Université Abou Bekr Belkaid
Tlemcen Algérie
جامعة أبي بكر بلقايد
تلمسان الجزائر

**République Algérienne Démocratique et Populaire**
**Université Abou Bakr Belkaid– Tlemcen**
**Faculté des Sciences**
**Département d'Informatique**

**Mémoire de Fin d'études**

**Pour l'obtention du diplôme de Master en Informatique**

***Option:*** *Réseaux et Système Distribués (R.S.D)*

*Thème*

# La gestion d'authentification dans un environnement Cloud

**Réalisé par :**

- Mr. Youcef Lammari

*Présenté le 2 juillet 2018 devant le jury composé de.*

- *Mr. Abdelkarim Benamar (Président).*
- *Mr. Mohamed MANA (Encadreur).*
- *Mr. Badr Benmammar (Examinateur).*
- *Mme. Zeyneb BENSAFI (Co-Encadrante).*

Année universitaire : 2017-2018

# Remerciements

Je remercie Dieu le tout Puissant qui m'a donné la force et la volonté pour réaliser ce modeste travail.

Je tiens à remercier sincèrement Monsieur Mana qui, en tant qu'encadreur de ce mémoire, s'est toujours montré à l'écoute et très disponible tout au long de la réalisation de ce mémoire, ainsi pour l'inspiration, l'aide et le temps qu'il a bien voulu nous consacrer et sans quoi ce mémoire n'aurait jamais vu le jour.

Je remercie Madame Bensafi qui m'a aidé durant la préparation de ce mémoire.

Mes remerciements vont également aux membres du jury d'avoir accepté de juger ce modeste travail.

Je remercie aussi toutes les personnes qui m'ont aidé durant la préparation de ce mémoire de près ou de loin.

Je conclurais, en remerciant vivement toute ma famille qui m'a toujours supporté moralement et financièrement pendant toutes mes longues années d'études.

# Dédicaces

*Á mes Parents*

*Á mes sœurs*

*Á toute la famille et*

*Á tous mes amis*

*Lammari Youcef*

# La Table des Matières

# La Table de Figures

# La Table des Tableaux

## Acronymes

| | |
|---|---|
| **NIST** | **N**ational **I**nstitue of **S**tandards and **T**echnology |
| **JEE** | **J**ava **E**nterprise **E**dition |
| **PC** | **P**ersonal **C**omputer |
| **SGBD** | Système de Gestion de Base de Données |
| **XML** | **E**xtensible **M**arkup **L**anguage |
| **SI** | **S**ystème d'**I**nformation |
| **LDAP** | **L**ightweight **D**irectory **A**ccess **P**rotocol |
| **KMV** | **K**ernel-based **V**irtual **M**achine |
| **SaaS** | **S**ervice **a**s **a** **S**oftware |
| **PaaS** | **P**latform **a**s **a** **S**oftware |
| **IaaS** | **I**nfrastructure **a**s **a** **S**oftware |
| **ONG** | **O**rganisation **N**on **G**ouvernementale |
| **OPT** | **O**ne **T**ime **P**assword |
| **API** | **A**pplication **P**rogramming **I**nterface |
| **IP** | **I**nternet **P**rotocol |
| **DOS** | **D**enial **O**f **S**ervice |
| **SQL** | Structured Query Language |
| **HTML** | **H**ypertext **M**arkup **L**anguage |
| **XSS** | Cross **S**ite **S**cripting |
| **TCP** | **T**ransmission **C**ontrol **P**rotocol |
| **IDS** | **I**ntrusion **D**etection **S**ystems |

| | |
|---|---|
| **MITM** | **M**an **I**n **T**he **M**iddle |
| **DNS** | **D**omain **N**ame **S**ystem |
| **ARP** | **A**ddress **R**esolution **P**rotocol |
| **RSA** | ronald **R**ivest adi **S**hamir leonard **A**dleman |
| **ECC** | **E**lliptic **C**urve **C**ryptography |
| **IEEE** | **I**nstitute of **E**lectrical and **E**lectronics **E**ngineers |
| **ECDSA** | **E**lliptic **C**urve **D**egital **S**ignature **A**lgorithme |
| **SHA** | **S**ecure **H**ash **A**lgorithm |
| **AES** | **A**dvanced **E**ncryption **S**tandard |
| **MD5** | **M**essage **D**igest **5** |
| **PKMS** | **P**ublic-**K**ey **C**ryptography **S**tandards |
| **CMS** | **C**ryptographic **M**essage **S**yntax |
| **XAdES** | **X**ML **A**dvanced **E**lectronic **S**ignatures |
| **CAdES** | **C**MS **A**dvanced **E**lectronic **S**ignatures |
| **VPN** | **V**irtual **P**rivate **N**etwork |
| **MAC** | **M**edia **A**ccess **C**ontrol |
| **SMS** | **S**hort **M**essage **S**ervice |
| **BLOB** | **B**inary **L**arge **OB**ject |

## Introduction générale :

Le Cloud Computing (informatique en nuage)est devenu maintenant le fondement de l'utilisation d'Internet. Email, moteurs de recherche, réseaux sociaux, médias en streaming, et d'autres services sont désormais hébergés dans "le Cloud ". Les collections des grands serveurs des produits de base en cours d'exécution, de coordinations logicielles rendent des hôtes individuels largement disponibles avec un coût réduit et une commodité accrue.

Avec une adoption croissante des technologies cloud computing, et avec son accessibilité et centralisation, des problèmes de sécurité sont devenus une réelle préoccupation pour les entreprises et les utilisateurs finaux. La prise en compte du caractère unique de ces problèmes, dès le début du plan d'implémentation, est le garant d'un investissement pérenne.

Afin de protéger les données sensibles et de respecter une certaine conformité, on doit relever des défis spécifiques en matière de sécurité. Dans ce but, notre travail vise à développer une solution de gestion d'authentification sécurisé dans un environnement cloud.

Ce manuscrit est organisé en trois chapitres. Le premier chapitre décrit le cloud computing et présente ses architectures ainsi que son modèle de déploiement. Le deuxième chapitre aborde les défis de sécurité, les attaques contre les environnements clouds ainsi que les différents mécanismes de sécurité déployés afin de protéger ces environnements. Enfin, le troisième chapitre présente notre travail qui consiste à développer une solution de gestion d'authentification dans un environnement cloud computing .

# Chapitre I :

# Présentation Générale des Concepts Cloud Computing

# Chapitre I. Présentation Générale des Concepts Cloud Computing

## I.1 Introduction :

Le Cloud Computing est un concept très puissant dans cette ère émergente de l'évolution technologique, qui est utilisé pour les applications grand public, mais aussi pour les applications professionnelles.

Cloud computing est le mécanisme de calcul centralisé, vers lequel chaque organisation s'est fortement penchée vers, dans cette dernière décennie.

Dans cette section, on présente les concepts du cloud computing, son architecture. En premier, on définit le Cloud et on met en évidence ses caractéristiques, Ensuite, on décrit des modèles de services Cloud communs et des modèles de déploiement Cloud.

## I.2 Définition du Cloud :

Il existe de nombreuses définitions du de cloud computing, et la définition la plus répandue est celle du NIST.

NIST définit le cloud comme étant « *Le Cloud Computing est un modèle qui permet un accès réseau pratique et sur demande à un pool partagé de ressources informatiques configurables (par exemple, des réseaux, des serveurs, du stockage, des applications et des services) qui peut être rapidement approvisionné et disponible sans trop d'efforts de gestion ou d'interaction d'opérateurs* » (NIST)

En d'autres termes, le Cloud est une technologie qui permet de mettre sur des serveurs localisés à distance des données de stockage ou des logiciels qui sont habituellement stockés sur l'ordinateur d'un utilisateur, voire sur des serveurs installés en réseau local au sein d'une entreprise. Cette virtualisation des ressources permet donc à l'entreprise d'accéder à ses données sans avoir à gérer une infrastructure informatique, souvent complexe et qui représente un certain coût pour l'entreprise.

## I.3 Caractéristiques du Cloud Computing :

Les cinq caractéristiques suivantes sont considérées comme inhérentes à des services de Cloud Computing(NIST):

- **Libre-service à la demande**: Le libre-service à la demande permet à l'utilisateur d'être en mesure d'allouer et de libérer des ressources distantes en temps réel en fonction des besoins, sans intervention de l'opérateur.
- **Large accès au réseau** : Quels que soient le type de clients: serveur, PC, client mobile, etc.), l'ensemble des ressources partagés doit être accessible et à disposition de l'utilisateur universellement et simplement à travers le réseau.
- **La mise en commun des ressources**: Des ressources telles que la bande passante réseau, machines virtuelles, mémoire, puissance de traitement, capacité de stockage, sont mises en commun pour desservir plusieurs clients à l'aide d'un modèle multi-locataire. Autrement dit, les ressources virtuelles et physiques sont affectées dynamiquement et réaffectées en fonction des besoins et des clients.
- **Élasticité rapide:** à la demande, les ressources et les capacités peuvent être rapidement et automatiquement déployées et mises à l'échelle à n'importe quelle quantité et à tout moment.
- **Service mesuré**: Les systèmes cloud doivent être capables de s'autocontrôler et de se gérer pour permettre l'optimisation interne du système. Pour cela, ils s'appuient sur des mesures de référence obtenues grâce à divers mécanismes de supervision.

On ne peut pas appeler un service du Cloud Computing s'il ne satisfait pas les caractéristiques énumérées ci-dessus

## I.4 Principes de l'architecture du Cloud Computing :

Avant parler de l'architecture du Cloud, il faut tout d'abord parler du Data Center, et puis, citer la différence entre le Cloud et Data Center :

### I.4.1 *Data Center :*

Le terme "Data Center" peut être interprété de différentes manières. Tout d'abord, une organisation peut gérer un centre de données interne géré par des informaticiens formés, dont le rôle est de maintenir le système opérationnel. Deuxièmement, il peut désigner un centre de stockage hors site composé de serveurs et d'autres équipements nécessaires pour garder les données stockées accessibles à la fois virtuellement et physiquement.

**Avantages**: Les Data Center viennent avec un certain nombre de pros. Les organisations capables d'avoir un centre de stockage de données interne dépendent beaucoup moins du maintien d'une connexion Internet. Les données seront accessibles tant que le réseau local restera stable. Le stockage à distance a également ses avantages. Si l'emplacement de l'organisation est compromis par le feu, l'effraction, l'inondation, etc., les données resteront intactes et indemnes à son emplacement distant.

**Inconvénients**: Le fait d'avoir la totalité ou la plupart des données stockées dans un seul endroit le rend plus facilement accessible à ceux qu'on ne veut pas avoir accès, virtuellement et physiquement, dans ce même contexte, on peut citer également les pannes, si le serveur tombe en panne alors tous le système cesse de fonctionner. Selon le budget de l'organisation, il pourrait s'avérer trop coûteux de maintenir un centre de données géré par cette dernière.

### I.4.2 *Différence entre Data Center traditionnel et Cloud Computing :*

On peut résumer la différence entre le DataCenter et le Cloud Computing dans le tableau ci-dessous [1] :

| | Data Center Traditionnel | Cloud |
|---|---|---|
| ***Serveurs*** | Co-localisé<br>Pas de tolérance de pannes | Intégré<br>Tolérance de pannes |
| ***Ressources*** | Partitionné<br>Performances inter-relié | Unifié<br>Performances isolé |
| ***Gestion*** | Séparé<br>Manuelle | Contrôle total centralisé<br>Avec automatisation |
| ***Planification*** | Planifier à l'avance<br>Sur-approvisionnement | Flexible<br>Scalable |
| ***Allocation*** | Par Machines physique | Par Usage Logique |
| ***Application/Services*** | fixé sur des serveurs désignés | Fonctionne et se déplace sur toutes les machines virtuelles |

*Tableau I-1 La différence entre Data Center traditionnel et le Cloud.*

### I.4.3 *Architecture N-tiers :*

La philosophie des architectures du Cloud Computing repose sur l'architecture 3-tiers (N-tiers).Le principe de l'architecture N-tiers se repose sur :

i. **Serveur de présentation** : produit des écrans visibles par les utilisateurs (interfaces utilisateur).
ii. **Serveur d'application** : joue le rôle de plate-forme d'exécution pour les applications de l'entreprise (JEE ou Microsoft .NET)
iii. **Système de persistance** : assure stockage et cohérence des données métiers de l'entreprise. Il est basé sur un SGBD relationnel ou système des fichiers ou SGBD XML, etc.
iv. **Serveur d'authentification** (gestion d'identités) : assure les services de sécurité aux applications du SI, peut utiliser un annuaire LDAP.
v. **Serveur d'intégration** : fournit une passerelle d'échange avec les autres applications du système d'information.

### I.4.4 *Architecture SOA :*

SOA (Service Oriented Architecture) : Les applications sont des assemblages des services métiers et des services génériques. Un service est une fonctionnalité oriente-métier.

Les offres **SaaS** reposent majoritairement sur des SOA, en exploitant aussi les services intégrables par des tiers fournisseurs. L'application Cloud Computing est une application composite.

### I.4.5 *Virtual Machine :*

La virtualisation des serveurs et des systèmes de stockage joue un rôle clé dans l'architecture de Cloud Computing, en offrant l'un des principaux avantages du Cloud : l'agilité.

Le concept de virtualisation désigne l'émulation complète, en isolation et en temps réel des environnements différents (systèmes d'exploitation) sur un même serveur. On obtient de cette manière deux ou plusieurs machines virtuelles qui fonctionnent sur un même serveur physique.

Quelques Outils de virtualisation utilisés pour le Cloud Computing sont: KVM (noyau Linux), VMware, VirtualBox, VirtualPC (gratuit).

### I.4.6 *Virtualisation du stockage :*

La virtualisation du stockage repose sur le principe qu'un fichier sera garder quelque part dans le réseau et pourra être manipule à tout moment même via de protocoles standard.

- **Systèmes de fichiers distribues :**
  - Google File System (GFS)
  - Hadoop Distributed File System (HDFS)
- **Systèmes de fichier de cluster** :
  - VMware vStorage (VMFS)
  - XenServer Storage Pool

## I.5 Types des services Cloud Computing :

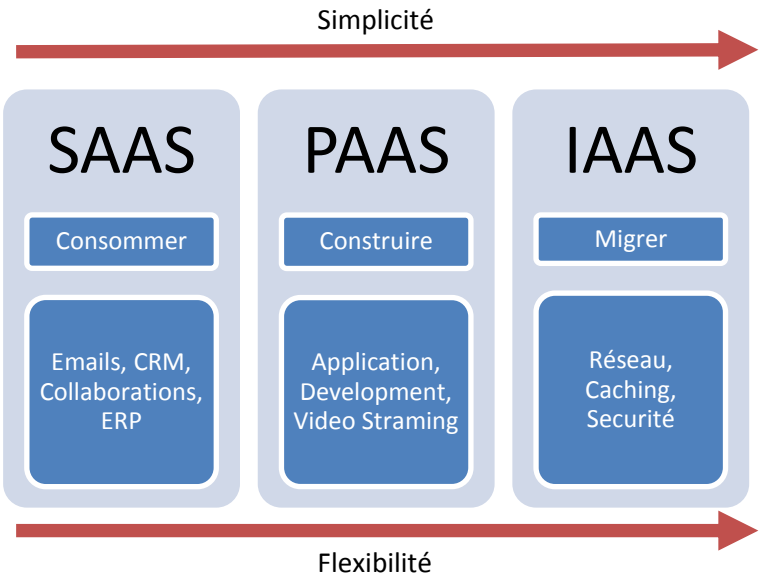



*Figure I-1 Types de Services Cloud Computing*

Le cloud computing offre aux développeurs et aux services informatiques la possibilité de se concentrer sur l'essentiel et d'éviter les tâches indifférenciées telles que l'approvisionnement, la maintenance et la planification des capacités. A mesure que le cloud computing a gagné une popularité, plusieurs modèles et stratégies de déploiement différents sont apparus pour répondre aux besoins spécifiques des différents utilisateurs. Chaque type de service de cloud et de méthode de déploiement offre différents niveaux de contrôle, de flexibilité et de gestion. Saisir les différences entre l'infrastructure en tant que service, la plate-forme en tant que service et le logiciel en tant que service et déterminer les stratégies de déploiement à utiliser peuvent aider à choisir l'ensemble de services dont on a besoin.

Le Cloud permet de rendre un certain nombre de **services**, qu'il est possible de définir en fonction des **rôles** et des **usages des entreprises** qui fournissent le service et des entreprises utilisatrices :

### I.5.1 Infrastructure as a service -IAAS- :

Le Cloud permet de mettre en œuvre une **infrastructure virtuelle** (serveur, couches de virtualisation, stockage, réseaux) sur laquelle l'entreprise utilisatrice va pouvoir héberger systèmes d'exploitation des serveurs et des logiciels applicatifs.

### I.5.2 Platform as a service -PAAS-:

Le Cloud permet de mettre en œuvre une plateforme d'exécution de logiciels et d'applications, sur laquelle l'entreprise utilisatrice va pouvoir installer, configurer et utiliser les applications voulues.

### I.5.3 Software as a service -SAAS-:

Le Cloud permet de rendre accessible une application aux utilisateurs finaux en mode "service".

## I.6 Types de déploiement du Cloud Computing :

Mais au-delà de ces modes de services, 4 typologies de Cloud Computing peuvent encore être définies, toujours en fonction des acteurs et des usages qui en sont fait :

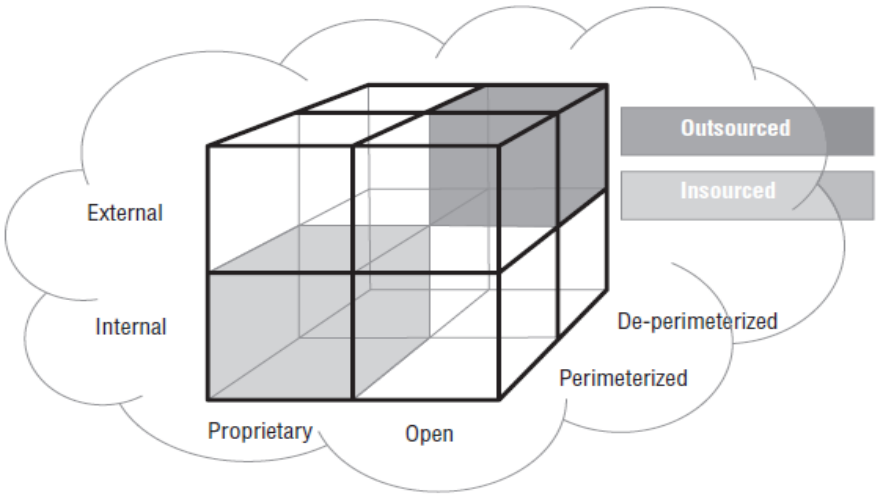



*Figure I-2 Le modèle cube du Cloud par Jericho*

Le modèle cube du Cloud de Jericho décrit le modèle Cloud comme ayant quatre "dimensions":

- ***Interne (I) / Externe (E)*** - Définit l'emplacement physique des données. Si c'est à l'intérieur de votre propre limite physique alors il est interne, si ce n'est pas à l'extérieur votre propre limite physique alors il est externe.
- ***Propriétaire (P) / Ouvert (O)*** - Propriétaire signifie que l'organisation qui fournit le service garde les moyens de fourniture sous leur propriété. Alors que dans le Cloud ouvert ils utilisent une technologie qui ne leurs est pas propriétaire, ce qui signifie qu'il y aura probablement plus de fournisseurs.
- ***Architectures Périmètré (Per) / Dé-périmètré (D-p)*** –Définie si c'est à l'intérieur du périmètre IT traditionnel ou à l'extérieur, De-Perimeterization est lié à l'échec / retrait / rétrécissement / effondrement progressif du traditionnel périmètre informatique.
- ***Insourced / Outsourced*** - Outsourced: Le service est fourni par une partie tiers, Insourced: le service est fourni par votre propre personnel sous votre contrôle.

## I.7 Modèles de déploiement de Cloud Computing :

Ces modèles de déploiement, tels que définis par le NIST, ne sont pas définis par l'opérateur, l'emplacement ou physiquement, mais par le service offert et le type de collectivité. Semblables aux modèles de services en nuage, les modèles de déploiement ne sont pas mutuellement exclusives. Les quatre (4) modèles de déploiement de Cloud sont :

### I.7.1 *Cloud publique :*

Cette infrastructure cloud est disponible pour un groupe de la grande industrie ou le grand public et est détenu par un vendeur de vendre des services de cloud computing.

### I.7.2 *Cloud privée :*

Cette infrastructure cloud est géré par l'organisation ou à un tiers et sont exploités uniquement pour les besoins de l'organisation. Cela peut exister sous ou hors tension prémisse.

### I.7.3 *Communauté nuage :*

Cette infrastructure Cloud est partagée par plus d'une organisation et le soutien d'une communauté spécifique qui a des considérations communes. Cela peut être géré par des organisations ou à des tiers. Cela peut exister sous ou hors tension prémisse.

### I.7.4 *Cloud hybride :*

Cette infrastructure Cloud est composé de deux ou plusieurs types de nuages énumérés ci-dessus qui restent des entités uniques, mais sont connectés via la technologie standardisée qui permet la portabilité des données et des applications.

Le schéma ci-dessous précise la relation entre les types de service, qui doivent nécessairement contenir les cinq(5) caractéristiques citées précédemment, et les modèles de déploiement de Cloud.

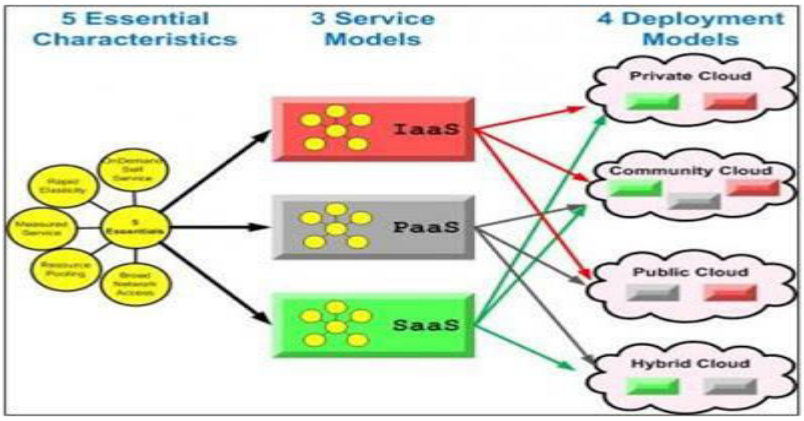



*Figure I-3 Modèle de déploiement du Cloud (Source :Marwin Britto).*

## I.8 Avantages du Cloud Computing :

Le Cloud Computing offre de multiples avantages aux entreprises et aux utilisateurs finaux. Voici ci-dessous les plus importants d'entre eux :

- **Un usage simplifié** : Le Cloud Computing simplifie les usages en permettant de s'affranchir des contraintes de l'outil informatique traditionnel (installation et mise à jour des logiciels, espace de stockage, portabilité des données…). Le Cloud Computing offre aussi plus d'élasticité et d'agilité car il permet d'accéder plus rapidement à des ressources IT (serveur, stockage ou bande passante) via un simple portail web et donc sans investir dans des équipements matériels supplémentaires. La mise à disposition est donc immédiate. De plus, l'utilisateur n'a pas d'infrastructure à gérer, c'est au fournisseur Cloud de maintenir le matériel serveur, le stockage, les réseaux.
- **La réduction des coûts :** La mutualisation des ressources informatiques et la facturation à l'usage rend le Cloud Computing économiquement attrayant.
- **L'accessibilité** : Les services de Cloud Computing sont accessibles à tout moment, sur tous les supports, via une connexion internet.

- **L'élasticité** : Le Cloud Computing permet d'allouer simplement et rapidement davantage de ressources à des applications en production afin de répondre à des montées en charge ponctuelles.
- **Le déploiement rapide et la simplicité d'intégration** : Le déploiement et la mise en fonctionnement d'un service de Cloud Computing nécessite peu de temps.
- **La disponibilité du service :** Le Cloud Computing permet de garantir les accès et la disponibilité des services. Le fournisseur de services de Cloud Computing s'engage contractuellement sur une interruption minimum des serveurs à travers des SLA (Service Level Agreements).
- **La flexibilité nécessaire pour vos projets :** Le Cloud Computing s'adapte en temps réel à vos projets et accompagne le développement d'une activité sans coûts supplémentaires.
- **La sécurité des données :** La sécurité des données est le principal frein d'adoption du Cloud Computing. Dans ce contexte, les fournisseurs garantissent aux utilisateurs un très haut degré de sécurité des données avec le chiffrement des données, la surveillance logicielle et la sécurisation des lieux de stockage (Datacenters).
- **L'adoption rapide par les utilisateurs finaux :** Les applications utilisant des services de Cloud Computing sont pour la plupart faciles à adopter. Le Cloud Computing simplifie les usages.
- **La réversibilité :** La restitution de l'intégralité des données d'une entreprise est garantie par les fournisseurs prévoyant dans leur contrat une clause de réversibilité.

## I.9 Applications du Cloud Computing :

Les applications du Cloud Computing sont pratiquement illimitées. Avec le bon middleware, un système de Cloud Computing pourrait exécuter tous les programmes qu'un ordinateur normal pourrait exécuter. Potentiellement, depuis logiciel de traitement de texte générique ou utilisation d'un service en ligne pour envoyer des courriers électroniques, regarder des films ou regarder la télévision, jouer à des jeux ou stocker des images ou autres fichiers en arrivant à des programmes informatiques personnalisés conçus pour une entreprise spécifique, pourrait fonctionner sur un système informatique en nuage.

Il est probable que le cloud computing intervienne dans les coulisses. Les premiers services de cloud computing n'ont pas encore dix ans, mais un grand nombre d'organisations, par exemple des starts-up, des multinationales, des services administratifs ou des ONG, adopte cette technologie pour de nombreuses raisons.

Voici ce qu'on peut faire avec le cloud :

- Créer des applications et des services
- Stocker, sauvegarder et récupérer des données
- Héberger des sites web et des blogs
- Diffuser du contenu audio et vidéo
- Diffuser des logiciels à la demande
- Analyser des données pour en tirer des informations et faire des prévisions.

## I.10 Conclusion :

En résumé, le cloud computing est une solution pour les petites entreprises et les utilisateurs finaux, qui n'ont souvent pas les moyens d'investir dans un équipement informatique hautement sécurisé. Cela dit, les grandes entreprises peuvent également en bénéficier en exportant une partie de leurs services vers le cloud. Mais dans tous les cas, on n'y échappe plus, le cloud étant devenu omniprésent dans notre société et notre quotidien : dès lors qu'on accède à des ressources informatiques sur le web, on fait du Cloud. Le web messagerie (Gmail, Yahoo…), le stockage de médias en ligne, les réseaux sociaux sont des exemples parmi tant d'autres de cloud computing.

# Chapitre II :

# La sécurité dans le Cloud Computing

# Chapitre II. Sécurité dans le Cloud Computing

## II.1 Introduction :

Le Cloud Computing prend de plus en plus une place stratégique dans notre vie. Ainsi la notion du risque lié à ce dernier devient une source d'inquiétude et une donnée importante à prendre en compte.

Par ailleurs, le Cloud Computing permet, non seulement, aux utilisateurs d'avoir accès aux ressources mais aussi de transporter une partie du système d'information en dehors de l'infrastructure sécurisée de l'entreprise. D'où la nécessité de mettre en place des démarches et des mesures pour évaluer les risques et définir les objectifs de sécurité à atteindre.

Dans ce qui suit nous allons définir les buts de la sécurité dans le cloud, les contraintes influençant cette dernière et les mécanismes de sécurité utilisés dans le cloud computing.

## II.2 Buts de la Sécurité :

Les organisations de sécurité informatique et les professionnels ont défini certains éléments qui sont considérés comme des concepts clés de la sécurité. L'ISO 7498-2[2] définit les catégories citées ci-dessous de services de sécurité:

### II.2.1 *La confidentialité des données :*

Consiste à s'assurer que les informations ne peuvent être divulguées à des utilisateurs non autorisés. La confidentialité des informations pourrait être assurée pendant le transfert du message, et au repos sur le serveur de stockage

### II.2.2 *Intégrité :*

Consiste à s'assurer que les données ne peuvent pas être modifiées de manière non autorisée ou non détectée. L'intégrité est violée lorsqu'un message est activement modifié en transit. Les systèmes de sécurité de l'information assurent généralement l'intégrité des données en plus de la confidentialité des données.

### II.2.3 *Authentification :*

Incluant l'authentification de l'origine et l'authentification de l'entité. L'authentification de l'origine est un service de sécurité qui vérifie l'identité d'une entité du système qui prétend être la source originale des données reçues. L'authentification d'entité est le processus de vérification d'une revendication selon laquelle une entité système ou une ressource système a une certaine valeur d'attribut. Cet attribut est généralement l'identité de l'utilisateur.

### II.2.4 *Disponibilité :*

La propriété d'un système ou d'une ressource système est accessible ou opérationnelle à la demande, par une entité système autorisée, selon les spécifications de performance du système.

### II.2.5 *Non-répudiation :*

Prévenir le déni d'actions et d'engagements.

### II.2.6 *Contrôle d'accès :*

Le contrôle d'accès est une technique de sécurité qui peut être utilisée pour déterminer les utilisateurs ou les programmes autorisés à voir ou à utiliser les ressources d'un environnement informatique.

Il existe deux types principaux de contrôle d'accès : physique et logique.

a) ***Le contrôle d'accès physique*** : permet de limiter les accès aux campus, aux bâtiments, aux salles et aux matériels informatiques.

b) ***Le contrôle d'accès logique*** : restreint les connexions aux réseaux informatiques, aux fichiers système et aux données.

## II.3 Analyse de vulnérabilités :

On peut noter les vulnérabilités suivantes dans un environnement Cloud Computing :

1. **L'existence de brèches de sécurité** : tant sur l'une des couches logiques du Datacenter que celles issues d'erreurs humaines ;
2. **La fragilité dans la gestion des accès et des identités** : bien que certains fournisseurs renforcent les interfaces d'authentification avec d'autres moyens tels que les certificats, les smartcards, la technologie OTP et bien d'autres ;
3. **L'utilisation d'API non sécurisées** pour l'intégration des applications avec les services Cloud;

4. **L'exploit de vulnérabilités** : des systèmes d'exploitation sur les serveurs du Cloud et même sur les applications hébergées;
5. **Le piratage de compte** : qui est un vieux type d'attaque informatique, vient avec une forte recrudescence depuis l'avènement d'Internet et encore celui du Cloud Computing;
6. **Une action malveillante initiée en interne dans les effectifs du fournisseur** : Une personne malveillante dans l'équipe de gestion du Datacenter peut facilement nuire à la confidentialité et l'intégrité des environnements hébergés;
7. **Les menaces persistantes avancées** : qui consistent en une forme d'attaque où l'hacker réussit à installer un dispositif dans le réseau interne de l'organisation, à partir duquel il peut extirper des données importantes ou confidentielles ;
8. **La perte de données** : qui peut être causée par une attaque informatique (logique) du Datacenter, une attaque physique (incendie ou bombardement), une catastrophe naturelle, ou même simplement à un facteur humain chez le fournisseur de services, par exemple en cas de faillite de la société;
9. **Les insuffisances dans les stratégies internes d'adoption ou de passage au Cloud** : Les entreprises ou les organisations ne prennent pas souvent en compte tous les facteurs de sécurité liés à leur fonctionnement avant de souscrire à un service Cloud. Certaines négligences, tant au niveau du développement d'application qu'au niveau de l'utilisation basique, leur sont parfois fatales;
10. **Utilisation frauduleuse des technologies Cloud** en vue de cacher l'identité et de perpétrer des attaques à grande échelle : Généralement, il s'agit de comptes créés pendant les périodes d'évaluation ou des accès achetés frauduleusement;
11. **Le déni de service** : qui est une attaque qui consiste à rendre indisponible un service par une consommation abusive des ressources telles que les processeurs, la mémoire ou le réseau. L'idée, pour le pirate, c'est de réussir à surcharger les ressources du Datacenter en vue d'empêcher d'autres utilisateurs de profiter des services;
12. **Les failles liées à l'hétérogénéité des technologies** : imbriquées dans l'architecture interne du Cloud, et l'architecture externe d'interfaçage avec les utilisateurs.

## II.4 Les attaques dans l'environnement Cloud :

Les composants de sécurité telle que les pares feux ou les systèmes de détection d'intrusion, ne sont pas adaptés pour détecter les attaques distribuées. Ces attaques sont donc subdivisées en sous attaques afin d'être indétectable par de tel système de sécurité :

### II.4.1 *Déni de service (DOS) :*

L'attaque par déni de service a pour but de rendre un service indisponible par une surcharge réseau. Cette attaque peut être évitée grâce à la scalabilité du Cloud. Néanmoins, les clients n'utilisant pas les services de scalabilité sont soumis aux risques de ces attaques, il est dans ce cas difficile de détecter ces attaques pour les bloquer cause du potentiel nombre d'attaques simultanées.

### II.4.2 *Les attaques de Session Hijacking :*

L'accès non autorisé à un système peut être réalisé par le détournement de session. Dans ce type d'attaque, un attaquant détourne une session entre un client de confiance et le serveur Cloud. L'ordinateur attaquant remplace son adresse IP par celle du client autorisé et le Cloud poursuit la session en supposant qu'il communique avec le client autorisé.

### II.4.3 *Les attaques SQL injection :*

Exploitant des défauts de conception communs au sein des applications Web, l'attaque par injection SQL reste une méthode de cyber-attaque simple et efficace. L'injection SQL est une sérieuse menace à la sécurité des bases de données des entreprises car elle est couramment utilisée par les pirates informatiques pour compromettre des sites Web.

### II.4.4 *Les attaques XSS (Cross Site Scripting) :*

Le cross site Scripting (abrégé XSS), est un type de faille de sécurité des sites web permettant d'injecter du contenu dans une page, permettant ainsi de provoquer des actions sur les navigateurs web visitant la page. Les possibilités des XSS sont très larges puisque l'attaquant peut utiliser tous les langages pris en charge par le navigateur, et de nouvelles possibilités sont régulièrement découvertes notamment avec l'arrivée de nouvelles technologies comme HTML. Il est par exemple possible de voler la session en récupérant les cookies.

### II.4.5 *Les attaques de fragmentation :*

Cette attaque consiste à envoyer une trame TCP fragmentée à une machine distante, mais dans laquelle il manque une petite quantité de données dans un ou plusieurs paquets.

Pour cela, on peut construire une trame altérée et changer la valeur de décalage des offsets dans les champs ou la valeur du champ "Content-lenght".

### II.4.6 *Les attaques de Spoofing :*

Les intrus utilisent IP Spoofing pour convaincre un système qu'il est en communication avec une entité connue de confiance afin de fournir l'intrus avec un accès au système. Usurpation d'adresse IP implique la modification d'un paquet au niveau de TCP, qui est utilisé pour attaquer les systèmes connectés à Internet qui offrent divers services TCP / IP. L'attaquant envoie un paquet avec une adresse IP source de, un hôte connu de confiance au lieu de sa propre adresse IP source à un hôte cible. L'hôte cible peut accepter le paquet et agir sur elle.

### II.4.7 *Balayage de port :*

L'attaque par balayage de port permet à celui-ci de découvrir des ports de communication exploitables. Cette attaque peut être évitée grâce à des systèmes de sécurité comme un pare-feu ou encore un système de détection d'intrusion. Les infrastructures du Cloud sont sensibles à ce type d'attaque si celle-ci est effectuée en parallèle. Un système tel que l'IDS analyse une partie du trafic et ne détecte donc pas une attaque par scan de port si celle-ci est effectuée avec différents scannés.

### II.4.8 *L'exploitation de bogue logiciel :*

Le client et le fournisseur doivent s'assurer que les logiciels qu'ils utilisent sont à jour afin d'éviter l'exploitation des bogues logiciels. Cette action ne permet pas de les éviter mais de limiter les risques.

### II.4.9 *L'attaque de l'homme du milieu :*

L'attaque man-in-the-middle (MITM) ou « attaque de l'homme du milieu » est une technique de piratage informatique consistant à intercepter des échanges cryptés entre deux personnes ou deux ordinateurs pour décoder les messages. L'attaquant doit donc être capable de recevoir les messages des deux parties et d'envoyer des réponses à une partie en se faisant passer pour l'autre. Le biais le plus couramment employé pour ce type d'attaque est une connexion Internet entre des ordinateurs et/ou des terminaux mobiles.

L'objectif principal d'une attaque MITM est de pouvoir espionner les communications voire, dans certains cas, modifier des contenus. Il existe différentes techniques parmi lesquelles :

- L'empoisonnement d'un Serveur DNS (*DNS poisoning*) ;
- le déni de service ou l'imposture ARP qui consiste détourné les communications sur un réseau local en se faisant passer pour un relai physique.

### II.4.10 *Analyseur de paquets :*

L'analyseur de paquets est une application ou un périphérique qui permet de lire, capturer les données qui transitent sur un réseau. Cette attaque permet à l'attaquant de récupérer les données puis les lire.

### II.4.11 *Attaque par injection malicieuse Cloud :*

Le principe de cette attaque est d'injecter sur une des plateformes du Cloud du code malicieux afin de compromettre l'infrastructure victime.

## II.5 Exemples des attaques dans l'environnement Cloud :

| Victime | Date | Type d'attaque | Description |
|---|---|---|---|
| VMWARE | Juin 2009 | CLoudBrust | Exécution de code à l'extérieur du VMWARE Guest |
| Playstation Network | Avril2011 | Injection SQL | Exploitation d'un défaut de chiffrement des données utilisateurs du PSN, obligeant la société à arrêter complètement son réseau en ligne de jeux vidéo et PlayStation Store. |
| CloudFlare | Mai 2012 | Exploitation d'une vulnérabilité Google Apps/Gmail | Une vulnérabilité dans le processus de récupération de Google Enterprise Applications qui a permis aux pirates de contourner l'authentification à deux facteurs de l'adresse URL utilisateur CloudFlare.com. |
| iCloud | Août 2012 | Vol de mot de passe et ingénierie sociale | Un journaliste possédant un compte iCloud a été victime du vol de plusieurs de ses comptes y compris l'effacement de ses données sur des périphériques Apple en utilisant iCloud. |
| Rackspace | Juin 2012 | Prédiction de mot de passe administrateur | Plusieurs failles de sécurité ont permis de prédire ou modifier le mot de passe administrateur de compte rackspace. |
| Dropbox | Juin 2012 | Vol de mot de passe et ingénierie sociale | Vol de mot de passe de compte Dropbox d'un employé et récupération d'informations concernant un projet confidentiel. Menant à une large campagne de spam. |

| | | | |
|---|---|---|---|
| Dropbox | Octobre 2012 | Analyse du client Dropbox | Analyse du client Dropbox et démonstration de vulnérabilités exploitables localement et à distance. |
| iCloud | Octobre 2014 | Violation des comptes des souscripteurs d'iCloud | La violation de plusieurs comptes des acteurs (ices), chanteurs (euses), et modèles américains. |

*Tableau II-1 Exemples d'attaques dans un environnement Cloud*

## II.6 La cryptographie :

L'homme a toujours ressenti le besoin de dissimuler des informations, bien avant même l'apparition des premiers ordinateurs et de machines à calculer. Depuis sa création, le réseau Internet a tellement évolué qu'il est devenu un outil essentiel de communication. Cependant, cette communication met de plus en plus en jeu des problèmes stratégique liés à l'activité des entreprises sur le Web. Les transactions faites à travers le réseau peuvent être interceptées, d'autant plus que les lois ont du mal à se mettre en place sur Internet, il faut donc garantir la sécurité de ces informations, c'est la cryptographie qui s'en charge.

### II.6.1 *Définitions :*

La cryptologie est la science des messages secrets. Cette discipline se décompose en cryptographie et cryptanalyse.

i) Cryptographie :

Ensemble des techniques et méthodes utilisées pour transformer un message clair en un message inintelligible. Le concept de base est celui de **chiffre** : il s'agit d'un système de cryptage où l'on remplace chaque lettre du message d'origine par une autre (ou par un symbole) en suivant un algorithme bien défini. On peut distinguer deux types de chiffres:

- ***Chiffre de substitution :*** Chaque lettre est remplacée par une autre mais garde sa place d'origine.
- ***Chiffre de transposition :*** Chaque lettre reste inchangée mais est mise à une autre place (principe de l'anagramme).

ii) Cryptanalyse :

Ensemble des techniques et méthodes utilisées pour retrouver le texte en clair à partir du texte crypté. On doit ici distinguer deux types d'opérations, selon que la personne voulant retrouver le message d'origine soit le destinataire ou un attaquant ayant intercepté le message :

- ***Déchiffrement:*** Opération par laquelle à partir d'un message chiffré on retrouve le message d'origine, connaissant l'algorithme de chiffrement et la clé.
- ***Décryptement:*** Même chose que le déchiffrement mais sans connaître la clé.

## II.6.2 *Types de cryptographie :*

**La cryptographie symétrique** et **asymétrique** est les deux familles d'algorithmes de chiffrement :

### a) La cryptographie symétrique :

Un système de chiffrement est dit **symétrique** si la clé utilisée lors du chiffrement est aussi celle utilisée lors du déchiffrement. Un tel système est aussi qualifié de **système de chiffrement à clé secrète**.

- *Exemples de chiffrement symétrique :*
  - ***Chiffre de César :*** *le décalage est de trois lettres que ça soit pour chiffrer ou déchiffrer (seul le sens du décalage change).*
  - ***Machine Enigma :*** *la position des rotors est la même lors du chiffrement ou du déchiffrement.*

Dans un tel système, les correspondants conviennent par avance d'une clé avant de commencer leurs échanges de messages. La communication des clés est d'ailleurs le problème majeur des systèmes symétriques. Il faut bien sûr qu'elle se fasse confidentiellement. D'autant plus que pour résister aux attaques des cryptanalyses, les correspondants doivent changer régulièrement de clé. Ces échanges de clés, outre le fait qu'ils soient risqués, engendrent des frais énormes. Dans les années 70 les grosses banques américaines utilisaient par exemple des courtiers pour échanger les clés. Mais la logistique devenait ingérable.

### b) La cryptographie asymétrique :

Un système de chiffrement est dit asymétrique si la clé utilisée lors du chiffrement est différente de celle utilisée lors du déchiffrement. Un tel système est aussi qualifié de système de chiffrement à clé publique.

Ce principe a été imaginé par Diffie et Hellman en 1976. Le premier algorithme le mettant en œuvre est dû à Rivest, Shamir et Adleman en 1977, et porte leurs noms : R.S.A. L'article de Diffie et Hellman contient les bases théoriques de la cryptographie asymétrique, mais ils n'avaient pas trouvé concrètement d'algorithme de chiffrement répondant à ce principe. Ce fut donc l'œuvre de Rivest, Shamir et Adleman.

Le principe est simple mais très astucieux. Les correspondants ont chacun une clé qu'ils gardent secrète et une clé dite publique qu'ils communiquent à tous. Pour envoyer un message, on le chiffre à l'aide de la clé publique du destinataire. Celui-ci utilisera sa clé secrète pour le déchiffrer. C'est comme si le destinataire mettait à disposition de tous des cadenas ouverts dont lui seul à la clé. Quand on lui écrit, on insère le message dans un coffre que l'on ferme avec un tel cadenas, et on lui adresse le tout.

- *Exemple de chiffrement asymétrique :*

  i) Chiffrement *RSA :*

Utilisation une paire de clés (des nombres entiers) composée d'une clé publique pour chiffrer et d'une clé privée pour déchiffrer des données confidentielles. Les deux clés sont créées par une personne, souvent nommée par convention Alice, qui souhaite que lui soient envoyées des données confidentielles. Alice rend la clé publique accessible. Cette clé est utilisée par ses correspondants (Bob, etc.) pour chiffrer les données qui lui sont envoyées. La clé privée est quant à elle réservée à Alice, et lui permet de déchiffrer ces données. La clé privée peut aussi être utilisée par Alice pour signer une donnée qu'elle envoie, la clé publique permettant à n'importe lequel de ses correspondants de vérifier la signature.

Une condition indispensable est qu'il soit « impossible à calculer » de déchiffrer à l'aide de la seule clé publique, en particulier de reconstituer la clé privée à partir de la clé publique, c'est-à-dire que les moyens de calcul disponibles et les méthodes connues au moment de l'échange (et le temps que le secret doit être conservé) ne le permettent pas.

Le chiffrement RSA est souvent utilisé pour communiquer une clé de chiffrement symétrique, qui permet alors de poursuivre l'échange de façon confidentielle : Bob envoie à Alice une clé de chiffrement symétrique qui peut ensuite être utilisée par Alice et Bob pour échanger des données.

### ii) *ECC (cryptographie sur les courbes elliptiques) :*

- *Présentation d'une courbe elliptique (Duquesne, 2005) :*

En mathématiques, une courbe elliptique est un cas particulier de courbe algébrique, munie entre autres propriétés d'une addition géométrique sur ses points.

On appelle courbe elliptique sur R toute courbe plane d'équation $\mathbf{y^2=x^3+ax+b}$, où le discriminant $\mathbf{-(4a^3+27b^2)}$ de $\mathbf{x^3+ax+b}$ est non nul. On rajoute à cette courbe un point à l'infini noté ***O***.

L'intérêt de ces courbes elliptiques est qu'on peut les munir d'une opération de groupe commutatif. Prenons ***P*** et ***Q*** deux points distincts de la courbe elliptique (et différents du point à l'infini ***O)***. On trace la droite ***(PQ)***. Deux cas peuvent se produire :

- La droite coupe la courbe en un 3$^{ème}$ point (on note qu'il y a au plus 3 points d'intersection entre une droite et la courbe). Le symétrique de ce 3$^{ème}$ point par rapport à l'axe des abscisses est ***P+Q***.
- La droite ne coupe la courbe qu'en ***P*** et ***Q***. Ceci n'est possible que si ***(PQ)*** est parallèle à l'axe des ordonnées. On définit alors ***P+Q=O*** (point à l'infini).

- ***Exemples de courbes elliptiques :***

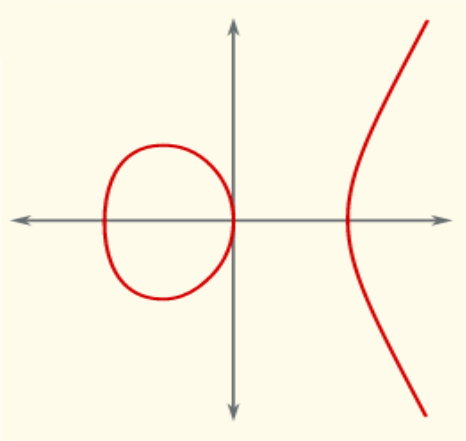


*Figure II-1 Représentation de la courbe elliptique y2=x3 –x*

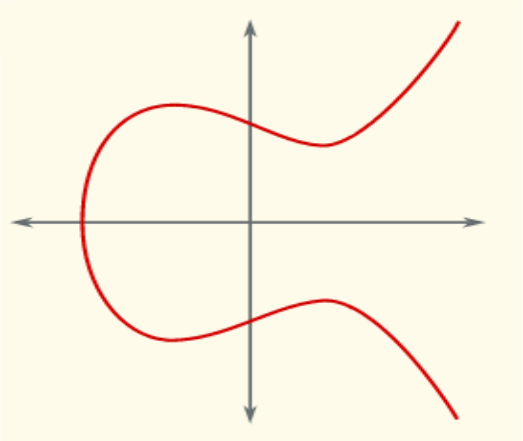


*Figure II-2 Représentation de la courbe elliptique y2 = x3 - x 1*

- *Cryptographie basée sur les courbes elliptiques :*

La cryptographie asymétrique basée sur les courbes elliptiques est née en 1985, indépendamment par V. Miller [3] et N. Koblitz [4].

ECC est un crypto-système asymétrique standardisé par le consortium IEEE [5]. La sécurité de ce crypto-système est basée sur la difficulté de résolution du problème du logarithme discret.

ECC utilise un groupe fini composé de points ***(x, y)*** se trouvant sur une courbe elliptique dont la procédure de cryptage et de décryptage est basée sur l'addition et la multiplication (addition successive du même point) des points mentionnés précédemment.

L'utilisation de ce crypto-système s'effectue en trois(3) étapes :

- **Génération des clés** :

Il s'agit d'un échange de clés à la manière de *Diffie et Hellman*, c'est à-dire sans se les communiquer directement. Le client et le Serveur se mettent d'accord ensemble et publiquement sur une courbe elliptique $E(a,b,K)$, c'est-à-dire qu'ils choisissent un corps fini $K$ (par exemple, $Z/pZ$) et une courbe elliptique $y^2=x^3+ax^2+b$. Ils choisissent aussi ensemble, et toujours publiquement, un point $P$ situé sur la courbe.

Ensuite, chacun de leur côté, et secrètement, le client choisit un entier $k_a$et le serveur choisit un entier $k_b$. Le client envoie au Serveur le point de la courbe elliptique $k_aP$, et le serveur envoie au client le point $k_bP$.

Chacun de leur côté, ils sont capables de calculer $k_a(k_bP)=k_a(k_bP)=(k_ak_b)\ P$. Ce point de la courbe elliptique constitue leur clé secrète.

Le tableau suivant permet de donner une explication plus simple sur la génération des clés basé sur les courbes elliptiques :

| | Client | Serveur |
|---|---|---|
| Etape 1 | Le client et le serveur choisissent ensemble une courbe elliptique $E(a,b,K)$ et un point $P$ sur la courbe. Cet échange n'a pas besoin d'être sécurisé. | |
| Etape2 | Le client choisit secrètement $k_a$ et envoie $k_aP$ au serveur. Cet échange n'a pas besoin d'être sécurisé. | Le Serveur choisit secrètement $k_b$ et envoie $k_bP$ au client. Cet échange n'a pas besoin d'être sécurisé. |
| Etape3 | Le client calcule $k_a(k_bP)=(k_ak_b)P$. | Le serveur calcule $k_b(k_aP)=(k_ak_b)P$. |

*Tableau II-2 génération et échange des clés ECC Deffie-Hellman*

On note que si quelqu'un a espionné leurs échanges, il connait $E(a,b,K)$, $P$, $k_aP$ et $k_bP$. Pour pouvoir retrouver la clé $k_ak_bP$, il faut pouvoir calculer $k_A$ connaissant $P$ et $k_aP$. C'est ce que l'on appelle résoudre le logarithme discret sur la courbe elliptique.

- ***Le Logarithme discret :***

Problème mathématique sous- jacent aux algorithmes asymétriques comme Diffie- Hellman et les Courbes Elliptiques. C'est le problème inverse de l'exponentiation modulo $N$, qui est une fonction à sens unique.

❑ ***Explication :***

Soit P un point de la courbe elliptique tel que ***k*P*** est une succession d'addition du point ***P*** qui donne le point à l'infini ***O,*** tel que***: k*P=P+P+P+P+P+P+P +…***

Le problème du logarithme discret dit que même si on connait la valeur ***k*P*** et la valeur de ***P*** on ne peut pas trouver la valeur de ***k***.

- **Chiffrement et Déchiffrement:**

Le client veut envoyer au Serveur un message en utilisant un algorithme de chiffrement par courbes elliptiques. Le serveur commence par fabriquer une clé publique de la façon suivante : Il choisit une courbe elliptique ***E(a,b,K)***, un point ***P*** de la courbe, et un entier $k_b$. Sa clé publique est constituée par la courbe elliptique ***E(a,b,K)*** et par les points ***P*** et $k_bP$ de cette courbe elliptique. Sa clé privée est l'entier $k_b$, qu'on ne peut pas retrouver même connaissant ***P*** et $k_bP$, par la difficulté de résoudre le problème du logarithme discret sur une courbe elliptique.

Lorsque le client veut envoyer de façon secrète un point ***M*** de la courbe elliptique au Serveur, voici l'échange qui se passe :

| | Client | Serveur |
|---|---|---|
| Etape 1 | Le client prend connaissance de la clé publique ***(E,a,b,K)***, ***P*** et $k_BP$ | |
| Etape 2 | Il choisit secrètement et aléatoirement un entier ***n***. | |
| Etape 3 | Le client calcule ***nP*** et $M+nk_BP$ et envoie ces deux points | |
| Etape 4 | | Avec sa clé privé $k_B$, le Serveur calcule $nk_BP$ à partir de ***nP***, puis il calcule $(M+nk_BP) - nk_BP$. Il retrouve ***M***. |

*Tableau II-3 exemple d'échange d'un point de la courbe envoyé d'une façon secrète au serveur.*

Le client et le serveur, tous les deux, fabriquent une clé secrète partagée qu'ils vont l'utiliser plus tard pour le chiffrement/déchiffrement en employant les méthodes qui conviennent.

### iii) ECDSA (Elliptic Curve Digital Signature Algorithm) :

***Elliptic Curve Digital Signature Algorithm*** (**ECDSA**) est un algorithme de signature numérique à clé publique, variante de DSA. Il fait appel à la cryptographie sur les courbes elliptiques.

Les avantages d'ECDSA sont des longueurs de clés plus courtes et des opérations de signature et de chiffrement plus rapides.

- *Signature :*

- ✓ Choisir de manière aléatoire un nombre *k* entre 1 et *n*-1.
- ✓ Calculer ***(i,j)=k*P.***
- ✓ Calculer ***x=i mod n*** ; ***si x=0***, aller à la première étape.
- ✓ Calculer $y=k^{-1}(H(m)+s*x) \bmod n$ où ***H(m)*** est le résultat d'un hachage cryptographique sur le message ***m*** à signer (le NIST et l'ANSSI conseillent de ne plus utiliser SHA-1 mais SHA-256 ou SHA-512).
- ✓ Si ***y=0***, aller à la première étape.
- ✓ La signature est la paire ***(x, y)***.

- *Vérification :*

- ✓ Vérifier que ***Q*** est différent de ***O*** (le point à l'infini) et que ***Q*** appartient bien à la courbe elliptique.
- ✓ Vérifier que ***nQ*** donne ***O.***
- ✓ Contrôler que ***x*** et ***y*** sont bien entre 1 et ***n-1.***
- ✓ Calculer $(i,j)= (H(m)y^{-1} \bmod n)G + (xy^{-1} \bmod n)Q.$
- ✓ Vérifier que ***x=i mod n.***

❖ *Sécurité :*

Puisque tous les algorithmes connus pour résoudre le problème du logarithme discret sur les courbes elliptiques sont en $O\sqrt{n}$ (Baby-step giant-step, L'algorithme de rho Pollard), la taille du corps doit donc être approximativement deux fois plus grande que le paramètre de sécurité voulu. Pour un degré de sécurité de ***128-bits*** (***AES-128, RSA-3072***), on prendra une courbe sur un corps $F_q$, où $q=2^{256}$.

## II.6.3 *Fonction de hachage :*

### a) Définition :

Une fonction de hachage est aussi appelée fonction de hachage à sens unique ou "one-way hash function" en anglais. Ce type de fonction est très utilisé en cryptographie, principalement dans le but de réduire la taille des données à traiter par la fonction de cryptage. En effet, la caractéristique principale d'une fonction de hachage est de prendre en entrée un message de taille quelconque, applique une série de transformations et réduit ces données. On obtient à la sortie une chaîne de caractères, le condensé qui résume en quelque sorte le fichier. Cette sortie a une taille fixe qui varie selon les algorithmes (128 bits pour MD5 et 160 bits pour SHA-1).

### b) Propriétés :

- ***La longueur de la signature :*** *elle* doit être toujours la même quel que soit la longueur des données en entrée.
- ***Résistance à pré-image*** : Il n'est pas possible de trouver les données originales à partir des empreintes : Les fonctions de hachage ne fonctionnent que dans un seul sens.
- ***Il ne doit pas être possible de prédire une signature***.
- ***Résistance aux collisions*** : Evidemment pour des données différentes les signatures doivent être différentes.
- ***Effet d'avalanche*** : C'est une caractéristique de l'algorithme de hachage qui est en plus aide à la résistance à la pré-image. Elle décrit le fait qu'il y ait des modifications de plus en plus importantes au fur et à mesure que l'on avance dans l'algorithme. Si ce critère est respecté alors deux données qui sont très semblables auront des hachés totalement différents.

❑ **Exemples :**

- **MD5** : L'algorithme MD5, pour Message Digest 5, est une fonction de hachage cryptographique qui permet d'obtenir l'empreinte numérique d'un fichier (on parle souvent de message). Il a été inventé par Ronald Rivest en 1991.Si l'algorithme MD5 présente un intérêt historique important il est aujourd'hui considéré comme dépassé et absolument impropre à toute utilisation en cryptographie ou en sécurité.
- **SHA** : L'acronyme SHA, pour Secure Hash Algorithm, désigne une fonction de hachage cryptographique conçue par l'Agence Nationale de Sécurité américaine. Il en existe

plusieurs versions. Parmi les plus connues, on peut citer le SHA-2, le SHA-256 ou encore le SHA-512. Tous définissent des algorithmes de hachage utilisés par des autorités administratives pour la signature de certificats. Tous génèrent des condensats uniques.

- **SHA-0** : le SHA d'origine, a été introduit au début des années 1990. Il a, depuis, été décliné et amélioré au fil des années pour proposer de nouveaux algorithmes plus performants et apporter une réponse aux nouvelles failles et aux nouveaux éléments de vulnérabilité des ordinateurs (qui eux aussi évoluent avec le temps). Le SHA-0 est ainsi devenu totalement obsolète aujourd'hui alors que les nouvelles déclinaisons de l'algorithme affichent une meilleure résistance face aux attaques.

### II.6.4 *La signature digitale :*

#### a) Définition :

La signature digitale est un mécanisme informatique, basé sur l'utilisation de fonctions cryptographiques, visant à apporter les mêmes fonctionnalités et garanties que la signature manuscrite. Ce concept est également désigné par les termes « signature électronique » ou « signature numérique ». L'adjectif « digital » ne se réfère donc pas aux doigts mais bien aux nombres (« digit » en anglais).

Au même titre que la signature manuscrite d'un document papier, la signature digitale d'un document électronique permet d'établir un lien entre le document et le signataire. Le lien ainsi établi peut avoir plusieurs buts définis par le document lui-même ou par le contexte dans lequel la signature s'applique, par exemple:

- Identifier l'auteur d'un document.
- Marquer l'accord du signataire sur les termes du document.
- Indiquer que le document a été lu par le signataire.

#### b) Propriétés :

Techniquement, il existe actuellement plusieurs formats standards en matière de signature digitale de document, ces formats définissent plusieurs niveaux de signature. Chacun de ces niveaux apporte des garanties supplémentaires au prix d'une complexité accrue du format de signature.

Les formats de signature simple, dont le représentant le plus connu est « PKCS#7/CMS », apportent toujours les garanties suivantes :

- ***Identification du signataire*** : la signature permet de déterminer avec certitude l'identité du signataire du document.
- ***Intégrité du document*** : la signature permet de vérifier que le document n'a pas été altéré depuis que la signature a été produite.
- ***Non-répudiation faible du signataire :*** le signataire ne peut pas nier avoir signé le document sauf si le moyen de signature utilisé a été compromis. Par exemple, si un utilisateur utilise sa carte d'identité électronique pour signer électroniquement un document, il ne pourra ultérieurement pas nier avoir signé le document à moins de pouvoir prouver le vol ou le piratage de sa carte d'identité électronique.

Les formats plus complexes sont connus sous la catégorisation de « formats de signature électronique avancée ». Les standards qui décrivent ces formats sont « CAdES » pour la signature dite binaire et « XAdES » pour la signature XML. Ces formats permettent à la signature de fournir des garanties supplémentaires, par exemple la non-répudiation forte du signataire (le signataire ne peut pas nier avoir signé le document à la date indiquée par la signature).

### c) Fonctionnement :

Pour signer un message :

1. L'expéditeur calcule d'abord le 'digest' (empreinte) du message d'origine à l'aide d'un algorithme de hachage.
2. Ensuite, il crypte ce digest, par cryptage asymétrique, en utilisant sa clé privée.
3. Il associe finalement à ce dernier résultat ses données d'identification, contenues dans un certificat. Il envoie le tout (message clair, digest crypté et certificat) au destinataire.

Le destinataire du message peut appliquer la technique inverse afin de vérifier la validité de la signature :

4. Il calcule lui-même le digest du message reçu.
5. Il extrait le certificat afin de déterminer l'identité de l'expéditeur supposé et sa clé publique ; il utilise cette clé publique pour décrypter le digest en utilisant le même algorithme de cryptage asymétrique que l'expéditeur.

6. Il compare le digest qu'il a calculé avec celui extrait de la signature: la concordance des valeurs des deux digests garantit l'authenticité du message.

### II.6.5 *Certificat numérique :*

#### a) Définition :

Un certificat électronique fait office de pièce d'identité électronique sur Internet et permet d'établir un environnement de confiance entre deux entités distantes qui ont besoin de s'authentifier pour communiquer entre elles et d'échanger des informations confidentielles.
Un certificat spécifie le nom d'une entité et certifie que la clé publique incluse dans le certificat lui appartient. Tout certificat électronique est émis par un tiers de confiance ou autorité de certification.

Le certificat numérique est :

- **infalsifiable** : il est crypté pour empêcher toute modification,
- **nominatif** : il est délivré à une entité (comme la carte d'identité est délivrée à une personne et une seule),
- **certifié** : il y a le « tampon » de l'autorité qui l'a délivré.

Le certificat est composé de 2 parties essentielles :

1. **Les informations d'identité du certificat :**
   - nom du porteur
   - adresse du porteur
   - les dates de début et de fin de validité
   - le nom de l'autorité de certification (CA : Certificate Authority)
   - …
2. **La signature de l'autorité de certification :**
   - cette signature est chiffrée. *(cela va permettre de vérifier que le certificat est bien délivré par l'autorité de certification)*

### b) Les types de certificats :

Il existe quatre(4) types de certificats électroniques :

- ***Certificat de signature:*** Il permet d'associer l'identité d'une personne à une clé publique. Il peut être utilisé pour signer des messages électroniques ainsi que pour s'authentifier lors d'une session sécurisée par exemple pour émettre un virement bancaire.
- ***Certificat serveur:*** Il associe l'identité d'un serveur Web à une clé publique. Il permet la sécurisation des échanges entre le serveur et ses clients lors de l'établissement d'une session sécurisée par exemple pour un achat ou paiement en ligne sur un site marchand.
- ***Certificats VPN:*** Il permet d'associer des informations relatives à certains nœuds du réseau (routeurs, firewalls, concentrateurs …) à une clé publique. Ce certificat est utilisé pour garantir la sécurité des échanges effectués entre une organisation et ses filiales à travers des tunnels sécurisés dans le réseau de communication.
- ***Certificat de signature de code:*** Il permet de signer un programme, un script ou un logiciel pour garantir son authenticité par la signature de son développeur. Il permet aussi de le protéger contre le risque de piratage.

## II.7 Conclusion :

Dans le monde moderne, les utilisateurs finaux et les entreprises utilisent les environnements Cloud pour le stockage et le partage de ses données, alors ces environnements deviennent très menacés par les cyber-attaquants, pour cela les experts de la sécurité d'information déploient plusieurs techniques de sécurité, comme ceux du chiffrement, le hachage, la signature digitale, et les certificats numériques…etc., afin d'assurer la sécurité du Cloud, et faire face à ces menaces.

# Chapitre III :

# Approche proposée pour la gestion d'authentification dans un environnement Cloud

# Chapitre III. Approche proposée pour la gestion d'authentification dans un environnement Cloud :

## III.1.1 *Introduction :*

Les environnements Cloud sont un sujet à la mode dans nos jours, l'utilisation vaste de ces derniers par les utilisateurs finaux et les entreprises les rendent très menacés par les cyber-attaquants dans le but de violations des comptes, des données, ou bien juste un challenge ; donc la sécurité de ces environnements est devenue un sujet prioritaire pour les experts de la sécurité informatique. Cette sécurité a plusieurs aspects, nous en avons cité quelques-uns précédemment, dans notre contexte on s'intéresse surtout par l'authentification.

Dans ce chapitre on va expliquer la contribution proposée en présentant la démarche à suivre et les outils nécessaires pour sa réalisation et son implémentation dans un Environnement Cloud proposé en utilisant des techniques de chiffrement basé sur les courbes elliptiques, le hachage, la signature digitale, et le certificat.

## III.1.2 *L'approche de sécurité proposée pour la gestion d'authentification :*

Le but de la majorité des attaques modernes sur les environnements Cloud est la violation de données des utilisateurs, d'où les hackers utilisent l'attaque 'l'homme au milieu' « Man In The Middle » dont l'attaquant récupère les informations de la victime et puis il les altère, par conséquent le compte sera à lui. En prenant ça en considération, on a décidé que la meilleure façon pour sécuriser un environnement Cloud c'est de faire une gestion du contrôle d'accès.

Pour cela, on utilise la cryptographie basée sur les courbes elliptiques pour chiffrer un haché généré depuis le nom d'utilisateur et le mot de passe de l'utilisateur légitime de l'application Cloud.

Avant de présenter notre contribution, on décrit tout d'abord l'environnement dans lequel sera appliquée ainsi que les outils matériels et logiciels pour y parvenir.

### III.1.3 *Environnement :*

En utilisant le langage java sur l'IDE NetBeans, on a essayé de développer une application client/serveur pour simuler un environnement Cloud, où l'utilisateur peut se connecter en toute sécurité pour stocker ses fichiers dans le serveur Cloud depuis n'importe quelle machine contenant l'application, et vice versa, il peut télécharger un de ses fichiers sur son disque dur à tout moment.

L'application simulé contient deux profiles, Client cité ci-dessus et Administrateur, qui s'occupe de la gestion manuelle de la sécurité de cet environnement, où il peut suivre les activités des attaquants, re-garantie la connexion au machines bannies, communiquer avec un utilisateur (alerte par mobile), supprime un fichier que lui semble malicieux (image.exe par exemple); et enfin, un administrateur peut ajouter un autre administrateur.

Dans cette optique, on propose un mécanisme de sécurité pour vérifier l'authentification dans ce type d'applications.

### III.1.4 *Les étapes de la contribution :*

Avant de présenter les étapes de la contribution, on décrit brièvement l'architecture de l'application qu'on va développer. La figure ci-dessous résume cette architecture.

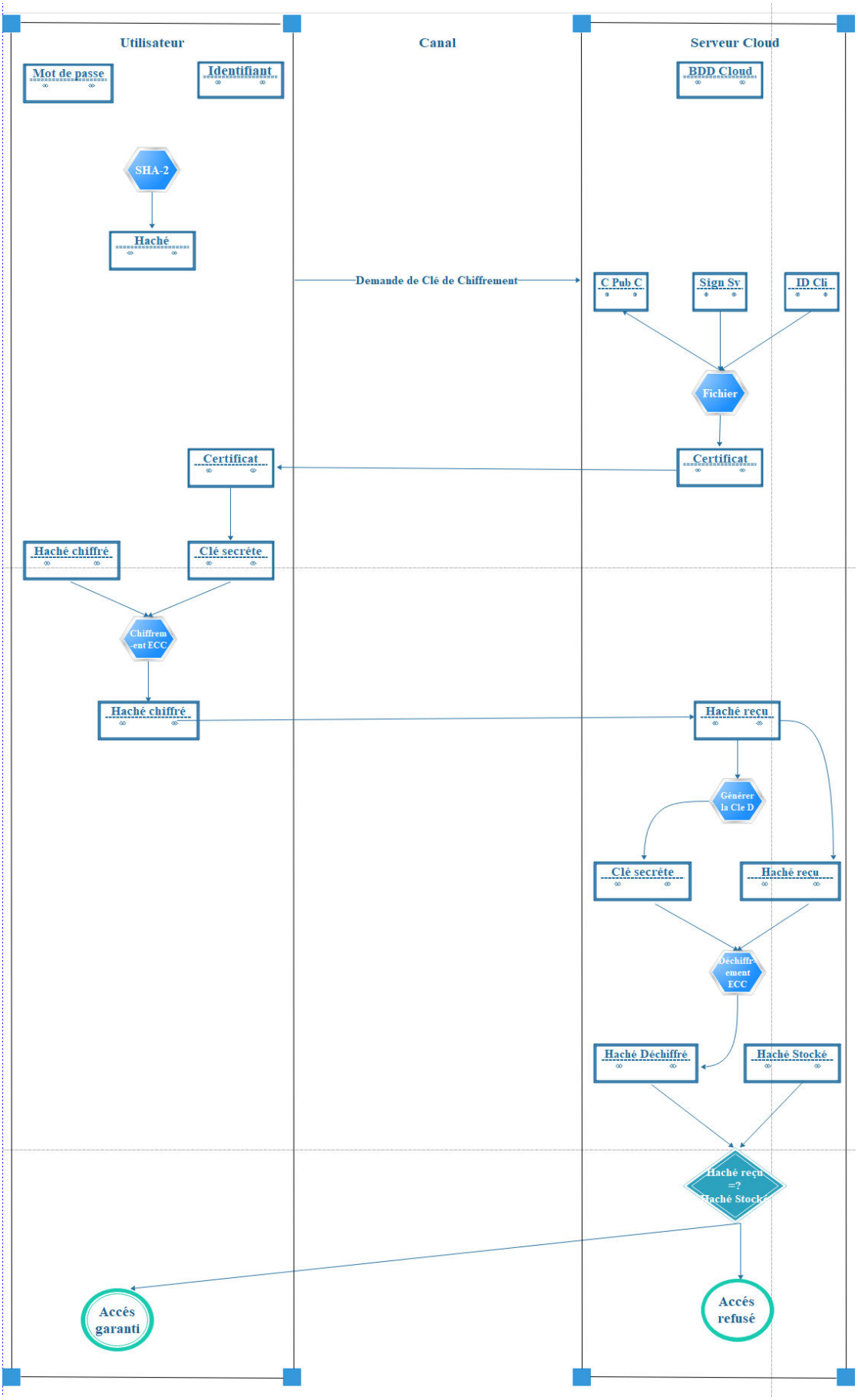



*Figure III-1 Schéma récapitulatif de la contribution*

La démarche qu'on a suivie pour établir notre mécanisme de sécurité s'exécute selon le schéma algorithmique suivant :

- Créer Compte () ;
  - Générer un mot de passe pour l'utilisateur **pwd = gen_mdp(X)** ;
  - Calculer le haché (**H**) à partir du mot de passe (**pwd**) et l'identifiant (**X**) en utilisant une fonction de Hachage **f ()** :

    **H = f (pwd, X)** ;
- Authentification (id, mdp) ;
  - Générer un haché ($H_1$) à partir du mot de passe (**mdp**) et l'identifiant (**id**)

    $H_1$**= f (pwd, X)** ;
  - Générer un certificat (**certificat : Fichier**) pour le client.
  - Générer deux signatures digitales Serveur: $S_1 (r_1, n_1)$, Client: $S_2 (r_2, n_2)$.
  - Echange $S_1$ et $S_2$ : **Client/serveur** protocole **Deffie_Hellman ;**
  - Vérification de signature (**V**) :
    - Utilisateur :
      - Si **V== vrai** alors Extraire clé publique depuis certificat
        - Générer clé secrète

          $k_{seccli}$**= KeyAgreement(**$K_{pubserv}$**,**$k_{privcli}$**)** ;
        - $H_{chiffré}$ **= Chiffrer (**$H_1$**,**$K_{seccli}$**)**;
        - Envoie de $H_{chiffré}$ au serveur
      - Sinon
        - **Sortir** () ;
    - Serveur :
      - Si **V== vrai** alors accepter clé publique du Client ;
        - Générer clé secrète

          $K_{secserv}$ **=KeyAgreement(**$K_{pubcli}$**,**$k_{privserv}$**)**
        - $H_{dechiff=}$ **Déchiffrer (**$H_{chiffré}$**,** $K_{secserv}$**)**
        - **Si** $H_{dechiff}$**==H**

          alors accès_garanti(**id**);

          sinon
          - **tentatives=tentative+1**;
          - accés_refusé (**id**);

          finsi ;

          finsi ;
- Si **tentatives==3**
  - alors Alert_email (**id**); finsi;
- Si **tentatives==6**
  - alors Alerte_mobile (**id**); Bannir_MAC (**id**);

    finsi ; fin ;

## III.2 Implémentation de l'algorithme :

Le but principal de l'application est la gestion du contrôle d'accès pour les utilisateurs, et comme cité précédemment, on a utilisé la cryptographie basée sur les courbes elliptiques pour le chiffrement et le déchiffrement. Voici les étapes de l'implémentation de ces algorithmes :

### III.2.1 *Fonction de hachage :*

Le choix de la fonction de hachage est décidé en prenant en compte les contraintes suivantes :

- ✓ Une fonction de hachage sans collisions.
- ✓ La robustesse du haché généré.
- ✓ Un haché assez léger par rapport aux environnements Cloud.

Les causes ci-dessus ont influencé notre décision pour l'utilisation de l'algorithme SHA-256.

- ➢ ***Implémentation :***
  - Générer un haché 'Digest' (empreintes) depuis l'identifiant et le mot de passe de l'utilisateur en utilisant la fonction de hachage SHA-256.
  - Pour utiliser le haché dans les autres étapes, on les affecte dans un Buffer de type String en effectuant les changements nécessaires.

### III.2.2 *Cryptage du haché avec le EC- DSA(Digital Signature Algorithme) :*

Dans cette étape, on utilise la cryptographie basée les courbes elliptiques pour sécuriser le haché échanger entre le client et le serveur Cloud. L'échange des clés entre le client et le serveur est assuré grâce au protocole de *Diffie-Hellman*. Voici l'implémentation de chiffrement/déchiffrement en utilisant les courbes elliptiques :

#### a) Fonction chiffrement ('crypter ') :

La méthode '***crypter***' sert à chiffrer une chaine de caractère en prenant en compte la clé privée du serveur en utilisant les bibliothèques de sécurité de java :

✓ Utiliser la bibliothèque '***Chiper***' en mode chiffrement(***ENCRYPT_MODE***) en utilisant la clé secrète calculé pour chiffrer le message qui est de type chaine de caractère en lui transformant en suite d'octets.

### b) Fonction déchiffrement ('decrypter') :

La méthode '***decrypter***' sert à déchiffrer une chaine de caractère chiffré en prenant comme paramètre une clé + une suite d'octets, et en utilisant bibliothèque '***Chiper***' en mode chiffrement(***DECRYPT_MODE***), c'est le sens inverse de l'implémentation de la méthode de chiffrement ('***crypter***').

### c) Génération de clés :

Dans cette étape on décrit l'algorithme qu'on a suit pour générer les clés du chiffrement et de déchiffrement .Cette étape contient elle même trois(**3**) sous étapes :

#### i) Préparation de clés :

- ✓ Le client et le Serveur génèrent une paire de clés publiques prét à être échanger selon le protocole *Deffie-Hellman*. en utilisant les instances fournisses par la bibliothèque '***BouncyCastle***' :
  - ***SecureRandom*** : dans le but de générer un nombre aléatoire fort en cryptographie (utilisé dans les spécifications de générateur de clé ('***KeyPairGenerator***'))
  - ***KeyPairGenerator*** : pour générer les clés publiques et privés .il faut mentionner le fournisseur de la courbe (chaque type de courbe a un fournisseur spécifié ; dans notre cas c'est (***EC,SunEC***).
  - ***ECGenParameterSpec*** : spécifié le type de courbe utilisé ( '***spec256r1***').

On utilise la notion de certificat lors de l'échange des clés entre l'utilisateur et le serveur ce qui permet au client de vérifier la source de cette clé.

#### ii) Signature :

- ✓ On génère une signature pour le client prés à être envoyé au serveur (la même démarche coté serveur) en basant sur l'instance ('***Signature***') : la signature générer est un couple ***(r,t)*** dont la taille de chacune égale à 20 octets.
- ✓ Le client et le Serveur échangent leurs signatures afin de les vérifier.

#### iii) Vérification :

- ✓ Le client vérifie la signature reçus avec la signature calculé ('***initVerify()***').la même chose coté serveur. Si vérification des signatures est validée alors :
  - Le client utilise sa clé privé et la clé publique du serveur pour générer la clé secrète ('***KeyAgreement***').
  - La même démarche coté serveur.

- Si l'opération s'effectue correctement alors les deux clés secrètes calculées sont égales (c'est le principe de la cryptographie basé sur les courbes elliptique).

L'algorithme de signature digitale assure l'intégrité des clés échangées entre le client et le serveur.

#### d) Chiffrement ECC :

- ✓ Le client demande récupère les clés depuis le certificat fournit par le serveur et donc générer la clé secrète.
- ✓ On déploie une méthode de chiffrement '***crypter*** ' qui prend en paramètre la clé secrète et le haché générer et qui lui rend chiffré (la méthode est déployer dans une autre méthode '***UseC*** 'pour le chiffrement).

#### e) Déchiffrement ECC :

- ✓ Le serveur quand il reçoit le haché du client lors de l'authentification chiffré, utilise sa clé secrète dans la méthode '***decrypter***' qui est déployer dans la méthode '***UseD***' pour déchiffrer ce haché reçu.

## III.3 Fonctionnement de l'application :

Dans cette section, on décrit l'architecture de l'application, qui est composé de deux parties : Client, Serveur Cloud, et le canal qui relie entre les deux: Internet.

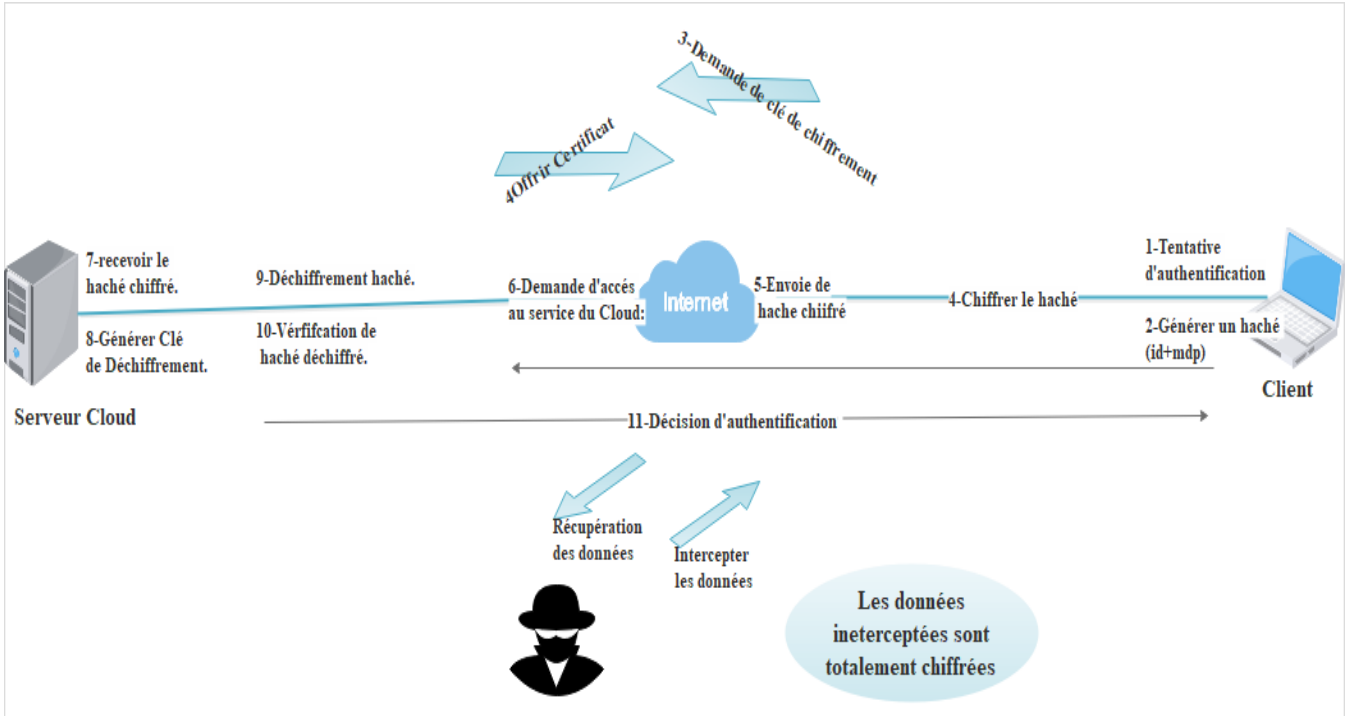



*Figure III-2 Fonctionnement générale de l'application.*

### III.3.1 *La base de données :*

Le schéma de la base de données (‘***CloudSec***’) du Serveur Cloud est comme sui :

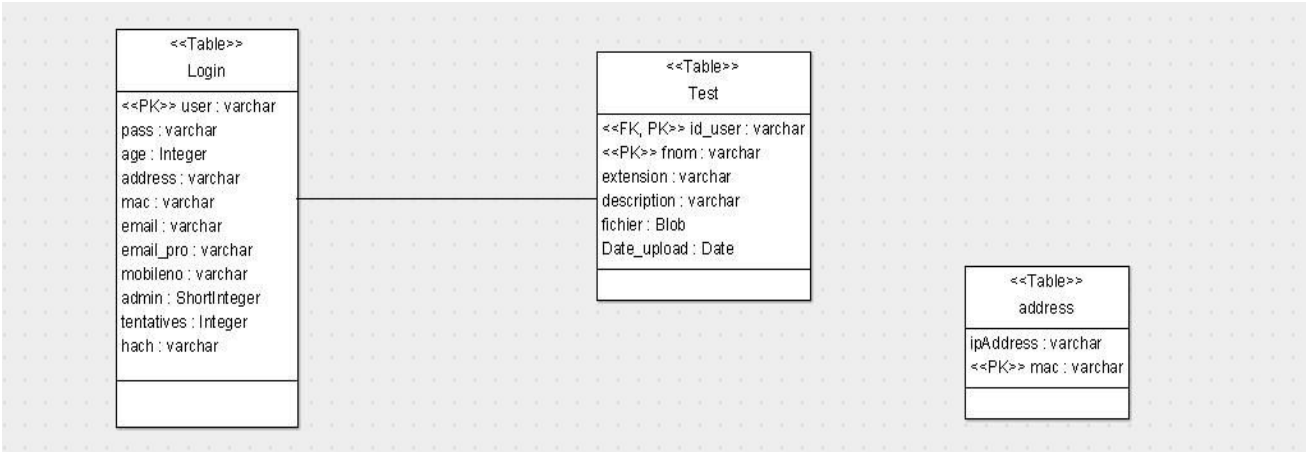



*Figure III-3 Diagramme de séquence décrit le schéma de la base de données 'CloudSec'*

- ✓ ***La table login*** : Contient les informations sur les différents utilisateurs :
  - ***user*** : le nom d'utilisateur du client/ administrateur qui utilise l'application.
  - ***pass*** : mot de passe du client/ administrateur qui utilise l'application.
  - ***age*** : l'âge de l'utilisateur.
  - ***address*** : l'adresse IP de la machine d'où le client vient de s'inscrire.
  - ***mac*** : l'adresse mac de la machine d'où le client vient de s'inscrire.
  - ***email*** : Adresse email de l'utilisateur.
  - ***email-pro*** : Seulement pour les administrateurs (e-mail fixe: *testCloud488@gmail.com*) ajouter automatiquement lors de la saisie des informations d'un nouvel administrateur.
  - ***mobileno*** : le numéro de téléphone de l'utilisateur.
  - ***admin*** : prend automatiquement la valeur 1 pour administrateur, 0 pour client.
  - ***tentatives*** : nombre de tentatives mis par un utilisateur sans succès (revient à 1 lors une connexion à succès, 0 lors de déconnexion).
  - ***hash*** : générer par SHA-2 hach(user,pass) .
- ✓ ***La table 'address'*** : Contient tous les adresses IP et les adresses mac bannies.
- ✓ ***La table 'test'*** : Contient les fichiers stocké par l'utilisateur :
  - ***id_user*** : l'utilisateur qui a téléchargé le fichier vers le Cloud.
  - ***fnom*** : nom de fichier.
  - ***extension*** : extension de fichier.
  - ***description*** : une description de fichier.

- ***fichier*** : le fichier sous forme octets (BLOB).
- ***Date_upload*** : date de stockage du fichier.

❑ ***Remarque :*** il n ya aucune relation entre la table '***login***' et la table '***adress***' malgré l'existence de '***ip***' et '***mac***' dans les deux table, car on banni tous les machines qui mit six(6) tentatives, même si l'utilisateur de cette machine ne possède pas un compte (donc les adresses n'apparait pas dans la tables login et pourtant ils seront bannies).

### III.3.2 *Client :*

Le client, qui possède déjà un compte dans l'application, a toutes les fonctionnalités qu'il peut trouver dans tous les environnements Cloud dédiés au stockage externe. Alors, il peut télécharger des fichiers vers le serveur Cloud, et les stocker là-bas ; comme il peut les télécharger sur disque dur du nouveau.

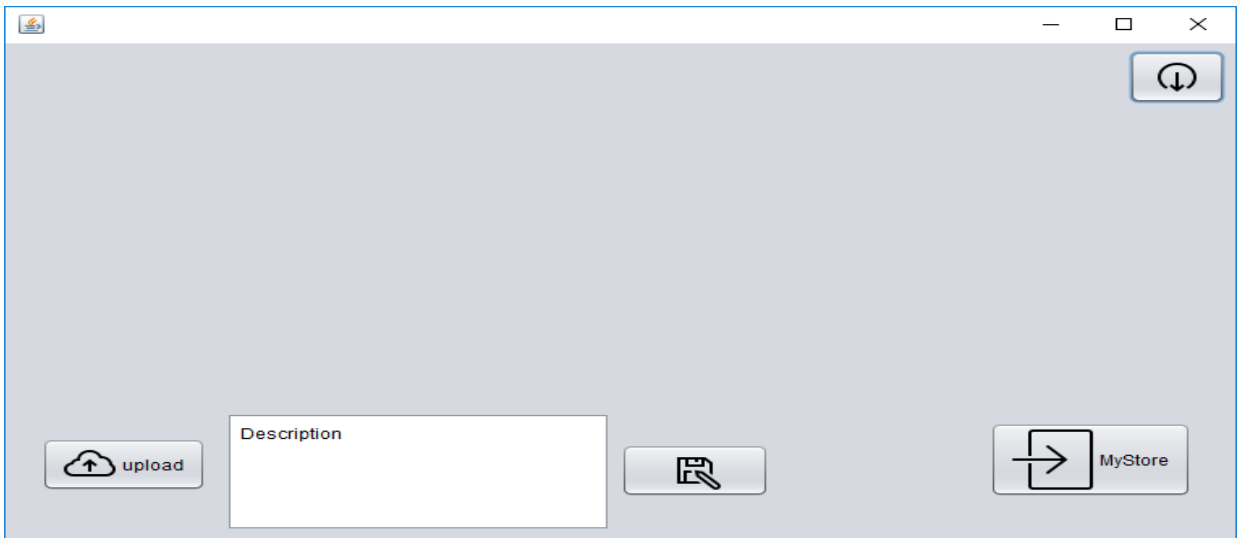



*Figure III-4 1ere interface client : Télécharger vers le Cloud.*

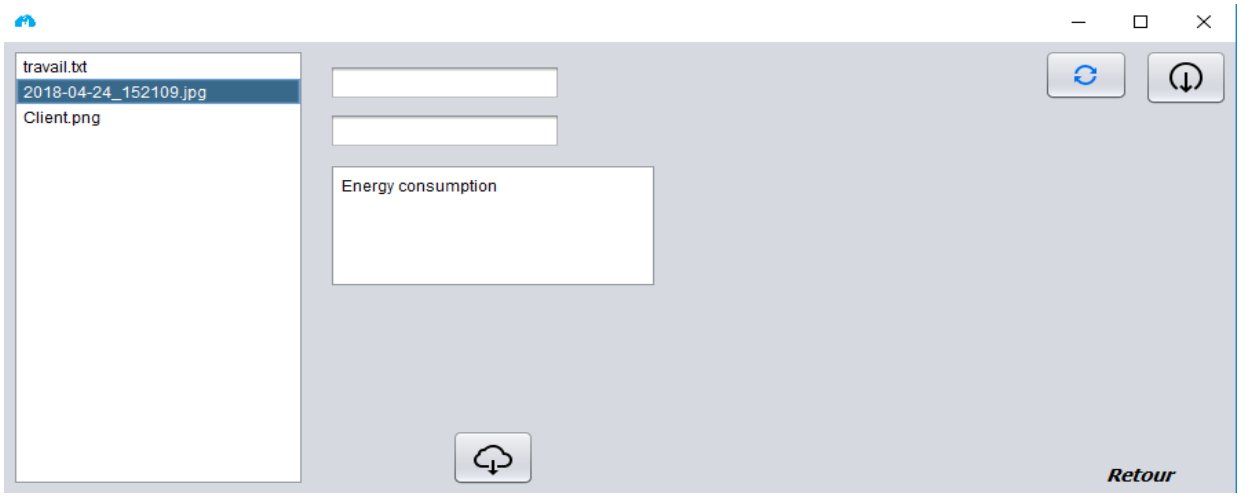



*Figure III-5 2emme interface client : Télécharger depuis le Cloud*

### a) Création de compte :

Pour une première utilisation de l'application, les utilisateurs qui n'ont pas de compte sur notre environnement Cloud, peuvent créer un, en introduisant ses informations nécessaires. Pour plus de sécurité, le mot de passe n'est pas proposé par le client, mais par l'application elle-même, dont la possibilité de trouver le mot de passe en devinant égale à $8^{96}$ possibilités, le mot de passe ensuite, va être envoyé d'une façon sécurisée vers le mail du client qui est introduis par lui. On note que c'est interdit à un utilisateur d'introduire un identifiant, un email, ou un numéro de téléphone qui existe déjà dans la base de données.


*Figure III-6 Interface Créer un compte.*

## III.3.3 *Administrateur :*

L'administrateur de l'autre côté, peut faire une gestion de sécurité manuelle, où il peut suivre les activités des attaques sur les comptes des utilisateurs, ré-autorisé la connexion à l'application aux machines bannies, supprimer des fichiers qui lui paraissent malicieux, et avertir un client sur son mobile, il peut aussi ajouter un autre administrateur comme cité ci-dessus.

Le premier utilisateur est un administrateur, et est ajouté manuellement par le développeur de l'application, cet administrateur peut également ajouter d'autres administrateurs.

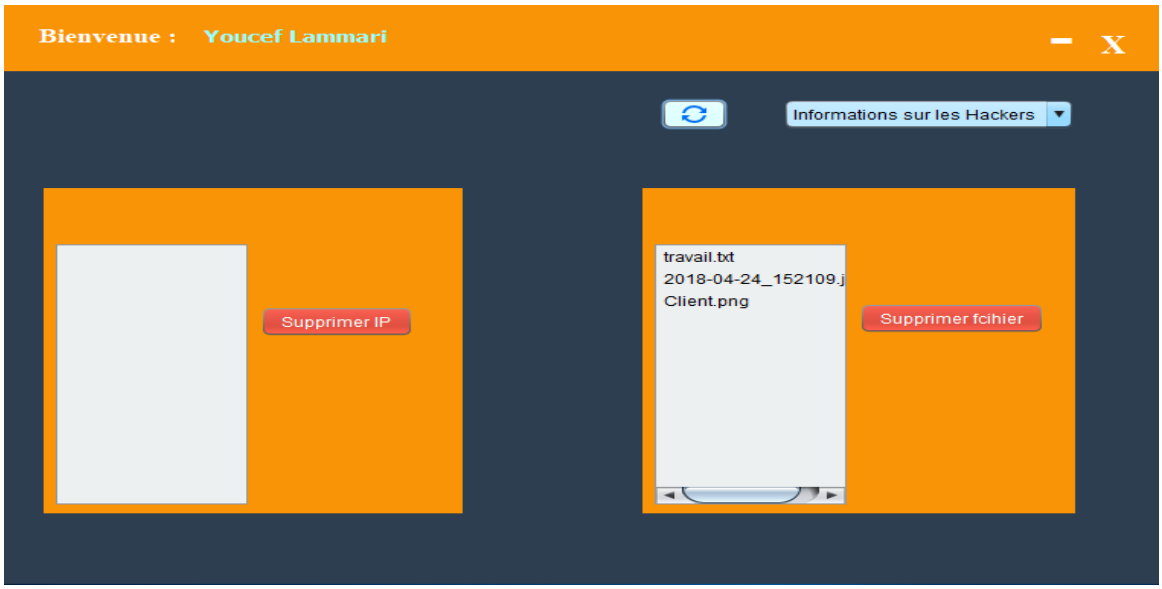



*Figure III-7 Interface Administrateur*

On peut résumer la différence entre un client et un administrateur en trois points :

i. L'email professionnel (email pro) qui est spécifié exclusivement pour les administrateurs.
ii. La valeur de la colonne 'admin', qui vaut à un(1), c'est cette colonne qui fait la différence lors de la connexion d'un utilisateur.
iii. La différence dans les fonctionnalités garanties aux administrateurs et aux utilisateurs.

### III.3.4 *Authentification :*

Quand le mot de passe est généré, l'application peut donc, générer le haché depuis ce mot de passe et l'identifiant introduise par le client, ce haché sera ensuite stocké dans la base de donnée pour l'utiliser dans l'authentification. Pour des raisons de sécurité, on récupère automatiquement les adresses IP et les adresses Mac des machines des utilisateurs qui s'inscrivent a notre serveur, et même les machines qui misent trop de tentatives de connexion sans succès.

Les clients ayant un compte peuvent se connecter à l'application en introduisant leur identifiants et leurs mots de passes, et après certaines vérifications la connexion au compte peut être garantie ou bien échouée. Lors de cette authentification, quand l'utilisateur tape son identifiant et son mot de passe, un haché est généré. Ce haché sera ensuite chiffrer en utilisant la méthode de chiffrement sur les courbes elliptique.

Sur l'autre côté, Le serveur reçoit le haché chiffré, il va le déchiffrer, puis le comparer avec le haché stocké dans sa base de données .Si la haché déchiffrer est identique au haché stocké dans la base de données alors la connexion est garantie, sinon, la connexion sera donc refusé.

On assume aussi qu'après 3 tentatives de connexion à un compte existant sans succès que c'est une tentative de violation de compte, pour cela un e-mail d'alerte va être envoyé au client dont le nom le compte est sous attaques, si le client prouve son identité, on peut lui offrir un nouveau mot de passe .Après 6 tentatives de connexion sans succès, un message d'alerte est envoyé vers le mobile de la victime et les adresses IP et mac de l'attaquant seront automatiquement bannies.

Une fois connecté, l'utilisateur peut utiliser tous les fonctionnalités du Cloud décrit précédemment.

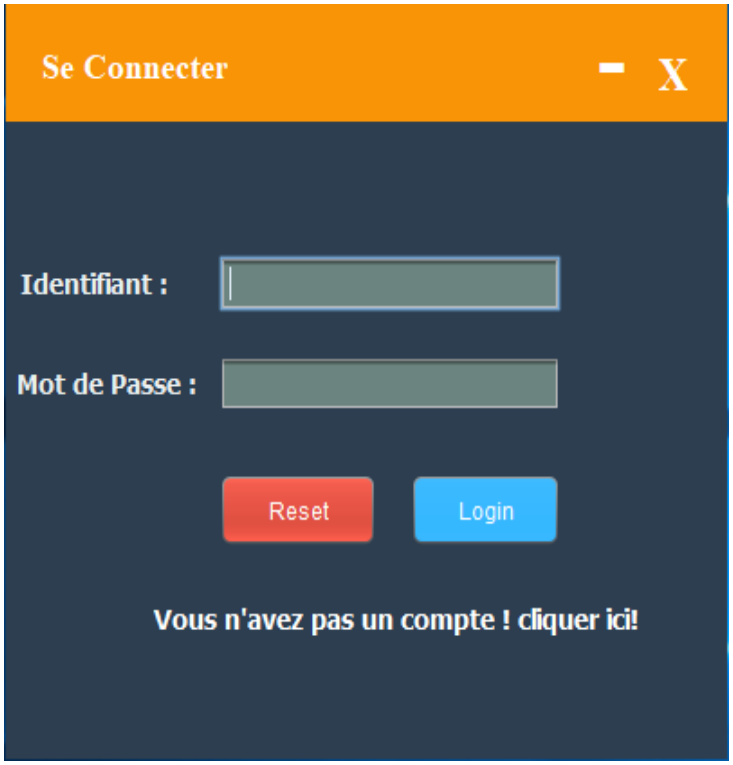
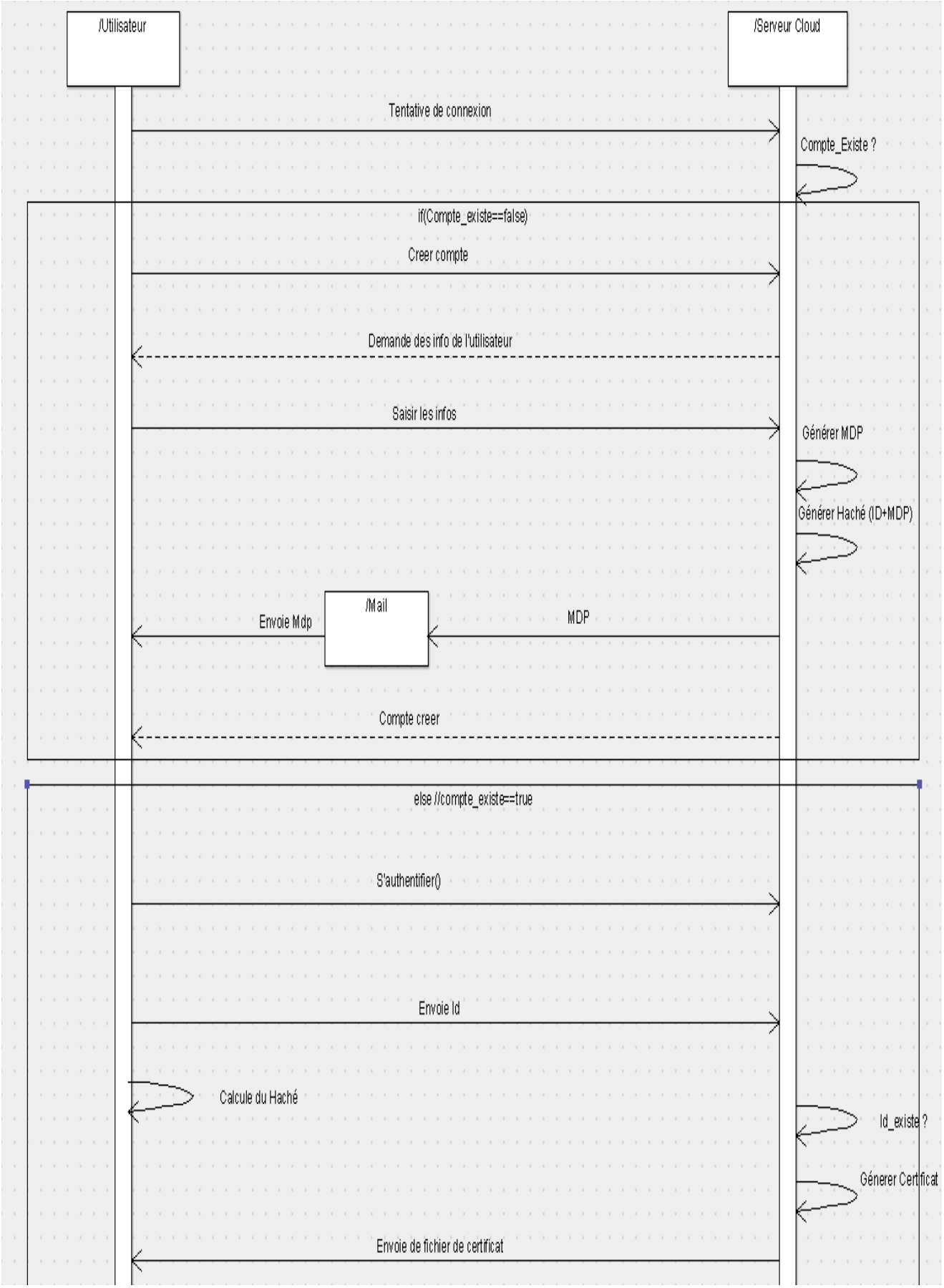



*Figure III-8 Interface index : S'authentifier*

## III.3.1 *Diagrammes :*

### a) Fonctionnement intérieur :


/Utilisateur
/Serveur Cloud
Tentative de connexion
Compte_Existe ?
if(Compte_existe==false)
Creer compte
Demande des info de l'utilisateur
Saisir les infos
Générer MDP
Générer Haché (ID+MDP)
/Mail
Envoie Mdp
MDP
Compte creer
else //compte_existe==true
S'authentifier()
Envoie Id
Calcule du Haché
Id_existe ?
Générer Certificat
Envoie de fichier de certificat

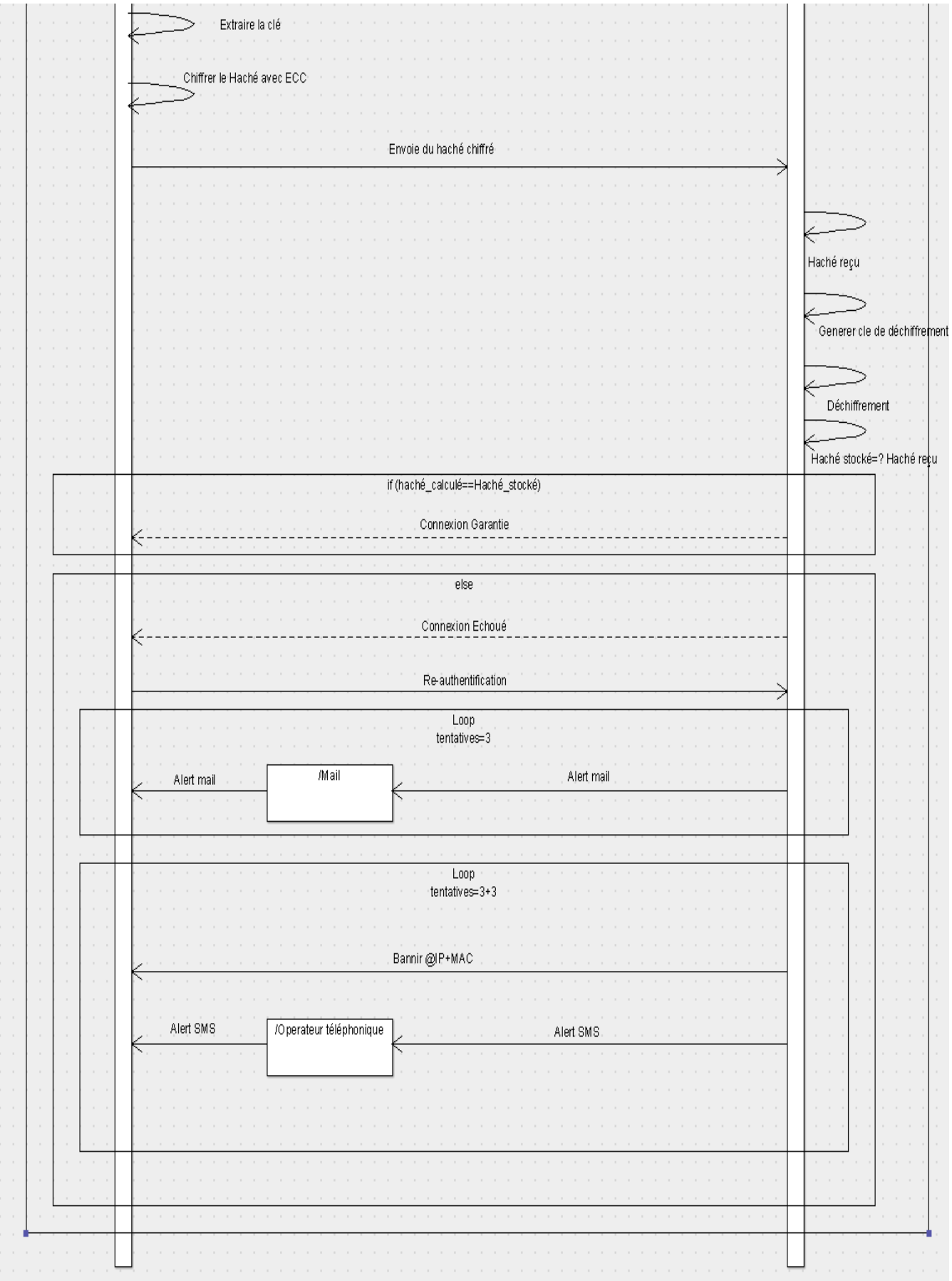



*Figure III-9 Diagramme de séquence décrit le fonctionnement intérieur de l'application*

### b) Administrateur :

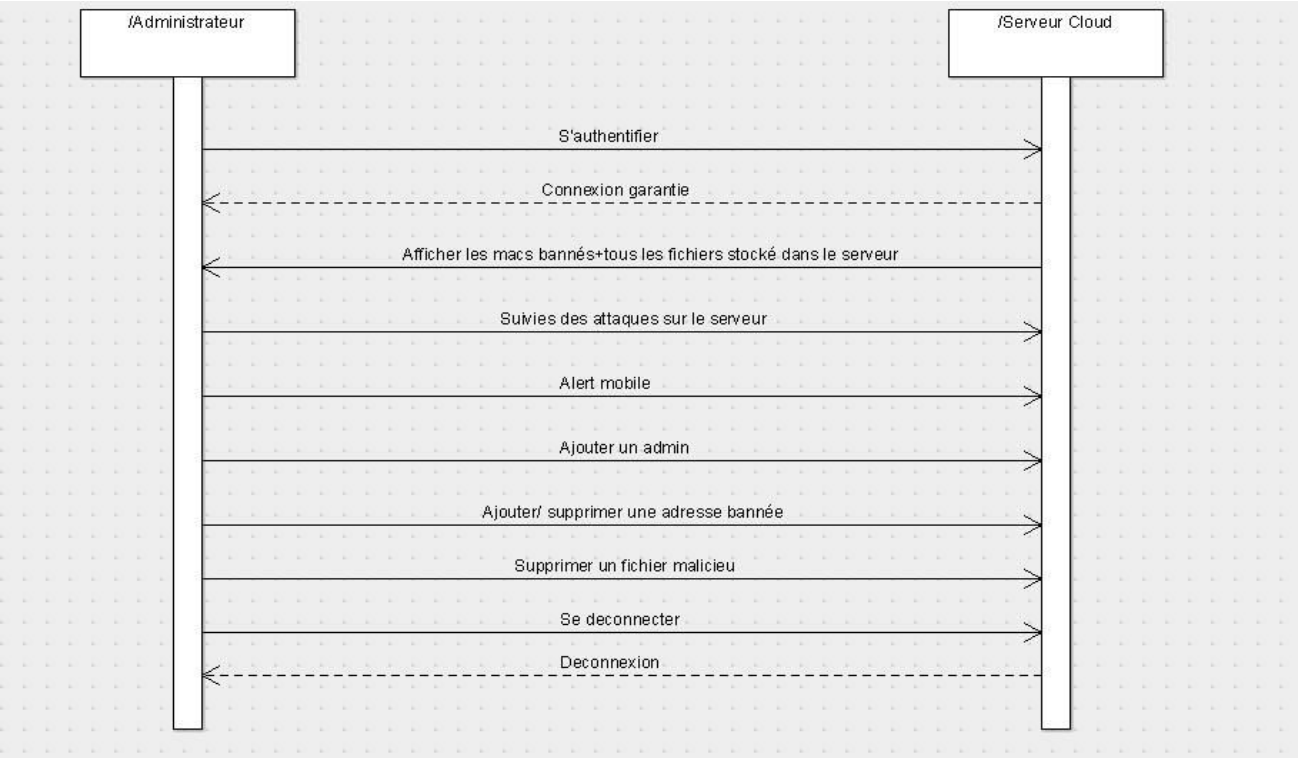



*Figure III-10 Diagramme de séquence décrit les fonctionnalités fournîtes à l'administrateur*

### c) Client :

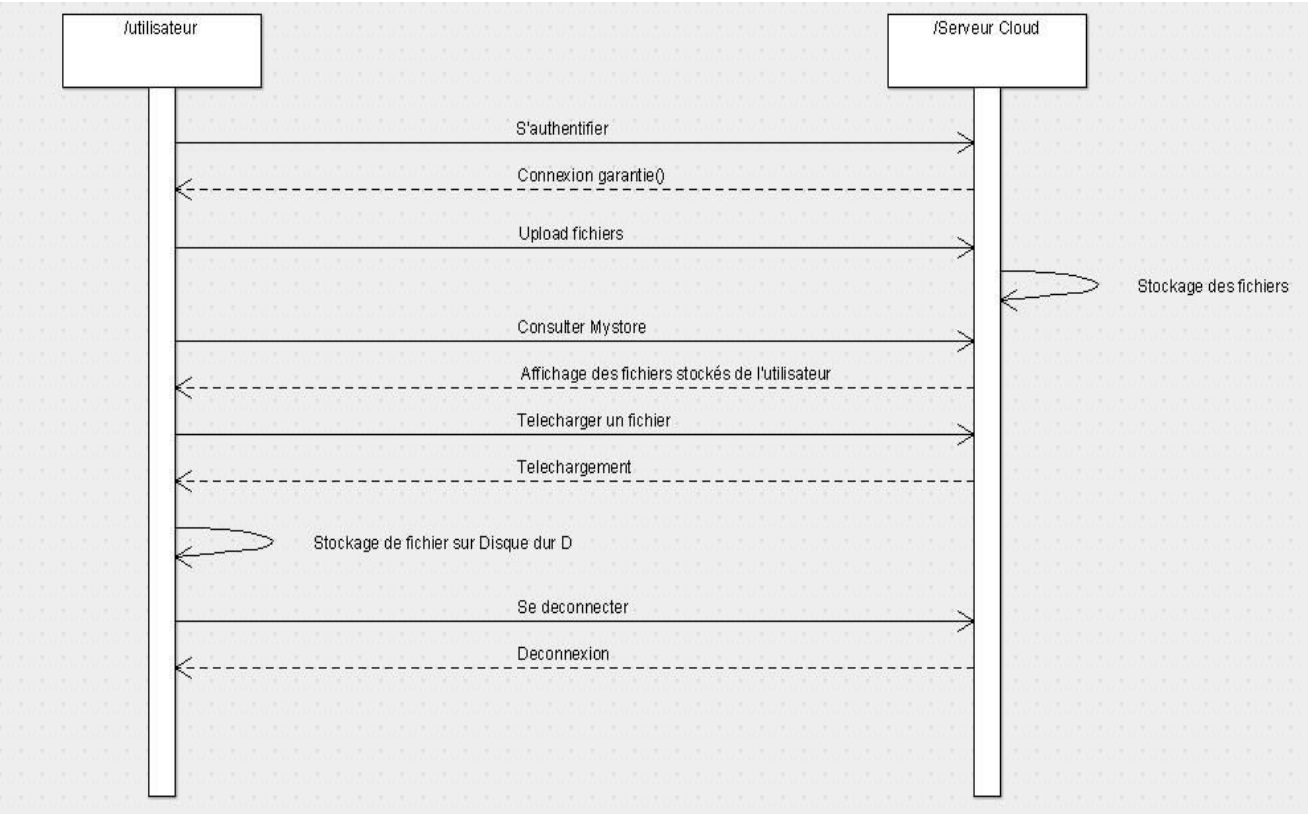



*Figure III-11 Diagramme de séquence décrit les fonctionnalités fournîtes aux Clients*

## III.4 Tests et Analyses de Sécurité :

Dans cette Section, on fournit une analyse de sécurité de notre mécanisme, on commence par décrire un test d'intrusion qu'on a déployé dans notre environnement de travail :

### III.4.1 *Le test d'intrusion :*

On a décidé de tester le fonctionnement de notre algorithme de chiffrement, pour atteindre ce but on a attaqué notre propre application en utilisant la technique « l'homme au milieu » en utilisant le logiciel '*Caïn & Abel*'. Voici les étapes qu'on a suit lors de l'attaque.

- ✓ Utilisation de trois machines :
  - **Serveur Cloud :** Contient la base de données globale des utilisateurs.
  - **Machine Client :** Un client qui veut stocker ses fichiers dans notre environnement Cloud.
  - **Machine de l'Attaquant :** Hacker qui utilise le logiciel 'Caïn & Abel' pour intercepter les données du client lors d'authentification.
- ✓ L'attaquant lance le logiciel et démarre l'écoute des paquets '*sniffer*'.
- ✓ Une fois l'attaquant récupère les adresses IP des machines qui sont connectées avec lui dans le même réseau, il lance la récupération des paquets des cibles '*poisening*'.
- ✓ Le choix des cibles se fait par la manière suivante :
  - Si l'attaquant connait les adresses IP du client et du serveur, il les choisi directement, cela lui permet de récupérer seulement les paquets qui sont échangés entre le client et le serveur.
  - Sinon, il lance l'attaque '*poisening*' sur le routeur du réseau et récupère tous les paquets qui sont échangés dans ce réseau.
- ✓ Comme le '*poisening*' est lancé, l'attaquant peut récupérer toutes les informations contendantes dans les paquets échangés entre ses victimes.

Les résultats de cette attaque étaient très satisfaisants, puisque l'attaquant peut récupérer des informations qui sont totalement chiffrées et qui ne peut pas les utiliser pour la violation du compte.

### III.4.2 *Analyse de sécurité par attaques :*

Les démarches de sécurité qu'on a suivie n'ont pas seulement garanti une gestion de contrôle d'accès très robuste, mais aussi, assure qu'on peut limiter même les attaques de types Dos et l'ingénierie sociale.

« Les attaques par déni de service non distribuées peuvent être contrées en identifiant l'adresse IP de la machine émettant les attaques et en la bannissant au niveau du pare-feu ou du serveur. Les paquets IP provenant de la machine hostile sont dès lors rejetés sans être traités empêchant que le service du serveur ne soit saturé et ne se retrouve donc hors-ligne.

Les attaques par déni de service distribuées sont plus difficiles à contrer. Le principe même de l'attaque par déni de service distribuée est de diminuer les possibilités de stopper l'attaque. Celle-ci émanant de nombreuses machines hostiles aux adresses différentes, bloquer les adresses IP limite l'attaque mais ne l'arrête pas. Thomas Longstaff de l'université Carnegie-Mellon explique à ce sujet que : « En réalité, la prévention doit plus porter sur le renforcement du niveau de sécurité des machines connectées au réseau [pour éviter qu'une machine puisse être compromise] que sur la protection des machines cibles [les serveurs Web] » [5] .

Donc quand on banni les adresses IP et les adresses MAC des utilisateurs qui misent plus que six(6) tentatives de connexion, on peut dire qu'on a pu limiter une telle forte attaque comme le Dos plus on assure la gestion du contrôle d'accès.

La communication continue entre le client et les administrateurs qui utilisent un email unifié : email professionnel cité ci-dessus (alerte par email, alerte mobile, et ré-autorisation des machines bannis après la signalisation du client) assure que le client est toujours au courant à propos des attaques probable sur son compte et qu'il connait vraiment l'identité de l'expéditeur, et comme ça on limite les attaques de type ingénierie sociale.

### III.4.3 *Calcul théorique :*

Dans cette partie, on essaye d'estimer le temps nécessaire pour cracker un message chiffré en utilisant un algorithme de chiffrement basé sur les courbes elliptiques. La puissance de chiffrement basé sur les courbes elliptique est c'est qu'on ne peut pas facilement résoudre le problème du logarithme discret.

Les deux algorithmes qui sont utilisé pour résoudre ce problème sont : Baby-step,giant-step et Pollard's rho. On note que Baby-step,giant-step ne peut pas être utilisée dans la pratique, en

raison des énormes besoins de mémoire. D'autre part, Pollard's rho nécessite très peu de mémoire. La complexité de calcule en basant sur Pollard's rho vaut à $O(\sqrt{n})$.

En 1998, Certicom a lancé un défi pour calculer des logarithmes discrets sur des courbes elliptiques avec des longueurs de bits allant de 109 à 359. A ce jour, seules des courbes longues de 109 bits ont été rompues avec succès. La dernière tentative réussie a été faite en 2004.Le prix a été décerné le 8 avril 2004 à un groupe d'environ 2600 personnes représentées par Chris Monico. Ils ont également utilisé une version d'une méthode Pollard's rho parallélisée, prenant 17 mois de calendrier [6].

En basant sur ces résultats: On utilise la courbe '***spec256r1'*** alors:
Pour cracker une courbe de 109 bits il faut 17 ***mois*** de temps Donc : Temps nécessaire(T) vaut à :

$$T = 17 * \frac{\sqrt{2^{256}}}{\sqrt{2^{109}}} \rightarrow T = 2.27 * 10^{23} \text{ Mois !}$$

Ce nombre nous donne une idée claire de comment il peut être difficile de casser un logarithme discret en utilisant de telles techniques.

### III.4.4 *Les choix techniques :*

- ✓ ***Java*** : Le langage de développement employé lors de l'implémentation de l'application.
- ✓ ***NetBeans*** : L'IDE utilisé pour le développement.
- ✓ ***WAMP Server*** : Offre les plateformes phpmyadmin et mysqlserver qui nous permet de créer la base de données, en apportant les modifications nécessaires, il permet la connexion à distance à la base de données.
- ✓ ***Caïn and Abel*** : Logiciel utilisé pour performer l'attaque homme au milieu 'Man In The Middle', utilisé spécifiquement pour intercepter les données.
- ✓ ***Launch4j*** : Logiciel utilisé pour générer un exécutable depuis un fichier .jar
- ✓ ***ArgoUml*** : Logiciel utilisé pour la création des diagrammes.
- ✓ ***FastStone*** : Logiciel utilisé pour les captures d'écran.
- ✓ ***EDraw Max*** : Logiciel utilisé pour la création des maquettes.

### III.4.5 *Conclusion :*

Enfin, avec les résultats du test d'intrusion effectué, on peut conclure que l'application assure la gestion de contrôle pour les utilisateurs, faire face aux attaques « l'homme au milieu » grâce a le système de cryptographie basé sur les courbes elliptiques et la signature digitale, ainsi limiter les attaques « ingénierie sociale » en assurant la communication continue entre l'utilisateur, et le Support technique. Alors cette approche offre, alors, une gestion de sécurité très performante aux utilisateurs, d'où ces derniers peuvent utiliser les fonctionnalités du Cloud en toute sécurité et sans risque de perdre ses comptes, ou bien, violation de ses données; en assurant le fonctionnement continu de l'application en limitant l'effet des attaques Dos.

## Conclusion Générale :

Le Cloud computing est devenu un sujet très critique dans notre vie quotidienne ; l'utilisation vaste de ses environnements dans tous les domaines, rend ces derniers une cible favorable pour les attaquants. A cet effet, la mise en place des mécanismes de sécurité est devenue une nécessité.

Dans ce mémoire, nous avons commencé par la présentation du concept cloud computing dans le premier chapitre, ainsi que ses services et son modèle de déploiement. Ensuite dans le deuxième chapitre, nous avons cité, d'une part, les différentes menaces qui peuvent affecter les environnements clouds et d'autre part nous avons présenté les différents mécanismes de sécurité qui visent à protéger les environnements clouds.

Enfin, et pour diminuer le risque des attaques et offrir un service d'authentification efficace dans un environnement cloud, nous avons développé dans le dernier chapitre un mécanisme d'authentification basé sur les courbes elliptiques. Notre mécanisme permet de s'assurer des identités des utilisateurs du Cloud et permet aussi de protéger les données échangées grâce à la technique du chiffrement.

## Notes et Références :

[1] Sahil Makhija, « What is the difference between data center and cloud? » [en ligne] Quora, 23 février 2017. Consulté le: 23 Mars 2018
Disponible en ligne https: https://www.quora.com/What-is-the-difference-between-data-center-and-cloud

[2] ISO 7498-2, « Architecture de sécurité » Systèmes de traitement de l'information -- Interconnexion de systèmes ouverts -- Modèle de référence de base, 02/1989, p.32 (ISO/IEC JTC 1).

[3] Victor S. Miller, « Use of elliptic curves in cryptography », *Crypto*, vol. 218, 1985, p. 417-426 (DOI 10.1007/3-540-39799-X_31).

[4] Neal Koblitz, « Elliptic curve cryptosystems », Mathematics of Computation, n° 48, 1987, p. 203-209 (DOI 10.1090/S0025-5718-1987-0866109-5).

[5] Le déni de service distribué - Agence nationale de la sécurité des systèmes d'information (ANSSI), 21 février 2000

[6] Certicom, « the Certicom Challenge », 8 avril 2004, Consulté le : 15 mai 2018
Disponible en ligne : https://www.certicom.com/content/certicom/en/the-certicom-ecc-challenge.html

# Bibliographie :

A view of cloud computing, ARMBRUST,Micheal… et al. Magazine Communications of the ACM - Volume 53 Issue 4, ACM, avril 2010, p. 50-58 (DOI 10.1145/1721654.1721672).

BIBM@TH.NET. Cryptographie et code secrets : Chiffrer à l'aide des courbes elliptiques. Consulter le: 29 Mars 2018.
Disponible sur internet : http://www.bibmath.net/crypto/index.php?action=affiche& quoi= complements/cryptoelliptique.

BROOK Jon-Micheal. Cloud Computing Top Threats in 2016, CSA (Cloud Security Alliance), 2016, Consulté le: 25 Mars 2018
Disponible sur internet: http://cloudsecurityalliance.org/group/top-threats.

CERTA-2000-INF-001-1.1, Le déni de service distribué , Agence nationale de la sécurité des systèmes d'information (ANSSI), 21 février 2000

GODEFROY, Laurent .Introduction à la cryptologie, EDUCINVEST Belgium - Avenue Louise, 534 - 1050 Brussels, Consulté le 25 Mars 2018, Cours. Disponible sur internet: https://www.supinfo.com/cours/1ARI/chapitres/01-introduction-cryptologie.

DURIEZ-MISE Johann, le 22 octobre 2014, modifié à 06h52, le 23 octobre 2014 «Apple confirme un piratage chinois d'iCloud.

JOUANNIC, Thibault, un peu de crypto sur les courbes elliptiques. [en ligne] Miximum, 17 juin 2014.Consulté le: 7avril 2018.
Disponible sur internet: https://www.miximum.fr/blog/cryptographie-courbes-elliptiques-ecdsa/

MELL Peter, GRANCE Tim, The NIST Définition of Cloud Computing, SP 800-145, Septembre 2011, Consulté le: 15 Mars 2018.
Disponible sur internet : https://csrc.nist.gov/publications/detail/sp/800-145/final

MIMOUNE, Moussa. Etude sur la sécurité du Cloud Computing, Les mécanismes de sécurité d'un Cloud Computing : Attaque XSS, Attaque par SQL Injection, 68 p. Mathématique et Informatique, Informatique, Université de M'Sila, 2015.

RIQUET, Damien. GRIMAUD, Gilles. HAUSPIE, Michaël.Large-scale attacks : Impact on the cloud security, The Second International Workshop on Mobile Commerce, Cloud Computing, Network and Communication Security *2012*, 6 juillet 2012, p. 558 – 563.

MAKHIJA,Sahil. What is the difference between data center and cloud? [en ligne] Quora, 23 février 2017. Consulté le: 23 Mars 2018 Disponible en ligne https: https://www.quora.com/What-is-the-difference-between-data-center-and-cloud

SECURITEINFO, les fonctions de hachage. (2001, novembre 18). Consulté le : Disponible en ligne https://www.securiteinfo.com/cryptographie/hash.shtml

SECURITE SOCIALE, Entreprise, La signature digitale, Consulté le: 25 Mars 2018 Disponible sur internet : https://www.socialsecurity.be/site_fr/ general/helpcentre/ digital_sign/ general/what.htm

## Résumé :

Avec tous ses avantages et ses services, le cloud a devenu une partie essentielle de notre vie quotidienne, que soit la vie professionnelle, ou bien la vie personnelle. L'utilisation vaste de ces environnements Cloud, donne la meilleure motivation aux les cybers attaquants, ce qui rend ces environnements une cible favorite pour eux.

Ces cyber attaquants utilisent des différents techniques dans ses attaques, et ces techniques se développe une année après l'autre, ce qui rend la sécurité de ces environnements une nécessitée indiscutable.

Dans ce mémoire on a essayé de donner, à la base, une approche de sécurité pour la gestion d'authentification dans un environnement Cloud, en basant sur la cryptographie sur les courbes elliptiques et le hachage, puis on a essayé de fortifier cette sécurité en ajoutant plus de fonctionnalités afin de limiter l'effet d'autres attaques comme les attaques dénie de service et ingénierie sociale.

Enfin, et dans le but de tester la sécurité de cet environnement simulé, on a essayé d'intercepter les données d'authentification afin de violer un compte en utilisant la technique 'l'homme au milieu' d'où les données interceptés étaient totalement chiffrées et incraquables.



- **Mots clés :** Cloud Computing , Cyber-attaques, cryptographie, courbe elliptique, authentification , sécurité.



## Abstract :

With all its benefits and services, the Cloud Computing has become an essential part of our daily lives, whether it's in our professional or in personal life. The vast use of the Cloud environments gives the hackers the best motivation to make these environments their new favorite target.

These hackers use some different types of technics to perform their attacks. These technics develops one year after the other, making the security of these environments an indisputable necessity and a top priority for the cybersecurity experts.

In this thesis, the aim was to give an approach to manage the authentication in a Cloud environment. to realize that, we used cryptography based on elliptic curves and hashing fucntions, then we tried to give this environment more strength that will always manage the access control plus limiting other types of attacks such as denial of service and social engeneering, by adding some other features and technics.

Finally in the aim to measure how much is stong our security in managing authentication, we tried to intercept the data used int the authentification procedure, the result was such satisfiying because the data intercepted was crypted and uncrackable.



- **Keywords :** Cloud Computing, Cyber-attacks, cryptography, elliptic curve, authentication, security.



## ملخص

مع كل الخدمات التي توفرها، أصبحت الحوسبة السحابية جزءًا أساسيًا من حياتنا اليومية ، سواء كان ذلك في حياتنا المهنية أو في الحياة الشخصية. إن الاستخدام الواسع للبيئات السحابية يمنح الهاكرز الدافع الأفضل لجعل هذه البيئات هدفهم المفضل الجديد.

يستخدم هؤلاء المتسللون أنواعًا مختلفة من التقنيات لتنفيذ هجماتهم. تتطور هذه التقنيات بعد عام واحد من الآخر ، مما يجعل أمن هذه البيئات ضرورة لا غبار عليها وأولوية قصوى لخبراء الأمن السيبراني.

في هذه الرسالة ، كان هدفنا إعطاء نهج لإدارة التحكم في الوصول في بيئة السحاب.

لإدراك ذلك ، استخدمنا التشفير استنادًا إلى المنحنيات الناقصية والتقطيعات ، ثم حاولنا أن نعطي هذه البيئة المزيد من القوة التي ستعمل دائمًا على التحكم في الوصول بالإضافة إلى الحد من الأنواع الأخرى من الهجمات مثل الحرمان من الخدمة والمشاركة الاجتماعية ، وذلك بإضافة بعض ميزات وتقنيات أخرى.
وأخيرًا، بهدف قياس مدى قوة نظام الحماية في التحكم في الدخول، حاولنا اعتراض البيانات المستخدمة في إجراء التحقق من صحة المعلومات، وكانت النتيجة مرضية للغاية لأن البيانات التي تم اعتراضها كانت مشفرة وغير قابلة للفك.



**الكلمات المفتاحية:** الحوسبة السحابية ، الهجمات السيبرانية ، التعمية ، المنحنى البيضاوي ، التوثيق ، الأمن