République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université Saad Dahlab Blida 1

Faculté des sciences

Département d'Informatique

Mémoire de fin d'études

Pour l'obtention de diplôme du Master en Informatique

Spécialité : Sécurité des Systèmes Informatiques

Contrôle d'Accès Sécurisé dans l'Environnement Infonuagique Mobile

Mémoire réalisé par :

Ayyoub BOULARES

Imene DAOUDI

Devant le jury composé de :

Présidente : Mme. Sana AROUSSI Université de Saad Dahlab Blida

Examinatrice : Mme. Ahlem NASRI Université Saad Dahlab Blida

Encadreur : Mr. Zakaria SAHNOUNE Université de Saad Dahlab Blida

Année Universitaire :2020/2021

Dédicaces

Je dédie ce présent mémoire :

À celle qui s'est toujours dévouée et s'est sacrifiée pour moi, celle qui m'a aidé du mieux qu'elle pouvait pour réussir, celle qui a toujours été là dans mes moments de détresse, ma très chère mère.

À mon père qui m'a toujours encouragé et soutenu moralement.

Amon cher frère Sife Dine Betach et mes amis pour leurs encouragements permanents, et leur soutien moral,

Nous tenons à remercier Monsieur Sahnoune Zakaria, notre professeur et tuteur tout au long de notre mémoire, pour son encadrement et pour ses précieux conseils, sa disponibilité et son soutien tout au long de mon travail.

Nous remercions également nos tuteurs professionnels respectifs de nous avoir guidés dans l'évolution de nos travaux et pour leurs précieux conseils.

Nous tenons, également, à remercier les membres du jury, qui ont accepté d'évaluer ce modeste travail.

BOULARES AYYOUB ….

Dédicaces

Je dédie ce travail
À mes chers parents, pour tous leurs sacrifices, leur amour, leur tendresse, leur soutien et leurs prières tout au long de mes études,
À ma chère grand-mère pour son appui et son encouragement,
À mes chères sœurs Soumia et Lydia pour leurs encouragements permanents, et leur soutien moral,
À mes chères amies Faiza et Chahinez et Soumia pour leurs aides et leurs encouragements illimités
À toute ma famille pour leur soutien tout au long de mon parcours universitaire, que ce travail soit l'accomplissement Devos désirs et le fruit de votre soutien continu.

Merci d'être toujours à mes côtés

DAOUDI IMENE....

Résumé

Au cours des dernières années, les avancées dans le domaine de réseaux informatiques et des applications Cloud computing mobile (MCC) ont été présentées comme une technologie potentielle pour services mobiles.
MCC est une nouvelle plateforme pour combiner les appareils mobiles et le Cloud computing pour créer une nouvelle infrastructure où :
L'utilisateur mobile est responsable de ses fonctionnalités, quelles que soient les limitations de ressources du dispositifs mobiles.
Donc si on parle de Cloud on parle aussi de ressources partagées ce qui nous pousse à protéger ces ressources et mettre en sorte un mécanisme de contrôler d'accès. Le contrôle d'accès est indispensable pour la sécurité dans les systèmes informatiques donc l'accès au modèle de contrôle est généralement conçu pour fournir l'autorisation, l'authentification, l'approbation d'accès, et vérification. Il peut protéger les données contre l'utilisation et la divulgation non autorisées (confidentialité) ; et la modification et la destruction non autorisées ou inappropriées (intégrité).
Dans ce contexte, l'objectif de ce mémoire est de définir un système de contrôle d'accès flexible et puissant au niveau de MCC tout en basant sur l'approche d'emplacement de LRBAC (un modèle de contrôle d'accès basé sur les rôles et tenant compte de la localisation) et l'aspect jeton avec la Plateforme sécurisé PASETO et l'intégration d'empreinte numérique de l'appareil.

Mots clés : Cloud Computing, Cloud Computing Mobile, contrôle d'accès, LRBAC (un modèle de contrôle d'accès basé sur les rôles et tenant compte de la localisation), jeton d'accès PASETO, empreinte numérique.

Summary

In recent years, advancements in computer networks and mobile cloud computing (MCC) applications have been exposed as a potential technology for mobile services.
MCC is a new platform for combining mobile devices and cloud computing to create a new infrastructure.
The major goal behind mobile cloud computing is to empower the mobile user by delivering functionality, regardless of mobile resource limitations.
Devices, so if we talk about Cloud, we also talk about shared resources which pushes us to protect these resources and set up an access control mechanism. Access control is essential for security in computer systems therefore access to the control model is generally designed to provide authorization, authentication, access approval and verification. It can protect data against unauthorized use and disclosure (confidentiality); and unauthorized or inappropriate modification and destruction (integrity).
In this context, the objective of this thesis is to define a flexible and powerful access control system at MCC level while basing on the location approach of LRBAC (an access control model based on roles and taking into account the location) and the token aspect with the PASETO secure platform and the integration of the digital fingerprint of the device.

Key words: Cloud Computing, Mobile Cloud Computing, control access, LRBAC (a location-aware role-based access control model), PASETO access token, fingerprint.

ملخص

في خضم السنوات الأخيرة وصف التقدم في مجال شبكات الكمبيوتر و كذا تطبيقات الحوسبة السحابية المتنقلة على أنها تقنية محتملة لخدمات المحمول باعتبارها مزيجا من الحوسبة السحابية والشبكات اللاسلكية و هذا لجلب مورد حوسبة عالي الجودة إلى مشغلي الشبكات ومستخدمي الهاتف المحمول وموفري الحوسبة السحابية المتنقلة هو نظام أساسي جديد يجمع بين الأجهزة المحمولة والحوسبة السحابية لإنشاء ملف البنية التحتية الجديدة و الهدف الرئيسي من وراءها هو تمكين مستخدم الهاتف المحمول من عدة وظائف بغض النظر عن القيود التي تفرضها موارد الأجهزة المحمولة.

لذلك إذا تحدثنا عن السحابة، فإننا نتحدث أيضًا عن الموارد المشتركة التي تدفعنا إلى حماية هذه الموارد والتحكم في الوصول لان هذا التحكم ضروري في امن أنظمة الكمبيوتر لذلك تم تصميم نموذج التحكم في الوصول بشكل عام; بغية تقديم التفويض والمصادقة والموافقة على الوصول والتحقق كما يمكننا من حماية البيانات ضد الاستخدام غير المصرح به والكشف (السرية) ; والتعديل والحجب غير المصرح به أو غير المناسب (النزاهة).

الهدف إذن من هذه الأطروحة هو تحديد نظام مرن للتحكم في الوصول على مستوى الحوسبة السحابية المتنقلة بالاعتماد على بصمة معلومات جهاز المستخدم وموقعه (نموذج للتحكم في الوصول يعتمد على الأدوار مع مراعاة الموقع) والرموز الأمنية المحايدة للنظام الأساسي.

الكلمات الأساسية :الحوسبة السحابية، الحوسبة السحابية المتنقلة، التحكم في الوصول، نموذج التحكم في الوصول القائم على الدور المدرك للموقع، والرموز الأمنية المحايدة للنظام الأساسي، بصمة معلومات جهاز المستخدم.

Table des matières

Liste des tables

Liste des Figures

Chapitre 2 :

Chapitre 3 :

Chapitre 4 :

Introduction générale

Depuis quelque temps, le Cloud Computing, ou « Informatique dans les nuages » est le « Buzz Word » le plus utilisé dans l'industrie informatique. Cela est, en grande partie, dû au fait quel Cloud Computing constitue la tendance actuelle qui promet une évolution majeure de l'informatique.
Il propose une nouvelle manière de produire et de consommé l'informatique dans laquelle les ressources sont fournies sous la forme de « services à la demande », accessibles de n'importe où, n'importe quand et par n'importe qui au travers d'Internet. Les utilisateurs n'ont ainsi besoin d'aucune connaissance ni expérience en rapport avec la technologie derrière les services proposés.
Aujourd'hui le Cloud computing est principalement utilisé pour le traitement des charges de travail informatiques très intensives et pour fournir de très grandes installations de stockage de données. Ces deux objectifs sont combinés avec le troisième but de réduire potentiellement les coûts de gestion et d'utilisation.
Le Cloud Computing Mobile (MCC) est introduit comme une intégration du Cloud Computing dans l'environnement mobile. Le Cloud Computing Mobile apporte de nouveaux types des services et d'installations pour les utilisateurs mobiles.
La sécurité dans le MCC est faite pour protéger les données des utilisateurs, ainsi que pour établir et maintenir la confiance des consommateurs dans l'environnement mobile et avec l'augmentation des services de Cloud Computing, la demande d'accès aux ressources des données (par exemple, les images, les fichiers, et les documents) est augmentée dans les nuages. En conséquence, une méthode pour traiter les ressources de données (stocker, gérer, et accès) sur les nuages devient un défi de taille. Cependant, la manipulation des ressources des données sur les nuages n'est pas un problème facile en raison de la faible bande passante, la mobilité, et la limitation de la capacité des ressources des dispositifs mobiles.

Problématique :

La recherche présentée dans cette mémoire été menée dans le but de fournir un mécanisme de contrôle d'accès sécurisés pour les utilisateurs mobiles autorisés du Cloud. En raison des risques associés à la sécurité et à la confidentialité des données stockées par les entreprises dans le Cloud, la plupart des services informatiques et les directeurs généraux sont préoccupés par l'utilisation de ce type de technologie. Ces préoccupations croissent davantage en raison du fait que les utilisateurs / employés ont tendance à utiliser des appareils sans fil (par ex. et téléphones intelligents) pour rester connectés tout en se déplaçant à travers / en dehors de l'entreprise au lieu de rester dans leurs bureaux et faire leur travail ou leurs activités quotidiennes. Plus précisément, fournir l'accès autorisé aux données stockées dans le Cloud est plus critique pour les ressources dynamiques limitées utilisateurs mobiles.

L'objectif est de proposer un mécanisme de contrôle d'accès léger, efficace, et qui permet l'exploitation de la puissance de MCC en toute sécurité.

Structure du mémoire :

Ce mémoire est constitué de quatre chapitres et d'une conclusion générale avec les perspectives :

- ✓ **Chapitre 01 :** Dans ce chapitre, nous présentons la sécurité dans le Mobile cloud computing en présentant les définitions et les caractéristiques du Cloud Computing. Après, nous passons au Mobile Cloud Computing en citant ses avantages, ses faiblesses, notamment ses problèmes de sécurité.

- ✓ **Chapitre 02 :** Dans ce chapitre, nous décrivons les mécanismes de sécurité utilisés dans notre travail à savoir : les modèles Contrôles d'accès Authentification par jetons dynamiques et l'empreinte digital.

- ✓ **Chapitre 03 :** Dans ce chapitre, nous expliquons notre approche proposée : l'architecteur et le fonctionnement du système et comment nous avons déployé ces mécanismes de sécurité : authentification par jetons dynamiques ; le modèle LRBAC et l'empreinte numérique.

- ✓ **Chapitre 04 :** Ce chapitre est consacré à l'implémentation de notre solution où nous présentons aussi les interfaces et points forts de de l'approche proposée.

Chapitre1 : La sécurité dans le cloud computing mobile

1. Introduction

Le Cloud Computing (CC) en français « informatique dans les nuages » est en train de révolutionner le monde informatique. Il consiste à externalisée des infrastructures informatiques vers des prestataires spécialisés. Ce modèle aura un impact très profond sur les utilisateurs et sur les stratégies informatiques des entreprises.

MCC est une nouvelle plateforme pour combinée les appareils mobiles et le Cloud computing pour créer une nouvelle infrastructure. Alors le MCC est un sous-ensemble du Cloud Computing (CC) qui permet un accès et un stockage réseau pratiques et à la demande qui peuvent être utilisé pour fournir différents types de services et d'applications aux utilisateurs mobiles,

Dans l'environnement MCC, CC, le mobile informatique et la mise en réseau sont combinées pour offrir des services aux utilisateurs mobiles où les données sont stockées et les demandes sont traitées dans un système informatique centralisé avec des applications situées dans les nuages.

Fournies par les fournisseurs (par exemple : Google, Amazon, Sales force) à faible coût, CC permet aux utilisateurs d'utiliser les ressources à la demande. En conséquence, les applications mobiles peuvent être rapidement approvisionnées et publiées.

Le Cloud Computing Mobile (MCC) est introduit comme une intégration du Cloud Computing dans l'environnement mobile. Le Cloud Computing Mobile apporte de nouveaux types des services et d'installations pour les utilisateurs mobiles.

Dans ce chapitre, nous commençons par présenter le concept et les caractéristiques du cloud computing ; ensuite nous faisons un passage au Cloud computing mobile, ces caractéristiques ces avantages et ces inconvénients et ces défis. Ensuite, nous présentons le problème du contrôle d'accès aux données comme l'un des principaux défis de sécurité dans le Cloud mobile et les Contrôles d'accès dans le Mobile Cloud Computing.

2. Cloud Computing

2 . 1 Définition du Cloud Computing :

Il n'existe pas actuellement une définition exacte du concept « Cloud Computing » acceptée universellement par les chercheurs concernés. Un extrait simplifié de la définition de NIST (National Institute of Standards and Technology (États-Unis) qui nous semble la plus générale.

« Le Cloud Computing est un modèle qui offre aux utilisateurs du réseau un accès à la demande à un ensemble de ressources informatiques partagées et configurables et qui peut être rapidement mis à la disposition du client sans interaction direct avec le prestataire de service. » [1].

Gartner a récemment défini le Cloud Computing comme « un type d'informatique dans

lequel des capacités très évolutives sont fournies sous forme de service à plusieurs clients via les technologies Internet » [2]. Cette définition est très appropriée, car elle caractérise le Cloud Computing comme un facteur d'optimisation de l'entreprise et non comme un concept technique.

Selon Syntec informatique le Cloud Computing peut se définir comme : « une approche permettant de disposer d'applications, de puissance de calcul, de moyens de stockage, etc. comme autant de « services ». Ceux-ci seront mutualisés, dématérialisés (donc indépendants de toutes contingences matérielles, logicielles et de communication), contractualisés (en termes de performances, niveau des sécurité, coûts...), évolutifs (en volume, fonction, caractéristiques...) et en libre-service » [3].

Pour le leader mondial des technologies réseau Cisco Systems, le Cloud Computing peut se définir comme : «IT ressources and services that are abstracted from the underlying infrastructure and provided " on-demand" and "at scale" in à multi tenant environnement » [4]. Autrement dit le Cloud Computing est une plateforme de mutualisation informatique fournissant aux entreprises des services à la demande avec l'illusion d'une infinité des ressources.

Nous observons que ces définitions engendrent la notion des services disponibles à la demande, extensibles et standardisés. En contradiction avec les systèmes actuels, les services sont virtuels, illimités et les détails des infrastructures physiques sur lesquels les applications reposent ne sont plus durs sorts de l'utilisateur. Elles incluent également la notion de Scalabilité, d'extensibilité à la demande et d'élasticité, c'est-à-dire qu'on ne paie que ce qu'on utilise.

Nous observons d'après ces définitions que le Cloud Computing n'est pas en soi une technologie nouvelle d'un point de vue technique, le Cloud Computing provient de l'aboutissement de plusieurs technologies existantes antérieurement : internet et la virtualisation le tout appuyé sur un réseau fiable et à haut débit.

2.2 Caractéristiques du Cloud Computing :

Le National Institute of Standards and Technology (NIST) donne une définition très précise des différents éléments qui caractérisent le Cloud Computing : « Ce modèle favorise la disponibilité et comprend les cinq caractéristiques suivantes » [16] :

1.On-Demand Self-Service (Libre-service à la demande) : le libre-service à la demande permet aux entreprises clientes des fournisseurs de Cloud Computing de faire évoluer automatiquement les capacités informatiques mises à leur disposition de façon continue.

2.Accès au réseau étendu : l'accès et les capacités sont disponibles sur le réseau au moyen de dispositifs standards, tels que les téléphones cellulaires, ordinateurs portables, PDA, etc.

3.Mutualisation des ressources ou la mise en commun des ressources ou encore la colocation de serveurs : Des ressources telles que la bande passante

réseau, les machines virtuelles, la mémoire, la puissance de traitement et la capacité des stockages sont mises en commun pour desservir plusieurs clients à l'aide d'un modèle multi locataire. En d'autres termes, afin de personnaliser les besoins des clients, des ressources virtuelles et physiques sont fournies dynamiquement.

4.Élasticité rapide (mise à l'échelle rapide) : en fonction de 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.

5.Service mesurée : le Cloud Computing permet au client de payer à l'usage, uniquement ce qui a été consommé selon le type et le temps d'utilisation du service. Par exemple avec la solution Cloud « Smart Cloud » d'IBM le client a la possibilité de choisir entre quatre types de configuration serveur : Copper, Bronze, Silver et Gold. **La table 1 résume les caractéristiques ainsi quel prix de chacune des offres** [5].

Machines virtuelles	Configurations 32-bit				Configurations 64-bit				
	Copper	Bronze	Silver	Gold	Copper	Bronze	Silver	Gold	Platinum
Virtual CPU's with 1.25GHz	1	1	2	4	2	2	4	8	16
Virtual Memory (Gigabytes)	2	2	4	4	4	4	8	16	16
Instance Storage (Gigabytes)	60	175	350	350	60	850	1024	1024	2048
Prix par heure d'utilisation (sans engagement)									
Avec Redhat Linux OS	€ 0,097	€ 0,113	€ 0,179	€ 0,280	€ 0,234	€ 0,312	€ 0,374	€ 0,576	€ 1,137
Avec SUSE Linux OS	€ 0,074	€ 0,090	€ 0,156	€ 0,257	€ 0,210	€ 0,288	€ 0,351	€ 0,553	€ 1,083
Avec Windows Server	€ 0,078	€ 0,093	€ 0,187	€ 0,288	€ 0,265	€ 0,312	€ 0,389	€ 0,748	€ 1,550
OS Linux fournit par le client	€ 0,058	€ 0,074	€ 0,140	€ 0,241	€ 0,195	€ 0,273	€ 0,335	€ 0,537	€ 1,067

Tableau 1 : Tarification IBM Smart Cloud [5].

3. Cloud Computing Mobile

3.1. Définition de Cloud Computing Mobile :

Le Forum-Cloud computing Mobile définit MCC comme suit [7] :

« Cloud Computing Mobile », se réfère à une infrastructure où à la fois le stockage et le traitement des données se font à l'extérieur de l'appareil mobile. Aepona [8] décrit MCC comme un nouveau paradigme pour les applications mobiles permettant le traitement et le stockage qui sont déplacés à partir des périphériques mobiles puissants et centralisés situés dans les nuages. Les périphériques centralisés sont ensuite accessibles via la connexion

sans fil basée sur un client léger ou un navigateur Web natif sur les appareils mobiles. Le MCC fournit aux utilisateurs mobiles le traitement des données et des services de stockage dans les nuages. Dans les appareils mobiles n'ont pas besoin d'une configuration puissante (par exemple, la vitesse du processeur et la capacité de mémoire), car tous les modules de calcul compliqué peuvent être traités dans les nuages [9].

3.2. Avantages et Inconvénients :

3.2.1. Avantages du Cloud Computing Mobile :

Le Cloud Computing Mobile est connu pour être une solution pour l'informatique mobile pour de nombreuses raisons [11]. Dans ce qui suit, nous décrivons comment le nuage peut être utilisé pour surmonter les obstacles dans l'informatique mobile, ce qui en soulignant les avantages du MCC.

- Extension de la durée de vie de la batterie.
- Améliorer la capacité de stockage des données et la puissance de traitement.
- Amélioration de la fiabilité.

En outre, le MCC hérite également des certains avantages de nuages pour les services mobiles comme suit [12] :

- **Évolutivité** : Les fournisseurs des services peuvent facilement ajouter et d'étendre une application et un service avec ou sans contraintes d'utilisation des ressources.
- **Multi-location** : Les fournisseurs des services peuvent partager les ressources et les coûts pour soutenir une variété d'applications et un grand nombre d'utilisateurs.
- **Facilité** d'intégration : les services des fournisseurs peuvent être intégrés facilement à travers le nuage et l'Internet pour répondre aux demandes des utilisateurs.

❖ **Cloud Computing Mobile Extension de la durée de vie de la batterie :**

La batterie est parmi les principales préoccupations des utilisateurs des appareils mobiles. Et on peut citer plusieurs solutions ont été proposées afin d'améliorer les performances du processeur [10, 13]et gérer le disque et l'écran d'une manière intelligente [14, 15] afin de réduire la consommation d'énergie. La technique de calcul du déchargement a été proposée avec l'objectif de migrer les calculs importants et complexes des machines limités à l'instar des dispositifs mobiles (smartphone, Android, etc.) vers des machines ingénieuses autrement dit les serveurs au niveau du Cloud. Cette solution évite de prendre une application avec un long temps d'exécution sur un dispositif mobile qui se traduit par une grande quantité de consommation d'énergie.

❖ **Amélioration de la capacité de stockage et la puissance de calcul :**

Le Cloud Computing Mobile donne l'accès aux utilisateurs mobiles pour stocker et accéder

aux données dans le Cloud, le premier exemple est AMAZON simple Storage de vices (AMAZON S3) [18] qui supporte le service de stockage de fichiers, le deuxième exemple est le iCloud conçu par APPLE qui permet aussi à ses clients de stocker leurs fichiers [20]. Au niveau du Cloud les utilisateurs peuvent bénéficier d'une quantité considérable d'espace sur leurs dispositifs mobiles.
Le Cloud Computing Mobile permet aussi de réduire le coût de fonctionnement des applications du calcul intensif vu la migration du calcul des dispositifs mobiles vers le Cloud, ce dernier fait toujours appel à des machines virtuelles VMs [19] et des cloudlet.[21]

- **Amélioration de la fiabilité :**

Pour améliorer la fiabilité le Cloud est un moyen efficace avec le stockage de données ou l'exécution des applications, car sont stockées et sauvegardées sur plusieurs ordinateurs ce qui permet de réduire le risque de perte de données et des applications sur les dispositifs mobiles. Par exemple le Cloud peut être utilisé pour protéger les droits d'auteur des contenus numériques [22]. Le Cloud peut offrir à distance pour les utilisateurs mobiles avec des services de sécurité, des antivirus, ce qui implique d'avoir un usage efficace et fiable.

3.2.2. Inconvénients du Cloud Computing Mobile :

Mobile Cloud Computing possède des inconvénients comme :

- Qualité de la connectivité.
- Soucis de sécurité.
- Il faut un bon nombre de puissances d'énergie.
- La largeur de bande fonctionnant est très moins.

4. Problèmes de sécurité du Cloud computing mobile

Le Mobile Cloud Computing est une combinaison de mobile et Cloud Computing. Ainsi, les problèmes de sécurité dans le Cloud computing mobile sont dus aux menaces de sécurité contre le Cloud, les appareils mobiles et les applications exécutées sur ces appareils. Ces menaces peuvent être classées en trois catégories :
Les menaces mobiles, les menaces Cloud, et les menaces technologiques.
Le principale but de ces menaces est pour volée les données personnelles ou pour exploitée les ressources des appareils mobiles.

4.1 Menaces mobiles :

Il y a peu de temps, le développement de logiciels malveillants pour les appareils mobiles était considéré comme un mythe en raison de leurs limites en termes de matériel et de logiciel. De nos jours, l'utilisation et le développement croissants des appareils mobiles (par exemple les smartphones) ont conduit à l'évolution des menaces mobiles ; du premier cas de malware sur les appareils mobiles en 2004 ciblant Symbian, au code de DroidDream,

DroidKungFu et Plankton
Découvert en 2011 sur l'Android Market officiel [34]. Des études récentes [33], [35] ont classé les attaques mobiles en plusieurs catégories telles que : attaques basées sur des applications, attaques basées sur le Web, attaques basées sur le réseau et les attaques physiques.
Les attaques basées sur les applications concernent à la fois les applications hors ligne et en ligne dans ces types d'attaques sont inclus :

Les logiciels malveillants : Est un logiciel qui exécute un comportement malveillant sur un appareil sans l'utilisateur étant conscient de ce comportement
Les logiciels espions : Les menaces à la vie privée sont causées par des applications (malveillantes ou non) pour s'exécuter ils ont besoin de données plus sensibles telles que la localisation
Les menaces à vie privée : Les menaces à la vie privée sont causées par des applications (malveillantes ou non) pour s'exécuter ils ont besoin de données plus sensibles telles que la localisation et le reconditionnement étaient les techniques les plus utilisées en 2011 pour infectée les applications exécutées sous Android [33]. Dans ce genre d'attaque, un attaquant prend une application ; la modifie avec un code malveillant puis le republie.

- **La divulgation trompeuse** :[33] est une technique utilisée par un attaquant pour masquer la fonctionnalité indésirable d'une application, de sorte qu'un utilisateur ne la remarque pas et serait d'accord. Ceux les applications sont difficiles à bloquer ou à supprimée, car elles ne violent pas leurs conditions d'utilisation ou contrat d'utilisation de tout marché d'applications.
- **La technique de mise à jour :** a été récemment utilisée par les auteurs de logiciels malveillants comme méthode d'attaque Marché Android [33].

Cela peut réduire le nombre de clients du marché et donc les bénéfices du marché.

4.2 Menaces sur le Cloud :

D'un point de vue utilisateur, le Cloud Computing doit répondre à plusieurs questions de la sécurité et la confidentialité des données, la propriété et l'emplacement des données, l'accès et l'intégrité des données.

Qui peut voir mes données ?
La confidentialité est l'une des préoccupations majeures des applications cloud Mobile
Par exemple, certaines applications pour les téléphones intelligents utilisent le Cloud pour stocker les données des utilisateurs. Un exemple concerne les applications géo-localisées telles que des applications qui trouvent des restaurants à proximité pour l'utilisateur ; ou des applications qui permettent à l'utilisateur amis et famille de recevoir des mises à jour concernant sa position [36].

Qui est le propriétaire de « mes » données ? Où sont situées mes données ?

La propriété des données fait référence à la propriété des données numériques achetées. Grâce à Cloud, il est possible de stocker des fichiers multimédias achetés, tels que des livres audio, vidéo ou électroniques à distance plutôt que localement. Si un utilisateur achète des médias en utilisant un service donné et que le média lui-même est stocké à distance, il y a un risque de perdre l'accès aux médias achetés. Par exemple, ou pourrait refuser l'accès à l'utilisateur pour d'autres raisons [37].

La localisation des données soulève de nombreux problèmes en raison du problème de conformité et de la confidentialité des lois différentes d'un pays à l'autre. Par exemple, les lois européennes L'Union (UE) et l'Amérique du Sud sont différentes des lois des Europe, concernant la confidentialité des données [39]. En vertu du droit de l'UE [38] et du droit sud-américain [41], les données personnelles ne peuvent être collectées que dans des conditions strictes et dans un but légitime. Aux États-Unis, il n'y a pas de loi globale réglementant la collecte et le traitement des données personnelles [40].

Qui peut accéder et modifiée mes données ?

Les problèmes d'accès et d'intégrité des données sont principalement liés aux politiques de sécurité fournies aux utilisateurs lors de l'accès aux données. Toute modification de ces données peut affectent l'utilisateur. L'accès aux données doit être effectué par un utilisateur identifié (application).

5. Solutions de sécurité dans le Mobile Cloud computing

Les solutions de sécurité existantes traitent indépendamment les différents types de problèmes de la sécurité. Ces solutions sont mises en œuvre et fournies par des plateformes mobiles et par les fournisseurs de Cloud pour sécuriser les appareils mobiles et les communications entre les appareils mobiles et le Cloud.

5.1 Solutions de sécurité mobile :

Les appareils mobiles sont limités par des limitations de traitement et de puissance.

Les protégés contre les menaces de sécurité est plus difficile que le protège d'un ordinateur.

Les fournisseurs de plateformes mobiles (par exemple, Android, iOS) ont mis en œuvre plusieurs mesures de solutions de la sécurité dans le système d'exploitation des appareils. Cinq types de fonctionnalités de la sécurité ont été implémentés dans les différentes plateformes : [33].

- ✓ Le contrôle d'accès traditionnel est une technique qui utilise des mots de passe et un écran d'inactivité verrouillage pour protéger l'appareil mobile.
- ✓ La provenance de l'application fait référence au fait que chaque application doit être étiquetée Avec l'identité de son auteur et également signé avec une signature numérique.
- ✓ Le cryptage est utilisé pour protéger et masquée les données enregistrées sur l'appareil mobile en cas de perte ou vol.

- ✓ L'isolement est une technique qui sépare chaque application sur l'appareil pour refuser l'accès aux données d'autres applications.
- ✓ Le contrôle d'accès basé sur les autorisations est la capacité de l'appareil mobile à fournir une application avec un certain niveau de contrôle d'accès aux données et au système de l'appareil.

Android et iOS (voir le tableau2) ont tenté de sécurisée les plateformes plutôt que de forcée les utilisateurs à se fier à des logiciels de sécurité tiers. Alors qu'iOS propose quatre des cinq solutions de sécurité (contrôle d'accès traditionnel, provenance des applications, cryptage et isolation), Android n'en propose que trois (contrôle d'accès traditionnel, isolation et contrôle d'accès basé sur l'autorisation) [33].
La plateforme Android est moins rigoureuse qu'iOS. Cette faiblesse a été exploitée par attaquants en 2010 et 2011 qui ont remplacé certaines des applications légitimes par des applications contenant du code malveillant.

Security Feature	Apple iOS	Google Android
Access Control	⏩	=
Application Provenance	✚	⏪
Encryption	⏩	⏪
Isolation	=	✚
Permission-based Access Control	=	=

Tableau 2 : Solutions de sécurité mobile [33]

5.2 Solutions de sécurité des communications mobiles dans le Cloud :

Les fournisseurs d'applications de Cloud mobile doivent sécurisée les données échangées entre les appareils mobiles et le Cloud. Le protocole de sécurité le plus utilisé pour sécuriser la transmission de données entre l'appareil mobile et le Cloud est SSL / HTTPS [51]. Cependant, ce protocole est d'une part très énergivore [52] et d'autre part fournit des propriétés de sécurité (intégrité, confidentialité et authenticité) comme un bloc sans tenir compte du type de données transmises ou des attentes des utilisateurs.
Pour optimiser la consommation d'énergie, une architecture basée sur des composants de sécurité appelée LECCSAM (une gestion de la sécurité à faible consommation d'énergie et centrée sur l'utilisateur architecture adaptée aux environnements mobiles) a été conçue pour

sécuriser la communication entre deux appareils mobiles ou entre un appareil mobile et un serveur [51].

5.3 Solutions de sécurité du Cloud mobile :

Pour protéger les environnements de Cloud mobile contre les attaques de sécurité, trois catégories de solutions de sécurité ont été proposées.

5.3.1 Solutions de sécurité des données :

Pour garantie la confidentialité et l'intégrité des données de l'utilisateur stockées dans le Cloud, plusieurs solutions ont été proposées.

Itani et coll. [53] proposent une solution pour garantir l'intégrité des fichiers stockés dans Nuage. De plus, cette solution proposée veut un cadre éco-énergétique pour les appareils mobiles.

Les concepts Utilisés pour le concevoir sont : la cryptographie incrémentale [54] et confiance en informatique [55]. Les principales entités définies sont :

1) Le client mobile,
2) fournisseurs de services cloud
3) faire confiance à un tiers.

Les auteurs ont discuté de ce qui suit opérations : téléchargement, insertion de bloc, suppression de bloc et vérification de l'intégrité des fichiers dans l'environnement cloud computing Mobile. Lors du téléchargement de fichiers dans le cloud, le client mobile génère un code d'authentification de message incrémentiel (MACf) à l'aide de la Clé secrète et stockez-la.

Lorsque le client mobile souhaite effectuer une insertion, une suppression ou une mise à jour opérations sur les fichiers téléchargés les étapes suivantes sont effectuées: 1) le client mobile demander un dossier; 2) le service Cloud envoie le fichier au client mobile et également au tiers de confiance; 3) le tiers de confiance reconstruit l'authentification du message code (MACcop) puis il l'envoie au client mobile; 4) le MACcop reçu est par rapport à MACfDe s'ils sont identiques, l'intégrité est vérifiée.

Après l'intégrité poing-à-poing, le client mobile peut effectuer des opérations d'insertion, de suppression ou de mise à jour, puis nouveau calcul de MACf. Dans [56], les auteurs proposent trois schémas pour garantir la confidentialité et l'intégrité des fichiers des utilisateurs stockés sur le Cloud en considérant trois hypothèses :

1) le l'appareil mobile est semi-fiable,
2) les serveurs cloud ne sont pas fiables ;
3) la communication le canal est sécurisé.

Les fichiers sont créés et modifiés sur l'appareil mobile et stockés sur les serveurs Cloud. Dans chaque schéma, l'appareil mobile est responsable du cryptage, décryptage et vérification de l'intégrité.

Le premier système est appelé « système basé sur le chiffrement ». Lorsque l'utilisateur veut télécharger un fichier depuis un appareil mobile vers un serveur Cloud, il doit fournir un mot de passe (PWD). Ensuite, l'appareil mobile exécute les étapes suivantes: 1) il génère le Clé de chiffrement (EK) et la clé d'intégrité en utilisant une fonction de hachage (H) sur concaténation du nom de fichier (FN), de la taille du fichier (FS) et du mot de passe (PWD); 2) il crypte le fichier en utilisant EK afin d'obtenir la confidentialité; 3) il génère le message code d'authentification (MAC) utilisant le fichier et l'IK pour l'authentification; 4) il télécharge sur le serveur Cloud le fichier crypté (EF), le hachage du fichier et le MAC; 5) il supprime l'IK et l'EK; 6) il stocke le FN dans la table des fichiers locaux.
Lors du téléchargement d'un fichier, l'appareil mobile calcule le hachage du FN et transfère la valeur de hachage sur le serveur Cloud. Le serveur Cloud recherche les EF et MAC correspondants à l'aide des données reçues. Si un fichier est friand, le serveur Cloud envoie EF et MAC sur l'appareil mobile.

L'appareil mobile exécute les étapes suivantes : 1) il invite 'utilisateur doit entrer un mot de passe pour le fichier ; 2) il régénère l'EK et l'IK ; 3) il décrypte l'EF ; 4) il régénère le MAC et 5) il vérifie l'intégrité du fichier.
Le second schéma est appelé « schéma basé sur le codage ». Il a été développé afin de réduire la surcharge de calcul de l'opération de chiffrement. La solution était d'éliminer l'opération de cryptage. Ainsi, lors du téléchargement d'un fichier sur un serveur cloud les étapes suivantes sont effectuées: 1) le fichier à protéger est divisé en de parties de t morceaux et chaque bloc a n bits; 2) pour chaque bloc, il est généré un vecteur de codage (α) en appliquant récursive la fonction de hachage sur la concaténation de PWD, FN et FS; 3) alors l'IK est calculé en appliquant une fonction de hachage sur la concaténation de chaque α généré; 4) leα est utilisé pour produire un code de confidentialité (SC) pour chaque partie du fichier; et enfin le MAC est généré. Sur le serveur, l'appareil mobile télécharge la SC de chaque bloc avec le MAC et le hachage de la concaténation entre FN et le numéro de bloc. Lors du téléchargement, le mobile régénère le hachage ; avec ce hachage le serveur peut fournir la SC et MAC. L'appareil mobile invite l'utilisateur à saisir un PWD pour le fichier afin de reproduire les α et les IK. Le fichier d'origine est décodé par multiplier SC par l'inverse de α. Le troisième système est appelé « système basé sur le partage ». Ce schéma introduit sur exclusif ou opération. En conséquence, on fait valoir que ce régime nécessite moins de puissance de calcul côté appareil, ce qui conduit à l'économie d'énergie de l'appareil mobile. Une autre solution est proposée par [57] pour garantir la confidentialité, l'intégrité et la confidentialité des données de l'utilisateur stockées dans le Cloud. Cette solution fait deux hypothèses : 1) le canal de communication est sécurisé ; et 2) le tiers est digne de confiance.

L'architecture proposée est chargée de gérer l'encodage / décodage, cryptage / décryptage, génération de signature et vérification d'intégrité au nom d'utilisateur mobile. Il contient trois entités principales : l'utilisateur final mobile, un tiers de confiance, et un service de stockage Cloud.

Un cadre pour sécuriser les services de stockage dans le Cloud computing mobile est proposé dans [58].

Ce Framework comprend quatre modules : 1) un appareil mobile qui utilise le cloud services, 2) un fournisseur de services cloud, 3) une autorité de certification qui authentifie l'appareil mobile et 4) un module de télécommunication qui génère et assure le suivies mots de passe des appareils mobiles. Dans ce cadre, la clé secrète, la clé publique et la clé des sessions sont distribuées en toute sécurité. Pour utiliser les services cloud, l'utilisateur mobile doit s'inscrire auprès du module de télécommunication par l'intermédiaire de l'autorité de certification. En cas de succès enregistrement, le module de télécommunication émet un mot de passe (PWD) pour l'appareil mobile pour utiliser les ressources cloud. Afin de garantir une livraison sécurisée de PWD à l'appareil mobile, le module de télécommunication le crypte avec la clé publique des appareils mobiles. Avant que lors du téléchargement d'un fichier, l'appareil mobile le crypte avec sa clé secrète. Lors du téléchargement d'un fichier, l'appareil mobile doit d'abord s'authentifier ; en cas de succès, le cloud envoie le chiffré fichier sur l'appareil mobile avec une signature. Le mobile vérifie d'abord la signature puis décrypte le fichier. Dans le tableau 3, présente un aperçu des fonctionnalités de sécurité fournies par chaque donnée de solution de sécurité.

5.3.2 Solutions de sécurité des applications :

Zhang et coll. [59] a conçu une solution pour résoudre les problèmes de sécurité d'une application cloud mobile élastique. Une application élastique consiste en une ou indépendamment sur l'appareil mobile ou dans le Cloud et communiquer entre eux pour effectuer les tâches de l'application. Ils peuvent migrer entre le mobile et le Cloud en fonction des évolutions sur le mobile appareil. Les principaux composants de ce modèle d'application sont : Device Elasticity Manager (DEM) et Cloud Elasticity Service (CES).

Solution	Security properties	Operations performed by mobile device	Energy saving considerations
[IKC10]	Integrity of files stored in Cloud	MAC generation; MACs comparison	yes
[LLL+12] Encryption based scheme	Confidentiality and Integrity of files stored in Cloud	EK, IK, MAC generation; Encrypt, decrypt files	no
[LLL+12] Coding based scheme	Confidentiality and Integrity of files stored in Cloud	IK generation; Additional computation	no
[LLL+12] Sharing based scheme	Confidentiality and Integrity of files stored in Cloud	exclusive or computation	yes
[QMS+12]	Privacy, Integrity and Confidentiality of users data in Cloud	No operations	yes
[HLL11]	Secure storage services	Encrypt, decrypt files	no

Tableau 3 **:** Un aperçu sur les fonctionnalités de sécurité offertes par les solutions de sécurité des données.

Le Device Elasticity Manager configure l'application au moment du lancement (par exemple, il décide où un weblet doit être lancé, dans le Cloud ou sur l'appareil mobile) et rend ajustements de configuration au moment de l'exécution. Cloud Elasticity Manager garantit la ressource d'exécution pour les weblets. La solution de sécurité proposée :
1) assure l'installation sécurisée de l'application élastique, 2) gère l'authentification des weblets, 3) sécurise la communication entre les weblets fonctionnant simultanément sur un appareil mobile et dans les nœuds Cloud, 4) sécurise la migration des weblets entre l'appareil mobile et le Cloud and 5) garantit l'autorisation de weblets pour accéder aux données des utilisateurs. Une solution, appelée Trust Cube, est proposée dans [60] pour sécuriser l'accès aux données. Cette la solution utilise la propriété d'authentification pour fournir ou refuser l'accès à un mobile client vers un serveur Web. À authentifier les utilisateurs mobiles les auteurs proposent d'utiliser des mots de passe courts ou des codes PIN, ce qui n'est pas assez pour garantir un niveau de sécurité élevé.
Huan et coll. [51] a proposé un nouveau cadre de cloud computing mobile, appelé MobiCloud qui fournit des services de calcul conventionnels et améliore la fonctionnalité du Mobile Adhoc Network (MANETS) en termes de gestion des risques, gestion de la confiance et routage sécurisé. MobiCloud fournit plusieurs fonctionnalités pour gérer la sécurité, l'évaluation des risques, les services géo-localisés, le réseau et l'état surveillance et routage sensible au contexte. De plus, MobiCloud peut 1) étendre et augmenter la fonctionnalité des MANET, et 2) prédire les futures situations MANET pourprise de décisions en utilisant des données historiques. L'architecture MobiCloud définie dans [51] ne prend pas en compte la confidentialité et la sécurité des données des utilisateurs stockées dans le cloud. Une version améliorée de MobiCloud est proposée dans [61] où un modèle de traitement de données sécurisé est ajouté. Ce modèle se compose de trois domaines :
1) service public cloud et domaine de stockage, 2) cloud de confiance domaine et 3) domaines mobiles et de détection dans le cloud. Les auteurs supposent qu'une l'autorité est toujours disponible pour contrôler la distribution des clés et gérer le certificat distribution et identité de l'utilisateur.

Solutions de confidentialité : Les utilisateurs doivent savoir quelles informations personnelles sont exactement visibles par le public et d'avoir le contrôle sur les informations personnelles stockées sur leurs appareils mobiles.
Il est très important que toutes les données privées ne soient partagées qu'avec le consentement des utilisateurs.
5.3.3 La sécurité pour les utilisateurs mobiles : Les appareils mobiles sont exposés à des menaces et à de nombreux codes malicieux tels que les virus, les vers, et le cheval de Troie, ils peuvent provoquer des problèmes pour le secret privé des abonnés deux questions principales posées sont les suivantes :
1. La sécurité pour les applications mobiles : l'Installation et l'exécution des logiciels des sécurité, et les programmes antivirus.
2.confidentialité : Avec les avantages des dispositifs de positionnement (GPS), le nombre d'utilisateurs mobiles en utilisant les services de géo-localisation (LBS)augmente.

3. La sécurité des données : les deux utilisateurs des téléphones mobiles et les développeurs d'applications bénéficient de stocker une grande quantité des données et application sur un nuage, ils devraient faire attention à des questions liées aux données de MCC tel que :

L'Intégrité : désigne l'état de données qui, lors de leur traitement, de leur conservation ou de leur transmission, ne subissent aucune altération ou destruction volontaire ou accidentelle, et conservent un format permettant leur utilisation.

L'Authentification : un processus permettant au *système* de s'assurer de la *légitimité* de la demande d'accès faite par une entité (être humain ou un autre système...) afin d'autoriser l'accès de cette entité à des ressources du système (systèmes, réseaux, applications…) conformément au paramétrage du contrôle d'accès.[17]

Les droits numériques : Les contenus numériques non structurés (par exemple, vidéo, image, audio, et e-book) ont souvent été piratés et distribués illégalement. La protection de ces contenus à partir de l'accès est importante pour les fournisseurs des contenus dans le MCC, comme le Cloud Computing traditionnelle et le Peer-to-peer.

6. Conclusion

Nous avons présenté dans ce chapitre, une idée générale sur le Cloud Computing, et avec un passage au mobile Cloud computing, nous avons vu ses avantages ses inconvénients, les Problèmes de sécurité dans le Mobile Cloud Computing et les Solutions de sécurité possible.

A partir de cette étude nous pouvons conclure que la grande gamme des avantages présentés par le Cloud comme la productivité, la souplesse, la facilité de gestion, la flexibilité, l'élasticité ainsi que les avantages économiques justifient l'adoption massive de services dans le Cloud, quelque soient

Les risques et la complexité encourus.

Chapitre 2 : Mécanismes de sécurité utilisés

1. Introduction

D'après nos recherches peu de travaux ont porté jusqu'à présent sur la mise en place d'un contrôle d'accès dans le Cloud Computing mobile au sein de la communauté de la sécurité dans le Cloud.
Le MCC à de nombreux avantages pour les utilisateurs mobiles et les fournisseurs des Services. En raison de l'intégration des deux domaines différents alors le MCC doit faire face à de nombreux défis dans le contrôle d'accès au MCC.
Dans cette partie de chapitre, nous allons essayer de définir notre Mécanismes de sécurité utilisé.

2. Modèles de Contrôle d'accès dans le Mobile Cloud Compting

2.1. Définition :

Un modèle de contrôle d'accès généralement conçu pour fournir une autorisation, une authentification, une approbation d'accès, et audit. Il peut protéger les données contre (a) une utilisation et une divulgation non autorisées (confidentialité) ; et (b) modification et destruction non autorisées ou inappropriées (intégrité).la protection peut être atteinte en s'assurant que les décisions, pour les demandes d'accès des utilisateurs pour les objets protégés (données), devraient passer par certaines opérations qui sont réglementées par un ensemble de contrôle d'accès politiques [63].

2.2. Contrôle d'accès et défis du Cloud computing :

Le partage de ressources physiques entre des locataires potentiels non approuvés peut entraîner une certaine sécurité et les défis de contrôle d'accès dans le cloud, qui augmentent le risque d'attaques par canal secondaire.
Prévenir des types d'attaques, un mécanisme de contrôle d'accès précis peut aider à mettre en œuvre des mesures de sécurité standard. Ces défis de contrôle d'accès et la complexité les liens associés à leur gestion nécessitent une architecture de sécurité adéquate pour satisfaire l'accès exigences de gestion et garantir une interopérabilité sécurisée sur plusieurs nuages [64].

La multi-location, l'élasticité, l'évolutivité massive et la mobilité sont à l'origine d'une Nouveauté unique défis à l'autorisation et au contrôle d'accès dans le cloud mobile.
La multi-location rend laco-résidence de machines (par exemple, machines virtuelles, moteurs de bases de données, etc.) et d'autres ressources, appartenant à différents locataires, Au même niveau d'accès privilégié dans le cloud par rapport à autre sent dynamicité du

Cloud mobile entraîne (a) un changement d'utilisateurs actifs au fil du temps
(b) créer ou modifier des ressources qui ont besoin de protection ; et (c) modifier
Les conditions d'accès des utilisateurs aux ressources pendant runtime des applications.
La mobilité des utilisateurs leurs permet de passer d'un fournisseur de services à un autre
Et obtenir les services et ressources demandés qui sont fournis, distribués et gérés
Par différents prestataires de services. Des techniques d'autorisation et de contrôle d'accès
Appropriés ne doivent pas seulement protéger les ressources divulgation non autorisée et
Modification des attaquants, mais devrait également permettre la séparation des locataires
Les uns des autres, et isolement des ressources de calcul, de stockage et réseau du
Fournisseur de cloud des locataires [65].

2.3 Différentes approches de contrôle d'accès :

Il existe quatre méthodes de contrôle d'accès aux données [66, 17] : a) Accès discrétionnaire modèle de contrôle (DAC) [68] ; (b) Modèle de contrôle d'accès obligatoire (MAC) [50] ; (c) Basé sur les rôles modèles de contrôle d'accès (RBAC) [49] ; et (d) modèle de contrôle d'accès basé sur les attributs (ABAC) [48, 47].

Modèle	Description	Avantages	Incontinents
DAC	Est un mécanisme logiciel qui permet de contrôler l'accès des utilisateurs aux fichiers et aux répertoires. Le DAC laisse à la discrétion du propriétaire la définition de la protection des fichiers et des répertoires ; Les propriétaires de données déterminent les décisions d'accès et sont basées sur l'identité de sujets (utilisateurs) et objets (données) (figure 1).	L'interface utilisateur est très facile à utiliser, il n'est donc pas nécessaire de tout planifier en même temps.[69]	Il n'est pas vraiment possible pour l'administration de surveiller les ACL de temps en temps, ce qui peut entraîner une fuite d'informations vers une personne extérieure à l'organisation.
MAC	Pour protéger les données ou les paramètres d'un système contre tout accès non autorisé ou contre une modification malveillante, les entreprises attribuent généralement à tout utilisateur un accès restreint aux fichiers dont il a besoin dans l'exercice de ses fonctions. Définir et attribuer ces droits d'accès reste	On peut être sûr que leurs données les plus confidentielles sont bien protégées et ne laissent aucune place aux fuites [70]	Elle nécessite une mise à jour régulière lorsque de nouvelles données sont ajoutées ou que d'anciennes données sont supprimées.

	cependant une tâche complexe pour les petites et moyennes entreprises ; Un administrateur de politique de sécurité Contrôle et détermine de manière centralisée les décisions de contrôle d'accès en fonction des étiquettes d'objet (sécurité étiquette de classification) et les sujets (étiquettes d'habilitation de sécurité) ; les propriétaires de données n'ont pas possibilité de contourner la politique (Figure 1).		
RBAC	L'accès aux données est basé sur le rôle des sujets ou leurs fonctions professionnelles spécifiques ; les données les décisions d'accès sont prises en fonction de la correspondance entre (a) les sujets et les rôles, et (b) rôles et autorisations, en fonction des affectations de sujets aux rôles et des rôles aux autorisations (Figure 1). RBAC prend en charge le contrôle d'accès à grain grossier et prédéterminé, en raison de l'utilisation des rôles et des attributions de rôles aux utilisateurs, il est difficile de définir et de structurer rôles prenant en charge les changements dynamiques des conditions d'environnement (par exemple, l'emplacement actuel de l'utilisateur, l'objet étant actuellement dans un état spécifique et l'heure de la journée à laquelle l'accès est demandé [46]) [50].	Vous pouvez réduire le besoin de paperasserie et de changement de mot de passe lorsqu'un employé est embauché ou change de rôle. Au lieu de cela, vous pouvez utiliser RBAC pour ajouter et changer de rôle rapidement et les mettre en œuvre à l'échelle mondiale sur les systèmes d'exploitation, les plates-formes et les applications.[71]	Vous ne pouvez pas configurer une règle à l'aide de paramètres inconnus du système avant qu'un utilisateur ne commence à travailler. Et Les autorisations ne peuvent être attribuées qu'aux rôles d'utilisateur, pas aux objets et aux opérations

ABAC	Utilise des attributs de sujets, d'objets et d'environnements pour décrire et différencier eux de tous les autres. Sur la base des attributs attribués à un sujet, les attributs attribués d'un objet, les conditions d'environnement et un ensemble de politiques, qui sont spécifiés en fonction de ces attributs et conditions, demandes d'accès du sujet pour effectuer une opération sur l'objet sont accordées ou refusés. [45, 66]	Le contrôle d'accès basé sur les attributs exploite plusieurs dimensions des attributs uniques des données et des consommateurs de données pour déterminer s'il faut accorder ou refuser l'accès aux données.[72]	Il n'y a pas beaucoup de déploiements car c'est encore un peu nouveau, et parce que vous n'obtenez tous les avantages que lorsque vous déployez une infrastructure suffisante

Tableau 4 : comparaison entre les modèles de contrôle d'accès aux données

- A cause de plusieurs problèmes ouverts dans DAC et MAC en termes d'évolutivité et d'adaptabilité dynamique aux changements des politiques de sécurité [50], c'était nécessaire de faire le choix sur une approche basé sur les rôles plus la limitation de ces rôles en basant sur la situation géographique comme une point forte.

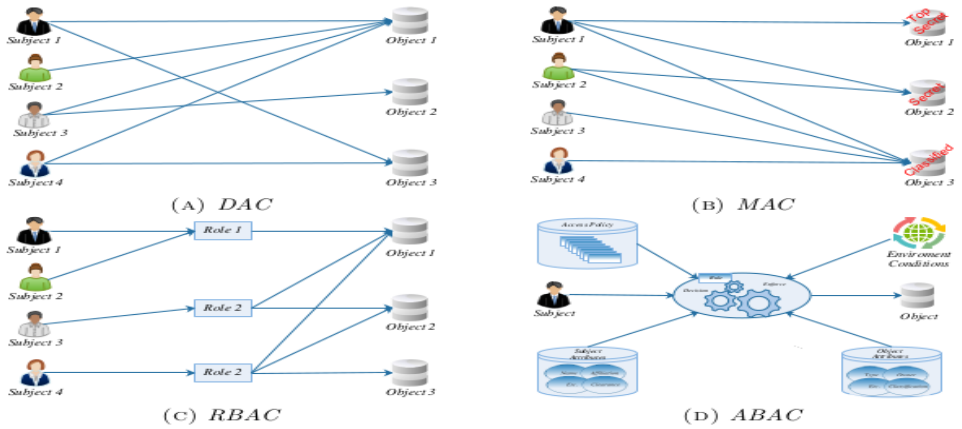

Figure 1:Contrôle d'accès : différentes approches [50]

2.4. Modèle LRBAC :

Le modèle LRBAC [Bertino et al. 2005], étend le modèle RBAC en définissant de
Nouveaux concepts spatiaux pour représenter la position des sujets et celles des objets.
Ces nouveaux concepts sont utilisés pour limiter géographiquement l'utilisation des rôles.
Le principe proposé dans LRBAC est de comparé une position physique, supposée obtenue de façon fiable (par exemple la localisation GPS), à des positions logiques (exemples : route, ville, région) auxquelles sont associées des rôles géographiques [Thion 2008].
Il est composé comme RBAC de sous-modèles de base, hiérarchique, et contraint.
Le modèle LRBAC comprend tous les concepts de base de RBAC et ajoute des nouveaux concepts : la notion de rôle spatial, et de position réelle/logique. Ce modèle est très précis pour répondre à la nécessité de prendre en compte la localisation géographique, dans la construction d'une règle de politique de contrôle d'accès.

a. Composants de LRBAC : [43]

LRBAC est un modèle complet, qui, est comme RBAC, se compose de trois composants
Respectivement appelés Core, Hierarchical et Constrained LRBAC
Les apports de nos travaux peuvent être résumés comme suit :
—Core LRBAC précise les concepts de base du modèle, donc la notion de rôle, schéma de rôle, position réelle/logique, rôle activé/activé, qui sont utilisés par le composants ultérieurs.
—Le LRBAC hiérarchique étend le concept conventionnel de hiérarchie en introduisant deux nouveautés majeures. Tout d'abord, deux hiérarchies distinctes sont fournies, l'une sur les schémas de rôles et un sur les instances de rôle. La hiérarchie du schéma de rôle prend en charge l'héritage de autorisations et appartenances d'utilisateurs parmi des ensembles de rôles homogènes et définition de rôle simple. La deuxième extension concerne la définition formelle du rôle activation et activation en présence de hiérarchies. A cet effet, nous présentons un modèle dans lequel la hiérarchie des instances de rôle est utilisée pour dériver les rôles qui sont non seulement activé mais également activé dans une session.
—Contrainte LRBAC prend en charge la spécification des contraintes de séparation des tâches (SoD) pour les rôles spatiaux et les schémas de rôles. Étant donné que les contraintes de rôle exclusif sont importantes pour accompagner la définition et la maintenance des politiques de contrôle d'accès dans les contextes mobiles, Les contraintes SoD sont étendues pour tenir compte des différentes granularités (schéma/instance niveau), dimension (spatiale/non spatiale) et différents temps de vérification (statique, dynamique au moment de l'activation, dynamique au moment de l'activation). L'ensemble de contraintes résultant représente une première classe complète de contraintes pour les applications spatiales.
—Propriétés du LRBAC contraint. Même si l'enquête sur les opérations administratives pour LRBAC est en dehors des objectifs de cet article, une analyse sur l'expressivité et la complexité des contraintes proposées est un enjeu pertinent pour établir l'utilisabilité du

modèle proposé. Certaines de ces propriétés étendent des résultats déjà connus aux nouvelles classes de contraintes que nous avons introduites. D'autres propriétés sont neuves et compte des caractéristiques spécifiques GEO-HRBAC.

L'objectif dans LRBAC peuvent être représentés par extension en listant les caractéristiques appartenant à l'ensemble ou en spécifiant intentionnellement une requête spatiale ou non spatiale sur un extension de type d'entité. L'objet dans ce cas correspond au résultat de la requête.

b. exemple de Modèle LRBAC

Dans LRBAC, nous supposons que les utilisateurs ont une position qui peut changer dans le temps. Les postes peuvent être réel ou logique. La position réelle correspond à la position sur Terre de l'utilisateur, obtenu à partir d'un terminal mobile donné tel qu'un dispositif de localisation de véhicule basé sur GPS ou un Téléphone cellulaire. Les positions réelles peuvent être représentées sous forme de géométries de différents types puisque, selon la technologie choisie et les exigences de précision, ils peuvent correspondre à points ou polygones. Par souci de généralité, nous ne faisons aucune hypothèse sur la type géométrique de la position réelle.

Outre les positions réelles, cependant, pour activer un rôle donné, il peut être utile de connaître non seulement la position réelle de l'utilisateur mais aussi la position logique. La position logique permet une position à représenter d'une manière presque indépendante du positionnement sous-jacent La technologie. La position logique est modélisée comme une caractéristique spatiale. Par exemple le L'emplacement logique d'un véhicule peut être une caractéristique polygonale de type, par exemple, une ville. Une telle caractéristique peut déjà exister dans la base d'informations ou être une nouvelle fonctionnalité entrée dans le système lorsque la position est notée Les positions peuvent également être représentées à différents niveaux de granularité qui peut dépendre du rôle joué par l'usager : par exemple pour un chauffeur de taxi la logique La position peut être un point le long d'une route alors que pour un conducteur de camion, il peut s'agir d'une portion de route.

Notez qu'une position grossière peut être demandée à des fins de préservation de la vie privée, afin de masquer la position réelle de l'utilisateur.

La position logique peut être calculée à partir de positions réelles en utilisant un mappage sphérique les fonctions. Par exemple, une fonction pourrait être définie pour cartographier un point acquis par GPS équipement basé sur le segment de route le plus proche.

3. L'authentification par jeton

L'authentification par jeton s'appuie sur un protocole qui permet à un utilisateur de recevoir un jeton d'accès unique après avoir confirmé son identité. L'utilisateur bénéficie alors, pendant toute la durée de vie du jeton, d'un accès à l'application ou au site web pour lequel le jeton lui a été accordé. Il n'a ainsi plus besoin de saisir ses identifiants à chaque

fois qu'il ouvre la même page web ou application, ou utilise toute autre ressource protégée par le même jeton.

Les jetons d'authentification fonctionnent à la manière d'un ticket d'entrée à validité limitée : ils accordent un accès en continu pendant leur durée de validité. Dès que l'utilisateur se déconnecte ou quitte l'application, le jeton est invalidé.

L'authentification par jeton est différente des mécanismes traditionnels basés sur un mot de passe ou un serveur. Les jetons constituent un deuxième niveau de sécurité et offrent aux administrateurs un contrôle accru sur l'ensemble des actions et opérations.

L'utilisation de jetons demande toutefois quelques connaissances en matière de codage. La plupart des développeurs se forment rapidement aux nouvelles techniques, mais la courbe d'apprentissage n'en est pas moins exigeante.

a. Types de jeton d'authentification

Tous les jetons d'authentification ont un objet pour autoriser l'accès, mais chaque type a ses spécificités. Les plus courants sont :

- **Les jetons par connexion :** clés, disques, lecteurs et autres supports physiques connectés à un système pour en permettre l'accès.
- **Les jetons sans contact :** le terminal est suffisamment proche du serveur pour établir une connexion, mais sans contact physique. Le projet de bague biométrique de Microsoft en est un bon exemple.
- **Les jetons à distance :** le terminal est capable de communiquer avec le serveur sur de très longues distances, même s'il n'entre jamais en contact avec un autre dispositif.

Dans ces trois scénarios, l'utilisateur est celui qui doit initier le processus d'authentification, en saisissant un mot de passe ou en répondant à une question. Toutefois, même s'il remplit ces étapes préliminaires sans aucun problème, l'accès ne pourra lui être accordé sans l'intervention d'un jeton d'accès.

Il existe d'autres types de jetons, comme les **jetons mobiles dynamiques** qui sont implantés dans le téléphone mobile pour générer un code formé par la méthode du mot de passe à usage unique et ne peut être utilisé que pour une session de connexion ou une transaction.

3.1. Les étapes de l'authentification par jeton [42] :

Pour mettre en place un système d'authentification par jeton, les identifiants des utilisateurs ne seront vérifiés qu'une seule fois. Ils bénéficieront en contrepartie d'un jeton qui leur garantit un accès continu pendant une période que vous définissez vous-même.

La procédure se déroule de la manière suivante :

- **Requête :** l'utilisateur demande l'accès à un serveur ou à une ressource protégée. Cela peut passer par une connexion via un mot de passe ou tout autre procédé de votre choix.
- **Vérification :** le serveur détermine si l'accès doit ou non être accordé à cette personne. Cela peut consister à vérifier la combinaison nom d'utilisateur/mot de passe, ou bien à utiliser n'importe quel autre procédé de votre choix.
- **Génération d'un jeton :** le serveur communique avec le terminal d'authentification, qu'il s'agisse d'une bague, d'une clé, d'un téléphone ou de tout autre dispositif. Une fois la vérification effectuée, le serveur émet un jeton et l'envoie à l'utilisateur.
- **Stockage :** le navigateur de l'utilisateur conserve le jeton pendant toute la durée nécessaire.

Si l'utilisateur essaie d'accéder à une autre section du serveur, le jeton communique à nouveau avec le serveur. L'accès est alors autorisé ou refusé en fonction des caractéristiques du jeton.

Ce sont les administrateurs qui définissent les limites applicables aux jetons. Il est ainsi possible de créer des jetons à usage unique qui sont immédiatement détruits lorsque l'utilisateur se déconnecte ou bien de programmer la destruction automatique d'un jeton après une certaine durée.

Figure 2 : représentation des étapes de l'authentification par jeton [42]

4. L’empreinte digitale

Une empreinte digitale ou une trace digitale de données est une trace de données unique des activités, actions, communications ou transactions d’un utilisateur sur un support numérique. Cette trace de données peut être laissée sur l’internet, les ordinateurs, les appareils mobiles ou d’autres supports. Une empreinte numérique peut être utilisée pour suivre les activités et les appareils de l’utilisateur. Un utilisateur peut laisser une empreinte numérique de manière active ou passive, mais une fois partagée, une empreinte numérique est presque permanente par nature.

Les utilisateurs de technologies sont souvent impliqués dans des activités numériques, soit activement soit passivement. Cependant, quoi qu’ils fassent, il reste toujours une trace de données qui montre les activités des utilisateurs. Si nécessaire, ces activités peuvent être retracées.[73]

5. Conclusion

Le Cloud étant une technologie à croissance rapide qui offre une vaste gamme d'avantages aux utilisateurs ainsi qu’aux entreprises. Cependant, la sécurité, la confidentialité des données personnelles et la confiance restent les principales préoccupations qui empêchent l'adoption massive du Cloud vu que la plupart des méthodes employées sont vulnérables à de nombreuses attaques, ce qui engendre l'insécurité des utilisateurs.
Les mécanismes d’authentification forte offrent par conséquent une limitation des accès illégaux, ils représentent la condition principale pour sécuriser le Cloud. Un mécanisme d’authentification conçu pour le Cloud doit être suffisamment solide afin de le protéger des diverses attaques possibles. Étant donné que l'identité de l'utilisateur et des informations sensibles sont régulièrement utilisées dans le processus d'authentification lors de l’accès aux services Cloud, un besoin primordial est de protéger et empêcher les utilisateurs de révéler leurs informations personnelles au Cloud Service Provider.
Alors dans ce chapitre on a traité le contrôle d’accès dans le MCC ensuite on a donné un aperçu sur l’authentification par jeton dynamique.

Chapitre 3 : Notre approche proposée

1. Introduction

Pour pouvoir tirer parti de tous les avantages offerts par le Cloud Computing, plusieurs Éléments de sécurité doivent être analysés : les processus, les technologies et les mécanismes de contrôle. Alors si on parle de Cloud on parle aussi de ressources partagées ce qui nous pousse à protéger ces ressources et a contrôlé l'accès. Le contrôle d'accès est indispensable pour la sécurité dans les systèmes informatiques.
Pour les applications critiques, un modèle de contrôle d'accès basé sur l'emplacement et les jetons est nécessaire pour augmenter la sécurité de l'application et garantir que les informations de localisation ne peuvent pas être exploitées pour causer des dommages.
L'objectif est de proposer un mécanisme de contrôle d'accès léger, efficace, et qui permet l'exploitation de la puissance de MCC en toute sécurité.

2. Architecture du système

Notre implémentation a pour l'objectif de proposer un mécanisme de contrôle d'accès léger, efficace, et qui permet l'exploitation de la puissance de MCC en toute sécurité.
Pour atteindre cet objectif, nous avons choisi d'utiliser :

- Le modèle LRBAC pour contrôler l'accès des utilisateurs. Ce modèle sert à combiner la localisation de l'utilisateur avec son rôle.
- L'authentification par jeton PASETO pour authentifier les actions des utilisateurs
- L'empreinte digitale de l'appareil afin de confirmer l'identité de l'utilisateur.

Ainsi, nous proposons l'architecture suivante de notre système, illustrée dans la figure 3 :

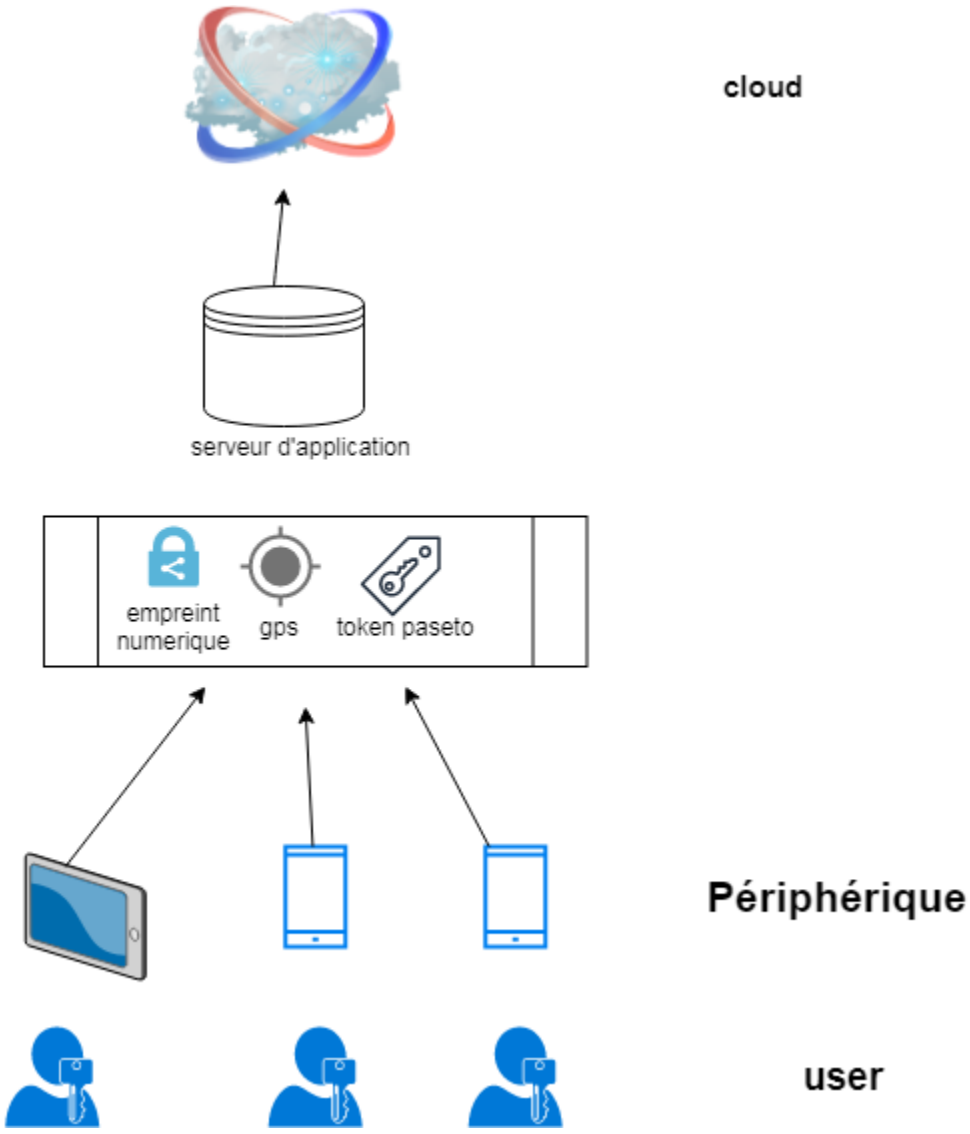

Figure 3 : Architecture du système de contrôle d'accès

3. Fonctionnement du système

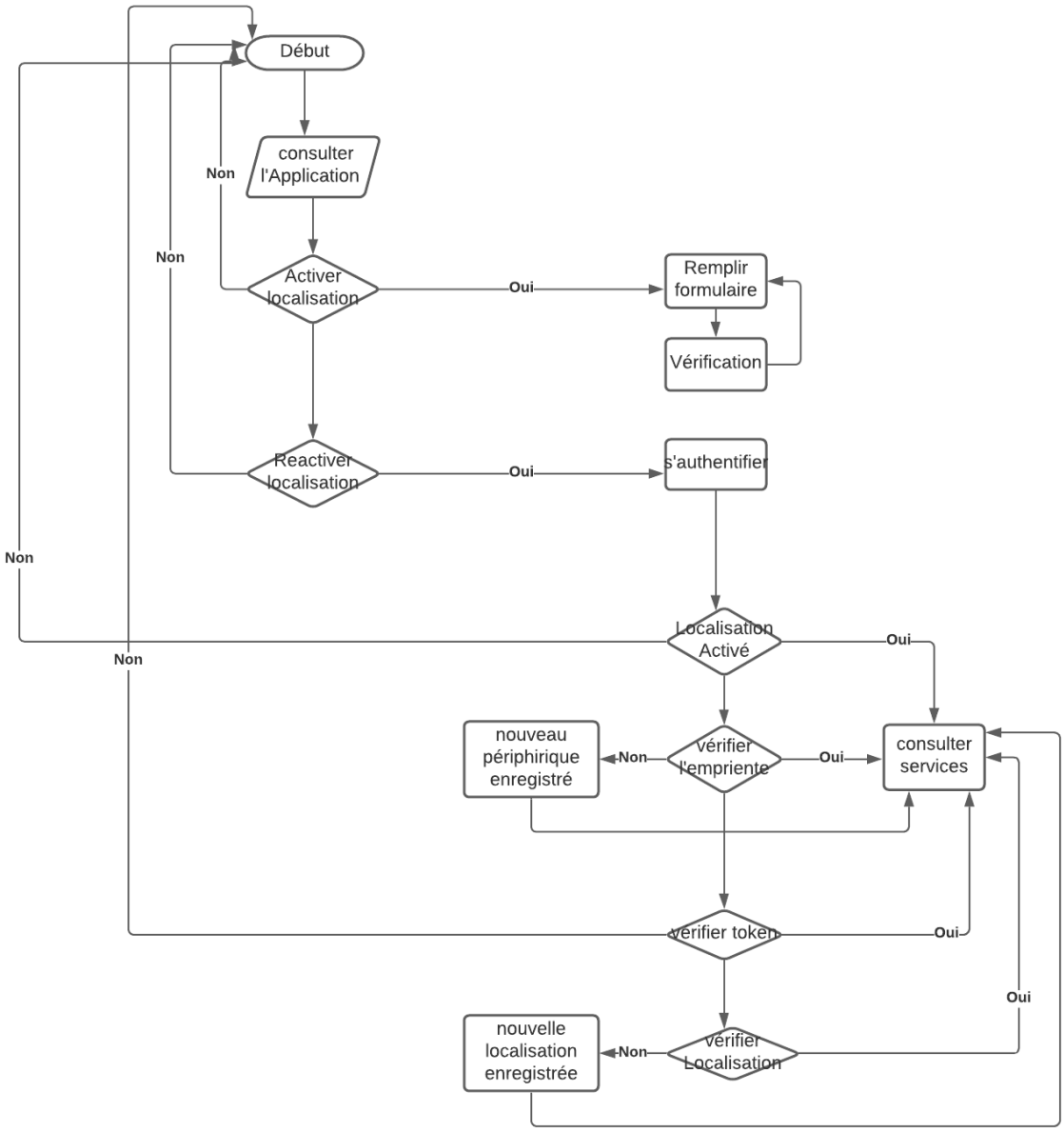

Figure 4 : organigramme de fonctionnement d'application

Le fonctionnement de notre système passe par les étapes suivantes :

1. **Inscription :** Dans un premier temps, l'utilisateur doit s'inscrire pour accéder à l'application qui est hébergé dans le cloud. Il doit obligatoirement activité sa localisation sinon il ne peut pas accéder (échec d'accès). Une fois la localisation est activée, l'utilisateur doit donner les informations suivantes : nom, email avec un

mot de passe, et son rôle. Ces informations avec la localisation et les paramètres de l'appareil (périphérique) sont sauvegardés au niveau de base de données.

2. **Connexion :** Une fois l'inscription est réussie, l'utilisateur peut se connecter à son compte à tout moment et de n'importe où. Sa localisation doit être toujours activée lors de l'authentification, sinon la connexion échouera. A la connexion, on vérifie l'empreinte digitale de l'appareil de l'utilisateur pour confirmer si l'utilisateur se connecte via le même périphérique. Dans le cas contraire, le nouveau périphérique sera enregistré dans la liste des appareils autorisée a connecté.
3. **Action :** Une fois connecté, l'utilisateur peut choisir une action à entreprendre et pour chaque action un token selon son rôle.
4. **Déplacement :** Une fois l'utilisateur se déplace le système vérifié la liste des localisations autorisée à connecté sinon la connexion échouera.

4. Conception de LRBAC

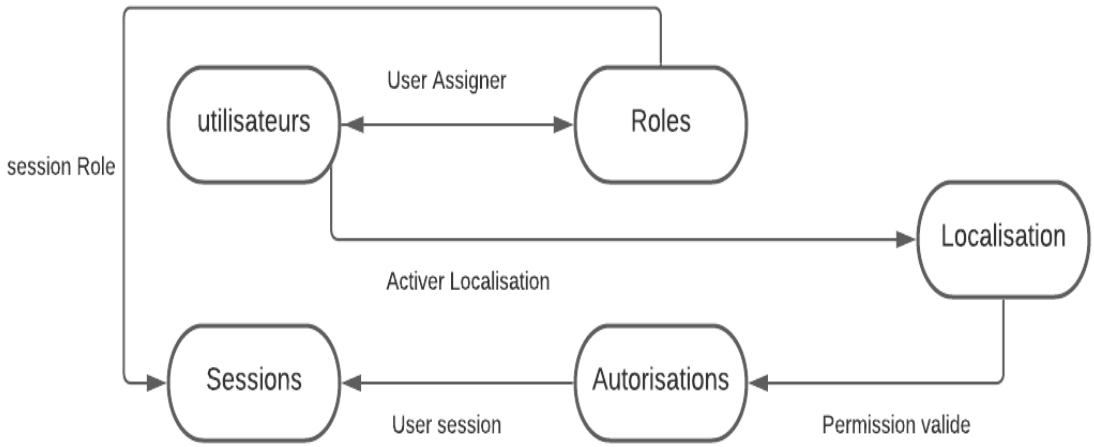

Figure 5 : formalisation de l'approche LRBAC

Comme illustré par la figure 5, notre modèle est composé de :

- **Utilisateur :** est une entité active, soit un utilisateur ou administrateur.
- **User assigner :** l'utilisateur au moment de l'inscription il établir son rôle.
- **Activer localisation :** l'utilisateur pour accéder à son compte où il doit activer sa localisation après le système compare la localisation de l'utilisateur avec le premier de l'inscription.
- **Rôle :** est une fonction de travail dans le cadre d'une organisation liée à une autorité et des responsabilités.
- **Session Rôles :** permet d'établir l'ensemble des rôles associés à une session.

- S**ession :** une correspondance entre un utilisateur et un ensemble de rôles autorisés si la localisation est correcte.
- **Autorisations :** afin d'effectuer des opérations sur un ou plusieurs objets protégés.
- **User session :** prend comme entrée l'autorisation de système et comme sortie la session de l'utilisateur.
- **Localisation :**de l'utilisateur après avoir un compte si sa localisation est incorrecte il ne peut pas consulter sa session mais s'il est correct il peut accéder avec une session
- **Permission valide :** si la localisation est valide ici le système donne l'autorisation pour accéder à son compte.

5. L'authentification par jeton dynamique

L'authentification par jeton dynamique utilise la cryptographie ou d'autres techniques pour créer un authentificateur par session. Un authentificateur dynamique change à chaque session d'authentification entre le demandeur et le vérificateur.

Dans notre solution, nous allons utiliser des jetons mobiles dynamiques pour les transactions (actions) des utilisateurs. En effet, lorsqu'une API est protégée par un jeton dynamique, un nonce temporel est inséré dans le jeton. Le jeton a une durée de vie (TTL) après laquelle l'utilisateur doit acquérir un nouveau jeton, sinon la transaction est interdite. Dans notre cas, le jeton est expiré aussi si l'utilisateur se déplace (change de localisation) car il doit s'inscrire parce que ce jeton dynamique permet aux données saisies par l'utilisateur ou bien le formulaire d'être accessible donc une vérification momentanée de l'information de la localisation qui permet de renforcer la sécurité au niveau de la limitation des rôles par emplacement et aussi a un usage unique et ne peut pas être utilisé que pour une session de connexion ou de transaction.
Apparemment est une solution simple et très efficace pour implémenter ces défenses et améliorer la sécurité implique des jetons dynamiques pour l'authentification multi-facteurs. Pour s'authentifier correctement, deux éléments d'authentification sont requis : quelque chose que vous connaissez comme un mot de passe, et quelque chose que vous avez tel un jeton mobile.
L'accès n'est accordé que lorsque les deux éléments sont présents si un attaquant vole les informations d'identification d'un administrateur, il ne pourra pas accéder à vos systèmes sans le contrôle du jeton.

6. Empreinte numérique de périphérique

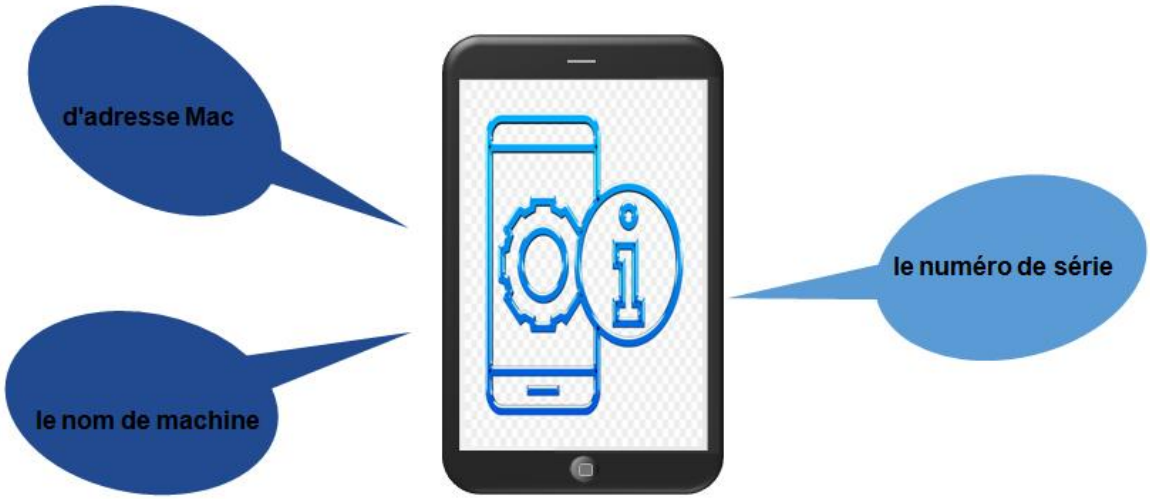

Figure 6 : l'empreinte numérique de périphérique

L'empreinte digitale d'appareil permet d'identifier l'appareil de manière unique en utilisant ses informations, telles que sa marque, son modèle, son système d'exploitation, son navigateur et même les logiciels qui y sont installés.
Dans notre cas, nous avons choisi une empreinte numérique qui est défini par le modèle de téléphone (ou l'appareil de manière générale), son numéro de série et son adresse MAC. Ces informations sont concaténées et hachées avec l'algorithme de hachage SHA-256 [67].

SHA256 autrement dit **Secure Hash Algorithm**, est un algorithme représentant une famille de fonctions de hachage mises en place par la National Security Agency des États-Unis. Il faut savoir qu'à l'origine Sha-2 a été créé en se basant sur Sha-0 ainsi que sur Sha-1, il représente donc la suite logique de ces algorithmes.
Quand on parle de SHA256 il s'agit en fait d'une **signature pour les fichiers de données**. Par exemple pour SHA256, il est ainsi possible de générer une signature de 32 octets (soit 256 bits).
Une fonction de hachage donne simplement un hachage identique pour une même entrée. Cela est réalisé pour n'importe quelle donnée et ne dépend pas de la façon dont l'algorithme est exécuté.
Il faut également préciser (c'est très important) que si des données d'entrée ou simplement si un caractère du texte est changé, le hachage de sortie s'en retrouve alors lui aussi également modifié.
De plus il faut aussi savoir qu'une fonction de hachage représente une fonction qui a la

particularité d'être à sens unique. Cela veut donc dire que des données d'entrée ne peuvent être générées à partir du hachage.
Cette fonction à sens unique permet de **convertir un texte de longueur différente en une chaîne de 256 bits** [68].

- Le choix de travailler avec cette norme de hachage à cause de ces avantages :
  - ✓ Respecte **« RGPD-friendly »**
  - ✓ Fonction non réversible
  - ✓ Échange et Partenariat.

7. Conclusion

Dans ce chapitre, nous avons proposé un contrôle d'accès qui est basé sur le modèle LRBAC et qui utilise aussi des jetons dynamiques pour les actions et l'empreinte numérique de périphérique. L'implémentation et le test de ce dernier est détallé dans le chapitre suivant.

Chapitre 4 : Implémentation et test de l'approche proposée

1. Introduction

Dans le chapitre précédent, nous avons présenté notre solution pour un système de contrôle d'accès des utilisateurs basé sur le modèle LRBAC (localisation + rôle), authentification par jeton dynamique des actions et empreinte digitale de périphérique. Nous allons décrire dans ce qui suit, les aspects techniques attachés à l'implémentation et à la réalisation de ce système.
Pour bien illustrer le fonctionnement de ce système, nous introduisons un exemple de déroulement d'application développée.

2. Environnement de développements

Notre implémentation a été déroulée sous Android studio en utilisant le langage java,
Les données sont stockées au niveau d'une base de données MySQL d'où la nécessité d'utiliser le langage PHP et le serveur local wamp server.

Android Studio :

L'environnement de développement intégré (IDE) officiel pour le développement d'applications Android, basé sur IntelliJ IDEA. En plus du puissant éditeur de code et des outils de développement d'IntelliJ, Android Studio offre encore plus de fonctionnalités qui améliorent votre productivité lors de la création d'applications Android,

Android Studio permet principalement d'éditer les fichiers Java/Kotlin et les fichiers de configuration XML d'une application Android.

Il propose entre autres des outils pour gérer le développement d'applications multilingues et permet de visualiser rapidement la mise en page des écrans sur des écrans de résolutions variées simultanément. Il intègre par ailleurs un émulateur permettant de faire tourner un système Android virtuel sur un ordinateur.

MySQL :

Est un système de gestion de bases de données relationnelles (SGBDR). Il est distribué sous une double licence GPL et propriétaire. Il fait partie des logiciels de gestion de base de données les plus utilisés au monde, autant par le grand public (applications web principalement)que par des professionnels, en concurrence avec Oracle, PostgreSQL et Microsoft SQL Server.

Java :

est un langage de programmation orienté objet créé par James Gosling et Patrick Naughton, employés de Sun Microsystems, avec le soutien de Bill Joy (cofondateur de Sun Microsystems en 1982), présenté officiellement le 23 mai 1995 au *SunWorld*.

PHP :

est un langage de programmation libre, principalement utilisé pour produire des pages Web dynamiques via un serveur HTTP, mais pouvant également fonctionner comme n'importe quel langage interprété de façon locale. PHP est un langage impératif orienté objet.

PHP a permis de créer un grand nombre de sites web célèbres, comme Facebook et Wikipédia. Il est considéré comme une des bases de la création de sites web dits dynamiques mais également des applications web.

WampServer :

Est une plateforme de développement Web de type WAMP, permettant de faire fonctionner localement (sans avoir à se connecter à un serveur externe) des scripts PHP. WampServer n'est pas en soi un logiciel, mais un environnement comprenant trois serveurs (Apache, MySQL et MariaDB), un interpréteur de script (PHP), ainsi que phpMyAdmin pour l'administration Web des bases MySQL.

Il dispose d'une interface d'administration permettant de gérer et d'administréces serveurs au travers d'un *trayicon* (icône près de l'horloge de Windows).

API RESTful :

Une API compatible REST, ou « RESTful », est une interface de programmation d'application qui fait appel à des requêtes HTTP pour obtenir (GET), placer (PUT), publier (POST) et supprimer (DELETE) des données, Aujourd'hui, l'utilisation croissante du Cloud entraîne l'apparition de différentes API visant à présenter les services Web. REST constitue un choix logique pour le développement d'API permettant à l'utilisateur final de se connecter à des services Cloud et d'interagir avec eux.

Actuellement, les modèles les plus répandus sont ceux fournis par Amazon Simple Storage Service (S3), OpenStack Swift et CDMI (Cloud Data Management Interface). [27]

Fonctionnalités de l'API REST expliquées [28]

Évolutivité : Comme les clients et les serveurs sont séparés, le produit peut être mis à l'échelle par l'équipe de développeurs sans trop de problèmes. De plus, il est également plus facile d'intégrer REST aux sites actuels sans re- factoriser l'infrastructure du site Web

Flexibilité et portabilité : Les utilisateurs peuvent facilement communiquer même si le client-serveur REST est hébergé sur différents serveurs,

Indépendance : l'API REST est ajustable à la syntaxe et à la plateforme opérationnelles, offrant la possibilité de tester de nombreux environnements pendant le développement.

3. Implémentation d'authentification par jeton dynamique

Pour implémenter ce mécanisme de sécurité nous avons utilisé PASETO [74] qui est une spécification et une implémentation de référence pour les jetons sans état sécurisé. PASETO est une norme concurrente de JOSE (JavaScript Object Signing and Encryption) et JWT (JSON Web Token) qui offre une suite de chiffrement versionnée.

Les messages PASETO sont constitués de trois ou quatre segments, séparés par un point (le caractère ASCII dont le numéro, représenté en hexadécimal, est 2E).
Sans le pied de page facultatif :
version.purpose.payload

Avec le pied de page facultatif :

version.purpose.payload.footer

- Si aucun pied de page n'est fourni, les implémentations ne devraient pas ajouter de point de fin à chaque charge utile.
- La version est une chaîne qui représente la version actuelle du protocole. Actuellement, deux versions sont spécifiées, chacune possédant ses propres suites de chiffrement. Valeurs acceptées : v1, v2.
- Le but est une courte chaîne décrivant le but du jeton. Valeurs acceptées : local, public.
- Local : chiffrement authentifié par clé partagée
- Public : signatures numériques à clé publique ;

Les PASETO sont destinés à être des jetons à usage unique, car il n'y a pas de mécanisme intégré pour empêcher les attaques de relecture pendant la durée de vie du jeton. De plus, les jetons publics sont destinés aux demandes d'authentification ponctuelles d'un tiers. Par exemple, PASETO public conviendrait à un protocole comme OpenIDConnect.
Pour créer un jeton dynamique PASETO, nous avons utilisé le langage PHP.

Ce dernier est enregistré dans notre base de données Puis, ce jeton sera décortiqué pour pouvoir rajouter la localisation de l'utilisateur. Enfin, si toutes les vérifications de connexion sont valides, le serveur génère le token qui comprend la localisation de l'utilisateur.
Ce dernier récupère ce token et l'utilise pour l'accès
Voici implémentation du jeton PASETO :

Algorithm 1:

```
function createtoken($email,$password,$address)
{
  $conn = OpenCon();

$sharedKey = new SymmetricKey('XYAXSJGS&T$&^$*&^E#');

 $token = Builder::getLocal($sharedKey, new Version4);

$token = (new Builder())
   ->setKey($sharedKey)
   ->setVersion(new Version4)
   ->setPurpose(Purpose::local())
   // Set it to expire in one day
   ->setIssuedAt()
   ->setNotBefore()
   ->setExpiration(
       (new DateTime())->add(new DateInterval('P01D'))
   )
   // Store arbitrary data
   ->setClaims([
       'email' => $email,
       'password'=>$password,
       'address'=>$address
   ]);
$sentencia = $conn->prepare("INSERT INTO tokens(token, email, password) VALUES
('$token', '$email', '$password')");
 $sentencia->execute();
 return $token;
}
 $tokennn = Builder::getLocal($sharedKey, new Version4);

$tokennn = (new Builder())
   ->setKey($sharedKey)
   ->setVersion(new Version4)
```

```
   ->setPurpose(Purpose::local())
   // Set it to expire in one day
   ->setIssuedAt()
   ->setNotBefore()
   ->setExpiration(
(new DateTime())
   )
   // Store arbitrary data
   ->setClaims([
       'email' => 'hgjh',
'password'=>'hgjh',
       'address'=>'hgjh'
   ]);
echo $tokennn;
```

4. Implémentation du modèle LRBAC adapté

Le modèle LRBAC intègre le rôle de l'utilisateur ainsi que sa localisation GPS qui sont vérifiées à la connexion. Voici l'implémentation de la classe de localisation NewGeocoder qui permet de récupérer la localisation GPS en chaîne de caractères et en fonction de latitude et longitude la localisation de l'utilisateur

Algorithme 2 :

```
public class NewGeocoder {
Contextcontext;

   public NewGeocoder(Contextcontext){
this.context = context;
   }

   public String getAddress(double latitude, double longitude) {
String strAdd = "";
Geocoder geocoder = new Geocoder(context, Locale.getDefault());
       try {
           List<Address> addresses = geocoder.getFromLocation(latitude, longitude, 1);
           if (addresses != null) {
               Address returnedAddress = addresses.get(0);
               StringBuilder strReturnedAddress = new StringBuilder("");

//                for (int i = 0; i<= returnedAddress.getMaxAddressLineIndex(); i++) {
                   strReturnedAddress.append(returnedAddress.getLocality()).append(",
").append(returnedAddress.getCountryName());
```

```
//                }
strAdd = strReturnedAddress.toString();
            }
        } catch (Exception e) {
e.printStackTrace();
        }
        return strAdd;
    }
```

5. Implémentation de l'empreinte numérique

Le code suivant représente implémentation de la classe de l'empreinte numérique où en hache l'adresse MAC, le modèle et le numéro de série de l'appareil en utilisant la fonction SHA256 :

Algorithm 3:

```
public class Encryt256 {

    public String getSHA256(String str){
MessageDigestmessageDigest;
        String encodestr = "";
        try {
messageDigest = MessageDigest.getInstance("SHA-256");
messageDigest.update(str.getBytes("UTF-8"));
encodestr = byte2Hex(messageDigest.digest());
        } catch (NoSuchAlgorithmException e) {
e.printStackTrace();
        } catch (UnsupportedEncodingException e) {
e.printStackTrace();
        }
        return encodestr;
    }

    private String byte2Hex(byte[] bytes){
StringBufferstringBuffer = new StringBuffer();
        String temp = null;
        for (int i=0;i<bytes.length;i++){
            temp = Integer.toHexString(bytes[i] & 0xFF);
            if (temp.length()==1){
stringBuffer.append("0");
            }
```

```
stringBuffer.append(temp);
        }
        return stringBuffer.toString();
}
```

6. Interfaces graphiques

Comme déjà mentionné auparavant, la première fois que le client veule accéder au Cloud (à l'application), il doit autoriser la localisation (Figure 7) puis s'inscrire (Figure 8). Si les informations sont valides (inscription réussie, voir Figure 9), le système prend l'empreinte numérique de l'appareil pour stoker dans la base de données. Ensuite, l'utilisateur peut consulter la page de connexion pour accéder à son compte (Figure 10). Si les informations de connexion sont toutes correctes alors le système compare la localisation de l'utilisateur avec la dernière localisation enregistrés dans la base de données (en stockant la nouvelle localisation si elle est différente) et l'utilisateur peut choisir une action à faire (Figure 12) pour laquelle le système créera un jeton PASETO.

Figure7 : Demande d'activation de la localisation

Figure 8 : Interface de création du compte

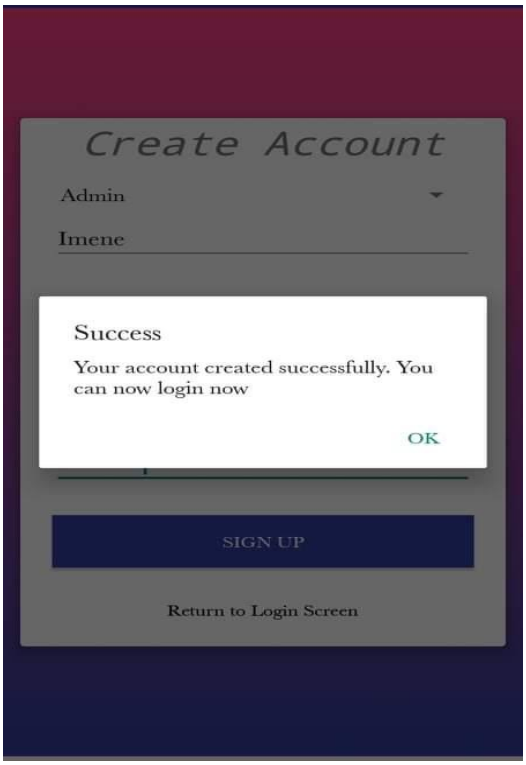

Figure 9 **:** un message succès affiché à l'utilisateur

Figure 10 : interface de connexion

Figure 11 : Les informations de l'utilisateur

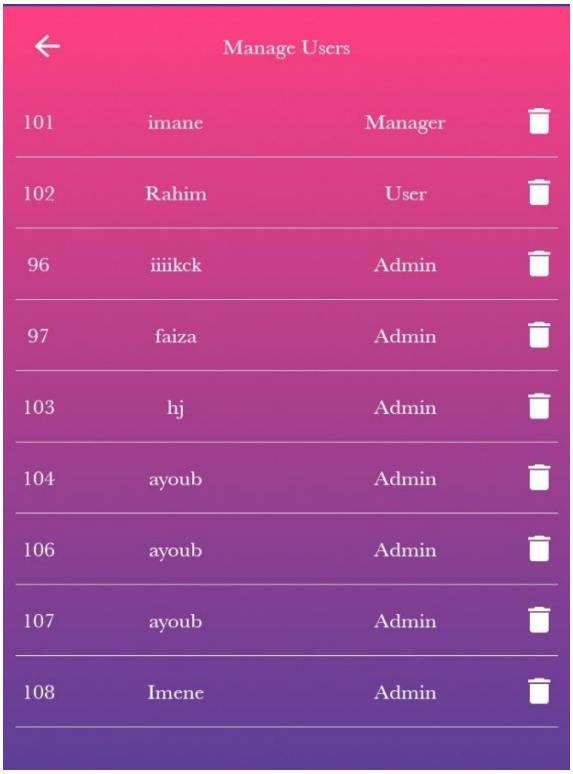

Figure 12 : Les opérations possibles faites par l'utilisateur

7. Conclusion

Dans ce chapitre, nous avons présenté l'implémentation de notre proposition. Nous avons d'abord présenté l'environnement dans lequel nous avons effectué l'implémentation de notre mécanisme. Nous avons ainsi présenté l'implémentation de chaque mécanisme de sécurité approche. Enfin, pour mieux expliquer les différentes fonctionnalités de notre système de contrôle d'accès nous avons effectué quelques prises d'écran illustrant la démarche de l'application.

Conclusion générale & Perspectives

De nos jours, les appareils mobiles sont devenus un élément essentiel de notre quotidien, grâce à la pléthore d'applications mobiles capables d'exécuter différentes applications, y compris les réseaux sociaux, les jeux et les services bancaires en ligne. Ceci est dû au fait qu'ils sont dotés d'une puissance de calcul importante et capacité de mise en réseau qui rivalise avec les ordinateurs portables et ordinateurs de bureau. Ainsi, des applications complexes, qui sont déjà utilisées dans les machines de bureau traditionnelles, sont migrées vers les appareils mobiles.

L'emplacement d'un appareil est l'une des politiques contextuelles, qui est utilisée pour améliorer la sécurité des données, authentifier l'utilisateur et donner accès aux services et aux informations utiles. Cependant, contrairement aux autres politiques et attributs utilisés dans le chiffrement basé sur les attributs, l'attribut de localisation est un attribut dynamique intrinsèque.

Dans ce contexte, l'objectif de ce mémoire était de définir un système de contrôle d'accès au Cloud Computing mobile pour mieux contrôler et sécuriser l'accès au Cloud via les dispositifs mobiles.

Pour ce faire, nous avons proposé une solution basée sur le modèle d'accès LRBAC qui intègre le rôle et l'emplacement des utilisateurs. Pour renforcer la sécurité de notre solution, nous avons utilisé l'empreinte digitale pour identifier l'appareil de l'utilisateur et les jetons dynamiques pour authentifier les actions entreprises par l'utilisateur.

Notre solution sert ainsi à

- ✓ Gérer et contrôler les accès logiques aux ressources informationnelles par des personnes ou des dispositifs.
- ✓ Préciser les règles à observer en matière d'identification, d'authentification et d'autorisation d'accès des personnes ou des dispositifs en détectant les altérations par des utilisateurs non autorisés.
- ✓ Assurer la confidentialité de l'information.
- ✓ Meilleur contrôle d'accès en conditions changeantes.

Les travaux réalisés dans le cadre de ce mémoire ouvrent des perspectives et plusieurs travaux futurs peuvent être envisagés. Parmi les perspectives de ce travail serait de :

- Tester le système développé dans un environnement réel afin de prouver son efficacité à long terme.
- Intégrer l'intelligence artificielle à notre approche,
- Rajouter des aspects techniques de développement dans un seul langage, et minimiser les failles à travers des politiques de sécurité qui fait un pas très implicite sur l'environnement Cloud mobile.

- Rajouter d’autres aspects mobiles de sécurité tell que reconnaissance faciale ou vocale.
- Développer une politique de cryptage basé sur les formules mathématiques très complexes à plusieurs niveaux et à plusieurs couches ou lieu de SHA256.
- Utiliser deux serveurs chacune à de différents cryptages pour garantir une sécurité supplémentaire et la perturbation de l’attaquant.

Enfin, rappelons que les problèmes de contrôle d’accès de sécurité dans un environnement ouvert et hétérogène tel que le Cloud Computing mobile demeurent toujours des problèmes ouverts. Par conséquent, beaucoup de pistes restent à explorer.

Ressources bibliographiques

[1] Takabi, H., Joshi, J. B., &Ahn, G. J. (2010). Security and privacy challenges in cloud computing environments. *IEEE Security & Privacy, 8(6), 24-31.*

[2] Garthner. (2014, Février). “IT Glossary, Cloud Computing”. Consulté le 05 mai 2014,sur Gartner: https://www.Gartner.com/doc/2662323?srcId=1-2819006590&pcp=itg.

[3] Syntec Informatique. (2006, Juin). “Cloud Computing”.2021,Surhttp://www.syntec-numerique.fr/content/livres-blancs-cloud-computing.

[4] Cisco Systems. (2009, Août). “Cisco Cloud Computing -Data Center Strategy, Architecture, and Solutions”. Consulté le 5 août 2021, sur Cisco Systems: Cisco Systems: http://www.cisco.com/web /strategy /docs /gov /CiscoCloudComputing_WP.pdf.

[5] IBM. (2011, Décembre). “IBM SmartCloud Enterprise”. Consulté le 5 août 2021, surIBM:http://www.935.ibm.com/services/fr/igs/pdf/Presentation_1_Page_SCE_05122011.pdf.

[6] R. Sandhu and Q. Munawer, “How to do discretionary access control using roles,” in Proceedings of the third ACM workshop on Role-based access control, pp. 47–54, ACM, 1998.

[7] http://www.mobilecloudcomputingforum.com/

[8] White Paper, “Mobile Cloud Computing Solution Brief,” AEPONA,

[9] L. Liu, R. Moulic, and D. Shea, “Cloud Service Portal for Mobile Device Management,” InProceedings of IEEE 7th International Conference on e-Business Engineering (ICEBE)

[10] JR. Kakerow, "Low power design methodologies for mobile communication".In Pro-ceedings of IEEE International Conference on Computer Design : VLSI in Computers and Processors, pp. 8, January 2003.

[11] G. H. Forman and J. Zahorjan,“The Challenges of Mobile Computing,” IEEE Computer Society Magazine

[12]T.Hoang T. Dinh, CH. Lee, D. Niyato, and P.Wang. A Survey of Mobile Cloud Computing: Architecture, Applications, and Approaches.

[13] Paulson,"Low-Power Chips for High-Powered Handhelds".In Computer (Volume :36, Issue : 1) ,2003 .

[14] J. W. Davis ,"EPower benchmark strategy for systems employing power manage-ment".In Proceedings of the IEEE International Symposium on Electronics and the Environment, pp. 117

[15] R. N. Mayo and P. Ranganathan ,"Energy Consumption in Mobile Devices : Why Future Systems Need RequirementsAware Energy Scale-Down".In Proceedings of theWorkshop on Power-Aware Computing Systems,

[16] NIST. (2011, Septembre). “The NIST Definition of Cloud Computing (Draft)”. Rapport consulté le 01 Juillet 2014, sur NIST: Http://csrc.nist.gov/publication/Drafts/800-145/Draft-SP-8006- 145é-cloud-definition.pdf.
[17] R. Sandhu and Q. Munawer, “How to do discretionary access control using roles,” in Proceedings of the third ACM workshop on Role-based access control, pp. 47–54, ACM, 1998.
[18] http ://aws.amazon.com/s3/.
[19] https://tel.archives-ouvertes.fr/tel-01430151/document.
[20] J. Douceur and J. S. Donath ,"The sybil attack". In Proceedings for the 1st Inter-national Workshop on Peer-to- Peer Systems, pages 251-260, Cambridge, MA, USA, Mar. 2002.
[21] Mahadev Satyanarayanan ,ParamvirBahl ,Ramón Cáceres And Nigel Davies , "The Case for VM-Based Cloudlets in Mobile Computing" ,In Pervasive Computing, IEEE (Volume :8 , Issue : 4) 2009 .
[22] P. Zou, C. Wang, Z. Liu, and D. Bao, "Phosphor : A Cloud Based DRM Scheme with Sim Card".,” In Proceedings of the 12th International Asia-Pacific on Web Conference (APWEB), pp. 459
[23] Krawczyk, H. and P. Eronen, "HMAC-based Extract-and-Expand Key Derivation Function (HKDF)", RFC 5869, DOI 10.17487/RFC5869
[24] Housley, R., "Using Advanced Encryption Standard (AES) Counter Mode With IPsec Encapsulating Security Payload (ESP)", RFC 3686, DOI10.17487/RFC3686.
[25] Nystrom, M., "Identifiers and Test Vectors for HMAC-SHA-224, HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512", RFC 4231, DOI10.17487/RFC4231
[26] Josefsson, S., "The Base16, Base32, and Base64 Data Encodings", RFC 4648, DOI 10.17487/RFC4648
[27] https://www.lemagit.fr/definition/API-RESTful
[28]https://www.astera.com/fr/type/blog/rest-api-definition/
[29] Jones, M., "JSON Web Algorithms (JWA)", RFC 7518, DOI 10.17487/RFC7518
[30] Jones, M., Bradley, J. and N. Sakimura, "JSON Web Token (JWT)", RFC 7519,DOI 10.17487/RFC7519
[31] Moriarty, K., Kaliski, B., Jonsson, J. and A. Rusch, "PKCS #1: RSA Cryptography Specifications Version 2.2" RFC 8017, DOI 10.17487/RFC8017,
[32] Josefsson, S. and I. Liusvaara, "Edwards-Curve Digital Signature Algorithm (EdDSA)", RFC 8032, DOI 10.17487/RFC8032
[33] Lookout Mobile Security, Lookout Mobile Threat Report
[34] C.A. Castillo, “White Paper: Android Malware Past, Present and Future”, Mobile Security Working Group, McAfee, available online http://www.mcafee.com/us/resources/white-papers/wp-android-malware-past-present-future.pdf,2011.
[35] C. Nachenberg, “A Window Into Mobile Device Security – Examining

the security approaches employed in Apple's iOS and Google's Android", Symantec Security Response, available online: http://investor.symantec.com/files/doc_news/2012/symc_mobile_device_security_june2011.pdf,2011
[36]H.Zhangwei and X. Mingjun, "A Distributed Spatial Cloaking Protocol for Location Privacy," in Proceedings of the 2nd International Conference on Networks SecurityWireless Communications and Trusted Computing (NSWCTC), vol. 2, pp. 468, June 2010
[37] "Top threats to cloud computing", version 1.0, Cloud Security Alliance CSA, available online: http://www.cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf, Retrieved March, 2010.
[38] EU Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data, 1995 O.J. L 281
[39] A. Archer "Boehm, Security guidance for critical areas of focus in cloud computing", Cloud Security Alliance, 2009.
[40] International Due Diligence: U.S. vs. European Privacy Laws Kroll an altegrity Company,availableonline:http://www.kroll.com/media/pdfs/International_Due_Diligence_US_vs_Euro_WP_040811P.pdf
[41] Personal Data Protection Act No. 25,326, (Arg.), available online www.privacyinternational.org/countries/argentina/argentine-dpa.html, Oct. 4, 2000.
[41] https://www.okta.com/fr/identity-101/what-is-token-based-authentication/

[42] Elisa Bertino, Barbara Catani; GEO-RBAC: A SPATIALLY AWARE RBAC , Center for Education and Research in Information Assurance and Security,Purdue University, West Lafayette, IN 47907-2086.
[44]Cotton, M., Leiba, B. and T. Narten, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 8126, DOI 10.17487/RFC8126
[45] V. C. Hu, D. Ferraiolo, R. Kuhn, A. R. Friedman, A. J. Lang, M. M. Cogdell, A. Schnitzer,K. Sandlin, R. Miller, K. Scarfone, et al., "Guide to attribute based access control (abac) Definitionand considerations (draft)," NIST special publication, vol. 800, no. 162,2013.
[46] Q. M. Rajpoot, C. D. Jensen, and R. Krishnan, "Attributes enhanced role-based access controlmodel," in International Conference on Trust and Privacy in Digital Business, pp. 3–17, Springer,2015.
[47] V. C. Hu, D. Ferraiolo, R. Kuhn, A. Schnitzer, K. Sandlin, R. Miller, and K. Scarfone, "Guideto attribute based access control (abac) definition and considerations," NIST Special Publication,vol. 800, p. 162, 2014.
[48] B. Stepien, S. Matwin, and A. Felty, "Advantages of a non-technical xacml notation in role-basedmodels," in Privacy, Security and Trust (PST), 2011 Ninth Annual International Conference on,pp. 193–200, IEEE, 2011.

[49] R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman, “Role-based access control models,” Computer, no. 2, pp. 38–47, 1996.
[50] S. Osborn, R. Sandhu, and Q. Munawer, “Configuring role-based access control to enforce man-datory and discretionary access control policies,” ACM Transactions on Information and SystemSecurity (TISSEC), vol. 3, no. 2, pp. 85–106, 2000.
[51] D. Huan, X. Zhang, M. Kang, J. Luo, “MobiCloud: building secure cloud framework for mobile computing and communication”, in: Proc. 5th IEEE Int. Symposium on Service Oriented System Engineering, SOSE ’10, Nanjing, China
[52] M. Kamel, K. Boudaoud, S. Resondry, M. Riveill “Low-Energy Consuming and User-centric Security Management Architecture Adapted to Mobile Environments” In Proceedings of the 12th IFIP/IEEE International Symposium on Integrated Network Management (IM'2011), Dublin, Ireland, May, 23 - 27, 2011.
[53]W.Itani, A. Kayssi, A. Chehab, “Energy-efficient incremental integrity for securing storage in mobile cloud computing”, in: Proc. Int. Conference on Energy Aware Computing, ICEAC ’10, Cairo, Egypt
[54] M. Bellare, O. Goldreicha, S. Goldwasser, “Incremental cryptography: the case of hashing and signing”, in: Proc. 14th Annual Int. Cryptology Conference on Advances in Cryptology, Santa Barbara, California, USA
[55] M. Bellare, O. Goldreich, S. Goldwasser, “Incremental cryptography and
[56] P. Lindberg, J. Leingang, D. Lysaker, S.U. Khan, J. Li, “Comparison and analysis of eight scheduling heuristics for the optimization of energy consumption and make span in large-scale distributed systems”, Journal of Supercomputing, pp. 323–360,2012.
[57] D.M. Quan, F. Mezza, D. Sannenli, R. Giafreda, “T -alloc: a practical energy efficient resource allocation algorithm for traditional data centers”, Future Generation Computer Systems, pp. 791–800, 2012.
[58] S.C. Hsueh, J.Y. Lin, M.Y. Lin, ”Secure cloud storage for conventional data archive of smart phones”, in: Proc. 15th IEEE Int. Symposium on Consumer Electronics, ISCE ’11, Singapore
[59] X. Zhang, J. Schiffman, S. Gibbs, A. Kunjithapatham, and S. Jeong. “Securing Elastic Applications on Mobile Devices”. In CCSW’09, November 13, Chicago, Illinois, USA, 2009.
[60] Z. Song, J. Molina, S. Lee, S. Kotani, and R. Masuoka. “TrustCube: An Infrastructure that Builds Trust in Client,” in Proceedings of the 1st International Conference on Future of Trust in Computing, 2009.
[61] D. Huang, Z. Zhou, L. Xu, “Secure Data Processing Framework for Mobile Cloud Computing”, Workshop on Cloud Computing, INFOCOM, June 2011.
[62] M.F. Mokbel, C. Chow, W.G. Aref, “The new casper: query processing for location services without compromising privacy”, in: Proc. 32nd Int. Conference on Very Large Databases, VLDB ’06, Seoul, Korea, Sep. 2006.
[63] D. Kim, M. G. Solomon, et al., Fundamentals of information systems security. Jones & Bartlett Publishers, 2013.

[64] A. Almutairi, M. Sarfraz, S. Basalamah, W. Aref, and A. Ghafoor, “A distributed access Control architecture for cloud computing,” Software, IEEE, vol. 29, pp. 36–44
[65] I. Ray, D. Mulamba, I. Ray, and K. J. Han, “A model for trust-based access control and Delegationin mobile clouds,” in Data and Applications Security and Privacy XXVII, pp. 242–257, Springer,2013.
[66] S. Alshehri, Toward Effective Access Control Using Attributes and Pseudoroles. PhD thesis, ThomasGolisano College of Computing & Information Sciences Rochester Institute of Technology.
[67] https://blog.avast.com/fr/fingerprinting-and-the-surveillance-economy
[68] https://cryptostrategie.com/sha256-algorithme-bitcoin/
[69] **https://thesecurepass.com/blog/discretionary-access-control-system**
[70] **https://thesecurepass.com/blog/mandatory-access-control-system**
[71] **https://digitalguardian.com/blog/what-role-based-access-control-rbac-examples-benefits-and-more**
[72] **https://www.immuta.com/articles/attribute-based-access-control/**
[73] https://jobphoning.com/dictionnaire/empreinte-numerique#
[74] https://github.com/paragonie/paseto