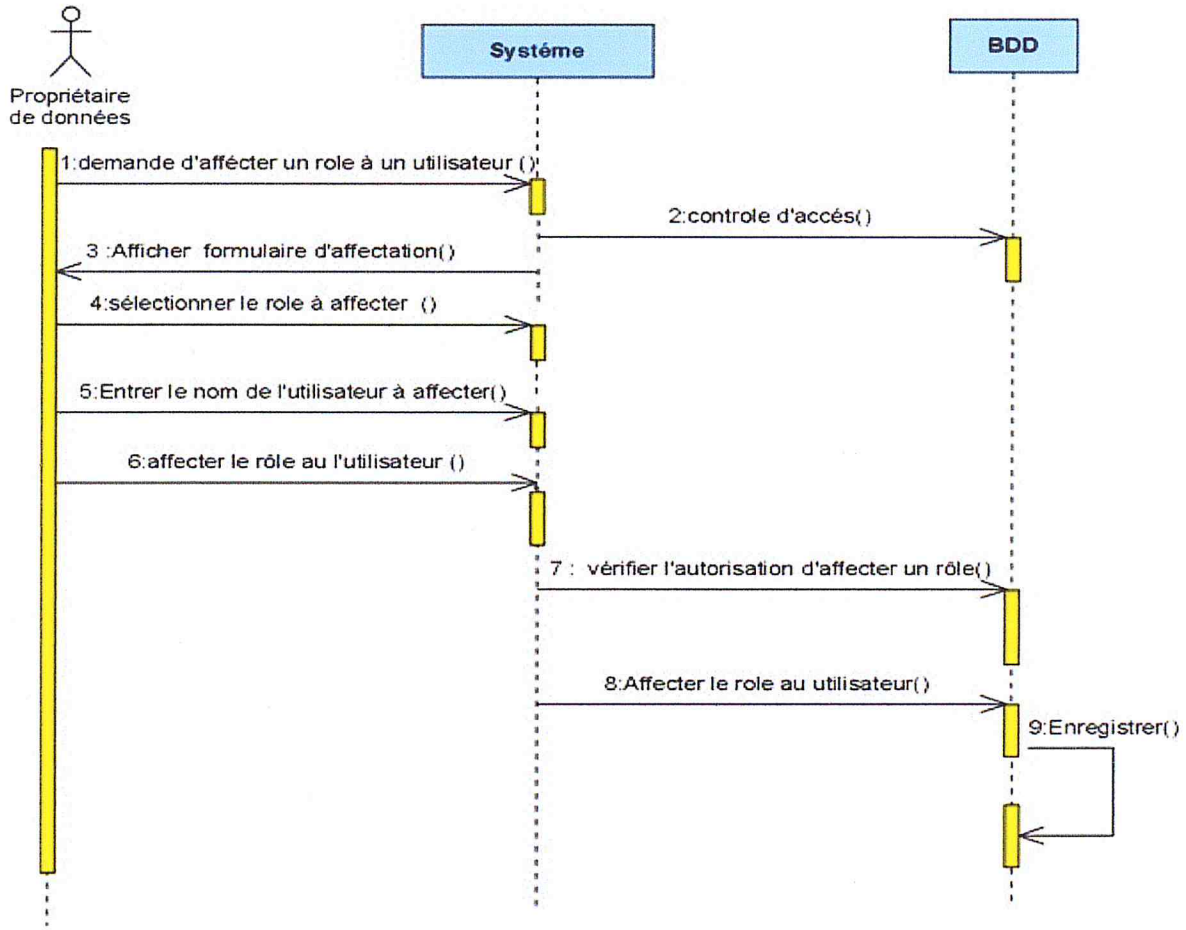


Figure IV .11 : *Diagramme de séquence* d'affecter d'un rôle à un utilisateur

Nous donnons ci-dessous la description textuelle détaillée de diagramme de séquence :

- **Description du scenario**

1. L'administrateur demande au système d'affecter un rôle à un utilisateur.
2. Le système lui affiche un formulaire d'affectation.
3. L'administrateur sélectionne le rôle à affecter.
4. L'administrateur saisit le nom de l'utilisateur.
5. L'administrateur affecte le rôle à l'utilisateur.
6. Le système envoie une requête à la BDD.
7. La BDD enregistre les informations saisie.
8. La BDD affiche la nouvelle liste.

4. Diagramme de séquence de cryptage des données

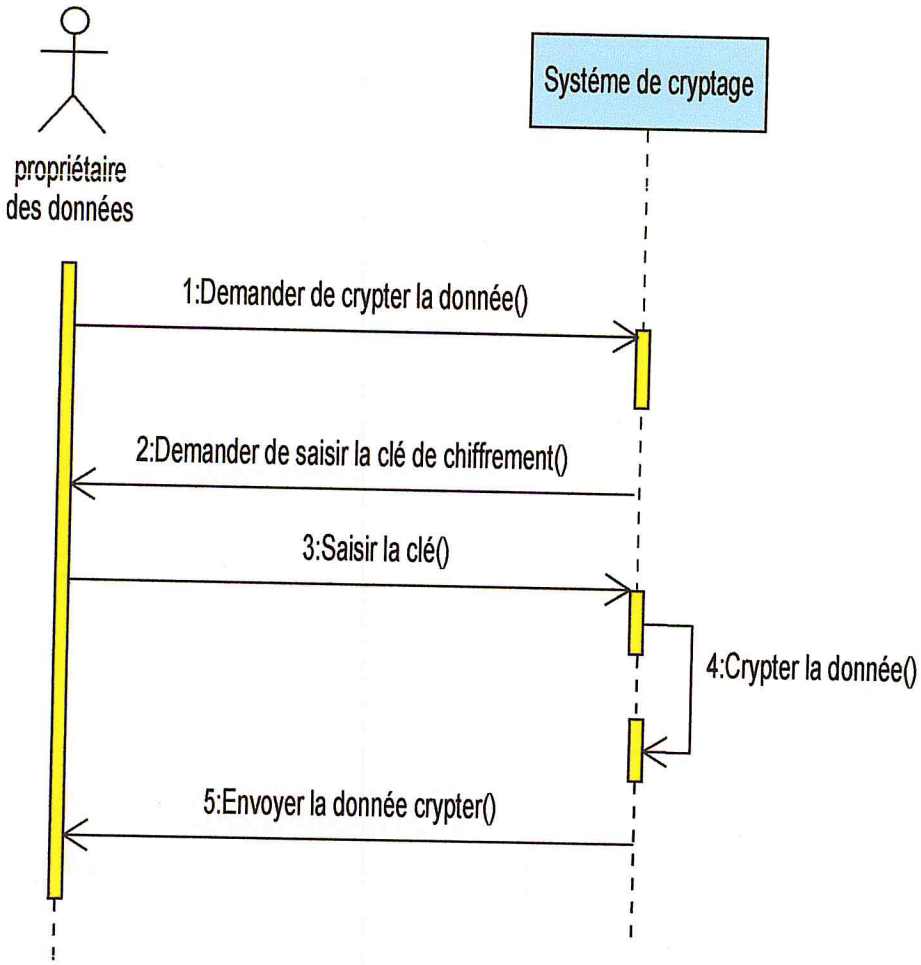


Figure IV .12 : *Diagramme de séquence* de stockage des données

Nous donnons ci-dessous la description textuelle détaillée de diagramme de séquence :

- **Description du scenario**

1. Le propriétaire des données demande au système de crypter les données.
2. le système demande à l'utilisateur de saisir la clé de chiffrement.
3. Le propriétaire des données saisit la clé.
4. Le système crypte la donnée.
5. Le système envoie la donnée crypté à l'utilisateur.

5. Diagramme de séquence de stockage des données

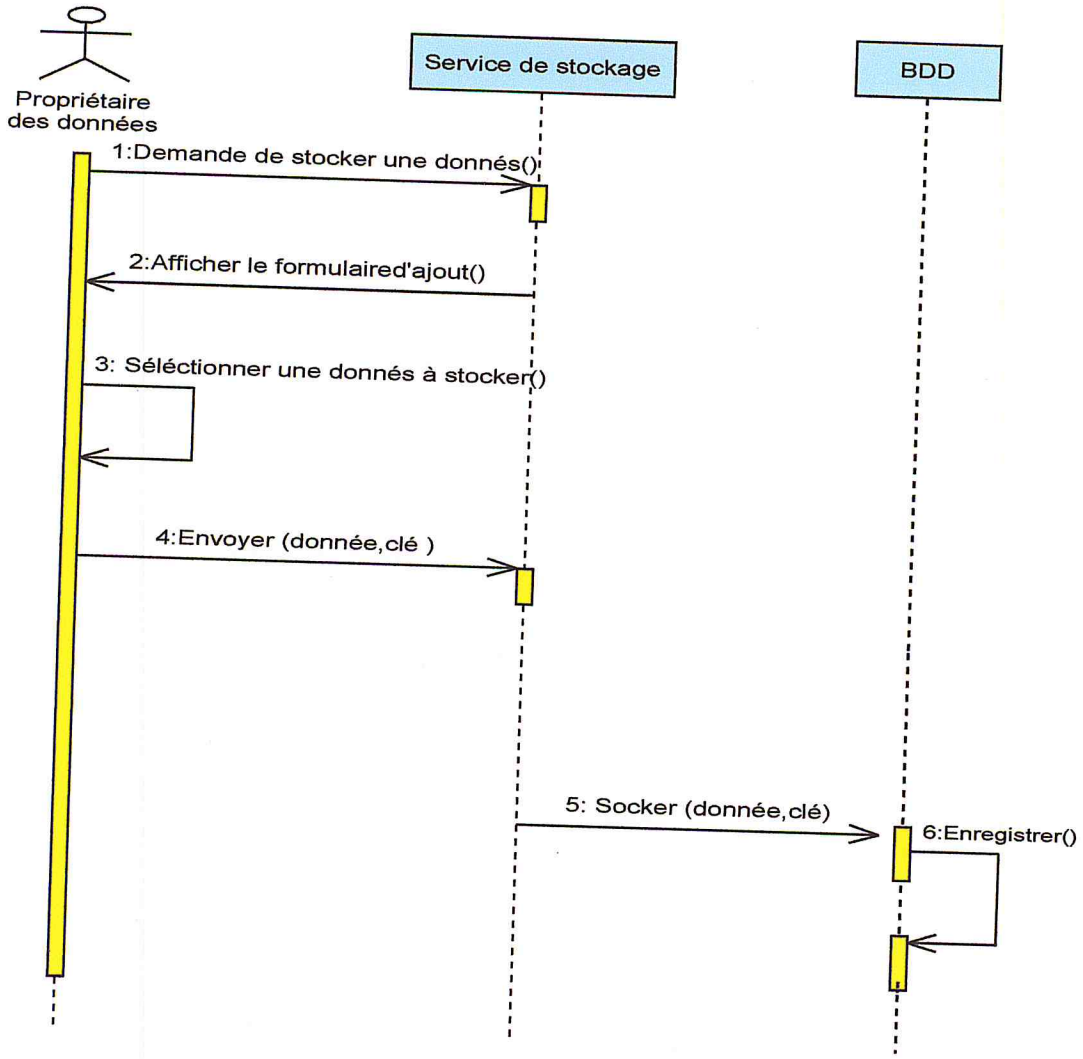


Figure IV .13 : *Diagramme de séquence* de stockage de données

Nous donnons ci-dessous la description textuelle détaillée de diagramme de séquence :

- **Description du scenario**

1. Le propriétaire de données demande de stocker une donnée.
2. le système lui affiche le formulaire d'ajout.
3. Le propriétaire de données sélectionne une donnée.
4. Le propriétaire envoie (donnée, clé).
5. Le système stocke (donnée, clé) dans la BDD.
6. BDD enregistre les données.

XII. Diagramme d'activité

C'est le diagramme qui décrive le comportement d'une méthode. Le déroulement d'un cas d'utilisation, les enchainements d'activités. Une activité désigne une suite d'actions.

SYMBOLE	SIGNIFICATION
	Nœud d'action
	Nœud de décision
	Nœud initial
	Nœud final

Table.4: Symbole utilisés dans le diagramme d'activité.

a. Représentation des diagrammes d'activité de système

1. Diagramme d'activité: « authentifier un utilisateur »

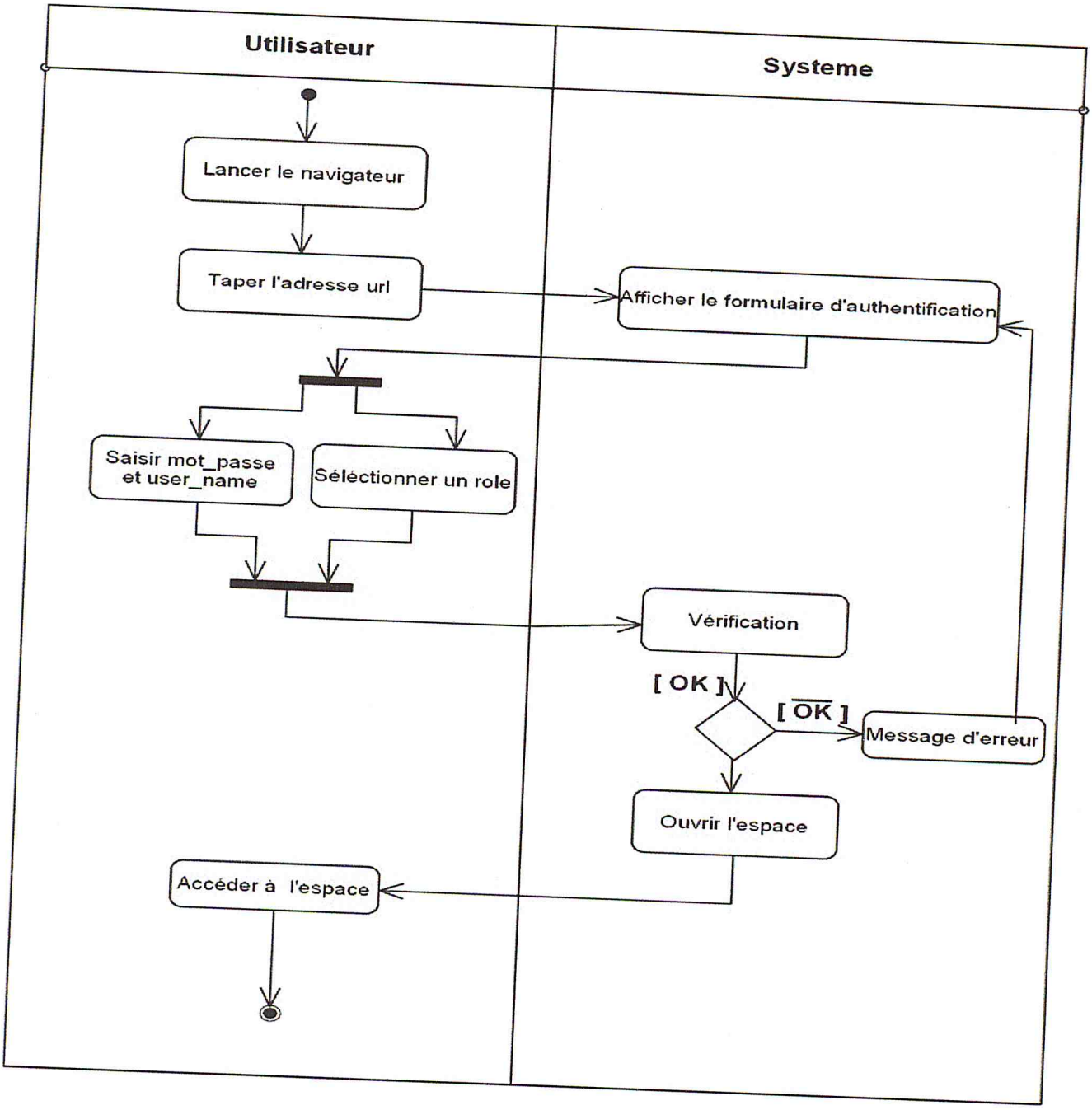


Figure IV .14 : ***Diagramme de d'activité d'authentification***

2. Diagramme d'activité : « supprimer un utilisateur »

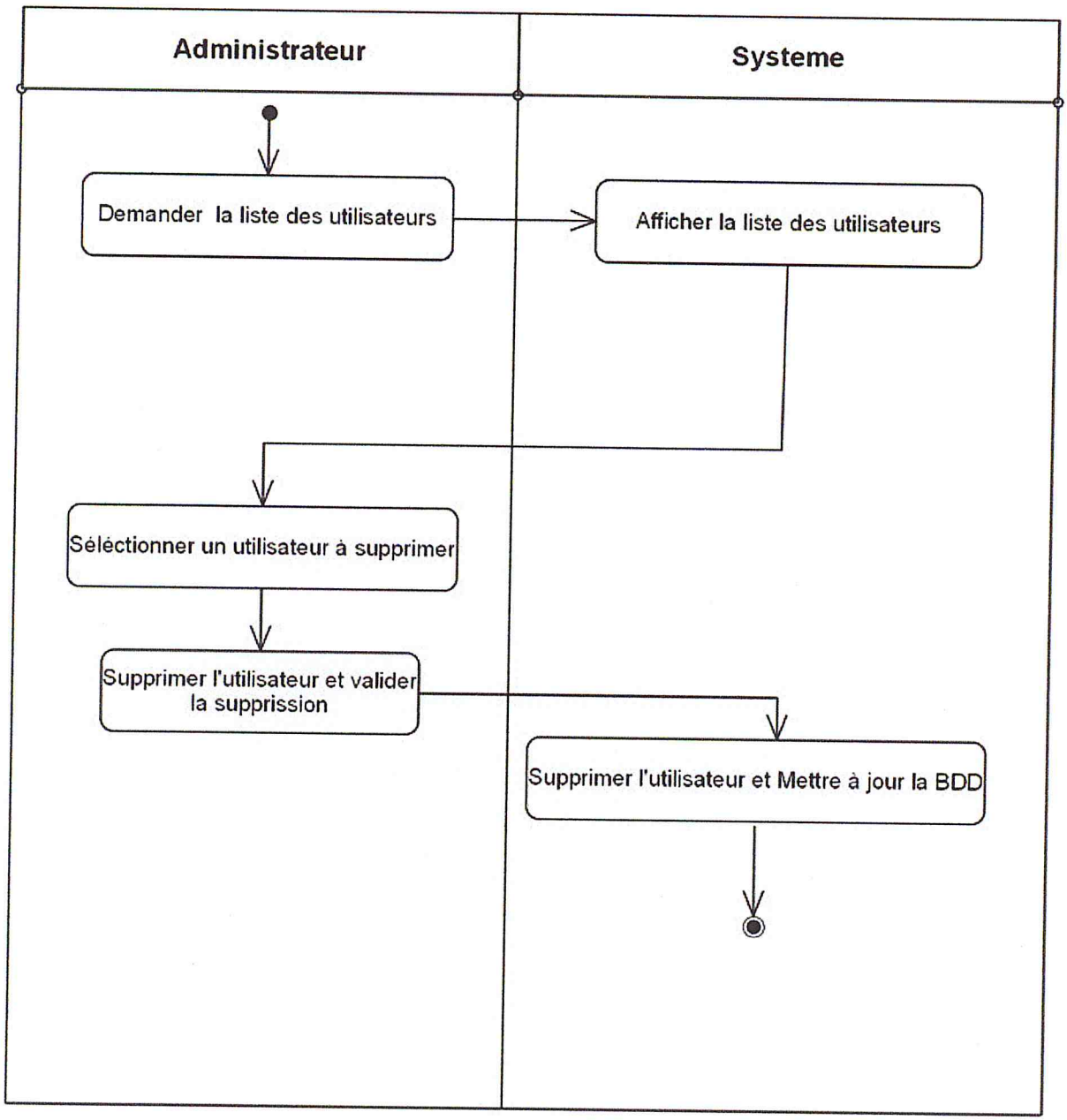


Figure IV .15 : ***Diagramme d'activité : Supprimer un utilisateur***

3. Diagramme d'activité : « Accès aux données »

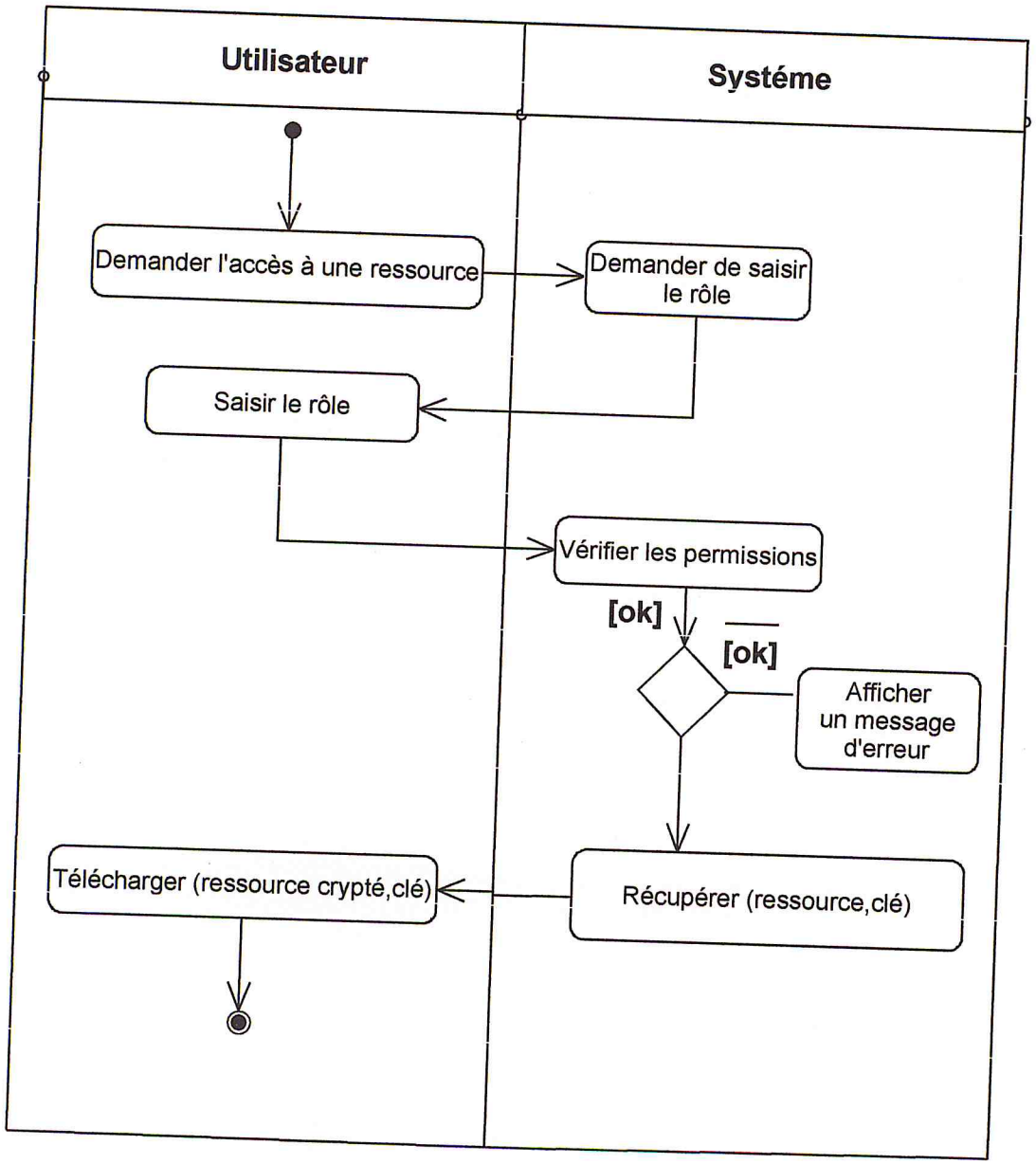


Figure IV .16 : *Diagramme d'activité :* Accès aux données

4. Diagramme d'activité : « Lire les données »

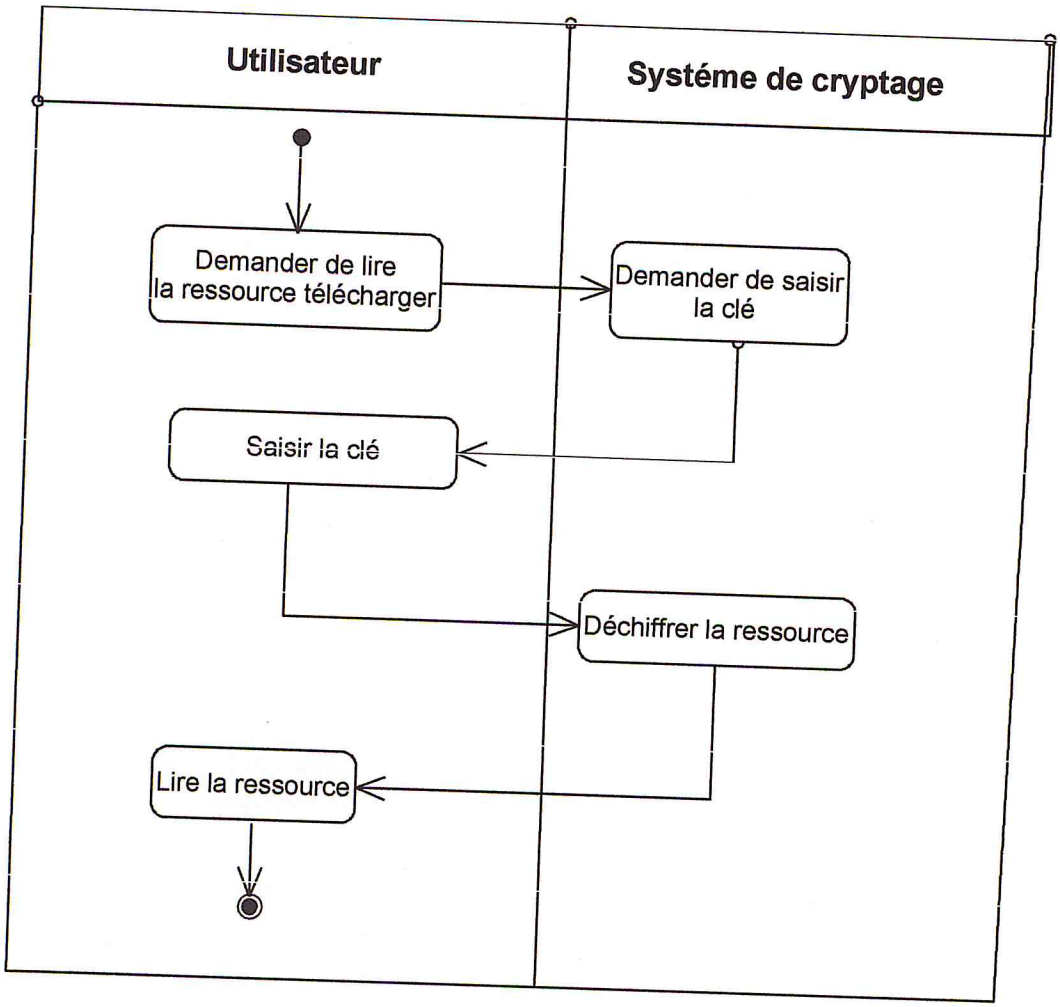


Figure IV .17 : *Diagramme d'activité :* Déchiffrer les données

XIII. Conception

Le modèle statique représente la structure de notre système en termes d'objets et de relations entre ces objets. Il repose essentiellement sur le diagramme des classes et sur les relations (ou associations) issues des cas d'utilisation recensés auparavant.

1. Diagramme de classe

Les digrammes de classes sont sans doute les diagrammes les plus utilisés d'UML.ils décrivent les types des objets qui composent un système et les différents types des relations statiques qui existent entre eux. Les diagrammes des classes font abstraction du comportement du système.

Pour élaborer les diagrammes de classes, on utilisera le formalisme suivant :

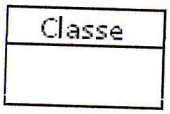
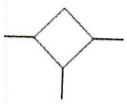
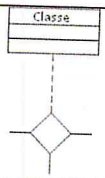
Symboles	Désignation
	Classe
	Association entre classe
	Association n-aire
	Héritage
	Composition
	Classe association

Tableau.5 : Symbole utilisés dans le diagramme de classe

2. Détermination des classes, attributs et méthodes

Nom de la classe	Identifient	Attribut	Méthode
User	**User_ Name**	Nom-U Email-U Mot-passe	Crée ( ) Modifier ( ) Supprimer ( )
Rôle	**Id_ rôle**	Nom_ rôle	Crée ( ) Supprimer ( )
Permission	**Id _ P**	Nom_ P	Crée ( ) Supprimer ( )
Operation	**Id_ OP**	Nom_ OP	Crée ( ) Supprimer ( )
Ressource	**Id_ rs**	File Nom_ File Type Clé	Crée ( ) Modifier ( ) Supprimer ( )

3. Dictionnaire de données

attribut	Désignation	Type
User_ Name	Nom d'utilisateur	Varchar(60)
Nom-U	Mot de passe	Varchar(60)
Email-U	E-mail de l'utilisateur	Varchar(60)
Mot-passe	Mot de passe	Varchar(60)
Id _rôle	Identifient de rôle	Varchar(10)
Nom _rôle	Nom de rôle	Varchar(60)
Id_P	Identifient de permission	Int(10)
Nom_P	Nom de permission	Varchar(60)
Id_OP	Identifient d'opération	Int(10)
Nom_OP	Nom d'opération	Varchar(60)
Id_rs	Identifient de ressource	Int(10)
Nom_File	Nom de ressource	Varchar(60)
File	ressource	BLOB
Type	Type de ressource	Varchar(60)
Clé	Clé de chiffrement de ressource	Varchar(15)

4. Schéma du diagramme de classe

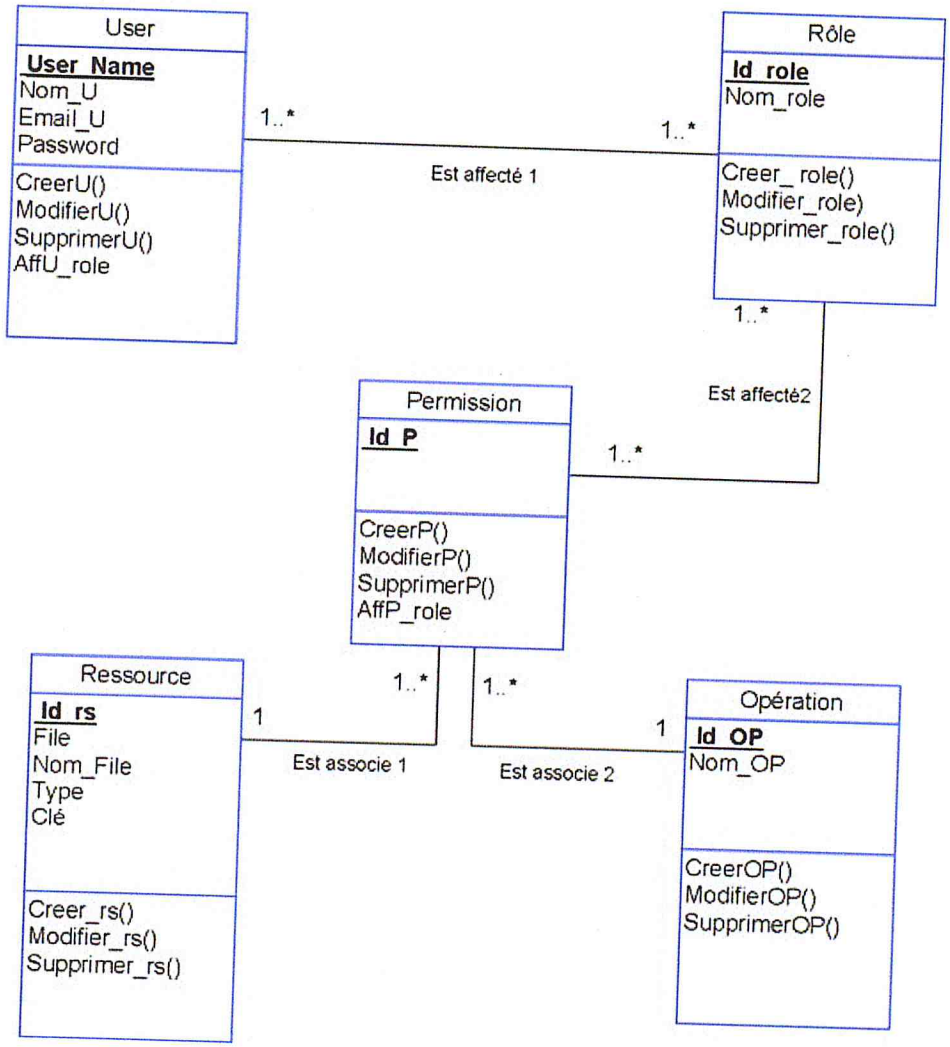


Fig. IV.18 : Diagramme de classe

5. Model relationnel

Règles de passage vers le relationnel :

Du modèle conceptuel au modèle relationnel : à partir de la description conceptuelle que nous avons effectuée, on peut réaliser le modèle relationnel.

NB : pour la notation, nous avons choisi de mettre en gras les clés primaires et de mettre * à la fin de chaque clé étrangère.

N°	Relation	Propriétés et identifiants
01	**User**	**User-Name** Nom-U, Email-U, Mot-passe
02	**Rôle**	**Id_rôle** Nom _rôle
03	**Permission**	**Id_P** Nom_ P, **Id_ rs*, Id _OP***
04	**Opération**	**Id_OP** Nom_OP
05	**Ressource**	**Id_rs** Nom_File, File, Type, Clé
06	**User_ Rôle**	**User_Name** **Id_role**
07	**Permission_Rôle**	**User_Name** **Id_role**

XIV. Conclusion

Ce chapitre regroupe principalement deux objectifs essentielles de notre travail qui sont : la conception de la base de donnée ainsi que la conception de notre application, pour cela nous nous sommes fixer, des étapes, ainsi que des concepts par les quels nous avons du passer pour y arriver.

Reste après cela la réalisation et l'implémentation de notre application, qui sera l'objet de notre prochain chapitre.

Chapitre 5
Implémentation

I. Introduction

La phase d'implémentation donne une description technique du système conçu. Elle permet de présenter l'architecture matérielle de ce dernier, ainsi de décrire les techniques utilisées dans sa réalisation.

Notre solution est réalisée sur un environnement virtuel de deux machines reliées dans un réseau local LAN (Local Area Network)

II.Architecture de déploiement

Notre application est destinée à être utilisée sous la forme d'application Client/serveur. Pour notre cas, nous avons utilisé l'architecture client serveur à trois tiers.

III. Matériel utilisé

PC portable Dell qui possèdent comme caractéristiques :

- Un processeur Intel Pentium® Core2 Duo, 2.49 GHz.
- Une mémoire vive de 3Go.
- Un disque dur 250 Go.
- Un écran 15 pouces.

IV.Outils utilisés

- **VM Ware Workstation**

C'est la version station de travail du logiciel. Il permet la création d'une ou plusieurs machines virtuelles au sein d'un même système d'exploitation . [38]

- **System d' exploitation**

- Windows XP

Windows® XP constitue l'innovation la plus importante en matière de système d'exploitation depuis Windows® 95. Cette nouvelle version consacre en effet la fusion des environnements NT/2000/9.X au sein d'un seul système pour les PC.[39]

-Windows Server 2003 :

Le choix du système d'exploitation (S.E) Microsoft Windows Server 2003 est principalement du au fait qu'il est l'un des outils les plus performants dans ce domaine et qu'il permet l'exploitation du serveur de manière à l'optimiser, afin d'utiliser le minimum de ressources possibles et d'y installer différents services : Bases de données, messageries, diffusion web .

Il convient de noter que Windows Server 2003 permet, surtout, de garantir une grande sécurité lors du déploiement de sites web, de l'utilisation des SGBD et du système d'exploitation lui-même.

- **Apache Tomcat**

  Apache Tomcat est un conteneur libre de servlets et JSP Java EE.
  Issu du projet Jakarta, Tomcat est un projet principal de la fondation Apache. [40]

- **MySQL**

  Est un serveur de base de données SQL multi-utilisateur et multi-thread (capacité d'une même application à effectuer plusieurs taches simultanées).
  Il a été conçu pour gérer de grandes bases de données très rapidement. [41]

- **Eclipse :**

  Est un environnement de développement intégré libre extensible, universel et polyvalent, permettant de créer des projets de développement mettant en œuvre n'importe quel langage de programmation. [42]

- **JSP :**

Les pages Web JSP sont une technologie développée par Sun basée sur Java qui simplifie le processus de développement de sites web dynamiques. L'utilisation du langage de programmation Java permet aux concepteurs de pages qui utilisent JSP d'incorporer rapidement des éléments dynamiques dans les pages web en intégrant du code Java, et en utilisant quelques balises (tags) simples.

Ces balises fournissent aux développeurs HTML la possibilité d'utiliser la logique d'objet Java, sans pour autant devoir maîtriser toute la complexité de développement de programmes Java. JSP est un langage script côté serveur. [43]

V.Architecture à 3tiers

Dans l'architecture à trois niveaux, les applications au niveau serveur sont délocalisées, c'est à dire que chaque serveur est spécialisé dans une tache (serveur web ou serveur de base de données par exemple), il existe un niveau intermédiaire, c'est à dire que l'on a généralement une architecture partagée entre :

- **Le client:** le demandeur de ressource.
- **Le serveur d'application:** le serveur chargé de fournir la ressource en faisant appel à un autre serveur.
- **Le serveur secondaire:** généralement c'est le serveur de base de données, fournissant un service au premier serveur.

Les deux serveurs de BDD et d'application sont déployées sur un seul Serveur (Machine virtuelle)

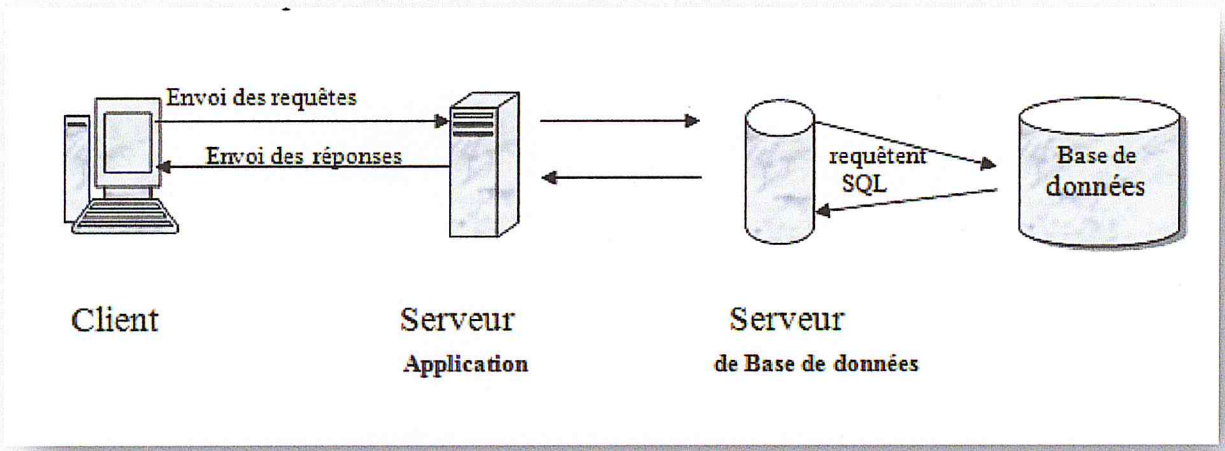


Fig. V.1. Architecture à 3 tiers.

VI. Configuration et installation des machines virtuelles

Nous avons créé deux machines virtuelles avec logiciel **VMWare Workstation**, qui permet de simuler un ou plusieurs PC virtuels sur un seul hôte physique.

1. Configuration réseau

N°	Nom de la Machine	IP	Masque de sous-réseau	passerelle	DNS
1	Serveur	192.168.56.25	255.255.255.0	192.168.56.1	192.168.56.1
2	Client	192.168.56.26	255.255.255.0	192.168.56.1	192.168.56.1

Tableau.6 : Configuration réseau

2. Configuration logiciel

N°	Nom de la Machine	Configuration logiciel	Description
1	Serveur	OS : Windows 2003 server JDK Apache tomcat MySQL	Serveur D'hébergement
2	Client	Windows XP	

Tableau .7: Configuration logiciel

3. Configuration matériel

Machine N° 1 :

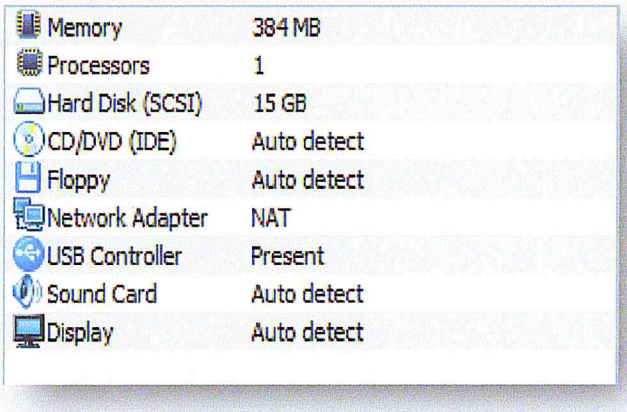


Figure. V.2 : Configuration matériel « Machine N° 1 »

Machine N° 2 :

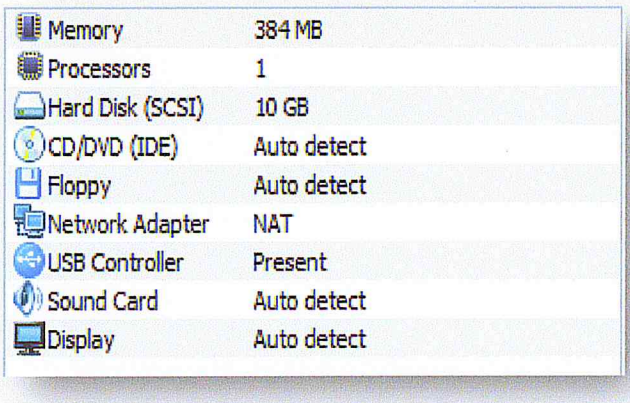


Figure. V .3 : Configuration matériel « Machine N° 2»

VII. Présentation de l'application

A travers le réseau, les utilisateurs peuvent avoir accès à un ensemble de ressources partagées selon leurs droits et privilèges d'accès.

Nous présentons dans ce qui suit quelques interfaces graphiques de notre application ainsi que quelques explications :

1. Authentification

L'utilisateur lance l'application via un navigateur web en tapant sont URL.

Une fenêtre d'identification et d'authentification s'affiche

Dans la page Authentification chaque utilisateur introduit son user_ Name son mot de passe et son rôle pour qu'il puisse accéder à son espace (cette tache est obligatoire pour tout les utilisateurs de l'application

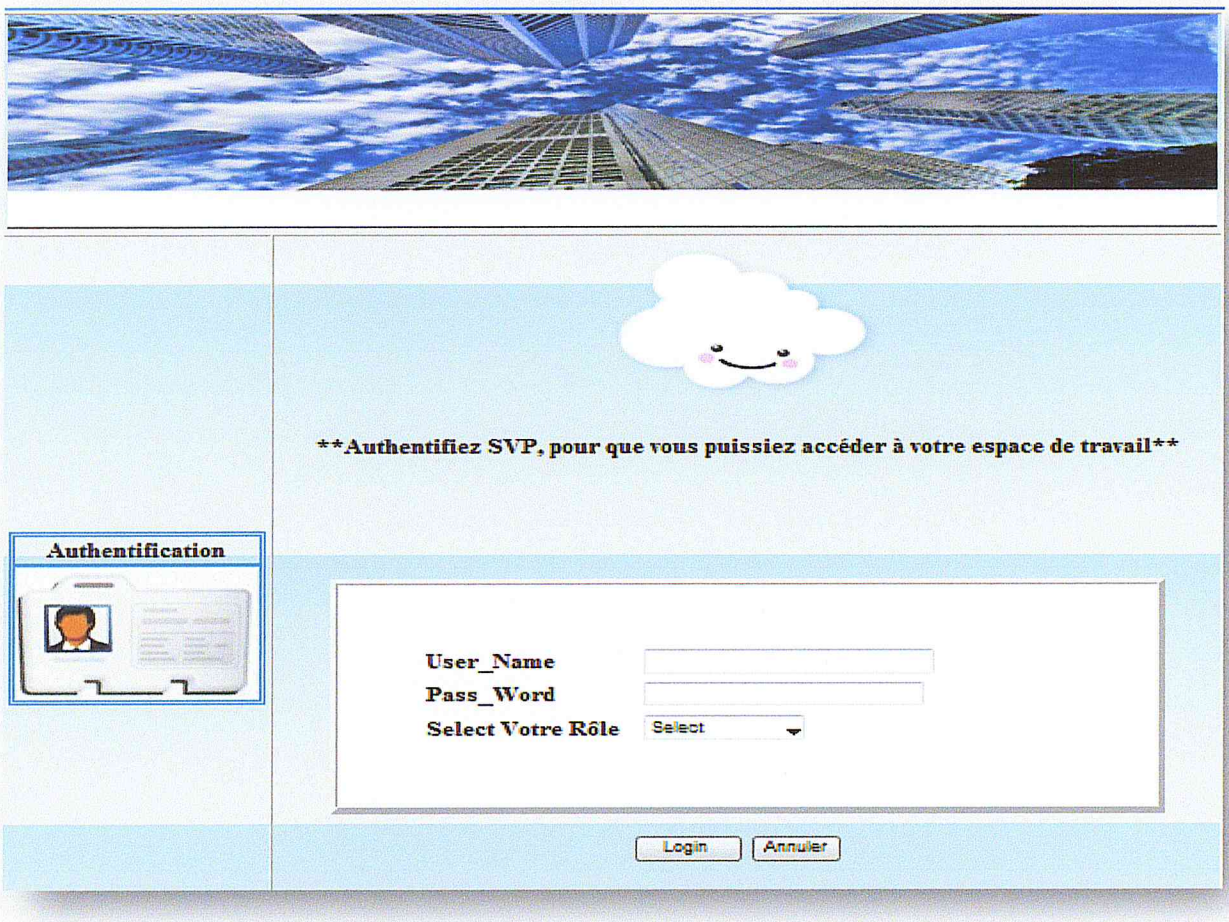


Figure V.4 : « Authentification ».

L'authentification donne accès à une des trois espaces suivant :

(Administrateur, Propriétaire de données, utilisateur)

2. Administrateur

Après l'identification de l'administrateur, la figure suivante permet d'afficher les choix possibles pour ce dernier.

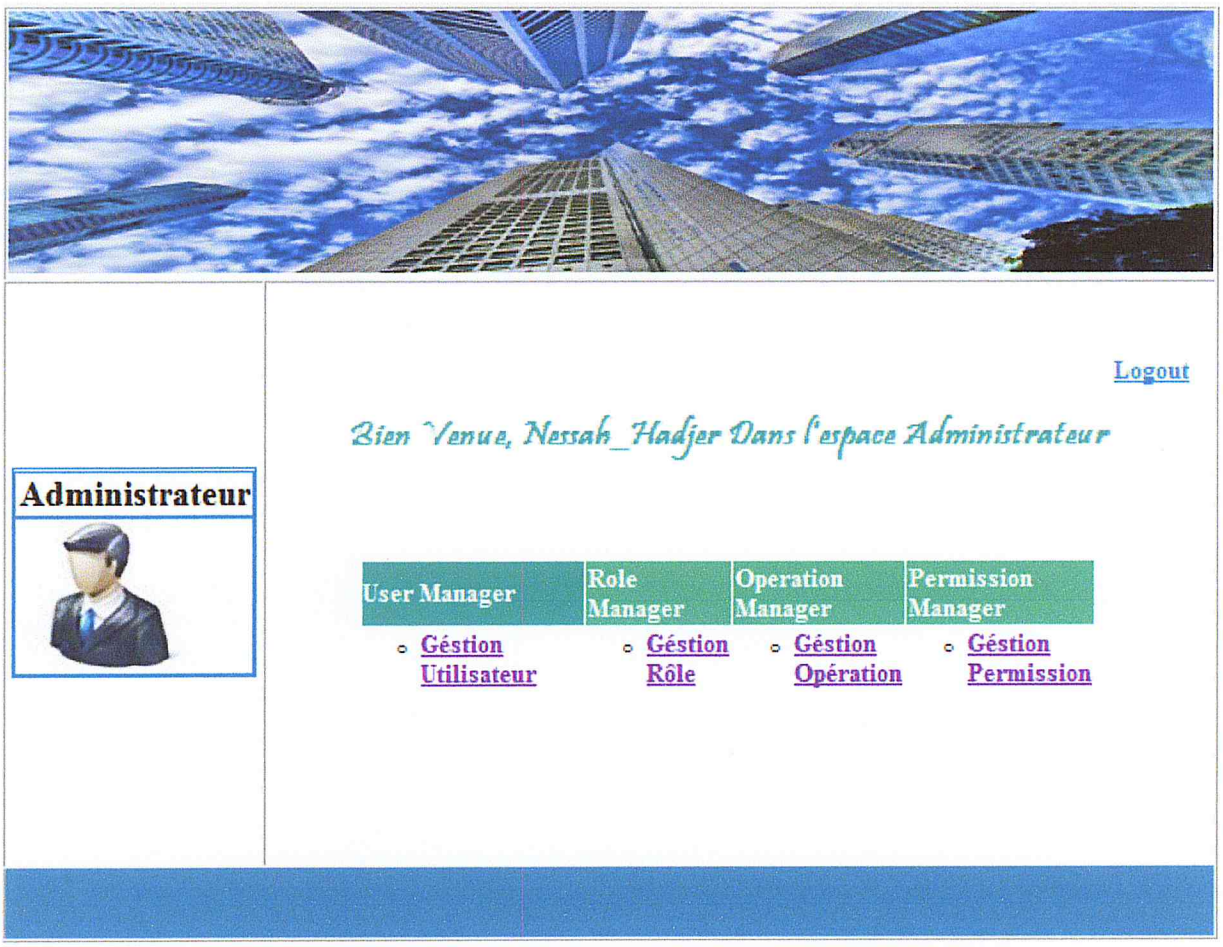


Figure V.5: Administrateur.

Les fonctionnalités spécifiques à l'administrateur sont :

3. Gestion d'utilisateur

Cette interface permet à l'administrateur d'ajouter, supprimer et modifier, consulter et d'affecter des utilisateurs.

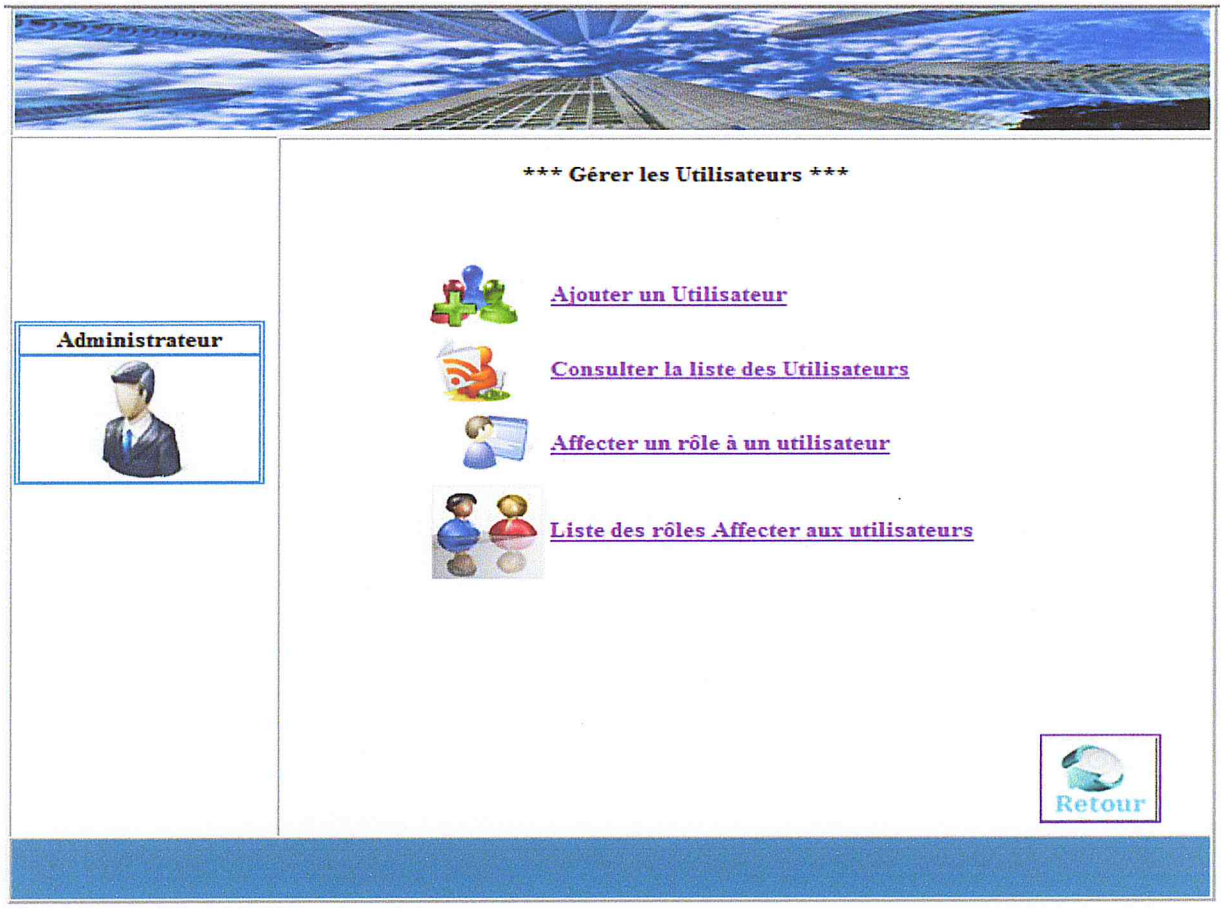


Figure V.6 : Gestion d'utilisateur.

4. Gestion de rôle

Cette interface permet à l'administrateur d'ajouter, supprimer et consultation des rôles.

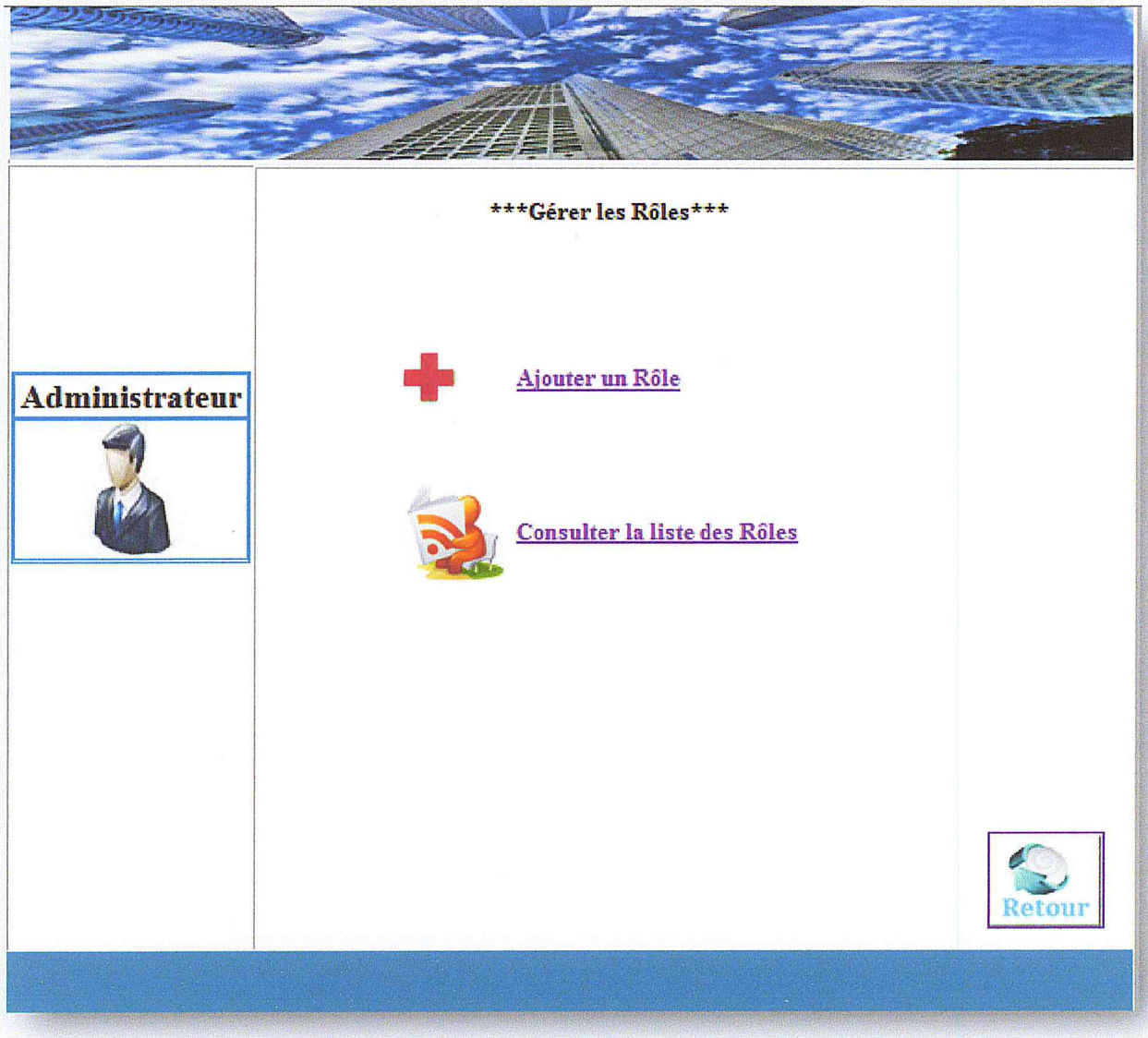


Figure V.6: Gestion de rôle.

5. Gestion d'opération

Cette interface permet à l'administrateur d'ajouter, supprimer et consultation des opérations.

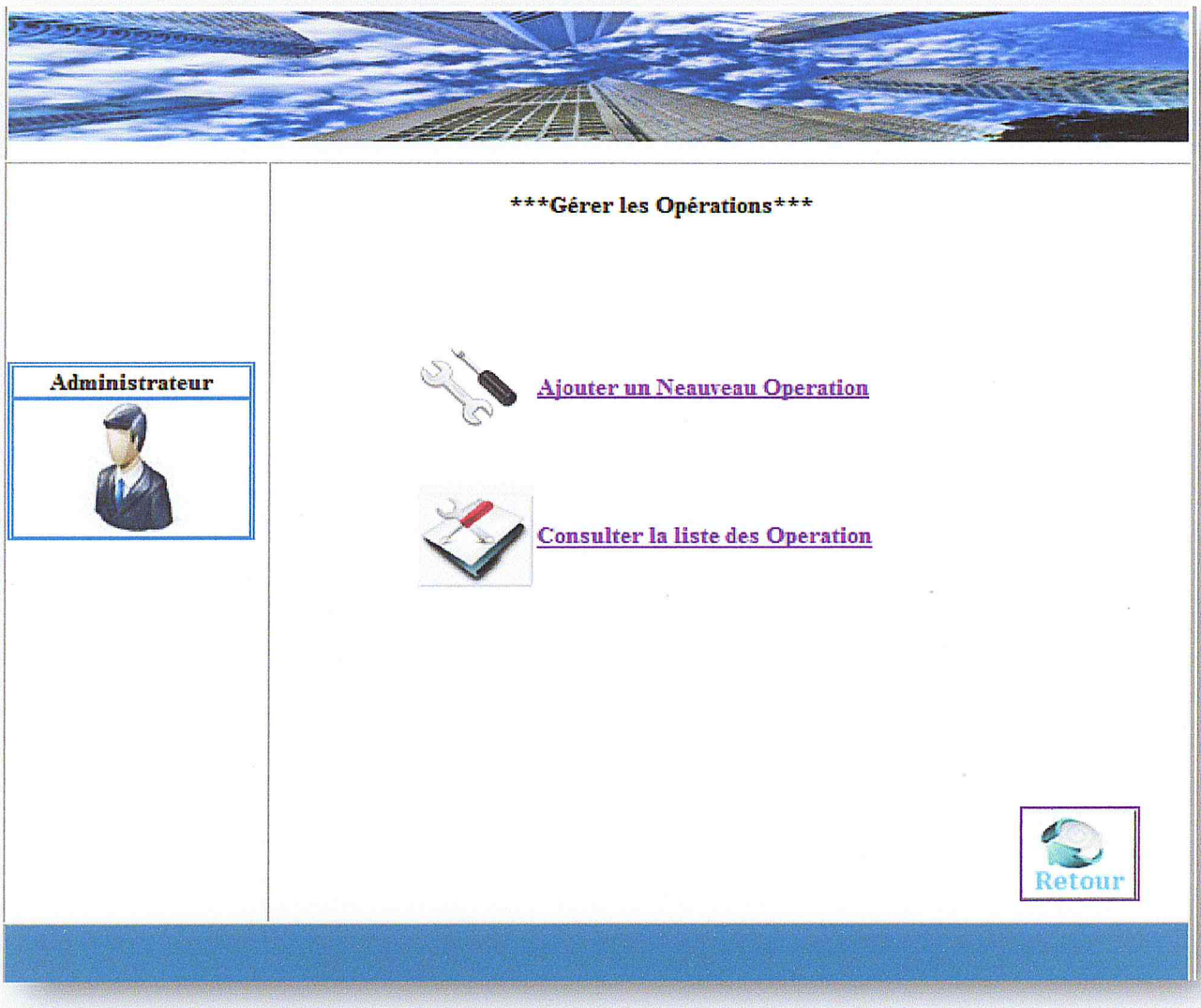


Figure V.7: « Gestion d'opération ».

6. Gestion Permission

Cette interface permet à l'administrateur d'ajouter, supprimer, consulter et d'affecter des permissions.

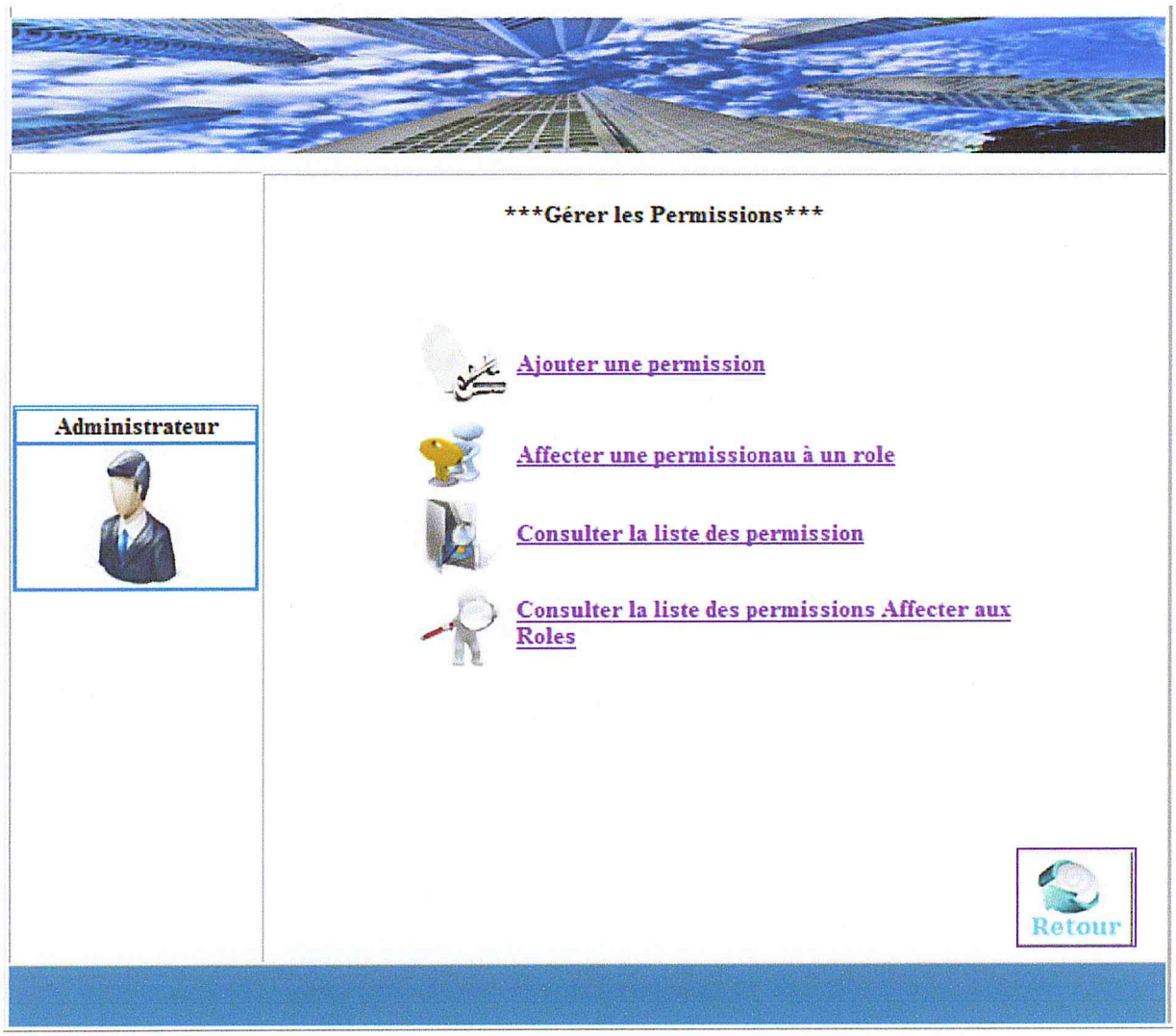


Figure V.8: Gestion de permission.

7. Propriétaire de données

Après l'identification du propriétaire, la figure suivante permet d'afficher les choix possibles pour ce dernier.

Figure V.9: Propriétaire de données

8. Stocker un Fichier

Cette interface permet de stocker les fichiers cryptés du propriétaire dans le serveur (virtuelle),

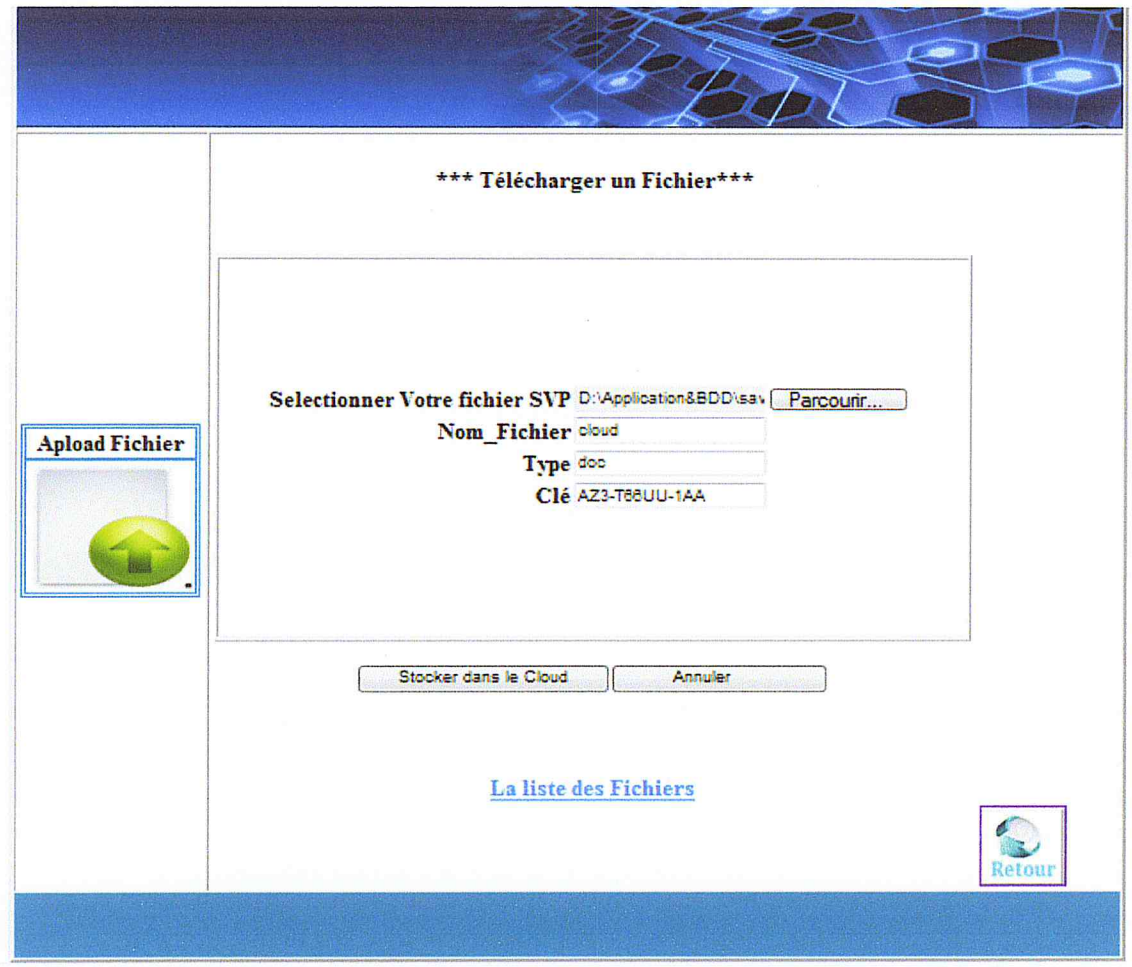


Figure V.10: « Gestion de permission ».

9. Utilisateur

Après l'identification de l'utilisateur, la figure suivante permet d'afficher les choix possibles pour le téléchargement des fichiers selon le rôle de ce dernier.

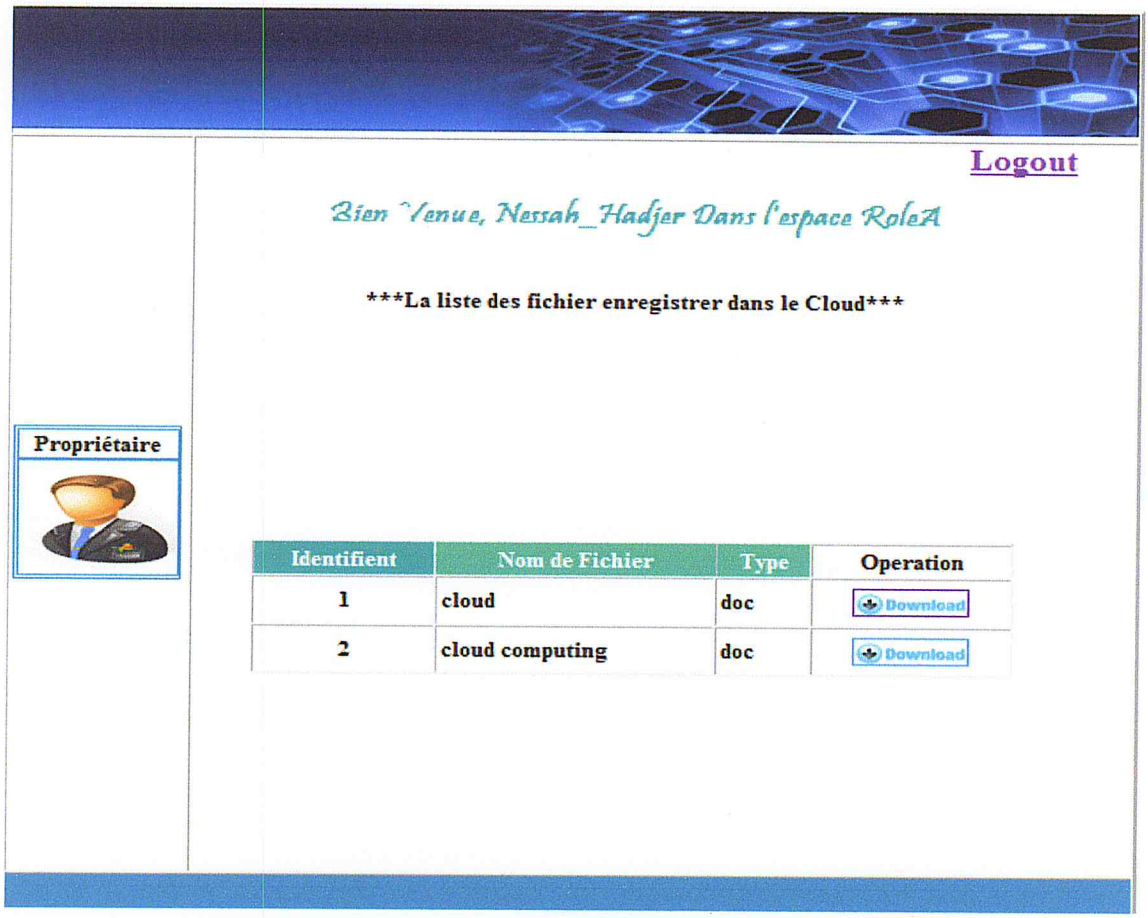


Figure V.11: Télécharger un Fichier

10. Vérification de rôle

Cette interface permet de vérifier le droit d'accès de l'utilisateur pour que se dernier puisse télécharger le fichier sélectionné.

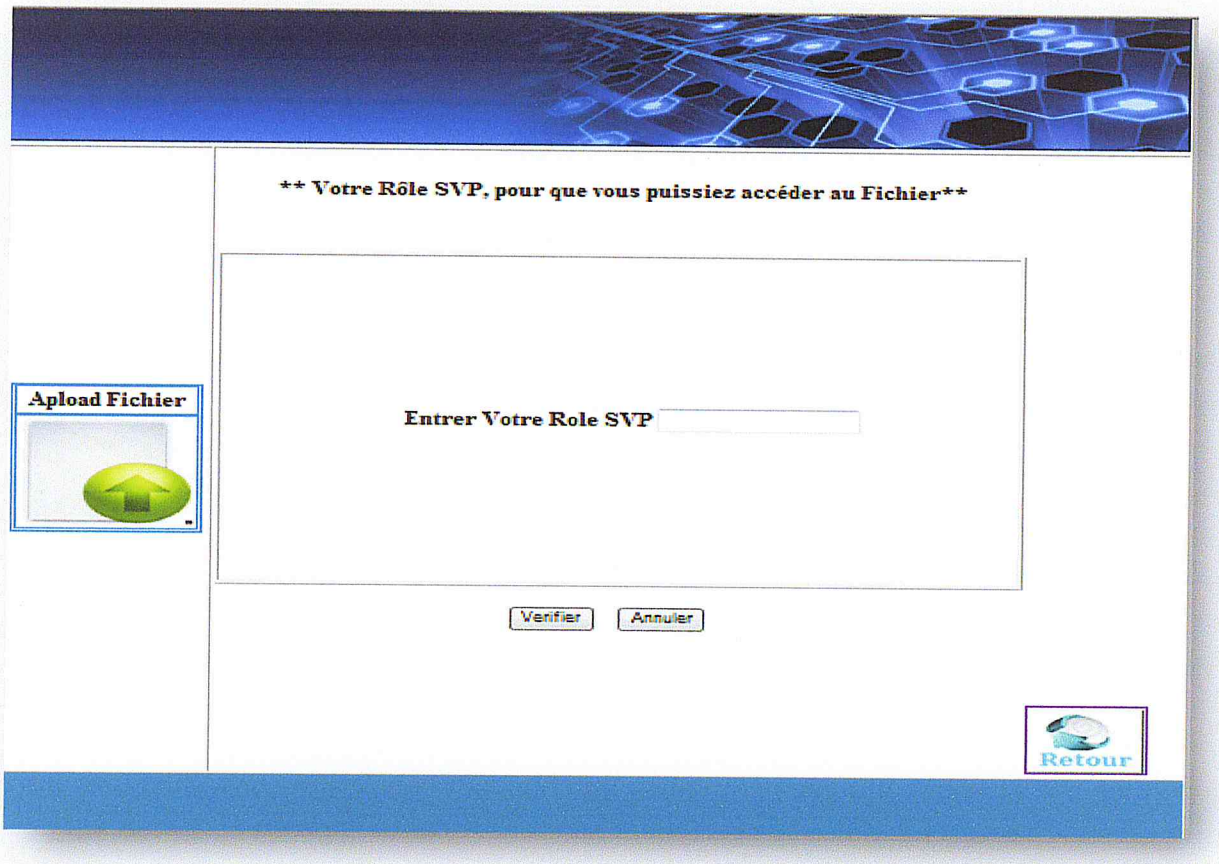


Figure V.12: Vérification de rôle

11. Téléchargement et décryptage d'un Fichier

Cette interface permet de télécharger un fichier crypté du serveur (virtuelle) au utilisateur.

Pour décrypté le fichier téléchargé l'utilisateur doit installer un logiciel (WinRaR),

Et de saisir la clé de chaque fichier

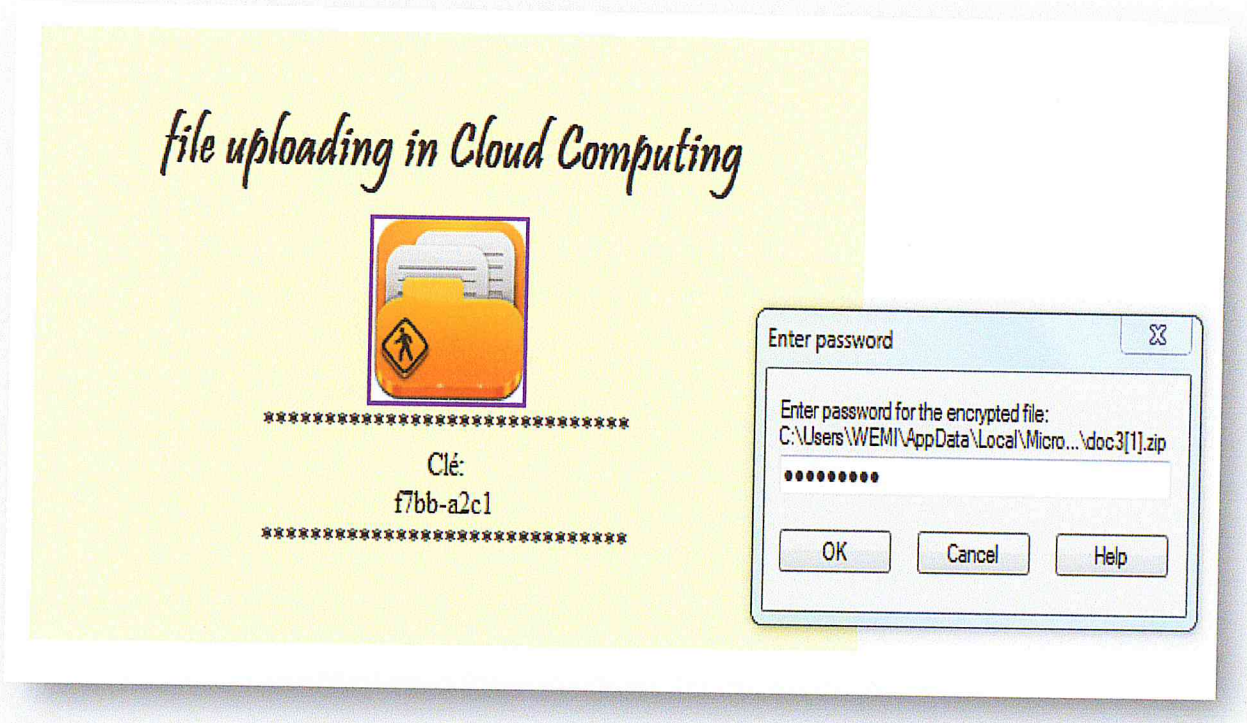


Figure V.13: Téléchargement et décryptage d'un Fichier

VIII. Conclusion

A travers ce chapitre, nous avons présenté la réalisation de l'application en justifiant nos choix technologiques, en représentant quelques interfaces graphiques que nous avons jugées.

Conclusion générale

Durant ce projet, nous avons été appelés a mettre en place un modèle de contrôle d'accès pour un Cloud privé.

Dans le but de Préserver la confidentialité, l'intégrité et la disponibilité des Données socket dans un Cloud privé nous avons choisi une politique de sécurité RBAC (contrôle d'accès a base de rôle) pour la gestion des identités et d'attribuer les droits d'accès aux utilisateurs d'un Cloud.

De ce fait nous avons crée un environnement virtuelle de stockage et développer une application pour sécurisé l'accès a ce dernier, les utilisateurs du système sont associés à un ou plusieurs rôles définis à l'avance Lorsque ceux-ci souhaitent effectuer une opération, ils vont activer un ou plusieurs rôles pour accéder aux ressources autorisées

Notre solution assure une stratégie solide de sécurité des accès mais nous avons tout de même éprouvé quelque difficultés qui nous ont empêché d'accomplir notre application jusqu'au bout à savoir le manque de la documentation.

Bibliographie

[31] : Amine Baina,29 septembre 2009,Contrôle d'Accès pour les Grandes Infrastructures Critiques :Application au réseau d'énergie électrique, Universite de Toulouse.

[29]:Amazon ElasticCompute Cloud(AmazonEC2) 07 janvier 2010,

[40] : Apache Tomcat, fr.wikipedia.org/wiki , consulté le 14/09/2013.

[17] :Bell et La Padula, Secure Computer System : Unified Exposition and Multics Interpretation.

[23]: Bertrand, Cloud Computing avec Amazon AWS, www.smile.fr.

[30] :Courtois,Thomas,Dramé, Yakhoub , Servoles, Sébastien,2011,Projet de session : Sécurité dans les bases de données.

[33] : Cheng Hong*, Zhiquan lv, Min Zhang, and Dengguo Feng, A Secure and Efficient Role-Based Access Policy towardsCryptographic Cloud Storage.

[24]: Christian Baun,Marcel Kunze , Jens Nimis, Stefan Tai ,Cloud Computing « Web-Based Dynamic IT Services»,.

[4] : Cloud computing, 2012, Livre blanc rédigé par le group Cloud computing d'ADIRA.

[7] : Cloud Computing, fr.wikipedia.org/wiki/Cloud_computing.

[18] : D.Ferrailo et R.Kuth.Role-based access control. Proceedings of the 15th NIST/NCSC National Computer Security Conference, page 554-563, 1992.

[22]: David Chappell, Mars 2009,Introducing Windows Azure.

[43]: Jean-Michel , 25 févr. 2013,Doudoux Développons en java , www.jmdoudoux.fr/java/dej/indexavecframes.htm .

[38] : Définition de vmware, www.formations-virtualisation.fr, 14-09-2013.

[3] : Etat de l'Art Cloud Computing, Mars 2009,Livre blanc par SOGETI Enterprise Services Consulting.

[35] : Enseignant : Mme S. Essanaa, 2007-2008,Les Diagrammes d' UML.

[13] : Jacques Le Maitre, « Sécurité des bases de données »,Université du Sud Toulon-Var.

[25] : http://aws.amazon.com.

[41] :http:/www.webotheque.fr/glossaire-web/sgbd-mysql-php.(Acess date :11 June 2011).

[42] :http://www.eclipse.org(Acess date : 10 June,2001).

[15] :I.Hattak, 2010, Analyse formelle des politiques de sécurité, université de Québec en Outaouais.

[19] : *Gregory Renard, 2009,* Livre Wygwam « Azure services plate forme online de Microsoft : Une nouvelle Ere».

[32] : Karine Al Makssoud ,9 décembre 2008, Thèse Système d'Accès Personnalisé à l'Information : Application au Domaine Médical.

[14] :L.Poinsot.Politiques et modèles de sécurité. Université Paris 13-Institut Galilée.

[20] : Leclère ,24 juin, *Mémoire : Mise en place d'un site web 2.0 sur un Cloud,* Olivier 2010

[26] : Laurent Wargon, 2012 Cloud Computin, Université de Marne-la-Vallée.

[36] : Laurent Piechocki , Mars 2005,Cours UML.

[37] : L. Audibert ,27 octobre 2006, UML 2.0 – Diagramme de cas d'utilisation.

[5] : Livre Wygwam « *Le Cloud Computing : Réelle révolution ou simple évolution ».*

[8] : Livre blanc produit par EuroCloud France *Novembre 2011.*

[9] : Livre blanc de Redpaper IBM « Cloud Computing » Septembre 2009 .

[10] : Livre blanc par SOGETI Enterprise Services Consulting, Mars 2009.

[11] : Le Cloud computing ,www.idf.direccte.gouv.fr, septembre 2012.

[1] : Maurice Audin, 2009, Etat de l'art du Cloud Computing et adaptation au logiciel libre.

[21] : Matthieu Denis, 26/10/2012, «Hébergez vos projets web dans le Cloud avec Windows Azure » www.siteduzero.com.

[28] : Mathieu Zarou,16 janvier 2013 ,Cloud Computing, www.developpez.com .

[16] : Raimundas Matulevicius, Marlon Dumas ,1976, A Comparison of Secure UML and UMLsec for Role-based Access Control, University of Tartu / STACC Tartu, Estonia

[6] : Stockage des données chez Google Année 2011-2012.

[12] : *Sécurité Informatique*, ,http://www.ducrot.org.

[27]: Dr. Stefan Hüsemann ,Les enjeux du Cloud Computing en entreprise, Université de Fribourg, Suisse.

[34]: Sofiene Boulares, Aout 2010, Memoire: Validation des politiques de sécurité par rapport aux modèles de contrôle d'accès.

[39] : Windows XP, www.mon-ordi.com/wxp.htm, consulté le 14/09 /2013.

[2] : Yohan PARENT, Maxime LEMAUX, Cyprien FORTINA, Hyacinthe CARTIAUX, 2010- 2011, « Cloud computing» .