TABLE DES MATIERES

Liste des Figures

Liste des tableaux

Sigles et Abréviations

ACL : Access Control List

ARP : Address Resolution Protocol

AWS : Amazon Web service

CC : Cloud Computing

CSP : Contrat de Sécurisation Professionnelle

CDMI : Cloud Data Management Interface

TCO : Coût Total de Possession

HE : Cryptage homomorphique

DNS : Domain Name System

DSS : Data Security Standard

FAI : Fournisseur d'accès à Internet

AH : Homomorphisme additif

HTTP : HyperText Transfer Protocol

IaaS : Infrastructure as a Service

ICMP : Internet Control Message Protocol

IDS/IPS : Intrusion Détection System/ Intrusion Prevention System

NIST : National Institute of Standards and Technology

PCI : Payment Card Industry

PCA : Plan de Continuité d'Activité

PaaS : Platform as a Service

SLA : Service Level Agreement

SaaS : Software as a Service

SGX : Software Guard Extensions

SI : Système Informatique

CRT : Théorème du reste chinois

UDP : User Datagram Protocol

VPN : Virtual Prive Network

Sommaire

Introduction Générale

De nos jours, de nombreuses personnes ont commencé à dépendre d'Internet pour tout. Une large utilisation d'Internet a augmenté les exigences en matière de stockage de données en ligne et hors ligne. Le Cloud Computing [CC] représente la cinquième génération de l'informatique après les mainframes, les ordinateurs personnels, le paradigme client/serveur et le web (World Wide Web). Il désigne un modèle dans lequel les ressources telles que la puissance de calcul, le stockage ou encore la bande passante sont fournies comme des services qui peuvent être loués par des utilisateurs via Internet à la demande.

La technologie et les ressources de l'informatique en nuage sont basées dans des centres de données centralisés, ajustés et réglés de manière dynamique pour atteindre une efficacité optimale, offrant une économie d'échelle sans précédent.

Le stockage des données dans le Cloud offre aux utilisateurs la commodité d'accès sans nécessiter une connaissance directe du déploiement et de la gestion du matériel ou de l'infrastructure. Bien que le CC soit beaucoup plus puissant que le personnel l'informatique, cela pose de nouveaux défis en matière de confidentialité et de sécurité, car les utilisateurs abandonnent le contrôle en externalisant leurs données, ils n'en ont plus physiquement la possession. En ayant un accès complet aux services Cloud, les données des utilisateurs sont exposées à une variété de menaces, des attaques malveillantes et des cas de failles de sécurité se produisent fréquemment. Par exemple, certains nuages peuvent être infidèles à la confidentialité des données pour des raisons monétaires ; des informations confidentielles peuvent être divulguées à des concurrents commerciaux ; ou le CSP peut dissimuler la perte de données pour maintenir sa réputation.

Or, bien que le CC soit économiquement attractif pour les consommateurs et les entreprises en offrant aux utilisateurs un partage de données à grande échelle, la sécurisation des données externalisées est le problème le plus important du stockage Cloud. En garantissant la confidentialité des données externalisées dans le Cloud, la sécurité des données peut être assurée dans le stockage Cloud. Motivé par ce fait, notre mémoire vise à assurer la confidentialité des données externalisées en atteignant les objectifs suivants :

- Identifier les différentes menacées qui existent dans le Cloud et leurs contremesures

- Présenter les vulnérabilités à tenir compte avant de migrer vers le Cloud
- Lister l'ensemble des attaques possibles et leurs défenses
- Pour s'assurer qu'une fois que les données sont stockées dans le Cloud, elles ne sont accessibles que par le propriétaire des données
- Pour masquer les données avant qu'elles ne soient téléchargées sur le stockage Cloud
- Mettre en place une solution de confidentialité

Dans le but d'atteindre ces objectifs prédéfinis : nous allons d'abord, étudier les cadres théorique et méthodologique, ensuite, traiter le cadre conceptuel et enfin aboutir à la mise en œuvre et l'exploitation des solutions adoptées.

Première Partie :

LES CADRES THEORIQUE ET METHODOLOGUE

I. CADRES THEORIQUE ET METHODOLOGIQUE

Toute recherche qui ambitionne de se hisser à un niveau scientifique doit être menée dans un cadre théorique et méthodologique explicite. Ces cadres théorique et méthodologique permettent en effet de préciser le sens donné aux concepts manipules. Dans cette optique, la première partie est composé de deux sections : la première traitera le cadre théorique de notre étude et la seconde abordera le cadre méthodologique.

I.1 Cadre théorique

Dans cette section seront présentées successivement, le contexte du sujet, la problématique, les objectifs de recherche, et la pertinence du sujet.

I.1.1 Contexte du sujet

Pendant les vingt dernières années, Internet a évolué d'un réseau simple de taille limitée à un système complexe à grande dimension. Alors, qu'il était initialement utilisé pour offrir du contenu statique organisé autour de simples sites web, aujourd'hui il fournit des services complexes ainsi que l'externalisation de calculs, de stockage et d'applications avec le CC. Ce dernier s'impose comme une nouvelle technologie informatique où tous les services requis sont disponibles en tant que service. Dans un environnement Cloud, la localisation des données est généralement gérée par un tiers (fournisseur de services / vendeur) et, par conséquent, un individu n'a aucun contrôle sur ses propres données.

D'après une étude menée auprès de 5000 responsables informatiques hébergeant des données et des ressources dans le cloud public ont montré que :

- 96 % des entreprises sont préoccupées par leur niveau de sécurité Cloud actuel. La perte de données, la détection et la réponse, et la gestion de plusieurs plateformes Cloud sont les trois principales préoccupations des entreprises [1].
- Les entreprises utilisant plusieurs plateformes Cloud ont signalé un plus grand nombre d'incidents de sécurité au cours des 12 derniers mois. 73 % des entreprises interrogées utilisent 2 plateformes de Cloud public ou plus, et ont déclaré d'avantage incidents de sécurité que celles n'en utilisant qu'une seule [2].

Malheureusement, ce cas de figure se présente très souvent. Les services informatiques ne sont pas toujours armés de toute l'expertise et de toute la compétence que requièrent la mise en place et le maintien d'une architecture de stockage efficace et sécurisée [3].

Dans ce contexte, la confidentialité des données est un enjeu important pour le CC à la fois en termes de conformité légale et de confiance des utilisateurs.

Pour répondre aux exigences de confidentialité de certains secteurs stratégiques ont adoptées plusieurs mécanismes de confidentialité telle que la gestion des identités et des accès, le cryptage homomorphe, les techniques d'obfuscations et la technologie matérielle de protection des données utilisateur dans les services Cloud au niveau matériel le plus bas c'est-à-dire dans le noyau CPU.

Apres avoir présenter le contexte, nous posons les problèmes à la quelles, nous tentons de les résoudre.

I.1.2 Problématique

Avec le développement des nouvelles technologies, les réseaux informatiques sont les centres nerveux de toute infrastructure informatique ils sont toujours au cœur des systèmes d'information. Le nombre de postes, d'équipements, de services et de ressources qui tournent dans le réseau croient de jour en jour. Tous ces éléments de par leur hétérogénéité sont déjà source de dysfonctionnements sans pour autant compter les problèmes liés à leur propre nature. Actuellement le CC est une révolution économique et technologique, dans lequel les ressources informatiques sont fournies en tant que service via internet. En particulier, ces ressources peuvent être provisionnées de façon dynamique et libérées en fonction de la demande de service et avec un effort minimal de gestion. Il présente une meilleure solution pour gérer les données, les infrastructures, etc. Le partage de données dans le Cloud, alimenté par les tendances favorables de la technologie émerge comme une technique prometteuse pour permettre aux utilisateurs d'accéder facilement aux données.

Or, le nombre croissant d'entreprises et de clients qui stockent leurs données sur des serveurs Cloud met de plus en plus en question la confidentialité des données ainsi que leurs sécurités.

Cependant, la confidentialité des données en transit dans le Cloud public reste un challenge pour les fournisseurs de Cloud. En effet, ces données sont la cible de plusieurs attaques réseau, qui ont pour but d'interrompre, d'intercepter, de modifier et de fabriquer des informations. Par conséquent, il est essentiel de faire face à ces attaques en vue d'améliorer l'utilisation et

l'adoption de Cloud. Nous pouvons nettement comprendre que, plus les services du Cloud sont accessibles, plus les problèmes de sécurité s'alourdissent. Maintenir et garantir le bon fonctionnement de ces services deviennent en ce moment un objectif pas très facile à atteindre pour tous chercheurs. Face à ce problème posé, des solutions sont mises en évidence, visant à alléger le travail des utilisateurs du Cloud. Pour réaliser ces idées, il est obligatoire de comprendre :

- Quelles sont les menaces auxquelles nous encourons ?
- Comment faire face pour contrecarrer ses menaces ?
- Comment pouvons-nous assurer une confidentialité dans un environnement de Cloud tout en réduisant la perte d'information ?
- Quelles approches peuvent être mises en place afin de réduire la quantité de perte d'information tout en s'efforçant la protection de la confidentialité des données dans un environnement de Cloud ?
- Comment mettre en œuvre une architecture sécurisé afin d'améliorer la confidentialité et l'utilité des données dans un environnement du Cloud ?

À partir de cela, nous pouvons choisir telle solution pour notre système. L'ensemble de ces interrogations constitue la problématique de notre sujet. Ainsi nous allons maintenant passer aux objectifs de recherche.

I.1.3 Les objectifs de recherche

Dans cette sous-section, nous aborderons les objectifs de recherche. Dans cette perspective, l'objectif général sera entamé en premier lieu avant de finir avec l'énumération des objectifs spécifiques.

L'objectif principal est de conserver à distance d'importantes quantités de données en garantissant leurs intégrités et permettre leur accès à partir de postes de travail, de tablettes ou de mobiles en toute sécurité.

Bien que le CC ait connu une évolution très rapide, il reste encore plusieurs barrières de sécurité qui découragent les utilisateurs à adopter ce système. Dernièrement, la sécurité a été répertoriée comme la préoccupation la plus importante du CC, selon l'enquête menée par International Data Corporation (IDC) [4].

Pour pallier aux problèmes rencontrés, l'objectif de notre mémoire est de pouvoir réalisé les points suivants :

- Identifier les différentes menaces qui existent dans le cloud et d'en proposer des solutions.
- Présenter les vulnérabilités à tenir compte avant de migrer vers le Cloud
- Lister l'ensemble des attaques possibles et leurs défenses
- Implémenter une solution de confidentialité

Ainsi nous allons maintenant passer à la dernière sous-section ; la pertinence du sujet

I.1.4 La pertinence du sujet

Dans chaque entreprise, l'information est devenue un élément fondamental et essentiel. La maîtrise de l'information est un enjeu stratégique pour les entreprises puisqu'elle leur offre des opportunités pour se différencier, favoriser l'innovation, bénéficier d'un avantage concurrentiel ou même se maintenir dans le marché. Une information est jugée utile notamment par sa valeur, sa fiabilité, sa pertinence et essentiellement sa disponibilité. C'est pourquoi, plus que jamais il est primordial et indispensable de protéger le système d'information pour qu'il reste en bon état et toujours disponible. En effet, pour assurer la disponibilité du système d'information, les entreprises et les particuliers peuvent utiliser le centre de données du Cloud pour le stockage sans charge supplémentaire. Les données peuvent être stockées et accessibles à distance partout et à tout moment. Les utilisateurs peuvent être soulagés du fardeau du stockage et de la maintenance des informations locales grâce à l'externalisation des données. Par conséquent, l'intégrité, la sécurité et la confidentialité des données stockées doivent être prises en compte dans le CC.

En effet, pour assurer la sécurité des données, les fournisseurs ont mis en place des outils de protection contre les attaques et la possibilité à ses utilisateurs de signaler au plus bref délai. En somme, cette première section nous a permis de comprendre un ensemble de questions soulevées par notre sujet.

A présent, nous allons étudier le cadre méthodologique de notre sujet.

I.2 Cadre méthodologique

Cette deuxième section a trait au cadre de référence méthodologique, qui est constitué de la présentation générale du sujet, de la délimitation du champ d'étude et des difficultés rencontrées au cours de l'élaboration du travail.

I.2.1 Présentation générale du sujet

Le développement rapide des techniques de protection de la vie privée et la prolifération de l'externalisation ont poussé le monde vers le CC. Le Cloud, avec sa capacité de stockage, a attiré beaucoup d'attention ces dernières années car il offre la possibilité d'apporter les ressources de stockage de manière rentable [5]. Pour contrôler l'accès à ces données, des mécanismes et politiques de sécurité appropriés sont nécessaires. Plus la sensibilité des données est élevée, plus les besoins de sécurité sur les mécanismes de sécurité sont stricts.

La sécurité a toujours été une préoccupation majeure dans l'environnement Cloud car l'externalisation conduit à de nouveaux problèmes de sécurité. Les risques pour la vie privée liés à l'affectation du poste sont les principaux obstacles dans les grandes organisations [6].

C'est dans cette contexte que s'articule notre sujet qui est : ***Etude de la sécurité du Cloud Computing et Mise en place d'une solution de confidentialité.***

I.2.2 La délimitation du champ d'étude

Cette partie consiste à la délimitation des champs d'études de notre sujet. Nous camperons le sujet dans un intervalle bien défini qui déterminera les points de départ et d'arrivée de notre étude. Dans cette partie, l'approche adoptée lors de nos recherches consistes-en :

- La définition de l'environnement et du domaine ; la définition des variables de confiance influant le CC ; les modèles de services de déploiements ; la définition de la notion de sécurité dans le Cloud.
- Présenter les vulnérabilités ainsi que les menaces de sécurité dans le Cloud.
- Lister l'ensemble des attaques et contremesures
- Mettre en place une solution de confidentialité si possible

Au total, cette première partie nous a permis de comprendre les cadres théorique et méthodologique de notre sujet. Cependant, nous allons passer à la deuxième partie qui parlera du cadre conceptuel.

Deuxième Partie :

LE CADRE

CONCEPTUEL

Sommaire

II. CADRE CONCEPTUEL

Cette deuxième partie, est constituée de deux sections : la première consiste sur l'étude de l'art du CC, et la deuxième, l'étude de la sécurité dans le CC.

II.1 Etude détaillé du Cloud Computing

Dans cette première section, nous allons d'abord définir le terme CC et ces caractéristiques, ensuite son historique, et enfin l'architecture et modèle de déploiement du CC.

II.1.1 Définitions et Généralités

L'informatique dans le nuage est plus connue sous sa forme anglo-saxonne : « Cloud Computing », mais il existe de nombreux synonymes francophones tels que : « informatique dans les nuages », « infonuagique » (Québec) ou encore « informatique dématérialisée » [7]. Même si les experts ne sont pas d'accords sur sa définition exacte, la plupart s'accordent à dire qu'elle inclue la notion de services disponibles à la demande, extensibles à volonté et à distance ou sur le Net. En contradiction avec les systèmes actuels, les services sont virtuels et illimités et les détails des infrastructures physiques sur lesquels les applications reposent ne sont plus du ressort de l'utilisateur. Il existe de nombreuses définitions du terme CC, et la définition du NIST est celle qui est la plus largement acceptée aujourd'hui.

Selon U.S. National Institute of Standards and Technology, le CC est un modèle permettant d'établir un accès à la demande en réseau vers un bassin partagé de ressources informatiques configurable. Ces ressources sont par exemple des réseaux, des serveurs, de l'espace de stockage, des applications et des services. Elles peuvent être **approvisionnées rapidement avec un effort de gestion et une interaction avec le fournisseur de services minimes**. Le modèle Cloud met en avant la disponibilité, et se compose de cinq caractéristiques essentielles, trois modèles de livraisons, et quatre modèles de déploiement.

Par exemple quelques définitions qui ont circulés :

- « Le CC est un modèle qui permet un accès réseau à la demande et pratique à un pool partagé des ressources informatiques configurables (telles que réseaux, serveurs, stockage, applications et services) qui peuvent être provisionnées rapidement et distribuées avec un minimum de gestion ou d'interaction avec le fournisseur de services. » [8]
- « Le CC est une plateforme de mutualisation informatique fournissant aux entreprises des services à la demande avec l'illusion d'une infinité des ressources » [9]

Un des points essentiels de ces définitions est la notion de « scalability » ; d'extensibilité à la demande, d'élasticité, c'est à dire qu'on ne paie que ce qu'on utilise. C'est un avantage considérable par rapport à une infrastructure propre à l'entreprise où les serveurs sont très souvent sous-utilisés.

L'idée principale à retenir est que le Cloud n'est pas un ensemble de technologies, mais un modèle de fourniture, de gestion et de consommation des services et des ressources informatiques.

Figure 1: Le Cloud Computing et ses offres [1w]

Le modèle CC se différencie par les cinq caractéristiques essentielles suivantes :

- ***Libre-service à la demande :*** Le client peut consommer les services Cloud automatiquement selon son besoin sans aucune nécessitée d'une interaction humaine avec le fournisseur.

- ***Large accès au réseau :*** les capacités sont disponibles sur le réseau et sont accessibles via des mécanismes standards qui favorisent l'utilisation par des plates-formes clientes minces ou épaisses et hétérogènes (par exemple, les téléphones mobiles, les ordinateurs portables et les assistants personnels numériques ou PDA).
- ***Mise en commun des ressources :*** Les ressources et les services fournis au client sont souvent virtuels et partagés par plusieurs utilisateurs.
- ***Une souplesse rapide :*** Les utilisateurs peuvent rapidement augmenter et diminuer leurs ressources en fonction des besoins, ainsi que de libérer les ressources pour d'autres utilisations quand ils ne sont plus nécessaires.
- ***Service mesuré :*** les systèmes de Cloud contrôlent et optimisent automatiquement l'utilisation des ressources en exploitant une capacité de comptage à un niveau d'abstraction approprié au type de service (par exemple stockage, traitement, bande passante et comptes d'utilisateurs actifs).

De ce fait, l'utilisation des ressources peut être surveillée, contrôlée et rapportée, ce qui permet une transparence pour le fournisseur et le consommateur du service utilisé.

Figure 2: Les caractéristiques du Cloud Computing [2w]

II.1.2 Architecture et modèles de déploiements

Tous les Cloud ne sont pas identiques et aucun type de CC ne convient pas à tout le monde. Plusieurs modèles, types et services différents ont évolués pour vous aider a trouvé des solutions adéquates à vos besoins.

Nous distinguons quatre formes de CC :

- **Cloud Public**
- **Cloud Prive**
- **Cloud Hybride**
- **Cloud Communautaire**

II.1.2.1 Cloud Public

Le Cloud public se définit comme un type de service informatique dans lequel un fournisseur met des ressources à la disposition du grand public via Internet.

Dans le cas du Cloud public, le fournisseur propose un environnement informatique avec une mutualisation optimale des ressources : l'environnement est ainsi virtuellement partagé avec un nombre illimité de clients.

Une telle offre privilégie l'élasticité et la flexibilité, et propose, avec la massification des clients, des prix plus attractifs.

Cependant, la mutualisation généralisée entraîne une difficulté plus grande pour le fournisseur de garantir un niveau de service spécifique à un client.

- **Avantages du Cloud public**

Les appréciations du Cloud public sont :

- **Pas de CAPEX :** Aucun investissement requis pour déployer et maintenir l'infrastructure informatique.
- **Agilité technique :** Évolutivité et flexibilité élevées pour répondre aux demandes de charge de travail imprévisibles.
- **Orientation commerciale :** La complexité réduite et les exigences en matière d'expertise informatique interne sont minimisées, car le fournisseur de cloud est responsable de la gestion de l'infrastructure.
- **Abordabilité :** Options de tarification flexibles basées sur différentes offres SLA
- **Agilité des coûts :** L'agilité des coûts permet aux organisations de suivre des stratégies de croissance Lean et de concentrer leurs investissements sur des projets d'innovation

- **Inconvénients du Cloud public**

Le Cloud public à des limitations :

- **Manque de contrôle des coûts :** Le coût total de possession (TCO) peut augmenter de façon exponentielle pour une utilisation à grande échelle, en particulier pour les entreprises de taille moyenne à grande.
- **Manque de sécurité :** Le Cloud public est le moins sécurisé, par nature, il n'est donc pas le meilleur pour les charges de travail informatiques sensibles et critiques.
- **Contrôle technique minimal :** La faible visibilité et le faible contrôle de l'infrastructure peuvent ne pas répondre à vos besoins de conformité.

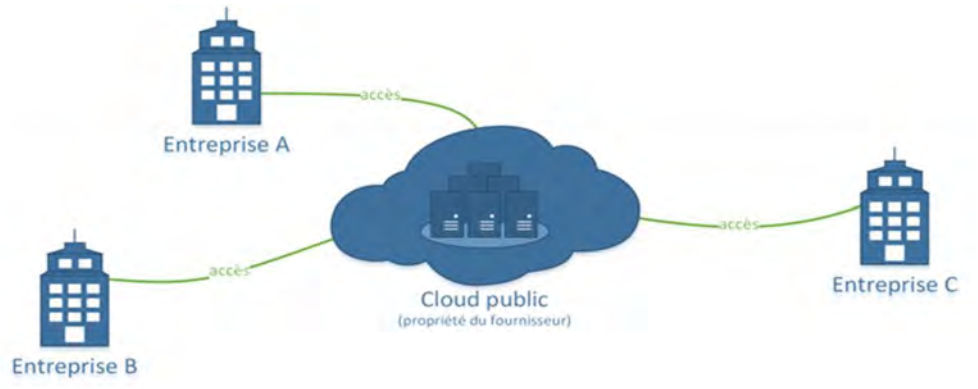

Figure 3:Modèle de déploiement d'un cloud public [3w]

II.1.2.2 Cloud Prive

Le Cloud privé fait référence à toute solution Cloud dédiée à une utilisation par une seule organisation. Le Cloud privé vient répondre aux exigences des clients souhaitant des garanties exclusives sur un contrat de service. Les ressources du centre de données peuvent être situées sur site ou exploitées par un fournisseur tiers hors site. Les ressources informatiques sont isolées et livrées via un réseau privé sécurisé, et non partagées avec d'autres clients.

Avec une plus grande visibilité et un meilleur contrôle de l'infrastructure, les entreprises peuvent gérer des charges de travail informatiques sensibles à la conformité sans compromettre la sécurité et les performances précédemment obtenues uniquement avec des centres de données dédiés sur site.

La virtualisation des serveurs et du stockage est généralement un préalable à la mise en œuvre d'un Cloud privé qui peut se déployer sous deux formes distinctes :

- **Cloud privé interne :** Hébergé par l'entreprise elle-même, parfois partagé ou mutualisé en mode privatif avec les filiales.
- **Cloud privé externe :** Hébergé chez un tiers, il est entièrement dédié à l'entreprise et accessible via des réseaux sécurisés de type VPN.

❖ **Avantages du Cloud privé**

Les avantages les plus populaires du Cloud privé incluent :

- **Environnements exclusifs :** Environnements dédiés et sécurisés auxquels d'autres organisations ne peuvent accéder.
- **Sécurité personnalisée :** Conformité aux réglementations strictes, car les organisations peuvent exécuter des protocoles, des configurations et des mesures pour personnaliser la sécurité en fonction des exigences de charge de travail uniques
- **Évolutivité sans compromis :** Évolutivité et efficacité élevées pour répondre aux demandes imprévisibles sans compromettre la sécurité et les performances
- **Performances efficaces :** Le Cloud privé est fiable pour des performances et une efficacité SLA élevées.
- **La flexibilité :** Le Cloud privé est flexible car vous transformez l'infrastructure en fonction des besoins commerciaux et informatiques en constante évolution de l'organisation.

❖ **Inconvénients du Cloud privé**

Le Cloud privé présente des inconvénients qui peuvent limiter les cas d'utilisation :

- **Prix :** Le Cloud privé est une solution coûteuse avec un TCO relativement élevé par rapport aux alternatives de Cloud public, en particulier pour les cas d'utilisation à court terme.
- **Difficulté mobile :** Les utilisateurs mobiles peuvent avoir un accès limité au Cloud privé compte tenu des mesures de haute sécurité en place.
- **L'évolutivité dépend :** L'infrastructure peut ne pas offrir une évolutivité élevée pour répondre à des demandes imprévisibles si le centre de données Cloud est limité aux ressources informatiques sur site

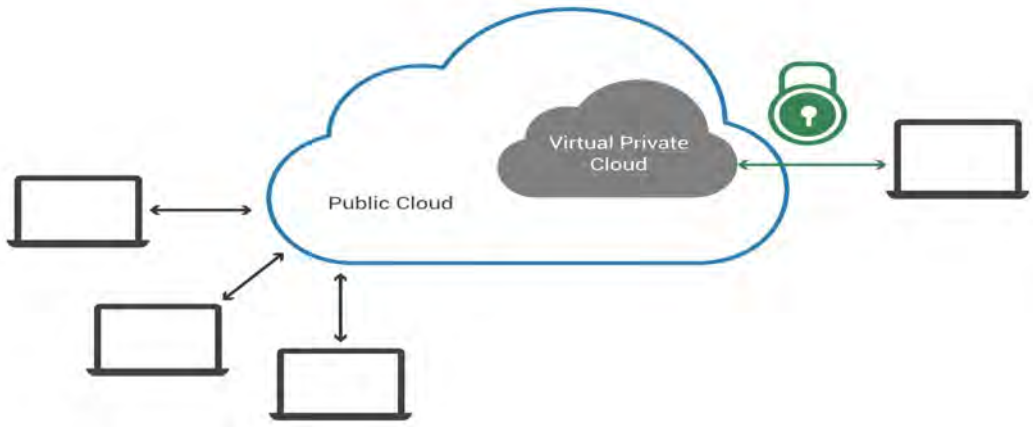

Figure 4: Modèle de déploiement d'un cloud privé [4w]

II.1.2.3 Cloud Hybride

Le Cloud hybride est un mode de déploiement combinant l'utilisation d'un Cloud public avec un environnement en Cloud privé afin de pouvoir absorber plus facilement des pics de charge ponctuels : l'environnement privé est réservé aux systèmes courants, tandis que les capacités du Cloud public sont utilisées pour absorber ponctuellement les montées en charge.

❖ **Avantages du Cloud hybride**

- **Option axée sur les politiques :** Déploiement flexible basé sur des politiques pour répartir les charges de travail entre les environnements d'infrastructure publique et privée en fonction des exigences de sécurité, de performances et de coût.
- **Évoluez en toute sécurité :** L'évolutivité des environnements de Cloud public est obtenue sans exposer les charges de travail informatiques sensibles aux risques de sécurité inhérents.
- **Fiabilité :** La distribution de services sur plusieurs centres de données, certains publics, d'autres privés, permet une fiabilité maximale.
- **Contrôle des coûts :** Amélioration de la sécurité, car les charges de travail informatiques sensibles s'exécutent sur des ressources dédiées dans le Cloud privé tandis que les charges de travail régulières sont réparties sur une infrastructure de Cloud public peu coûteuse pour compenser les investissements

❖ **Inconvénients du Cloud hybride**

Les inconvénients courants du Cloud hybride sont les suivants :

- **Prix :** Le basculement entre public et privé peut-être difficile à suivre, ce qui entraîne un gaspillage de dépenses.
- **La gestion :** Une compatibilité et une intégration solides sont requises entre l'infrastructure Cloud couvrant différents emplacements et catégories. Il s'agit d'une limitation avec les déploiements de Cloud public, pour lesquels les organisations n'ont pas de contrôle direct sur l'infrastructure.
- **Ajout de complexité :** Une complexité d'infrastructure supplémentaire est introduite à mesure que les organisations exploitent et gèrent un mélange évolutif d'architecture de Cloud privé et public.

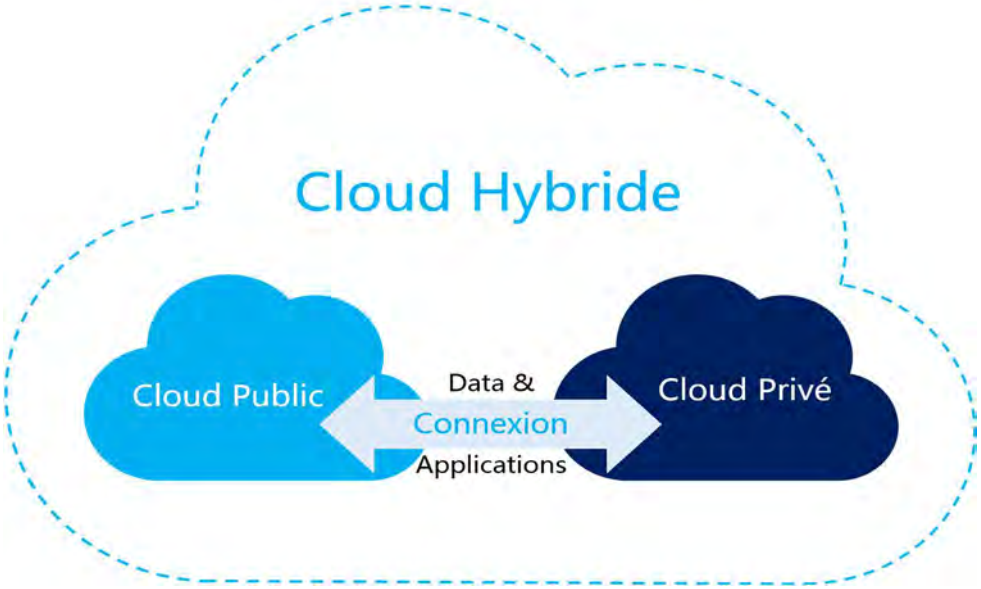

Figure 5: Modèle de déploiement d'un cloud hybride [5w]

II.1.2.4 Cloud Communautaire

C'est un type de Cloud possédant des capacités mutualisées pour une communauté d'intérêt général identifiée. L'infrastructure d'un nuage communautaire est partagée par plusieurs organisations indépendantes et elle est utilisée par une communauté qui est organisée au tour des mêmes besoins, vis-à-vis de son utilisation.

Ce mode de déploiement vise à abaisser la barrière à l'entrée du Cloud privé tout en bénéficiant d'un niveau de service spécifique. Il est adapté à la mutualisation au sein d'un écosystème où la co-gouvernance est envisageable (regroupement de collectivités ou d'acteurs publics, communautés d'universités, GIE interentreprises). ***Il est très important de noter que c'est le seul modèle de Cloud qui garantit actuellement, la localisation et le contrôle total des données transitant sur le réseau.***

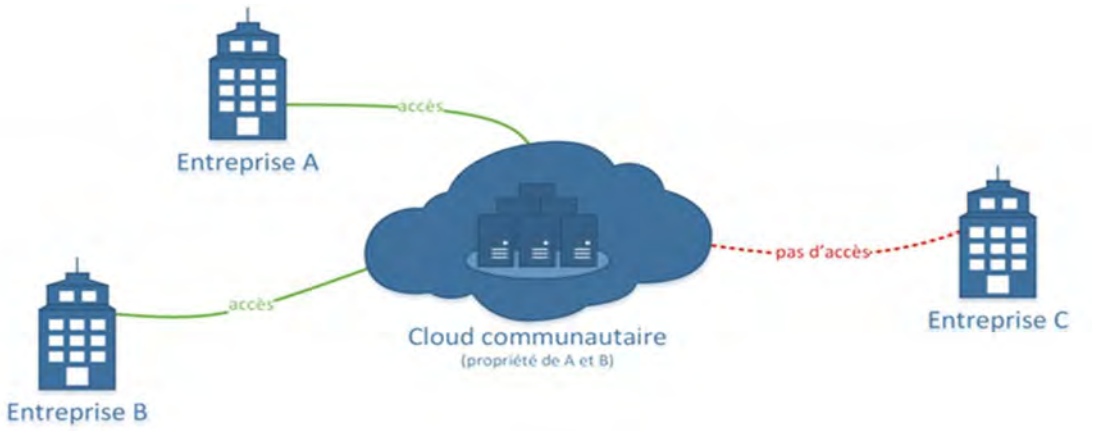

Figure 6: Modèle de déploiement d'un cloud communautaire [3w]

Le tableau ci-dessous résume l'ensemble des avantages et inconvénients ainsi que les cas d'utilisation dans l'architectures du CC :

Types de cloud	*Avantages*	*Inconvénients*	*Cas d'utilisation*
Cloud Public	- *Pas de CAPEX* - *Agilité technique* - *Orientation commerciale* - *Abordabilité* - *Agilité des coûts*	- *Manque de contrôle des coûts* - *Manque de sécurité* - *Contrôle technique minimal*	- *Des besoins informatiques prévisibles, tels que des services de communication pour un nombre spécifique d'utilisateurs* - *Applications et services nécessaires pour effectuer des opérations informatiques et commerciales* - *Besoins en ressources supplémentaires pour répondre aux différentes demandes de pointe* - *Développement de logiciels et environnements de test*
Cloud Prive	- *Environnements exclusifs* - *Sécurité personnalisée* - *Évolutivité sans compromis* - *Performances efficaces* - *La flexibilité*	- *Prix* - *Difficulté mobile* - *L'évolutivité dépend*	- *Industries et agences gouvernementales hautement réglementées* - *Données sensibles* - *Une sécurité solide sur leurs charges de travail informatiques et l'infrastructure sous-jacente*

			- *Grandes entreprises qui ont besoin de technologies avancées de datacenter pour fonctionner efficacement et à moindre coût* - *Organisations qui peuvent se permettre d'investir dans des technologies haute performance et disponibilité*
Cloud Hybride	- *Option axée sur les politiques* - *Évoluez en toute sécurité* - *Fiabilité Contrôle des coûts*	- *Prix* - *La gestion* - *Ajout de complexité*	- *Organisations desservant plusieurs secteurs verticaux confrontés à différentes exigences de sécurité informatique, de réglementation et de performances* - *Améliorer la sécurité des solutions cloud existantes telles que les offres SaaS qui doivent être fournies via des réseaux privés sécurisés* - *Approche stratégique des investissements dans le cloud pour basculer en permanence et faire des compromis entre le meilleur modèle de prestation de services cloud disponible sur le marché*

Cloud Communautaire	- ***Modèle multitenant*** - ***Sécurisé par l'ensemble des participants*** - ***Garantie la localisation et le contrôle des données***	- ***Dédié par un groupe restreint et cible*** - ***Cout financière très chère*** - ***Utilisation collective des besoins***	- ***Un regroupement de commissions scolaires pourraient mettre en commun des services Web afin d'optimiser leurs ressources.*** - ***Des organismes gouvernementaux, des hôpitaux ou des entreprises de télécommunication qui auraient des contraintes de réseau, de sécurité, de stockage, de calcul ou d'automatisation similaires pourraient trouver des intérêts communs à déployer collectivement un cloud communautaire.***

Tableau 1: Avantages/Inconvénients des architectures Cloud Computing

❖ Résumé

Grâce au CC, de nombreuses ressources peut être connectées via des réseaux privés ou publics. Cette technologie simplifie le déploiement d'infrastructures en offrant un support dynamique et évolutif pour héberger des services dont il est souvent compliqué de prévoir l'évolution temporelle. Les entreprises peuvent choisir de déployer leur infrastructure de Cloud en interne, en collaboration avec des partenaires partageant une vision commune, en utilisant les services d'un prestataire de service Cloud public, ou bien en alliant plusieurs de ces solutions. La figure suivante illustre les quatre modèles de déploiement, ainsi que leurs principales caractéristiques.

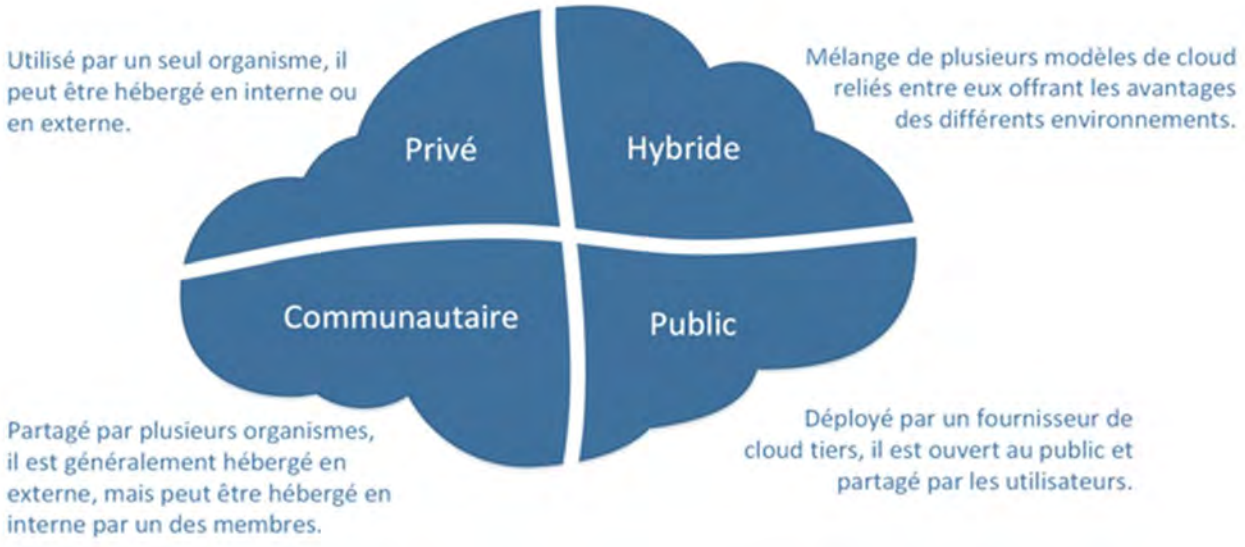

Figure 7: Les différents types d'environnements de déploiement des services de cloud [6w]

II.1.3 Les services du Cloud Computing

Le CC peut être décomposé en trois couches de services qui sont :

- ☞ ***Infrastructure (IAAS, Infrastructure as a service)***
- ☞ ***Plateforme (PAAS, Platform as a service)***
- ☞ ***Applicative (SAAS, Software as a service)***

Pour les distinguer, il faut considérer les différentes couches fonctionnelles qui composent un service numérique.

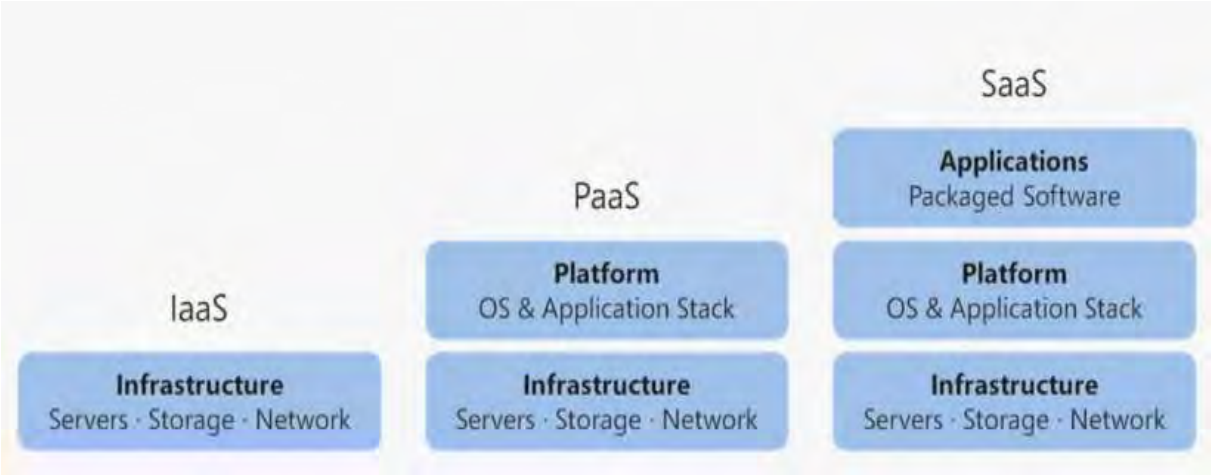

Figure 8: Les différentes composantes des services Cloud Computing [7w]

II.1.3.1 Infrastructure as a service (IAAS)

L'infrastructure en tant que service, est un modèle dans lequel vous sous-traiter l'intégralité de votre centre de données à un hébergeur Cloud. Le fournisseur héberge quasiment tout : des serveurs de stockage au matériel réseau, en passant par la virtualisation de l'environnement.

Dans un service IaaS, le fournisseur met à disposition et administre les ressources matérielles virtualisées comprenant :

- ✓ La puissance de calcul ;
- ✓ Les unités de stockage des données ;
- ✓ Les réseaux ;
- ✓ Les couches de virtualisation ;
- ✓ Les systèmes d'exploitation ;

Le client prend en charge la gestion et l'exploitation de toutes les couches supérieures, middlewares, bases de données, applications.

La souscription à une offre IaaS permet au client d'externaliser son parc matériel serveur et de s'affranchir des compétences de conception et d'exploitation des infrastructures techniques.

❖ **Avantages :**

- Flexibilité : Les ressources matérielles sont ajustables à la demande et en fonction du besoin
- L'abonnement en fonction de la consommation : le tarif est calculé par heure, par semaine ou par mois. Certains fournisseurs facturent en fonction de la quantité d'espace de machine virtuelle utilisée.
- Connexion facile de plusieurs sites de l'entreprise à l'environnement IaaS loué

❖ **Inconvénients :**

- Accès à internet indispensable avec une connexion satisfaisante
- Dépendance vis-à-vis du fournisseur
- Disposer des compétences en interne car vous assurez la gestion du middleware et des applications

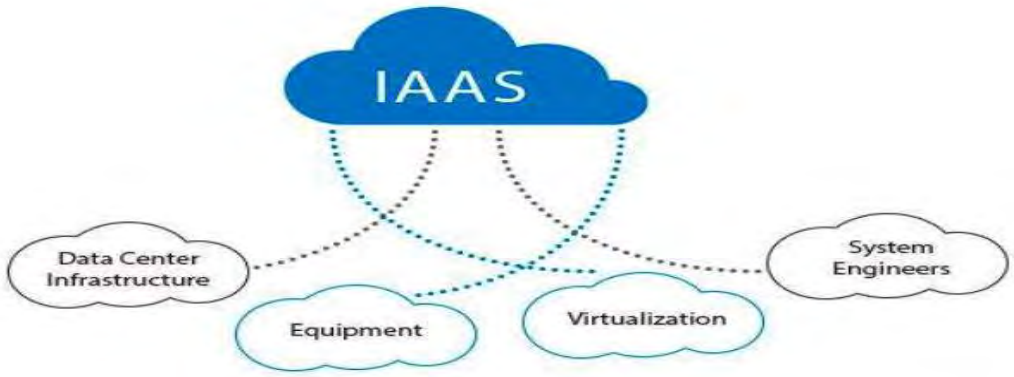

Figure 9: Infrastructure as a Service [8w]

II.1.3.2 Platform as a service (PAAS)

Plate-forme en tant que service est un modèle informatique qui vous permet de développer des logiciels sans avoir à maintenir l'infrastructure sous-jacente.

Le fournisseur met à disposition une plateforme middleware opérationnelle, incluant des serveurs d'applications, des bases de données et les outils permettant au client de développer et de déployer ces propres applications.

Cette configuration est très employée pour disposer de plateformes de développement ou de tests disposant de l'ensemble des outils et middleware nécessaires, en évitant ainsi les tâches de construction et de maintenance de ces plateformes non critiques. Elle se destine donc naturellement avant tout aux développeurs.

❖ **Avantages :**

- Gain de temps et flexibilité pour les projets de développement : plus besoin de se soucier de la mise en place de la plateforme. La production est donc immédiate.
- Gain de temps et financier : L'installation et la maintenance sont assurées par le prestataire.

- Conserver une parfaite maîtrise de ses applications déployées

❖ **Inconvénients :**

- Dépendance importante auprès du fournisseur car il maitrise l'infrastructure et l'environnement logiciel

Figure 10: Platform as a Service [9w]

II.1.3.3 Software as a service (SAAS)

Le logiciel en tant que service est un modèle de Cloud dans lequel un hébergeur distribue des logiciels hébergés dans le Cloud. Vous pouvez accéder rapidement et facilement à l'application via Internet. Ce modèle vous permet d'éviter d'installer un logiciel sur votre ordinateur personnel. Cela réduit les besoins en matériel de l'organisation et réduit les coûts de support et de maintenance. Le client externalise ainsi ses applications (logiciels métiers ou solutions techniques à destination des DSI), auxquelles il accède à la demande. Il paie à l'usage, selon le nombre d'utilisateurs et/ou le temps d'utilisation du logiciel.

❖ **Avantages :**

- La synchronisation : Les données sont synchronisées entre vos appareils et accessibles partout et à n'importe quel moment. De plus, vous êtes assuré que tous les collaborateurs d'une entreprise travaillent sur une même version.
- L'abonnement en fonction de la consommation : Les SaaS sont proposés sous forme d'abonnements mensuels en fonction du nombre d'utilisateur. Vous ne payez que ce que vous consommez.
- Pas de logiciel à installer

❖ **Inconvénients :**

- L'entreprise est entièrement dépendante du fournisseur. Cela peut être très dérangeant en cas d'arrêt d'activité du fournisseur par exemple
- Les données sont entièrement externalisées
- En cas de changement de prestataire, la situation peut être délicate puisqu'il nécessite le transfert de la base de données

Figure 11: Software as a Service [10w]

❖ Autres services également disponibles :

- ***Data as a Service :*** Correspond à la mise à disposition de données délocalisées quelque part sur le réseau. Ces données sont principalement consommées par ce que l'on appelle des *mashups*.
- ***BPaaS :*** Il s'agit du concept de *Business Process as a service* (BPaaS) qui consiste à externaliser une procédure d'entreprise suffisamment industrialisée pour s'adresser directement aux managers d'une organisation, sans nécessiter l'aide de professionnels de l'informatique
- ***Desktop as a Service* :** le *Desktop as a Service* (DaaS ; aussi appelé en français ≪ bureau en tant que service ≫, ≪ bureau virtuel ≫ ou ≪ bureau virtuel héberge ≫) est l'externalisation d'une Virtual Desktop Infrastructure auprès d'un fournisseur de services. Généralement, le Desktop as a Service est proposé avec un abonnement payant.
- ***Network as a Service (NaaS) :*** le Network as a Service correspond à la fourniture de services réseaux, suivant le concept de Software Defined Networking (SDN).

- ***STaaS :*** STorage as a **S**ervice correspond au stockage de fichiers chez des prestataires externes, qui les hébergent pour le compte de leurs clients. Des services grand public, tels que Microsoft OneDrive, SugarSync et Box.net, proposent ce type de stockage, le plus souvent à des fins de sauvegarde ou de partage de fichiers.
  Voici d'autres exemples : Microsoft SharePoint, Amazon S3, Dropbox, Google Drive, HubiC, iCloud, Ubuntu One, Windows Live Mesh, Wuala.
  - ***Workplace as a Service (WaaS) :*** Espace de travail distribue.
  - ***Communication as a Service (CaaS) :*** correspond à la fourniture de solutions de communication substituant aux matériels et serveurs locaux (PABX, ACD, SVI...) des ressources partagées sur Internet.

❖ Résumé

Dans le modèle classique, l'utilisation de logiciels d'entreprise classiques nécessite des investissements matériels (coût des locaux, des serveurs, du matériel de sauvegardes, des équipements réseau), logiciels (coût d'achat des licences, coûts annuels de l'assistance, des mises à jour, des changements de versions) et humains conséquents. En contrepartie, l'entreprise garde son indépendance et une totale maitrise de son infrastructure. Avec le modèle IaaS, le prestataire héberge l'infrastructure informatique de l'utilisateur ou plus généralement de l'entreprise. Cette dernière peut gérer à distance son infrastructure comme si celle-ci se trouvait dans ses propres locaux, les contraintes matérielles en moins. Le prestataire s'occupe ici de la virtualisation, du stockage, des réseaux, du matériel, et de la continuité de service. Le PaaS désigne de manière générale l'environnement fourni par le prestataire au client. C'est un socle fonctionnel et prêt à l'emploi qui lui est mis à disposition. L'utilisateur aura donc la possibilité de gérer ses applications au sein de celui-ci. Enfin, le SaaS consiste à fournir des applications hébergées et accessibles en ligne par le biais d'un navigateur web. Les logiciels se présentent sous la forme de services. Une inscription et le paiement d'un droit d'accès permettent généralement à l'utilisateur d'exploiter ces derniers. La figure suivante illustre les principaux composants de ces quatre modèles, ainsi que les niveaux de responsabilités qui incombent à l'entreprise et au fournisseur de Cloud sur chacun des composants.

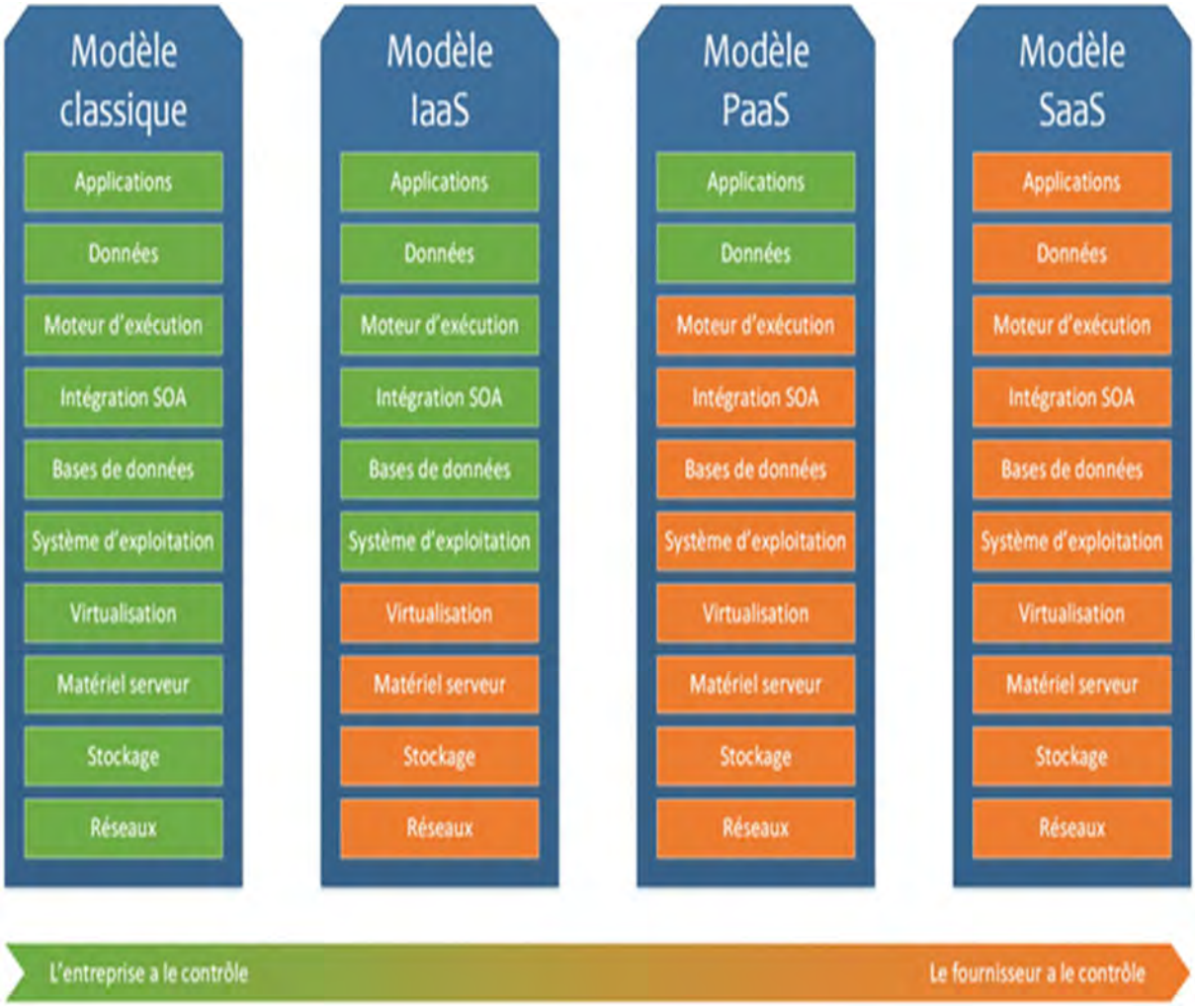

Figure 12: L'impact du Cloud Computing sur la structure de gouvernance des organisations informatiques [11w]

En définitive, dans cette première section, nous avons fourni une base théorique sur le CC, en présentant les différents types de services et modèles de déploiements, évalué les avantages et inconvénients, afin d'appliquer ses concepts à notre contexte. De ce fait, nous allons passer à l'étude de la sécurité dans le CC.

Sommaire

II.2 L'étude de la sécurité dans le Cloud Computing

La sécurité et la conformité émergent systématiquement comme les principales préoccupations des responsables informatiques lorsqu'il est question de CC. La sécurité permet de garantir la confidentialité, l'intégrité, l'authenticité et la disponibilité des informations.
Dans cette deuxième section, il s'agira d'établir les concepts généraux de la sécurité dans le Cloud, présenter les vulnérabilités, identifier les menaces de sécurité, lister les différentes attaques existentielles et de proposer des solutions pour contrecarrées ces derniers.

II.2.1. Objectifs de la sécurité informatique

La sécurité informatique c'est l'ensemble des moyens mis en œuvre pour réduire la vulnérabilité d'un système contre les menaces accidentelles ou intentionnelles. Il convient d'identifier les exigences fondamentales en sécurité informatique. Elles caractérisent ceux à quoi s'attendent les utilisateurs de systèmes informatiques en regard de la sécurité :

- Disponibilité :

La disponibilité des données a pour but de maintenir en condition opérationnelle tous les équipements, logiciels qui composent l'infrastructure informatique d'une société. L'attribution de bande passantes et de mesures pour éviter les éventuelles latences est également une composante de ce principe. La disponibilité repose sur des techniques de redondance (multiplication d'un équipement assurant le même service), de bascule en cas d'indisponible.

- Confidentialité :

La confidentialité des données est un des aspects fondamentaux de la gestion des données au sein d'un système d'information. Des mesures de tous types peuvent être établies afin d'assurer que les données soient vues par les personnes autorisées : les mesures physiques sont communément mises en place pour accorder l'accès aux bonnes personnes comme l'installation d'un lecteur biométrique à l'entrée de locaux informatiques. D'autres mesures logiques peuvent être configurées notamment sur des équipements, comme des règles de flux venant d'un pare-feu, ou encore une gestion des groupes et des autorisations associées.

- L'authentification :

Assurer qu'une personne ou une entité soit bien celle qu'elle prétend être, cela inclut donc de pouvoir vérifier la véracité de ses propos à son égard.

- Intégrité :

L'intégrité est un autre aspect de la gestion des données. Il s'agit ici de s'assurer par divers moyens que les données ne soient pas altérées au cours de leur acheminement. Il est impensable de faire fonctionner une infrastructure critique avec des données erronées ou changées.

- La non-répudiation :

Joue un rôle majeur également dans la sécurité. L'objectif est de n'empêcher toute personne de dénier le fait d'avoir effectué certaines actions, donc de pouvoir consulter un historique complet des actions faites avec un horodatage précis. Cet aspect de la sécurité a un impact évident sur la disponibilité, puisqu'il s'applique aussi sur la possibilité d'une erreur humaine qui aurait pour conséquence une interruption de service.

II.2.2 La sécurité des données

La sécurité des données occupe une place de plus en plus centrale dans les entreprises, au fur et à mesure que celles-ci se digitalisent. Pour la sécurité des données, on peut naturellement se diriger vers des solutions de chiffrement. Notamment la méthode classique consistant à créer un couple clé publique/clé privée où seul le destinataire est en mesure de déchiffrer les données qui lui sont destinées grâce à sa clé privée. Il est important de mentionner que même le fournisseur de Cloud ne détiendra pas la clé privée. Cette solution permet de bien sécuriser les données (selon la taille de la clé) et le client à la possibilité de ne chiffrer qu'une partie de ses données. La méthode pose cependant certaines problématiques d'implémentation. Lors de certains traitements tels que la sauvegarde ou l'indexation, il peut s'avérer nécessaire de manipuler des données décryptées. Parmi les plus fréquents, on citer :

❖ **La non-interopérabilité des fournisseurs**

Un client peut éprouver le besoin de changer de fournisseur de Cloud. Celui-ci ne peut aujourd'hui pas effectuer un transfert de stockage directement de son fournisseur vers un autre. Néanmoins, la norme CDMI (Cloud Data Management Interface) décrit un format d'échange qui permet de déplacer les données d'un environnement Cloud vers un autre.

❖ **Le chiffrement dans le Cloud**

Le client peut utiliser le chiffrement des données pour le stockage dans le Cloud, mais il reste à définir qui doit contrôler les clés de chiffrement et de déchiffrement. En toute logique, ceci doit être géré par le client.

❖ **L'intégrité des données**

Dans le Cloud, il est nécessaire d'assurer l'intégrité des données pendant un transfert ou un stockage. Il faut donc que les opérations sur les données soient contrôlées afin de n'effectuer que les opérations qui sont autorisées. Il n'existe actuellement pas de standard commun entre les fournisseurs.

❖ **La gestion des logs**

Dans le respect du Payment Card Industry Data Security Standard (PCI DSS), les logs doivent être fournis au gestionnaire de sécurité.

❖ **Le stockage**

Les données peuvent être transférées entre plusieurs datacenter géographiquement éloignes. Le particulier ou l'entreprise ne connait pas la position des données entre chaque datacenter.

II.2.3 La sécurité des infrastructures

Tout chef d'entreprise cherchant à optimiser son infrastructure informatique (SI), qu'il cherche à la développer ou à minimiser les coûts engendrés par celle-ci, doit prendre en compte la sécurité. Le SI est à la fois l'outil de travail majeur de vos collaborateurs et une barrière permettant de réduire les risques de sécurité lorsqu'il est correctement paramétré, notamment en matière de protection des données. Parmi les plus fréquents, on citer :

☞ **La sécurité physique :**

La dématérialisation des données permet donc d'avoir de multiples datacenters où peuvent être stockées ces données. Il faut un contrôle et une traçabilité d'accès dans le but de prévenir tout dommage sur le matériel. Faire attention au va-et-vient dans certaines zones, protéger l'accès à certaines salles et même les interdire d'accès peuvent être un bon moyen de protection. Il est

impératif de protéger également certaines zones plus que les autres contre les incendies et autres risques environnementaux, ainsi que bien les climatiser

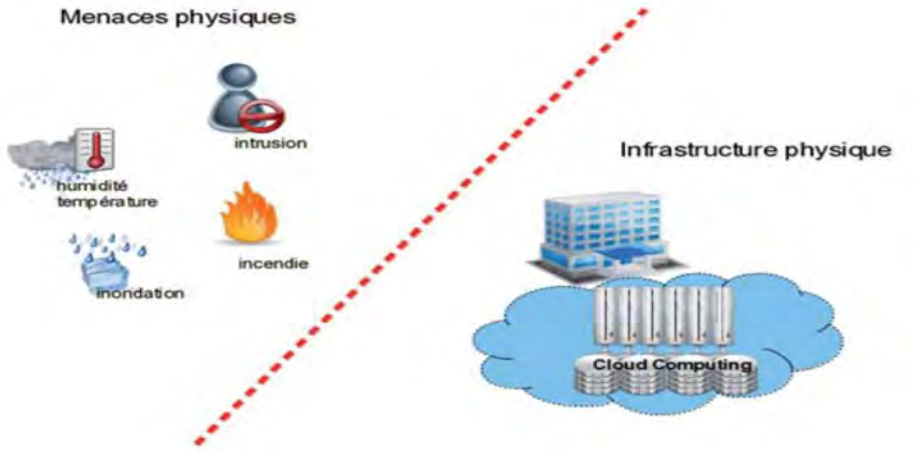

Figure 13: Architecture de fonctionnement de la sécurité physique

Les redondances matérielles sont également très utilisées pour garantir l'accès au service en très haute disponibilité avec des performances optimales. Penser à la réplication de configuration entre les équipements et également à une redondance avec une sélection d'équipements différents (exemple : constructeur différent) permet de prévenir plusieurs problèmes importants. Enfin, il est possible de mettre en place comme sécurité géographique, un système de secours géographiquement éloigné, au cas de la perte totale de l'infrastructure. Il permet de réaliser un PCA (plan de continuité d'activité) sans interruption.

- **La sécurité logique :**

La sécurité que l'on souhaite intègre à des plateformes virtualisées. Il faut cependant appliquer la même règle de sécurité que dans une architecture physique. Mais il faut en plus s'intéresser à la problématique sécurité spécifique au cloud. La sécurité et la confidentialité des données peuvent être gérés de différentes façons d'un point de vue logique : la segmentation réseau sera ainsi sécurisée par des équipements de filtrage (pare-feu, proxy, sondes IPS/IDS, etc.) et des solutions antivirus. Le but est ici de contrôler les requêtes entrantes. Un processus d'authentification et par ailleurs nécessaire. Il faut également insister sur deux bonnes pratiques de sécurisation logique dans un environnement cloud. Premièrement, il faut paramètre le système d'exploitation des machines virtuelles pour les sécurisées comme le conçoit l'éditeur de la solution de virtualisation. La deuxième bonne pratique consiste à bien isoler le trafic réseau en fonction des besoins lors de la conception du réseau virtuel.

II.2.4 Les Vulnérabilités dans le Cloud

Dans cette sous-section, il s'agira de définir l'ensemble des vulnérabilités qu'on doit prendre en compte pour migrer vers le Cloud [10]. Parmi ces dernières, nous pouvons citer :

II.2.4.1 Session Riding

La session riding se produit lorsqu'un attaquant vole le cookie d'un utilisateur pour utiliser l'application au nom de l'utilisateur. Un attaquant peut également utiliser des attaques CSRF pour inciter l'utilisateur à envoyer des requêtes authentifiées à des sites Web arbitraires pour réaliser diverses choses.

II.2.4.2 Virtual Machine Escape

Dans les environnements virtualisés, les serveurs physiques exécutent plusieurs machines virtuelles sur les hyperviseurs. Un attaquant peut exploiter un hyperviseur à distance en utilisant une vulnérabilité présente dans l'hyperviseur lui-même - de telles vulnérabilités sont assez rares, mais elles existent. En outre, une machine virtuelle peut sortir de l'environnement de sandbox virtualisé et accéder à l'hyperviseur et, par conséquent, à toutes les machines virtuelles qui s'exécutent dessus.

II.2.4.3 Fiabilité et disponibilité du service

Nous nous attendons à ce que nos services et applications Cloud soient toujours disponibles lorsque nous en avons besoin, ce qui est l'une des raisons de passer au Cloud. Mais ce n'est pas toujours le cas, surtout par mauvais temps avec beaucoup de foudre où les pannes de courant sont fréquentes. Les CSP ont des alimentations ininterrompues, mais même celles-ci peuvent parfois tomber en panne, nous ne pouvons donc pas compter sur les services Cloud pour être opérationnels à 100% du temps. Nous devons prendre en compte un peu de temps d'arrêt, mais c'est la même chose lorsque nous exécutons notre propre Cloud privé.

II.2.4.4 Cryptographie non sécurisée

Les algorithmes de cryptographie nécessitent généralement des générateurs de nombres aléatoires, qui utilisent des sources d'informations imprévisibles pour générer des nombres aléatoires réels, ce qui est nécessaire pour obtenir un grand pool d'entropie. Si les générateurs de nombres aléatoires ne fournissent qu'un petit pool d'entropie, les nombres peuvent être forcés brutalement. Dans les ordinateurs clients, la principale source de randomisation est le mouvement de la souris de l'utilisateur et les pressions sur les touches, mais les serveurs fonctionnent principalement sans interaction de l'utilisateur, ce qui signifie par conséquent un nombre inférieur de sources de randomisation. Par conséquent, les machines virtuelles doivent

s'appuyer sur les sources dont elles disposent, ce qui pourrait entraîner des nombres facilement devinables qui ne fournissent pas beaucoup d'entropie dans les algorithmes cryptographiques.

II.2.4.5 Protection et portabilité des données

Lorsque nous choisissons de changer de fournisseur de services Cloud pour un fournisseur moins cher, nous devons résoudre le problème du mouvement et de la suppression des données. L'ancien CSP doit supprimer toutes les données que nous avons stockées dans son centre de données pour ne pas les laisser traîner. Alternativement, le CSP qui sort de l'entreprise doit fournir les données aux clients, afin qu'ils puissent passer à un autre CSP, après quoi les données doivent être supprimées. Que faire si le CSP cesse ses activités sans fournir les données ? Dans de tels cas, il est préférable d'utiliser un CSP largement utilisé qui existe depuis un certain temps, mais dans tous les cas, la sauvegarde des données est toujours en ordre.

II.2.4.6 CSP Lock-in

Nous devons choisir un fournisseur de Cloud qui nous permettra de passer facilement à un autre fournisseur en cas de besoin. Nous ne voulons pas choisir un CSP qui nous obligera à utiliser ses propres services, car parfois nous aimerions utiliser un CSP pour une chose et l'autre CSP pour autre chose.

II.2.4.7 Dépendance Internet

En utilisant les services Cloud, nous dépendons de la connexion Internet, donc si Internet échoue temporairement en raison d'un coup de foudre ou d'une maintenance du FAI, les clients ne pourront pas se connecter aux services Cloud. Par conséquent, l'entreprise perdra lentement de l'argent, car les utilisateurs ne pourront pas utiliser le service requis pour l'exploitation commerciale. Sans parler des services qui doivent être disponibles 24/7, comme les applications dans un hôpital, où des vies humaines sont en jeu.

II.2.5 Les menaces de sécurité dans le cloud

Outre les avantages que le CC offres, il existe de nombreuses menaces de sécurité empêchant aux consommateurs d'utiliser ces services en toute sécurité [11].

Dans cette section, il s'agira de définir les menaces de sécurité ainsi que leurs techniques d'atténuation possible.

II.2.5.1 Perte de données

Elle peut se produire de différentes manières en dehors d'attaques malveillantes. Les données peuvent être compromises en raison de suppression, mo[1]dification, perte de la clé de chiffrement et par d'autres moyens comme les tremblements de terre, les inondations et les incendies, etc. Les organisations doivent maintenir une sauvegarde complète de leurs données pour éviter de telle menaces.

II.2.5.2 Violations de données

Elle se référé à une fuite de sensible informations aux utilisateurs non autorises. Des violations de données peuvent survenir en raison d'une authentification incorrecte et mécanismes d'autorisation, contrôles d'audits, utilisation non fiable des clés de cryptage, des défis d'élimination et du fonctionnement défaillance du système. ICloud d'Apple, Microsoft, Yahoo, Google, etc. sont des entreprises qui ont fait face à ce problème.

II.2.5.3 Détournement de compte ou de service

Elle se produite si un attaquant accède aux identifiants de connexion, puis compte compromis devient une base de lancement et l'attaquant peut écouter les conservations des utilisateurs, rembourser de fausses informations, manipuler les données et répondre à session et rediriger le consommateur vers des sites illégitimes et peut lancer diverses attaques.

II.2.5.4 Interfaces et API non sécurisées

Reportez-vous aux interfaces de programmation d'application, qui sont des normes et des protocoles que les consommateurs utilisent pour se connecter aux services Cloud. Comme la sécurité des services Cloud dépend de ces API, celles-ci doivent avoir des normes de certification sécurisées, des contrôles d'accès appropriés et des mécanismes de surveillance des activités pour éviter les menaces telles que l'accès anonyme, l'authentification en texte clair, les jetons ou mots de passe réutilisables, les autorisations inappropriées, la surveillance limitée et la journalisation.

II.2.5.5 Insiders malveillants

Ils peuvent être des personnes de confiance au sein d'un organisation qui peut accéder aux données confidentielles. Ils peuvent effectuer des activités non privilégiées pour infiltrer les actifs de l'organisation et peut nuire à la marque, pertes de productivité et financières, mener

[1] Naseer Amara , Huang Zhiqui , Awais Ali 2017 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery

différentes activités comme le pare-feu ou système de détection d'intrusion (IDS) prétendant être une activité légale

II.2.5.6 Diligence raisonnable insuffisante

Elle se produite quand les organisations se lancent dans l'utilisation des services offerts par les fournisseurs de services sans avoir une connaissance suffisante des modèles du Cloud et ses opérations, sans comprendre quel modèle leur convient et les risques qui y sont associes

II.2.5.7 Utilisation abusive des services cloud

Peut-être décrit en tant qu'actions non éthiques et illégales du consommateur pour abuser les services. Infrastructure à faible cout, haute ressource, approvisionnement, les procédures d'enregistrement faibles ont facilite l'anonymat des spammeurs, des criminels et autres utilisateurs malveillants pour atteindre leur cible en attaquant le système. Les fournisseurs de services Cloud tels que Amazon, Google, Facebook, Twitter, etc. ont été utilisés pour lancer des chevaux de Troie et des botnets.

II.2.5.8 Problèmes technologiques partagés

Ils se produisent dans une infrastructure multi-locataire, où les services à la demande sont fournis à l'aide d'une infrastructure partagée entre différents utilisateurs ayant accès à la même machine virtuelle. Les vulnérabilités des hyperviseurs virtualisés (à utiliser à des fins d'isolation) permettent aux consommateurs malveillants d'avoir un accès inapproprié et de contrôler les VM de consommateurs légitimes.

II.2.5.9 Profil de risque inconnu

Peut se produire avec des avantages importants comme le gain de temps en maintenant l'infrastructure et en assurant la propriété. Cependant, les consommateurs ne sont pas tenus de suivre des procédures de sécurité internes, des correctifs, des durcissements, des audits et des processus de journalisation, etc., ce qui donne lieu à un profil de risque inconnu pouvant entraîner de graves menaces.

II.2.5.10 Vol d'identité

Il se produit lorsqu'un attaquant se fait passer pour quelqu'un d'autre pour obtenir les informations d'identification des utilisateurs afin d'accéder à ses actifs.

II.2.5.11 Modifications du modèle d'entreprise

Elle est une menace grave où les données des consommateurs peuvent résider sur différents territoires régis par différentes lois fédérales. Le fournisseur de services fournit divers services aux consommateurs sans savoir où ils résident et le consommateur perd le contrôle de

l'infrastructure qui est en fait la plus grande menace et peut altérer la vie des consommateurs de Cloud

II.2.5.12 Lock-IN

La condition fait référence au manque de capacité à passer d'un nuage à un autre. Cette menace se produit lorsque les organisations se lancent dans le fournisseur de services Cloud avec une mauvaise connaissance du modèle Cloud qui leur convient le mieux en fonction de leurs besoins pour éviter le verrouillage.

Ainsi les techniques d'atténuation et les plateformes dans lequel ces menaces affecteront seront résumes suivant le tableau ci-dessous

Tableau 2: les différentes et les techniques d'atténuation sur les plateformes CC

Menaces de sécurité dans le cloud	Les plateformes affectées	Techniques d'atténuation
Perte de données	IaaS, PaaS, SaaS	- Sauvegardes régulières. - En utilisant des techniques de cryptage appropriées. - En protégeant les données en transit. - Mise en œuvre d'une génération, d'un stockage et d'une gestion de clés solides. Indiquer légalement les techniques de renforcement et de maintenance des fournisseurs.
Violations de données	IaaS, PaaS, SaaS	- En utilisant des techniques de cryptage appropriées. - Pour protéger les données, elles doivent être analysées à la fois lors de la conception et de l'exécution. Mettre en œuvre une génération, un stockage et une gestion de clés solides. - Indiquant légalement au fournisseur d'effacer les médias persistants avant qu'ils ne soient libérés dans le pool. - Indiquer légalement les stratégies de sauvegarde et de rétention. - En mettant en œuvre des interfaces de programmation d'applications (API) solides.

Détournement de compte ou de service	IaaS, PaaS, SaaS	- Bonne compréhension des politiques de sécurité et du contrat de niveau de service (SLA). - Utilisation de méthodes d'authentification multifactorielles. - Surveillance stricte pour détecter les activités non autorisées. - Empêchez le partage d'informations d'identification entre les consommateurs et les services.
Interfaces et API non sécurisées	IaaS, PaaS, SaaS	- Mécanismes d'authentification et de contrôle d'accès solides. Utilisation du cryptage pour la transmission de données. - Analyse des interfaces des fournisseurs de cloud. - La bonne compréhension de la chaîne de dépendances associée aux API.
Insiders malveillants	IaaS, PaaS, SaaS	- Intégrez la gestion des ressources humaines (GRH) à un accord juridique Application stricte de la procédure de gestion de la chaîne d'approvisionnement. - Donner une clarté appropriée à la sécurité et au processus administratif.
Diligence raisonnable insuffisante	IaaS, PaaS, SaaS	- Utilisation des normes de l'industrie pour mettre en œuvre des applications et des services cloud. - Évaluation des risques à l'aide de méthodes qualitatives et quantitatives. Divulguer les journaux, données et détails d'infrastructure applicables. Utilisation d'une autorisation et d'une authentification fortes.
Utilisation abusive des services cloud	IaaS, PaaS	- Auditer correctement le trafic réseau. Surveillance améliorée de la fraude par carte de crédit

Problèmes technologiques partagés	IaaS	- Utilisation de meilleurs mécanismes d'authentification et de contrôle d'accès. Inspectez les vulnérabilités et la configuration. - Surveiller l'environnement pour les changements / activités non autorisés
Profil de risque inconnu	IaaS, PaaS, SaaS	- Utilisation du SLA pour les correctifs et la correction des vulnérabilités. Divulguer les journaux, données et détails d'infrastructure applicables. Audit du système d'alerte pour les violations de données.
Vol d'identité	IaaS, PaaS, SaaS	- Mot de passe fort, authentification et mécanismes de contrôle d'accès.
Modifications du modèle d'entreprise	IaaS, PaaS, SaaS	- Mise à disposition du système de contrôle et de surveillance des services offerts.
Lock-IN	IaaS, PaaS, SaaS	- Surveillance grâce au système de détection d'instructions (IDS), au système de prévention des intrusions (IPS) et à la mise en œuvre du pare-feu.

II.2.6 Les attaques et leurs techniques d'atténuations dans le Cloud

Alors que le monde évolue vers le CC, il devient de plus en plus sophistiqué et les attaquants cherchent à le suivre. Dans cette sous-section, il s'agira de définir l'ensemble des attaques possible ainsi que leurs techniques d'atténuation

II.2.6.1 Attaques par déni de service (DoS)[2]

Dans l'attaque DoS, un attaquant surcharge le système Cloud cible avec des demandes de service afin qu'il cesse de répondre à tout nouveau demandes et rendre les ressources indisponibles pour ses utilisateurs. Certains professionnels de la sécurité ont identifié que le Cloud est plus vulnérable aux attaques DoS, car il est utilisé par de nombreux utilisateurs, ce qui le rend beaucoup plus dommageable.

Les attaques DoS sont de plusieurs types et ils peuvent se trouver sur plusieurs niveaux dans lesquels nous pouvons citer [12] :

1) Un attaquant peut surcharger la cible avec une grande quantité de données indésirables qui consomment la bande passante et les ressources du système, par exemple les inondations UDP, les inondations ICMP, etc.

2) Un attaquant peut utiliser un espace vide (lacune) associé à divers protocoles réseau pour surcharger la ressource cible, par exemple les inondations SYN, les attaques des paquets de fragments, le ping de la mort, etc.

3) Un attaquant peut faire une requête HTTP en grande quantité afin qu'elle ne puisse pas être manipulée par le serveur par exemple Attaque HTTP DDOS, attaque XML DDOS, etc.

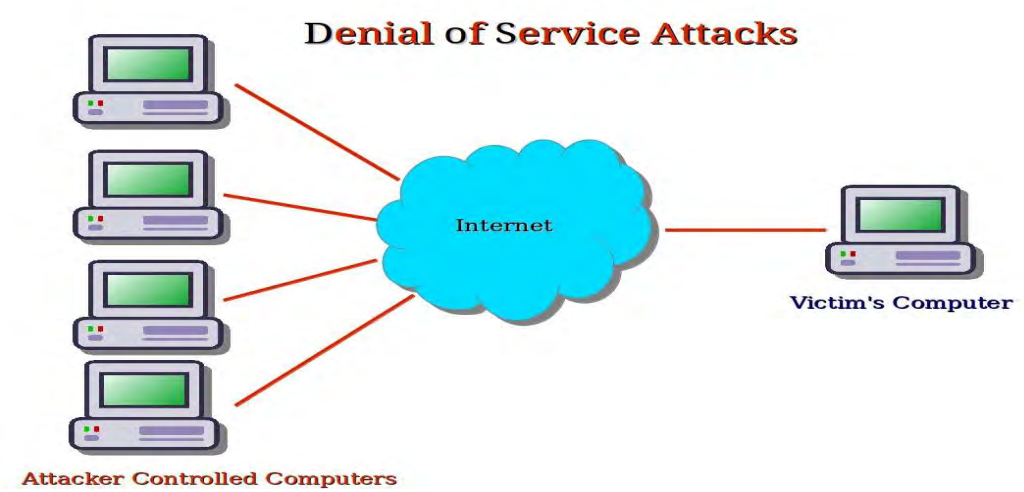

Figure 14: Architecture de fonctionnement des attaques DoS [12w]

[2] International Journal of Advanced Research en Informatique et genie logiciel Volume 6, numero 1, janvier 2016 www.ijarcsse.com

- **Solutions possibles contre les attaques DoS :**

Pour restreindre les attaques DoS, nous pouvons classer le trafic sur la base d'une autorisation, afin de pouvoir bloquer ou autoriser le trafic identifié.

Pour cela, les pares-feux peuvent être utilisés pour autoriser ou refuser le trafic sur la base des protocoles d'accès, des ports ou des adresses IP.

Aujourd'hui, la plupart des commutateurs ont la capacité de limiter le débit sur la base de la liste de contrôle d'accès qui peut fournir une limitation automatique du débit, façonner le trafic, un faux filtrage IP et peut profondément inspecter les paquets. Semblables aux commutateurs, les routeurs ont également des capacités telles que l'ACL et la limitation de débit qui peuvent être définies manuellement pour créer des règles de filtrage. Le matériel frontal d'application peut être utilisé sur les réseaux en collision avec des routeurs et des commutateurs qui peuvent analyser les paquets de données lorsqu'ils entrent dans le réseau pour vérifier leur autorité et leur priorité afin que le flux de trafic puisse être contrôlé.

Après une attaque DoS, on peut envoyer tout le trafic sur le paquet attaqué vers une interface nulle ou vers une interface non existante, cela peut aider à réduire l'effet des attaques DoS.

II.2.6.2 Attaques par injection de logiciels malveillants dans le cloud

Une première tentative d'attaque considérable vise à injecter un service malveillant ou une machine virtuelle dans le Cloud. Dans ce type d'attaque l'attaquant crée son propre module d'implémentation de service malveillant (SaaS ou PaaS) ou machine virtuelle instance (IaaS) et essayez de l'ajouter au système Cloud. Ensuite, l'attaquant doit se comporter de manière à en faire un service valide pour le système Cloud.

Il s'agit d'une nouvelle instance d'implémentation de service parmi les instances valides. Si l'attaquant réussit en cela, le Cloud redirige automatiquement les requêtes de l'utilisateur valide vers l'implémentation du service malveillant, et le code de l'attaquant commence à s'exécuter. Le scénario principal derrière l'attaque Cloud Malware Injection est qu'un attaquant transfère une instance de service malveillant dans le Cloud afin qu'elle puisse accéder aux demandes de service de la victime.

Le but de l'injection de malware dans le Cloud peut être tout ce qui intéresse un attaquant ; il peut inclure des modifications de données, une fonctionnalité complète changements et inversions ou blocages.[3]

[3] International Journal of Advanced Research en Informatique et genie logiciel Volume 6, numero 1, janvier 2016 www.ijarcsse.com

Figure 15: Architecture de fonctionnement des attaques injection logicielle [13w]

- **Solutions possibles contre les attaques par injection de logiciels malveillants :**

Dans le système de CC, les applications exécutées par le client sont considérées avec une efficacité et une intégrité élevée de manière à empêcher les attaques par injection de logiciels malveillants. Nous pouvons combiner l'intégrité avec le matériel car pour un attaquant, il est difficile de s'introduire dans le niveau IaaS. Pour cela, nous pouvons utiliser une allocation de fichiers table (FAT).

Nous pouvons déterminer aussi la validité et l'intégrité de la nouvelle instance en comparant les instances précédentes. Pour cela, nous devons déployer un hyperviseur du côté du fournisseur. Dans un système Cloud, l'hyperviseur est considéré comme la partie la plus sûre et la plus sophistiquée de celui-ci dont la sécurité ne peut être brisée par aucun moyen. Le fournisseur est responsable de la planification de toutes les instances et services afin que nous puissions créer un hyperviseur pour vérifier l'allocation des fichiers table pour valider et intégrer une instance de client. Une autre approche est que nous pouvons conserver les informations de la version de type de plate-forme qu'un utilisateur client pour accéder au Cloud dans la première phase lorsqu'un client ouvre un compte et peut utiliser ces informations pour vérifier la validité d'une nouvelle instance du client.

II.2.6.3 Attaques de canal latéral

Les attaques par canaux auxiliaires (*side-channel attacks* en anglais) sont une famille d'attaques consistant à extraire une information par la récupération et l'interprétation de signaux émis « involontairement » par un système (vibrations, activité électromagnétique, consommation électrique, bruit, temps d'exécution…).

Un attaquant tente de compromettre le système Cloud en plaçant une machine virtuelle malveillante à proximité immédiate d'un système de serveur Cloud cible, puis lancer une attaque de canal secondaire. Les attaques par canal secondaire sont apparues comme une sorte

[4]de mise en œuvre efficace d'algorithmes cryptographiques du système de ciblage des menaces de sécurité. Les attaques par canal secondaire utilisent deux étapes pour attaque :

- VM CO-Résidence and Placement, c'est-à-dire qu'un attaquant peut souvent placer son instance sur la même machine en tant qu'instance cible.

- Extraction de VM, c'est-à-dire la capacité d'une instance malveillante à utiliser des canaux secondaires pour apprendre des informations sur les instances co-résidentes. Il peut être très facile d'obtenir des informations secrètes à partir d'un appareil, donc la sécurité contre l'attaque de canal secondaire dans le CC doit être fournie

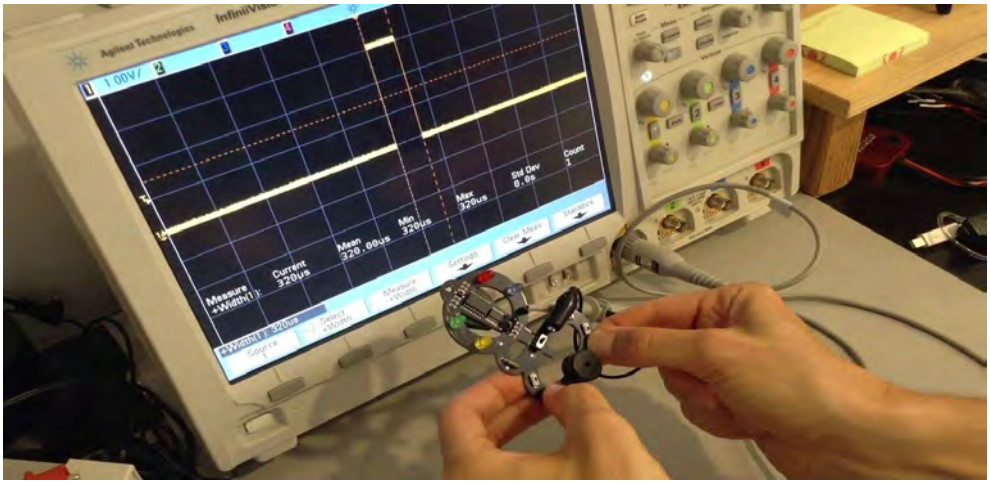

Figure 16: Architecture de fonctionnement des attaques de canal latéral [14w]

- **Solutions possibles contre les attaques de canal latéral :**

Pour empêcher les attaques des canaux secondaires dans le Cloud, nous pouvons utiliser une combinaison de pare-feu virtuel. Selon le cas étude du service Amazon EC2, il est possible pour un attaquant d'instancier une nouvelle machine virtuelle vers une machine virtuel ciblé identifié dans le cloud et extrait certaines informations confidentielles mais un pare-feu virtuel empêche cette tentative de placement de machine virtuelle malveillante lors d'une attaque par canal secondaire. Une autre approche consiste à utiliser le décryptage par cryptage aléatoire (en utilisant le concept de diffusion de confusion) car il empêche l'extraction de la deuxième étape de l'attaque de canal latéral.

La sécurité à la fois contre les côtés frontaux et l'arrière de l'architecture de CC est fournie par cette combinaison et fournissent également RAS (fiabilité, disponibilité et sécurité). Lorsque nous utilisons un cryptage aléatoire nous entendons que les données ou les informations client

[4] International Journal of Advanced Research en Informatique et genie logiciel Volume 6, numero 1, janvier 2016 www.ijarcsse.com

sont cryptées via un algorithme de cryptage différent afin que l'attaquant soit confronté plus de difficultés pour détecter ou extraire la clé de cryptographie.

II.2.6.4 Attaques d'authentification

L'authentification est un point faible des services de CC qui est fréquemment ciblé par un attaquant. Aujourd'hui, la plupart des services utilisent toujours un nom d'utilisateur et un mot de passe simples pour l'authentification basée sur les connaissances, mais certaines exceptions sont les institutions financières qui utilisent diverses formes d'authentification secondaire (telles que les questions secrètes partagées, le site touches, claviers virtuels, etc.) qui compliquent les attaques de phishing courantes.

Parmi les attaques d'authentification, on peut citer :

- **Attaques Brute Force :** Dans ce type d'attaque, toutes les combinaisons possibles de mot de passe s'appliquent pour casser le mot de passe. L'attaque par force brute est généralement appliquée pour casser les mots de passe cryptés où les mots de passe sont enregistrés sous forme de texte chiffré.
- **Attaques par dictionnaire :** ce type d'attaque est relativement plus rapide que l'attaque par force brute. Contrairement à tout vérification des possibilités en utilisant une attaque par force brute, l'attaque par dictionnaire essaie de faire correspondre le mot de passe avec la plupart des mots ou des mots d'usage quotidien.
- **Surf à l'épaule :** Le surf à l'épaule est un nom alternatif de « espionnage » dans lequel l'attaquant espionne l'utilisateur en mouvements pour obtenir son mot de passe. Dans ce type d'attaque, l'attaquant observe l'utilisateur, comment il entre son mot de passe c'est-à-dire sur quelles touches du clavier l'utilisateur a appuyé
- **Attaques de relecture :** Les attaques de relecture sont également appelées attaques par réflexion. C'est une façon d'attaquer le défi du mécanisme d'authentification de l'utilisateur de réponse.
- **Attaques de phishing :** il s'agit d'une attaque Web dans laquelle l'attaquant redirige l'utilisateur vers le faux site Web pour obtenir mots de passe ou codes PIN de l'utilisateur.
- **Enregistreurs de frappe :** Les enregistreurs de frappe sont les logiciels qui surveillent les activités de l'utilisateur en enregistrant chaque touche pressée par l'utilisateur.

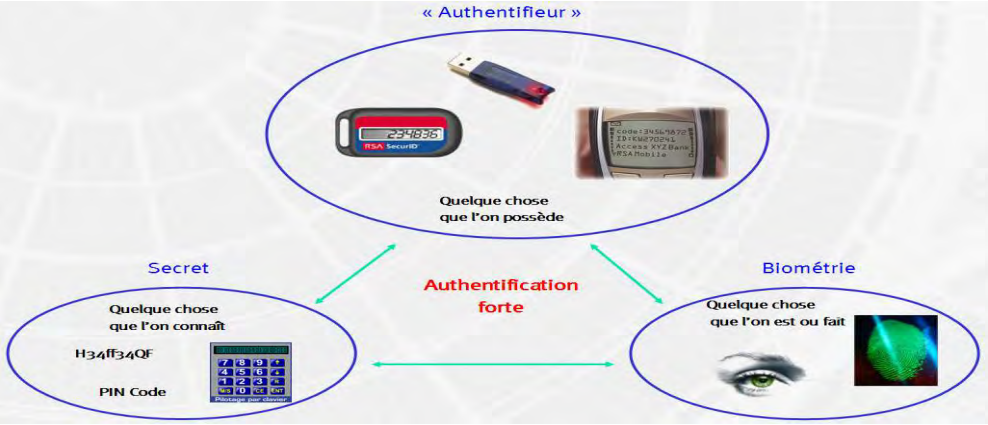

Figure 17: Architecture de fonctionnement des attaques d'authentifications [15w}

- **Solutions possibles contre les attaques d'authentification :**

Parmi les solutions utilisent pour contrecarres ses attaques, on peut citer :

- **Réponse retardée :** étant donné une paire nom de connexion et mot de passe, le serveur fournit une réponse oui ou non légèrement retardée (disons pas plus vite une réponse par seconde). Cela devrait empêcher un attaquant de vérifier suffisamment de mots de passe dans un délai raisonnable du temps.
- **Verrouillage de compte :** les comptes sont verrouillés après quelques tentatives de connexion infructueuses (par exemple, un compte est verrouillé pour une heure après cinq tentatives infructueuses.) Comme la mesure précédente, cette mesure vise à empêcher les attaquants de vérifier suffisamment de mots de passe dans un délai raisonnable.
- **Biométrie :** La biométrie est un système d'authentification basé sur l'image dans lequel les empreintes digitales, le visage, l'iris, la rétine, la parole, la signature sont utilisées pour vérifier par rapport à l'échantillon original. L'image est d'abord prétraitée, puis la classification des images sont terminées. L'avantage de cette méthode est qu'il s'agit d'une signature réelle et unique et ne peut pas être volée. L'inconvénient est qu'il est coûteux et difficile à mettre en œuvre. Ce n'est pas une méthode complètement mûrie et elle peut être facilement compromis et prend également du temps.

II.2.6.5 Attaques cryptographiques Man-In-The-Middle

Une attaque d'homme au milieu est une attaque dans laquelle l'attaquant intercepte des messages dans un échange de clé publique, puis les retransmet, en substituant sa propre clé publique à celle demandée, de sorte que les deux parties d'origine semblent toujours être communiquer les uns avec les autres. Dans le processus, les deux parties d'origine semblent communiquer normalement. Le message de l'expéditeur ne reconnaît pas que le destinataire est un attaquant

inconnu essayant d'accéder ou de modifier le message avant retransmission au récepteur. Ainsi, l'attaquant contrôle toute la communication.

Certains types d'attaques MITM sont :

- **Communication de protocole de résolution d'adresse (ARP) :** Dans la communication ARP normale, le PC hôte enverra un paquet qui a l'adresse IP source et de destination à l'intérieur du paquet et le diffusera à tous les appareils connectés au réseau. L'appareil qui a l'adresse IP cible n'enverra que la réponse ARP avec son adresse MAC dedans, puis la communication a eu lieu. Le protocole ARP n'est pas un protocole sécurisé et le cache ARP n'a pas de mécanisme infaillible, ce qui pose un gros problème.
- **Empoisonnement du cache ARP :** Dans l'empoisonnement du cache ARP, l'attaquant reniflerait sur le réseau en contrôlant le commutateur réseau pour surveiller le trafic réseau et usurper les paquets ARP entre l'hôte et le PC de destination et effectuez l'attaque MITM.
- **Usurpation DNS :** la cible, dans ce cas, recevra de fausses informations qui entraîneraient la perte d'identifiants. Comme expliqué précédemment, il s'agit d'une sorte d'attaque MITM en ligne où l'attaquant a créé un faux site Web de votre banque, donc lorsque vous visitez le site Web de votre banque, vous serez redirigé vers le site Web créé par l'attaquant, puis l'attaquant obtiendra toutes vos informations d'identification.
- **Détournement de session :** une fois que la session est établie entre le PC hôte et le serveur Web, l'attaquant peut obtenir certaines parties de l'établissement de la session qui se fait en capturant les cookies qui ont été utilisés pour l'établissement de la session.

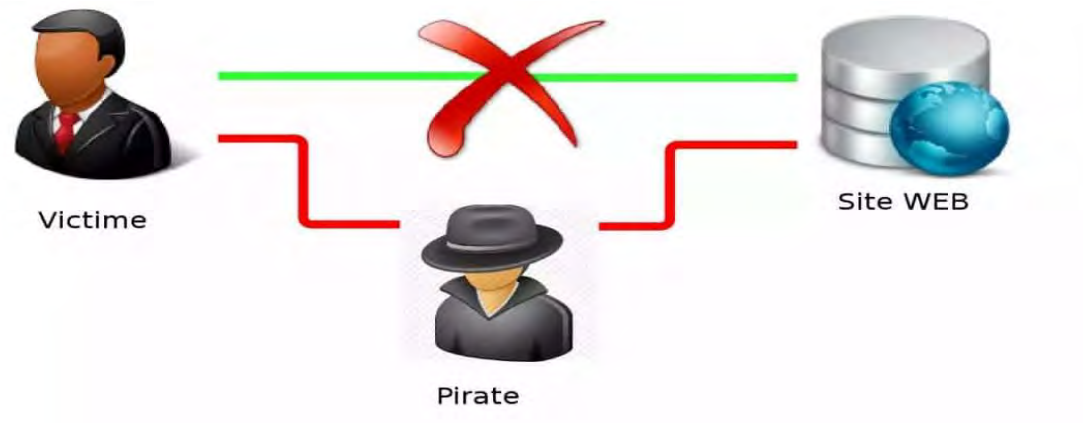

Figure 18: Architecture de fonctionnement des attaques MITM [16w]

- **Solutions possibles contre les Attaques Man-In-The-Middle :**

Parmi les solutions possibles contre les attaques MITM, on peut citer :

- ❖ En utilisant un mot de passe unique car un mot de passe unique est immunisé contre les attaques MITM.
- ❖ Par analyse médico-légale des attaques MITM

• Adresse IP du serveur

• Le certificat est-il auto-signé ?

• D'autres clients, ailleurs sur Internet, obtiennent-ils également le même certificat ?

• Le certificat est-il signé par une autorité de certification approuvée ?

- ☞ En utilisant l'authentification mutuelle, avec de nombreuses implémentations client et serveur, la confiance initiale n'est que confirmée par une vérification à sens unique entre le client et le serveur. Avec l'authentification mutuelle, la vérification se fait dans les deux sens entre le client et le serveur pour s'assurer que des communications légitimes sont échangées. La vérification peut être effectuée en utilisant des clés publiques et privé.

Cependant le reste des attaques ainsi que leurs solutions seront résumes dans ce tableau ci-dessous :

Tableau 3: les différentes types d'attaques/défenses du cloud computing

Attaques de Sécurité	Définition de l'attaque	Mécanisme utilise	Niveau de Sécurité/ Catégorie d'attaque	Conséquences de l'attaque	Techniques d'atténuation
Injection SQL Attaques	L'injection SQL est une vulnérabilité de sécurité Web qui permet à un attaquant d'interférer avec les requêtes qu'une application fait à sa base de données	Pour effectuer une attaque par injection SQL, un attaquant doit d'abord trouver les entrées utilisateurs vulnérables dans la page Web ou l'application Web L'attaquant peut créer du contenu d'entrée appelé une charge utile malveillante et constitue l'élément clé de l'attaque. Utiliser des commandes SQL	Niveau de base : Niveau d'application Attaques base sur l'authentification	Un accès autorisé à des données sensibles Modifier ou supprimer les données Compromettre le serveur sous-jacent ou une autre infrastructure dorsale.	Évitez d'utiliser du SQL généré dynamiquement dans le code. Utilisez une filtration appropriée pour désinfecter l'entrée utilisateur. Utilisation d'une architecture basée sur un proxy pour détecter et extraire dynamiquement les entrées de l'utilisateur.

Scripts intersites (XSS) Attaques	Les attaques XSS (Cross-Site Scripting) sont un type d'injection, dans lequel des scripts malveillants sont injectés dans des sites Web par ailleurs bénins et de confiance. Elle peut être classée en deux : **Attaques XSS stockées et Attaques XSS reflétées**	Les attaques XSS se produisent lorsque : Les données entrent dans une application Web via une source non approuvée, le plus souvent une requête Web. Les données sont incluses dans le contenu dynamique qui est envoyé à un utilisateur Web sans être validées pour le contenu malveillant.	Niveau de base : Niveau d'application Attaques base sur les plateformes	Les attaques XSS les plus graves impliquent la divulgation du cookie de session de l'utilisateur, permettant à un attaquant de détourner la session de l'utilisateur et de prendre le contrôle du compte Des vulnérabilités XSS	Utilisation du filtrage de contenu actif. Utilisation de la collaboration de navigateur. Utilisation de la technologie de prévention des fuites de données basée sur le contenu. Utilisation de la technologie de détection de vulnérabilité des applications Web. Approche basée sur un plan directeur pour minimiser la dépendance au navigateur Web. Configuration correcte de Secure Socket Layer (SSL). Utilisation d'un logiciel anti-malware.

Empoisonnement des cookies	L'empoisonnement des cookies est l'acte de manipuler ou de falsifier un cookie dans le but de contourner les mesures de sécurité ou d'envoyer fausses informations à un serveur.	Une attaque d'empoisonnement de cookie utilise des techniques d'ingénierie sociale pour manipuler et exploiter les cookies pour envoyer de fausses informations au serveur et enfreindre les murs de sécurité.	Niveau de base : Niveau Application Attaques base sur les données	Permettre de surveiller les détails importantes lies aux informations de navigateur d'un site Web spécifique Les pirates peuvent utiliser le cookie d'un site particulier, le modifier pour obtenir un accès non autorisé aux informations de l'utilisateur	Nettoyer régulièrement les données des cookies. En utilisant la politique de sécurité du navigateur. En créant des sessions et en utilisant d'autres mécanismes d'authentification

Attaques de zombies	L'attaque de zombies est l'une des attaques avancées dans L'environnement cloud qui vise à dégrade la performance et le débit du réseau informatique	Zombie est utilisé par un utilisateur malveillant pour lancer des attaques DoS ou DDoS grâce a un port de communication ouvert	Niveau de base : Niveau VM Attaques base sur les infrastructures	Le contrôle total du système par l'utilisateur malveillant Vulnérabilité des sites Web	Utiliser une meilleure authentification et autorisation. Utilisation du système de détection d'intrusion (IDS) / système de prévention d'intrusion (IPS).

En définitive, dans cette deuxième partie, nous avons fourni une base théorique sur la sécurité dans le CC, en présentant les différents types de menaces, les vulnérabilités, les différentes attaques et défenses, afin d'appliquer ses concepts à notre contexte. De ce fait, nous allons passer aux trois parties de la mémoire : Exploitation des solutions et mise en œuvre de la solution adoptée.

Troisième Partie : mise en œuvre et exploitation des solutions adoptées

Sommaire

III. Mise en œuvre et l'exploitation des solutions adoptées.

Dans cette troisième partie de la mémoire, nous présentons d'une part l'étude et conception des solutions et d'autre part.la mise en œuvre de la solution adoptée.

III.1 L'Etude et conception de la solution

La confidentialité des données est l'un des défis pressants de la recherche en cours dans le CC. Dès que la confidentialité devient une préoccupation, les données sont cryptées avant d'être sous-traitées à un fournisseur de services.

Dans cette section, il s'agira de définir d'abord les concepts généraux de la confidentialité des données dans le Cloud, ensuite l'étude des différentes solutions existentielles et la synthèse des solutions

III.1.1 Définition

La confidentialité des données est le processus de protection des données contre l'accès et la divulgation illégaux du serveur externalisé et des utilisateurs non autorisés. Cela se fait en chiffrant les données afin que seuls les utilisateurs autorisés puissent les déchiffrer. Grâce à cette méthode, une entreprise ou une organisation est en mesure d'empêcher que des informations hautement sensibles et vitales ne tombent entre les mains des mauvaises personnes tout en les rendant accessibles aux bonnes personnes [13].

III.1.2 Outils de confidentialité

Figure 19: Les Outils de la confidentialité [17w]

- **Chiffrement**

Le chiffrement est une méthode de transformation des informations pour les rendre illisibles pour les utilisateurs non autorisés à l'aide d'un algorithme. La transformation des données utilise une clé secrète (une clé de chiffrement) afin que les données transformées ne puissent être lues qu'en utilisant une autre clé secrète (clé de déchiffrement). Il protège les données sensibles telles que les numéros de carte de crédit en encodant et en transformant les données en texte chiffré illisible. Ces données chiffrées ne peuvent être lues qu'en les déchiffrant. La clé asymétrique et la clé symétrique sont les deux principaux types de chiffrement.

- **Contrôle d'accès**

Le contrôle d'accès définit des règles et des politiques pour limiter l'accès à un système ou aux ressources physiques ou virtuelles. C'est un processus par lequel les utilisateurs ont accès et certains privilèges aux systèmes, aux ressources ou aux informations. Dans les systèmes de contrôle d'accès, les utilisateurs doivent présenter des informations d'identification avant de pouvoir bénéficier d'un accès, comme le nom d'une personne ou le numéro de série d'un ordinateur. Dans les systèmes physiques, ces informations d'identification peuvent prendre de nombreuses formes, mais les informations d'identification qui ne peuvent pas être transférées offrent le plus de sécurité.

- **Authentification**

Une authentification est un processus qui garantit et confirme l'identité ou le rôle d'un utilisateur. Cela peut être fait de différentes manières, mais il est généralement basé sur une combinaison de

- ✓ Quelque chose que la personne possède (comme une carte à puce ou une clé radio pour stocker des clés secrètes),
- ✓ Quelque chose que la personne sait (comme un mot de passe),
- ✓ Quelque chose que la personne est (comme un humain avec une empreinte digitale).

L'authentification est la nécessité de toutes les organisations car elle permet aux organisations de sécuriser leurs réseaux en permettant uniquement aux utilisateurs authentifiés d'accéder à ses ressources protégées. Ces ressources peuvent inclure des systèmes informatiques, des réseaux, des bases de données, des sites Web et d'autres applications ou services basés sur le réseau.

- **Autorisation**

L'autorisation est un mécanisme de sécurité qui donne la permission de faire ou d'avoir quelque chose. Il est utilisé pour déterminer qu'une personne ou un système est autorisé à accéder aux ressources, sur la base d'une politique de contrôle d'accès, y compris des programmes informatiques, des fichiers, des services, des données et des fonctionnalités d'application. Il est normalement précédé d'une authentification pour la vérification de l'identité de l'utilisateur. Les administrateurs système se voient généralement attribuer des niveaux d'autorisation couvrant toutes les ressources système et utilisateur. Pendant l'autorisation, un système vérifie les règles d'accès d'un utilisateur authentifié et accorde ou refuse l'accès aux ressources.

- **Sécurité physique**

La sécurité physique décrit les mesures conçues pour empêcher l'accès non autorisé aux actifs informatiques tels que les installations, l'équipement, le personnel, les ressources et autres biens contre les dommages. Il protège ces actifs contre les menaces physiques, notamment le vol, le vandalisme, les incendies et les catastrophes naturelles.

III.1.3 Les 5 commandements pour la confidentialité dans le Cloud

Pour maintenir la confidentialité des clients, les fournisseurs de cloud doivent suivre les cinq commandements suivants :

- Connaissez vos exigences. Les clients doivent bien comprendre leurs données et leurs exigences en matière de sécurité. Les plates-formes basées sur le Cloud, comme les solutions déployées localement, peuvent fournir la sécurité dont les clients ont besoin si elles sont correctement configurées. Les clients doivent définir leurs besoins et examiner les capacités du fournisseur à fournir le niveau de sécurité approprié
- Votre régulateur est partout, alors suivez tous les commandements de votre régulateur. Les fournisseurs basés sur SaaS doivent être proactifs avec les agences de réglementation mondiales pour comprendre les mandats et les recommandations de meilleures pratiques. Ces politiques traiteront de la conservation et de l'accès aux données et doivent être intégrées dans les politiques internes de l'organisation, couvrant tous les employés et applications.
- Tu dois apprendre et enseigner. Les fournisseurs doivent continuellement éduquer et former leurs employés sur les procédures et les meilleures pratiques. La sensibilisation à la sécurité et la confidentialité des clients doivent être régulièrement discutées. Les simulations sont un excellent moyen de tester la réaction du personnel interne face à des scénarios contraires à l'éthique.
- Tu devrais avoir confiance, mais vérifier. Ayez confiance que vos employés sont honnêtes, mais vérifiez que les contrôles en place fonctionnent. La technologie peut auditer les pistes d'accès pour s'assurer que seuls les employés et les applications autorisés accèdent aux données. Recherchez de manière proactive les accès non autorisés aux données et examinez régulièrement les droits, à la fois des employés et des applications, pour ceux qui ont accès aux informations sensibles des clients. Les utilisateurs finaux devraient demander des audits sur place pour avoir confiance dans les contrôles que les fournisseurs de technologie ont mis en œuvre.

III.1.4 Etude des solutions proposées sur la confidentialité

Dans cette sous-section, il s’agira d’étudier les solutions proposées sur la confidentialité des données dans le CC. Parmi ces derniers, on étudiera quelques solutions tels que :

III.1.4.1 Schémas homomorphiques Fast Cloud – Paillier

La confidentialité des données externalisées est devenue une préoccupation majeure des consommateurs du Cloud. En règle générale, la plate-forme CC garantit la confidentialité des données pendant leur transfert par cryptage. Mais, le problème est que pour répondre à la demande d'un consommateur, le fournisseur de Cloud doit avoir accès aux données brutes [14]. Ainsi, ils sont constamment préoccupés par la confidentialité des données externalisées, surtout s'il s'agit de données sensibles et privées.

Le calcul sur des données cryptées peut être considéré comme un moyen efficace de surmonter ces préoccupations. En fait, les chercheurs ont suggéré une nouvelle forme de cryptage, appelée cryptage homomorphique (HE), qui peut effectuer des opérations sur des données cryptées sans découvrir aucune information sur des données simples. Cette propriété rend la méthode HE utile dans une large gamme d'applications de protection de la vie privée ; par exemple, les soins de santé électroniques, le vote à distance, etc.

III.1.4.1.1 Objectifs

Elle sert à protéger la confidentialité des données sensibles dans le CC en se basant sur le cryptage homomorphique (HE).

Le concept de technique HE a été découvert par Rivest et al, et c'était plus attrayant quand Gentry (2009) a inventé le premier schéma qui permet plusieurs calculs sur les textes chiffrés. Depuis lors, de nombreux schémas de chiffrement prenant en charge les propriétés homomorphes ont été proposés. Les schémas peuvent être divisés en deux groupes : un peu (SHE) et un cryptage homomorphique complet (FHE). Les schémas du groupe SHE supportent une propriété homomorphique (généralement un homomorphisme additif ou multiplicatif) ou même plus mais de manière limitée. Considérant que les schémas FHE supportent simultanément de nombreuses propriétés homomorphiques.

III.1.4.1.2 Fonctionnement

Le principe du chiffrement homomorphique est le suivant : Les données sont envoyées chiffrées par le client vers le Cloud. Les données sont ensuite l'objet d'un traitement (un calcul par exemple) qui va être effectué sur les données chiffrées, ce traitement générant un résultat. Ce résultat est lui-même chiffré, donc incompréhensible pour le prestataire du Cloud. Enfin le prestataire du Cloud va retourner le résultat au client qui le déchiffrera pour obtenir le résultat final. On peut donc dire qu'avec le chiffrement homomorphique, le résultat du traitement est le même que si les données n'avaient pas été chiffrées. Avec le chiffrement homomorphique, les données ne sont jamais en clair lors de leur transmission ni lors de leur traitement. Avec ce type

de chiffrement, le Cloud n'est plus seulement un espace de stockage sécurisé mais devient également un espace de calcul et de consultation sécurisé. Il va vraiment servir, non seulement à héberger l'information sensible, mais aussi à l'utiliser au sien d'elle. Seuls les résultats après traitements seront sortis pour être déchiffrés et exploités.

III.1.4.1.3 Architecture utilisée

Un modèle consommateur-fournisseur Cloud appliquant les schémas HE peut être illustré à la Figure suivante où :

Génération de clé : le consommateur Cloud génère à la fois la clé d'évaluation (ek) et clé privée (pk).

Chiffrement : le consommateur du Cloud crypte les textes en clair (m 1, m 2, …, m n) en dessous de pk. Il / elle envoie ensuite les textes chiffrés (ek) au fournisseur de Cloud sélectionné.

Stockage : Les textes chiffrés et (ek) sont stockés dans l'environnement du fournisseur de Cloud.

Demande : le consommateur demande au fournisseur de Cloud d'effectuer des opérations sur les textes chiffrés.

Évaluation : le fournisseur de Cloud exécute les opérations demandées par le consommateur, en utilisant (ek).

Réponse : Le fournisseur de Cloud renvoie au consommateur le résultat traité sous sa forme cryptée.

Déchiffrement : le consommateur déchiffre le résultat renvoyé sous sa clé privée (pk), le résultat déchiffré correspond au résultat des calculs exécutés sur les textes peints.

Toutes les communications entre le fournisseur de Cloud et le consommateur se font à l'aide d'un canal sécurisé pour garantir leur confidentialité et leur intégrité.

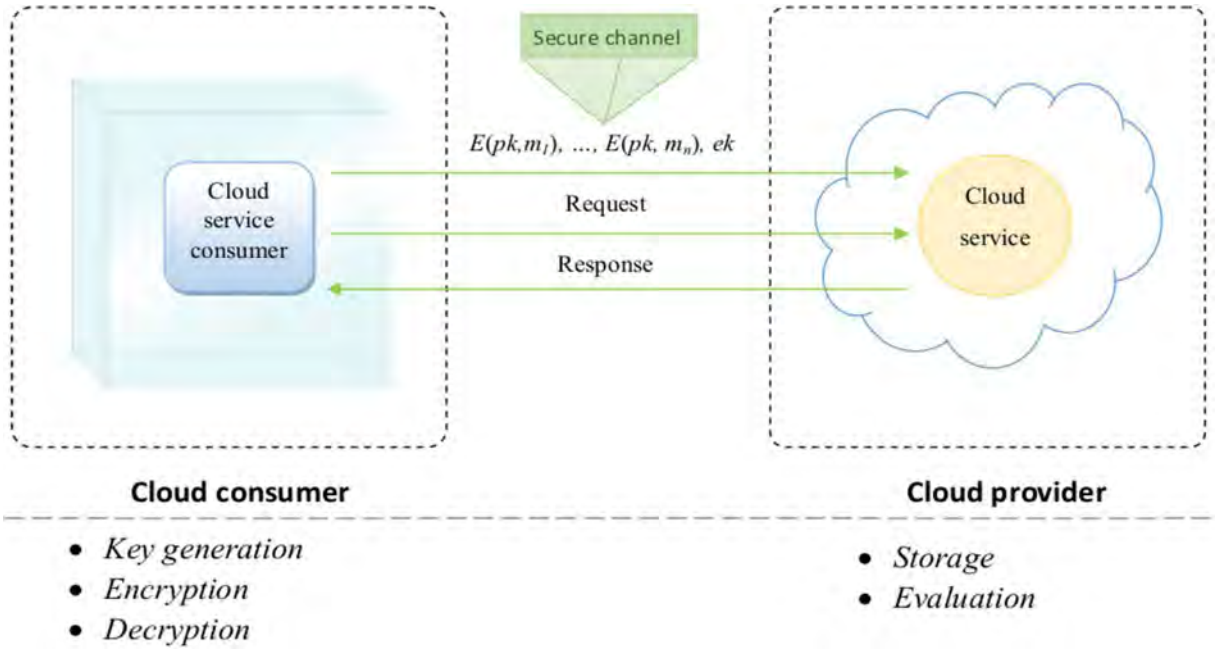

Figure 20:Modèle consommateur-fournisseur cloud appliquant HE [8]

III.1.4.1.4 Algorithme utilise

Le fast Cloud-Paillier se base sur les algorithmes suivants :

- ☞ Génération rapide de clés Cloud-Paillier

Le Fast Cloud – Paillier est basé sur la génération d'un composite entier n = p 1 … p k formé de k ≥ 2 distinct grands nombres premiers et sur la génération d'un entier g ∈ $\mathbb{Z}*n2$ satisfaisant g ≠ 1 + n, g ≡ 1 (mod n) et pgcd (L (g (mod n 2)), n) = 1, où ≥ 1 et 2 ≤ ≤. Nous montrons que si g = 1 + n, la variante proposée sera non probabiliste. Sur l'autre, nous montrons qu'en utilisant = min {p 1 - 1, …, p k - 1} est efficace et sécurisé. Le module (n) est rendu public et représente la clé d'évaluation. Les entiers g et sont rendues privées. Pour conserver approximativement le même temps de chiffrement que dans le schéma Cloud– Paillier, on précalcule la valeur g ≡ g n (mod n 2). D'autre part, pour obtenir une accélération de décryptage supplémentaire, on précalcule la valeur l = (L (g (mod n 2))) - 1 (mod n). On stocke ensuite les valeurs (g, l) en tant que partie de la clé privée. Le processus de génération est mis en évidence dans l'algorithme suivant :

Équation 1: Algorithme de génération rapide de clés Cloud-Paillier [8]

Input: $k \geq 2$ large and distinct primes $p_1, \ldots, p_k$ of equal bit-size.
Output: An evaluation key $ek = (n)$ and a private key $pk = (n, g, \alpha, g', l)$.

1: Compute: $n = \prod_{i=1}^{k} p_i$ and $\lambda = lcm(p_1 - 1, \cdots, p_k - 1)$.
2: Pick an integer α between 2 and λ.
3: Pick an integer $g \in \mathbb{Z}^*_{n^2}$ such that $g \neq 1 + \delta n$ for $\delta \geq 1$, $g^\alpha \equiv 1 \pmod{n}$ and $gcd(L(g^\alpha \pmod{n^2}), n) = 1$.
4: Compute: $g' \equiv g^n \pmod{n^2}$.
5: Compute: $l = (L(g^\alpha \pmod{n^2}))^{-1} \pmod{n}$.
6: Return (n) and (n, g, α, g', l).

☞ Cryptage rapide Cloud-Paillier

Équation 2: Algorithme de cryptage rapide Cloud-Paillier [8]

Input: A private key (n, g, α, g', l) and plaintexts $m \in \mathbb{Z}_n$.
Output: $c = E(pk, m)$.

1: Pick a random $r \in \mathbb{Z}_n$.
2: Compute $c \equiv g^m \cdot (g')^r \pmod{n^2}$.
3: Return c.

☞ Décryptage rapide Cloud-Paillier

Équation 3: Algorithme de décryptage rapide Cloud-Paillier [8]

Input: A private key (n, g, α, g', l) and the returned ciphertext C.
Output: $M = (m_1 + \ldots + m_j) \in \mathbb{Z}_n$.

1: Compute $M \equiv L(C^\alpha \pmod{n^2}) \cdot l \pmod{n}$.
2: Return M.

III.1.4.2 MONcrypt

L'obscurcissement des données est une forme de masquage des données où les données sont délibérément brouillées pour empêcher l'accès non autorisé à des matériaux sensibles. Il en résulte des données inintelligibles ou déroutantes [15].

Les techniques d'obfuscation des données sont utilisées pour empêcher l'intrusion de données privées et sensibles, telles que les dossiers de santé électroniques (DSE). Cependant, des problèmes découlent d'une incapacité à empêcher vigoureusement les attaques de sécurité (Data Obfuscation, 2010).

III.1.4.2.1 Objectif

Elle sert à assurer la confidentialité des données externalisées dans le stockage Cloud en se basant sur une technique d'obfuscation. L'obscurcissement est un processus de masquage du texte original en texte non pertinent sans utiliser de clé contrairement au cryptage.
Elle utilise la clé pour la désobfuscation et applique seulement sur les données numériques.

III.1.4.2.2 Méthodologie de fonctionnement

Les données externalisées sont obscurcies avant d'être téléchargées vers le stockage Cloud. La technique d'obfuscation proposée est appliquée uniquement sur des données numériques. La figure suivante montre la conception de la technique proposée. Le module d'obfuscation est utilisé pour masquer les données des utilisateurs. Une fois que les données sont obscurcies, elles sont transférées vers le stockage Cloud. Pendant le module d'obscurcissement, pour le message d'origine, une valeur de comptage est générée. Cette valeur est conservée du côté des utilisateurs sous forme de métadonnées. Pour récupérer les données du stockage en nuage, le module de désobscurcissement est utilisé pour convertir le texte masqué en texte brut original du côté des utilisateurs. Le module de désobfuscation utilise les informations de métadonnées pour obtenir le texte d'origine.

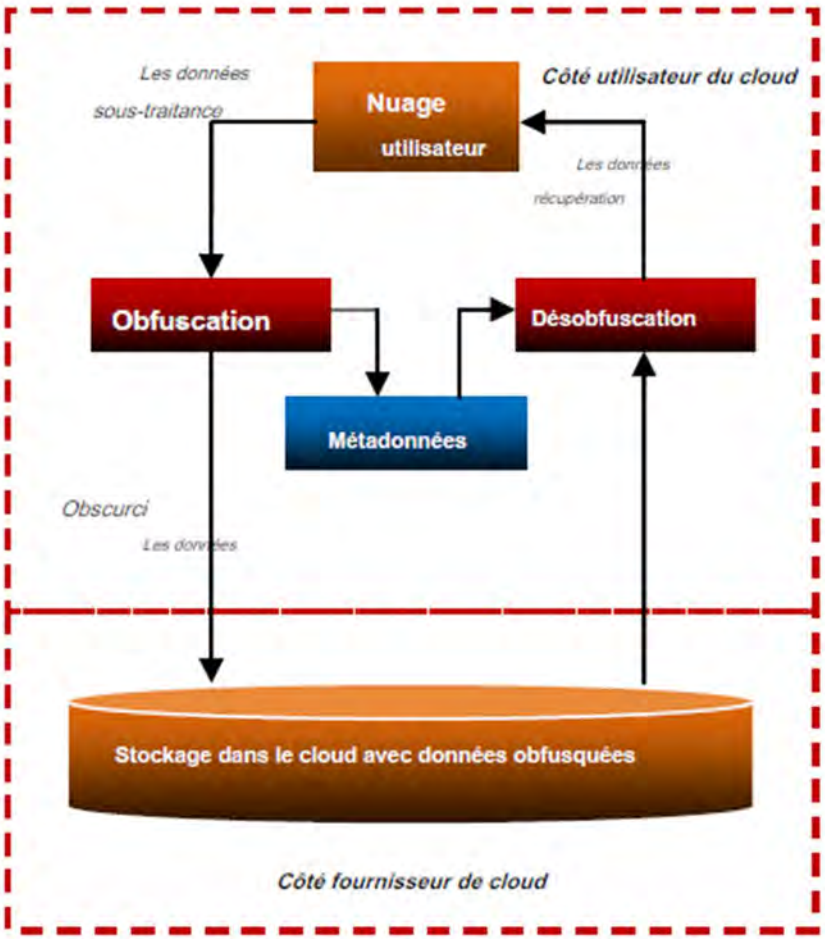

Figure 21: Scénario d'obfuscation et de désobscurcissement [15]

III.1.4.2.3 Algorithme

Elle a un algorithme pour l'obfuscation et la désobscurcissement. Généralement, l'obscurcissement n'utilise aucune clé pour masquer les données des utilisateurs. Mais, la technique proposée utilise une clé pour la désobfuscation. Pendant le processus d'obfuscation, une valeur de comptage est générée pour le texte original. Cette valeur de comptage est utilisée comme clé pour la désobfuscation. La clé est conservée en tant que métadonnées côté client. Elle engendre deux algorithmes suivants :

- ☞ Algorithme 1 pour l'Obfuscation
- ☞ Algorithme 2 pour la Désobscurcissement

L'algorithme 1 représente l'algorithme d'obfuscation. Cet algorithme est exécuté dans le module d'obscurcissement. Il est appelé lorsque les utilisateurs téléchargent des données sur le stockage Cloud. Au départ, les valeurs de texte brut sont organisées sous forme de tableau de valeurs numériques T = T (1), t (2), T (3) … T (n). La fonction mathématique à savoir pow () est appliquée sur le texte brut T (i). La fonction pow () est utilisée pour trouver une valeur carrée T (i) (D (i) = pow (T (i), 2)). [36] D (i) la valeur est divisée par 256 pour trouver le compter (i)

valeur et aussi pour obtenir la valeur de rappel dans RD (i), compter (i) représente le nombre de fois D (i) est divisé par 256. RD (i) la valeur est comprise entre 0 et 255. Enfin, le texte obscurci est obtenu en convertissant le RD (i) en valeur de caractère ASCII. Les données de utilisateurs sont transmises à la fin de ce module d'obscurcissement.

Équation 4: Algorithme d'Obfuscation [15]

Algorithm 1 Obfuscation

```
obfuscation_digits(T)
1  start
2  T ← array of plaintext
3  N ← sizeof (T)
4  for i ← 1 to n
            //find square value of plain text value
   D(i) ← pow(T(i),2)
       count(i) ← D(i)/256
       RD(i) ← D(i)%256
            //count ← no. of time RD divided by 256
   end for
5  Convert the RD(i) into ASCII code C
6  C ← array of cipher Text
7  end
```

L'algorithme 2 est utilisé pour la désobfuscation. Cet algorithme est exécuté dans le module de désobfuscation. Il est appelé lorsque les données sont extraites du stockage Cloud. Pour obtenir le texte original complet, les données doivent être désobscurcies côté client à l'aide des détails des métadonnées. C'est exactement le processus inverse d'obfuscation décrit précédemment dans l'algorithme n ° 1.

Équation 5 Algorithme Désobfuscation [15]

Algorithm 2 De-obfuscation

```
deobfuscation_digit(C)
1  start
2  C ← array of ciphertext
3  N ← sizeof(C)
   //find the square of AC
4  for i ← 1 to n
   DC(i) ← numerical value for C(i)
   AC(i) ← count(i)*256 + DC(i)
   T(i) ← sqrt(AC(i))
5  end for
6  T ← array of plaintext
7  end
```

III.1.4.3 Utilisation d'Intel SGX

L'un des problèmes de sécurité dans les systèmes Cloud est la protection des données des utilisateurs contre les attaques du fournisseur de services Cloud. Actuellement, la confidentialité des données utilisateur des services Cloud n'est assurée que par la confiance dans le fournisseur de services cloud. Cela signifie qu'il ne peut être garanti que le fournisseur de services Cloud n'accèdera pas aux données des utilisateurs privés qui ont été stockées dans le cloud. Malheureusement, la société de fournisseur de services Cloud a techniquement accès à toute date privée de tout utilisateur, car elle a un accès illimité à tout le matériel et les logiciels fonctionnant dans le système Cloud.

Ce problème peut être résolu avec succès en utilisant la technologie matérielle de protection des données utilisateur dans les services Cloud au niveau matériel le plus bas dans le noyau CPU. À partir de la sixième génération (Skylake), la technologie Software Guard Extensions (SGX) est implémentée dans les processeurs Intel Core. Cette technologie introduit un nouveau mode d'exécution de code dans le processeur, un mode de protection de la mémoire et un ensemble de nouvelles instructions qui assurent le fonctionnement de SGX. Intel appelle le SGX un bac à sable inversé, c'est-à-dire qu'au lieu d'essayer d'isoler les logiciels potentiellement malveillants ou non fiables de l'ensemble du système, le programme développé peut isoler son code et ses données de l'ensemble du système en utilisant la technologie SGX. Cette technologie est principalement destinée aux développeurs d'applications qui ont besoin de protéger le code source et les données contre les accès et les altérations non autorisés, même si l'application malveillante s'exécute à un niveau de privilège supérieur. Du point de vue du développeur,

l'enclave représente une bibliothèque dynamique ordinaire. L'idée principale de cette technologie est de créer une enclave logicielle, une zone de mémoire protégée, dont l'accès est contrôlé par le processeur et n'est autorisé qu'à l'application utilisateur qui a créé l'enclave [16].

III.1.4.3.1 Objectif

L'objectif de l'introduction de la technologie Intel SGX est de permettre de fournir une protection de haut niveau aux parties de l'application qui ne doivent pas du tout être accédées, ce qui est idéal pour protéger les données des utilisateurs dans les systèmes Cloud.

Il est proposé pour une utilisation en technologie SGX dans le domaine des technologies Cloud comme suit : les utilisateurs reçoivent des machines virtuelles PaaS ou IaaS en fonction de leurs besoins. Du côté du fournisseur, il devrait y avoir des équipements prenant en charge Intel SGX. Du côté de l'utilisateur, il est nécessaire de développer une pile applicative qui fonctionnera dans l'enclave afin d'assurer la confidentialité des données. Grâce à cette approche, les données utilisateur restent inaccessibles au fournisseur de Cloud.

Une autre option pour cette technologie est le développement d'un service cloud de type SaaS pour stocker, traiter et échanger différents documents.

III.1.4.3.2. Fonctionnement

L'application développée à l'aide de la technologie Intel SGX se compose de deux parties : non protégée et protégée (enclave). Au démarrage, la partie non protégée crée une enclave dans la mémoire protégée, transfère le code et les données de la mémoire non protégée vers l'enclave et l'initialise en effectuant des contrôles d'intégrité. Seules les fonctions protégées voient les données de l'enclave en clair. Tout autre accès externe, y compris par le système d'exploitation, est interdit, en raison du cryptage total des données et du code. Les enclaves sont des zones de mémoire remplies de pages cryptées de code et de données. Les enclaves sont déchiffrées directement sur le processeur central lorsque toutes les vérifications sont terminées. Cela protège complètement contre la menace de fuite d'informations sous forme ouverte vers la RAM ou d'autres périphériques d'E / S.

Avec cette approche, la surface d'attaque ou base de calcul de confiance (TCB) est réduite à l'application et au processeur, qui exécute son code

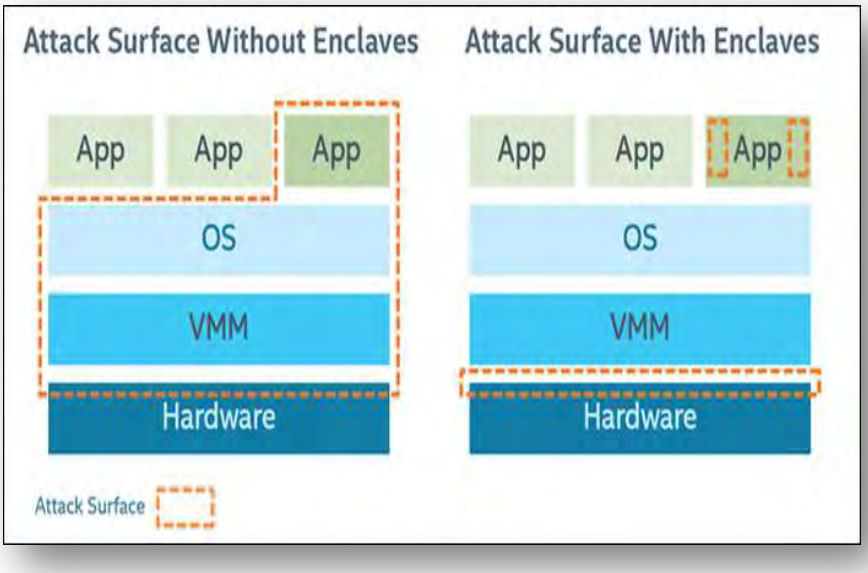

Figure 22: Comparatif de la surface d'attaque avec et sans enclave [18w]

Ainsi, quels que soient les privilèges dont dispose le sujet, y compris les privilèges du noyau, du VMM, de l'OS, il ne pourra pas lire ou écrire des pages de mémoire enclave.

III.1.4.3.3 Architecture

Les enclaves se trouvent dans la mémoire protégée appelée Enclave Page Cache (EPC). Cette mémoire est utilisée à la fois pour stocker les pages de l'enclave elle-même et pour les différentes structures nécessaires aux opérations avec l'enclave. La zone de mémoire avec l'EPC configure le BIOS et le réserve au processeur. Cette zone de mémoire est appelée mémoire réservée au processeur (PRM). Un ensemble d'attributs est défini pour chaque page EPC. Ces attributs sont stockés dans une structure spéciale appelée carte de cache de page d'enclave (EPCM). L'accès aux adresses EPC memory est contrôlé au niveau matériel par le cœur du processeur. Lorsqu'il y a une tentative d'accès à l'enclave, il est vérifié si les données du processus appelant sont à l'adresse donnée. Ensuite, les privilèges de la fonction sont vérifiés et l'accès requis n'est fourni qu'une fois toutes les vérifications terminées avec succès. Sinon, une erreur de segmentation se produit.

La protection contre l'accès direct à la mémoire physique est mise en œuvre par le cryptage de la mémoire EPC, c'est-à-dire que lorsqu'il est connecté au module DRAM, l'attaquant ne pourra lire que des données chiffrées. La clé de cryptage est stockée dans la mémoire interne du CPU et est générée de manière aléatoire à chaque fois que l'ordinateur est mis sous tension. Le

mécanisme qui protège la mémoire EPC est appelé le moteur de chiffrement de la mémoire (MEE). Ce mécanisme est une unité matérielle qui protège les données lors de la communication entre le processeur et la mémoire et assure la confidentialité et l'intégrité des données. Afin d'exécuter des instructions à partir de la mémoire de l'enclave, le processeur reçoit des données via le contrôleur de mémoire, qui comprend que des données sont demandées à partir de la zone de mémoire cryptée (zone MEE) et qu'il est nécessaire de décrypter ces données. Ensuite, les instructions sont envoyées au processeur et stockées dans le cache du processeur déjà sous forme décryptée.

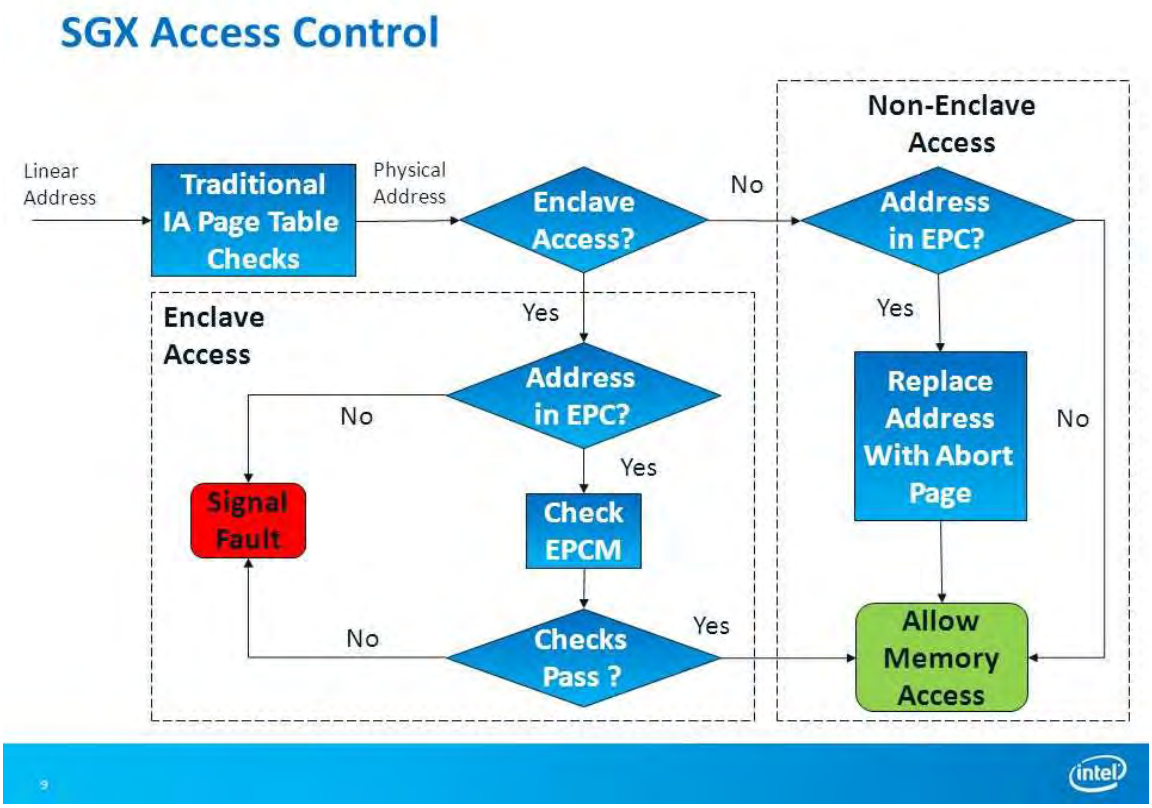

Figure 23: Contrôle d'accès enclave. [19w]

III.1.4.3.4 L'attestions et l'échange de clés

Avant que le client ne soumette ses données personnelles à l'enclave qui s'exécute dans le Cloud, il est nécessaire de vérifier l'intégrité de l'enclave et de s'assurer que la plate-forme sur laquelle s'exécute l'enclave prend en charge Intel SGX. Dans cette technologie, le mécanisme d'attestation est implémenté. L'attestation est un mécanisme par lequel une partie du système peut vérifier que le code qui est exécuté en toute sécurité dans l'enclave est celui qui doit être exécuté et que la plate-forme sur laquelle l'enclave s'exécute prend en charge Intel SGX.

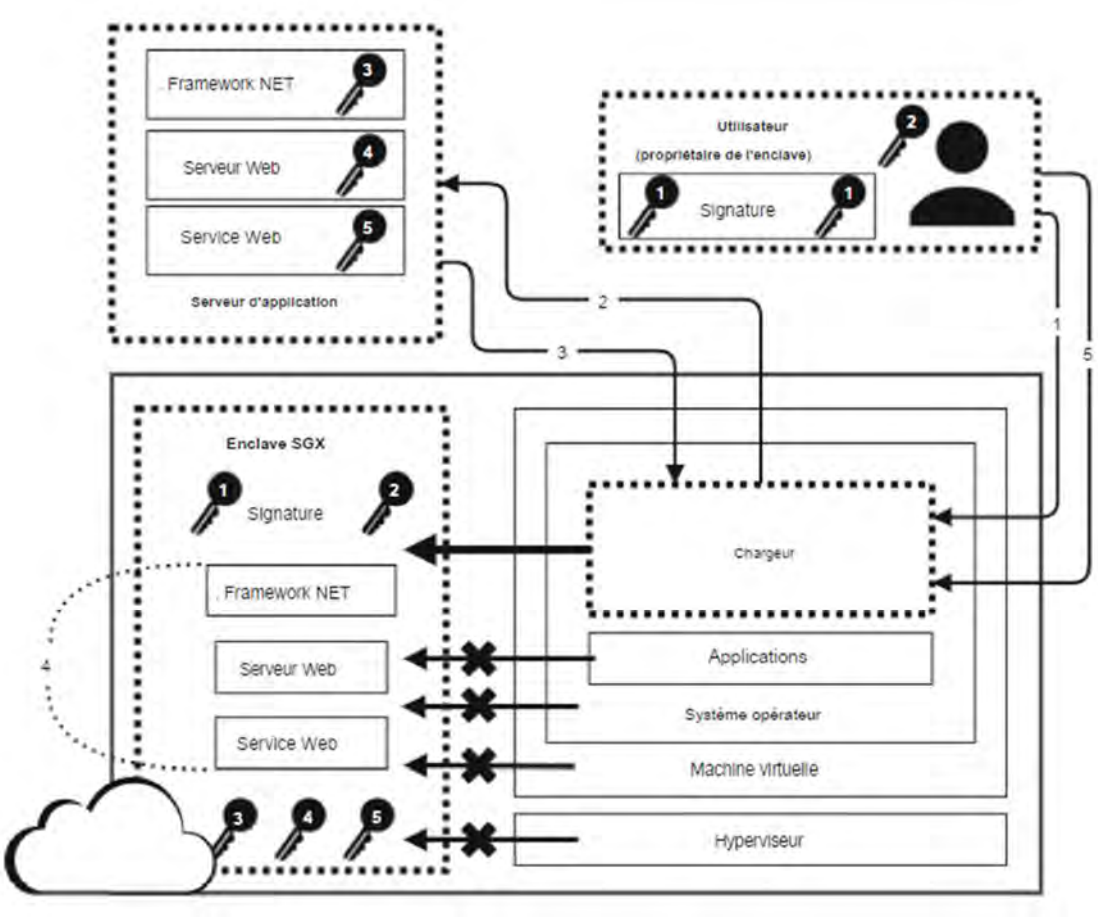

Figure 24: SGX avec l'utilisation des services cloud [16]

Afin d'utiliser ses propres applications, le client doit les signer et les télécharger sur le serveur d'applications du système Cloud. La connexion entre l'utilisateur et le service cloud est protégée par la clé de session. L'étape d'utilisation du service cloud représentée sur la figure 6 comprend les étapes suivantes :

(1) L'utilisateur envoie une demande au chargeur pour démarrer le service WEB.

(2) Le chargeur accède au serveur d'applications pour obtenir les applications nécessaires.

(3) Le serveur envoie les applications.

(4) Le chargeur crée des enclaves dans lesquelles chacune des applications reçues est placée. Lors de l'initialisation des enclaves, la signature et l'intégrité des données d'application sont vérifiées. Si toutes les vérifications réussissent, l'enclave est lancée et le client a accès au service WEB.

(5) Les données sécurisées sont échangées avec le service WEB à l'aide de la clé de session définie précédemment.

Tous les mécanismes, tels que le cryptage de la mémoire, le contrôle d'intégrité et le contrôle d'accès, sont exécutés sur le processeur, ce qui permet d'introduire facilement Intel SGX dans un système cloud déjà configuré.

III.1.5 Synthèse et comparaison des solutions proposées

Bien comprendre les différentes caractéristiques des solutions de confidentialité des données dans CC est essentiel pour choisir la solution la plus adaptée à son besoin. Cette synthèse permettra d'avoir une vision globale des solutions proposées en mettant en avant plusieurs critères. Le tableau ci-dessous présente les différents aspects de la cryptographique en fonction des solutions proposées sur la confidentialité des données dans CC :

Tableau 4: Les aspects de la sécurité par rapport aux solutions proposées

Solutions	Propriétés homomorphes	Chiffrement (Complexité)	Déchiffrement (Complexité)	Nombre d'opérations	Nombre de clés cryptographiques
Fast Cloud – Paillier	+(additif)	Pour chiffrer m € ZN, choisir aleatoirement r € Z*N. $c = g^m r^N \bmod N^2$	$m = \frac{L_N\left(c^{\lambda(N)} \bmod N^2\right)}{L_N\left(g^{\lambda(N)} \bmod N^2\right)} \bmod N$ Notons que $L_N\left(g^{\lambda(N)} \bmod N^2\right)$ est inversible du moment où on a choisi qu'il soit premier avec N.	6 Opérations pour la génération de clé Cloud-Paillier 3 Opérations pour le cryptage rapide Cloud-Paillier 2 Opérations pour le décryptage rapide Cloud-Paillier	Utilise deux clés de cryptographiques : 1. une clé d'évaluation → (ek) 2. une clé privée → (pk)
MONcrypt	Pas cryptage	Chiffre les données numériques par l'obfuscation	Déchiffre les données numériques par désobfuscation	6 opérations pour l'Obfuscation 6 opérations pour la Désobscurcissement	Utilise une seule clé cryptographique → une clé pour la désobfuscation.
Utilisation d'Intel SGX	+(additif) et Multiplicatif	Cryptage total des données et du code en utilisant la technologie Intel SGX	Les enclaves sont déchiffrées directement sur le processeur central lorsque toutes les vérifications sont terminées.	Pas d'opérations	Une seule clé est utilisée pour protège la connexion entre le client et le service cloud. Ce dernier est appelé la clé de session.

Puisque dans chaque solution il y'a un objectif vise, dans l'étude suivant, on va essayer de donner les avantages et les inconvénients des différentes solutions proposées sur la confidentialité des données dans le CC :

Tableau 5: Avantages et Inconvénients des solutions proposées

Solutions	Avantages	Inconvénients	Remarques
Fast Cloud – Paillier	-La dureté de la factorisation de grands entiers composites et Résiduosité composite décisionnelle dure (HDCRA). - Renforcé le seau principal cryptosystème de Paillier au niveau de la sécurité - Offrir une grande vitesse de décryptage en utilisant un entier -Possède les propriétés homomorphes additifs ou multiplicatifs -Figure aussi parmi les schémas les plus efficaces (facteur d'expansion = 2) - Possibilité d'agréger les données des utilisateurs sans avoir besoin de les décrypter -Chiffrement sémantiquement sécurisé - le cloud devient en plus un espace de calcul et de consultation sécurisé	-Ces algorithmes mis en œuvre sont actuellement très couteux en temps de calcul, et généralement implantes sous forme logicielle. - La difficulté du chiffrement homomorphe est de maintenir le "bruit numérique" -Il ne permet pas, par exemple, de consulter une base de données chiffrée pour obtenir le résultat souhaité en clair. -Limité à certains types d'opérations en raison de problèmes d'efficacité -lenteur de décryptage si l'entité n'est pas un entier	- Le schéma Fast Cloud – Paillier est inspiré d'une variante de Paillier -L'application phares pour le vote électronique (par Internet) et la monnaie électronique -Le chiffrement « cherchable » offre une solution pour consulter une base de données chiffrée
	-l'obscurcissement n'utilise aucune clé pour masquer les données des utilisateurs -La clé désobfuscation est conservée en tant que métadonnées côté client.	-Incapacité à empêcher vigoureusement les attaques de sécurité -S'appliquer uniquement sur des données numériques.	- Il existe une autre technique appelée AROcrypt qui est utilisée pour les données non numériques - Empêcher l'intrusion de données privées et sensibles, telles que les

MONcrypt	-Compresse la taille du texte brut en convertissant sa valeur en caractère 8 bits sans altérer son fonctionnement. -la moins coûteuse en termes financiers -La plus facile à mettre en place en termes d'architecture -Totalement transparente pour l'utilisateur et les développeurs. -Le temps nécessaire à l'obscurcissement est en millisecondes. -Rendre le binaire plus difficile à détecter, en modifiant sa signature.	-Assurer uniquement la confidentialité des données externalisées cote utilisateur -Ne permet plus de réaliser les opérations réflexives sur le code générique -L'augmentation de la complexité algorithmique et de la modification des structures de données augmentent le temps d'exécution. -La qualité (algorithmique) du code source baisse considérablement et peut être un frein à la certification par des organismes tiers.	dossiers de santé électroniques (DSE). -Utiliser pour les cartes à puce
Utilisation d'Intel SGX	-S'appuie sur un pilote et/ou le système d'exploitation fournis par Intel pour accéder aux instructions Intel SGX et à la gestion des ressources. -l'accès est contrôlé par le processeur et n'est autorisé qu'à l'application utilisateur qui a créé l'enclave - Déchiffrement se fait directement dans le processeur central lorsque toutes les vérifications sont terminées - la surface d'attaque ou base de calcul de confiance (TCB) est réduite -l'utilisation de primitives cryptographiques résistantes aux erreurs -Reste protégé même lorsque le BIOS, le VMM, le SE et les pilotes sont compromis	-Destinée principalement aux développeurs d'applications -Intégrer uniquement les équipements Intel SGX -Difficile à mettre en œuvre -l'hyperviseur ne nécessite aucune modification -Manipulation de la tension des puces pour déclencher des erreurs de calcul de manière contrôlée. -Ne résiste pas aux attaques par injection de fautes appelée Plundervolt.	- Créer son propre infrastructure cloud -selon les recommandations Intel SGX -Préserver la confiance du côté de l'utilisateur

A présent, on va passer au dernier tableau qui consiste la partie choix de la solution.

Apres avoir faire l'étudie des différentes solutions en présentant leurs points forts et faibles, leurs algorithmes de chiffrement et déchiffrement ainsi que leur fonctionnement, on peut dire la solution 3, c'est à dire la solution Intel SGX engendre en dort de son avantage, l'avantage des deux autres solutions.

Ceux-ci je résume dans le tableau ci-dessous :

Tableau 6: Comparaison des solutions adoptées

Problèmes	Solutions
Accès aux données sensibles par le fournisseur	Solution 3
Calcul sur des données cryptées	Solutions [1, 3]
Cryptage des données en cours d'exécution	Solution 3
Cryptage des données en transition	Solutions [1, 2, 3]
Cryptage des données au repos	Solutions [1, 2, 3]
Obscurcissement des données	Solutions [2, 3]
Problème de rechiffrement direct	Solution 3

Donc cette solution sera adoptée pour la partie mise en œuvre.

III.2 Mise en œuvre de la solution adoptée

Dans cette partie, il s'agira de déployer la solution Intel SGX dans notre infrastructure Cloud. Pour cela nous allons présenter les prérequis, ensuite, l'installation de la technologie Intel SGX et enfin de tester le bon fonctionnement de ce dernier suivant des tests fonctionnels.

III.2.1 Prérequis

Pour utiliser Intel SGX dans une machine virtuelle, vous devez répondre aux exigences suivantes :

- Le système hôte doit prendre en charge Intel SGX.
- Intel SGX doit être activé, soit explicitement dans le BIOS.
- Disposer d'un accès administrateur (root) à votre serveur via SSH

- Ubuntu 18.04 ou équivalent installé sur le serveur

Tableau 7: Environnements de fonctionnement des solutions proposées

	Système d'exploitation utilise	Langage de programmation	Année de production
Utilisation Intel SGX	Implémentée dans les processeurs Intel Core, Linux, Windows	Implémentée en C/C++	2017

III.2.2 Procédure d'installation

Dans la machine virtuelle, avant d'effectuer les installations, préparons notre système.

Pour cela effectuons les commandes suivantes :

*sudo apt update

*sudo apt -y upgrade

*sudo apt -y dist-upgrade

*sudo reboot

A partir de cela, passons au but du sujet.

Nous allons maintenant construire et installer notre noyau dans le cadre de ce processus.

Installons-les packages logiciels nécessaires à la construction du noyau et de QEMU :

```
root@ubuntu:~# sudo apt install fakeroot libelf-dev build-essential libncurses-d
ev flex bison libssl-dev libfdt-dev libncursesw5-dev pkg-config libgtk-3-dev lib
spice-server-dev libssh-dev python3 python3-pip
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances
Lecture des informations d'état... Fait
Note : sélection de « libncurses5-dev » au lieu de « libncurses-dev »
python3 est déjà la version la plus récente (3.6.7-1~18.04).
python3 passé en « installé manuellement ».
Les paquets supplémentaires suivants seront installés :
  adwaita-icon-theme at-spi2-core autoconf automake autopoint autotools-dev
  binutils binutils-common binutils-x86-64-linux-gnu cpp cpp-7
  dconf-gsettings-backend dconf-service debhelper dh-autoreconf dh-python
  dh-strip-nondeterminism dpkg-dev fontconfig fontconfig-config
```

Figure 25:installation des packages pour la construction du noyau

Clonez le référentiel kvm-sgx. Cela prend plusieurs minutes, même sur une connexion haut débit / haut débit.

```
root@ubuntu:~/drame# git clone https://github.com/intel/kvm-sgx
Clonage dans 'kvm-sgx'...
remote: Enumerating objects: 8013855, done.
remote: Counting objects: 100% (7267/7267), done.
remote: Compressing objects: 100% (2842/2842), done.
remote: Total 8013855 (delta 5123), reused 5462 (delta 4417), pack-reused 800658
8
Réception d'objets: 100% (8013855/8013855), 2.12 GiB | 1.01 MiB/s, fait.
Résolution des deltas: 100% (6756464/6756464), fait.
Extraction des fichiers: 100% (71501/71501), fait.
root@ubuntu:~/drame#
```

Figure 26: Construction du KVM-SGX

Avec cet ensemble de variables Shell pratiques, vous êtes prêt à configurer le noyau.

```
root@ubuntu:~/drame/kvm-sgx# make $opt menuconfig
  HOSTCC  scripts/basic/fixdep
  UPD     scripts/kconfig/mconf-cfg
  HOSTCC  scripts/kconfig/mconf.o
  HOSTCC  scripts/kconfig/lxdialog/checklist.o
  HOSTCC  scripts/kconfig/lxdialog/inputbox.o
  HOSTCC  scripts/kconfig/lxdialog/menubox.o
  HOSTCC  scripts/kconfig/lxdialog/textbox.o
  HOSTCC  scripts/kconfig/lxdialog/util.o
  HOSTCC  scripts/kconfig/lxdialog/yesno.o
  HOSTCC  scripts/kconfig/confdata.o
  HOSTCC  scripts/kconfig/expr.o
  LEX     scripts/kconfig/lexer.lex.c
  YACC    scripts/kconfig/parser.tab.[ch]
  HOSTCC  scripts/kconfig/lexer.lex.o
```

Figure 27: Compilation du noyau

Pour activer la prise en charge d'Intel SGX dans les invités KVM, vous devez activer la fonctionnalité principale du noyau à partir du menu **Type de processeur et fonctionnalités**. Faites défiler jusqu'à **Software Guard eXtensions (SGX)** et assurez-vous qu'il est sélectionné. Il peut être désactivé par défaut si vous construisez à partir d'une nouvelle arborescence source. Lorsque cet élément est sélectionné, le menu se développe pour révéler la **virtualisation de Software Guard eXtensions (SGX)**. Sélectionnez ceci également

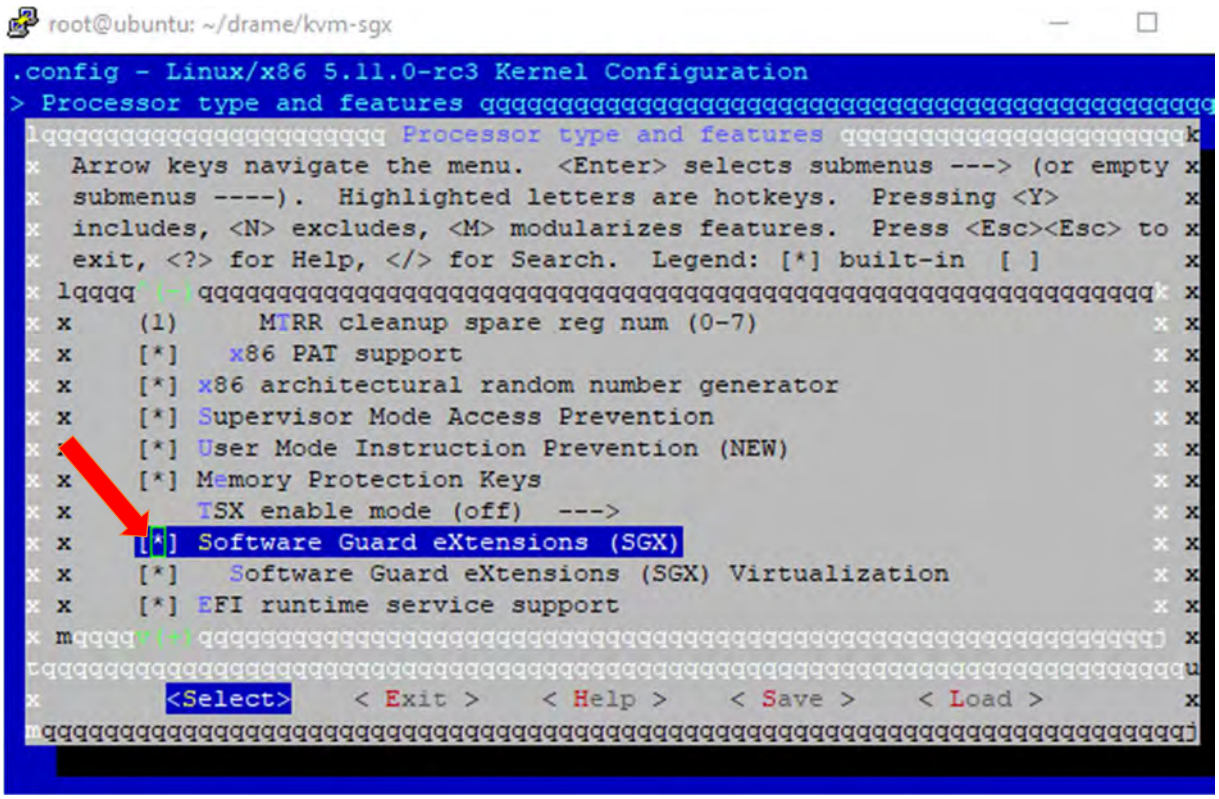

Figure 28: Activation Intel SGX sur le noyau KVM

Ensuite, vous devez vous assurer que la virtualisation KVM est activée. Dans le menu de niveau supérieur, accédez au menu Virtualisation et assurez-vous que les fonctionnalités suivantes sont sélectionnées.

- Prise en charge de la machine virtuelle basée sur le noyau (KVM)
- Prise en charge des processeurs KVM pour Intel (et compatibles)

Ceux-ci devraient déjà être activés en tant que modules chargeables (un «M» au lieu d'un astérisque «*»), vous ne devriez donc rien changer ici.

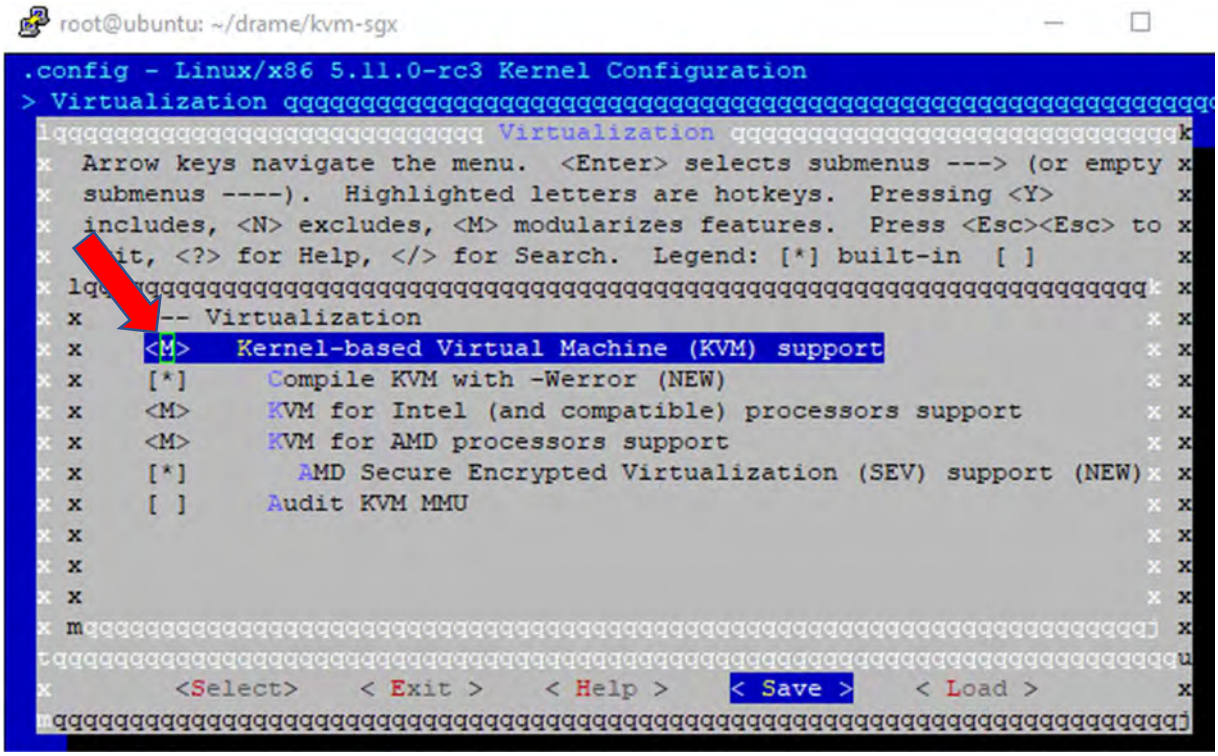

Figure 29: Assurance des fonctions de virtualisation

Cliquez OK pour terminer.

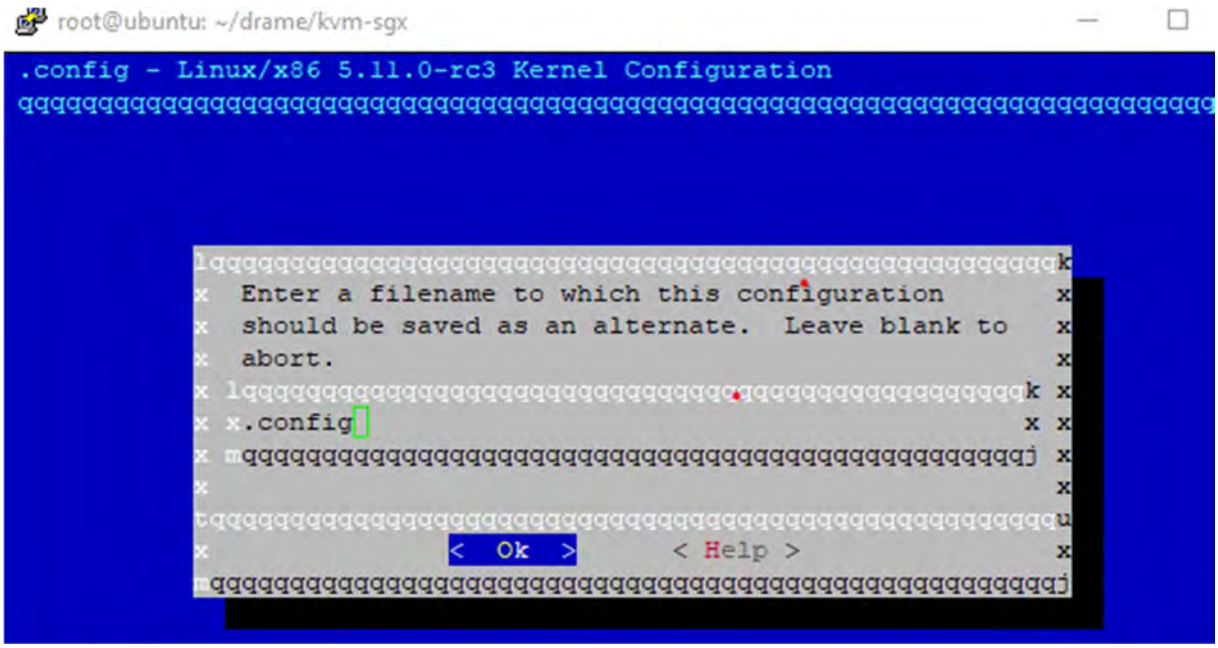

Figure 30: terminaison de l'activation

Enregistrez vos paramètres et **quittez** l'écran de configuration du noyau.

L'étape suivante consiste à compiler le noyau. Une première construction à partir de l'arborescence source est un processus long qui peut prendre quelques heures, selon votre matériel.

```
root@ubuntu:~/drame/kvm-sgx# make $opt
Makefile:644: include/config/auto.conf: Aucun fichier ou dossier de ce type
Makefile:688: include/config/auto.conf.cmd: Aucun fichier ou dossier de ce type
  SYNC    include/config/auto.conf.cmd
  HOSTCC  scripts/kconfig/conf.o
  HOSTLD  scripts/kconfig/conf
```

Figure 31: Compilation du noyau

Apres avoir installer le noyau avec KVM pour le fournisseur cloud, passons maintenant à l'installation de la pile SGX cote utilisateur.

Il faut maintenant installer le driver Intel et SDK pour pouvoir développer et exécuter des applications SGX. En premier lieu, il faut installer quelques dépendances :

```
[[ -d $BASE_DIR ]] || sudo mkdir -p $BASE_DIR && sudo chown `whoami` $BASE_DIR
```

Figure 32: création de la base de données

Ensuite, téléchargez, créez et installez la pile logicielle SGX :

```
--2021-04-25 01:36:00--  https://download.01.org/intel-sgx/linux-2.6//SHA256SUM_
prebuilt_2.6.txt
Résolution de download.01.org (download.01.org)… 23.10.68.237, 2a02:26f0:7900:29
3::4b21, 2a02:26f0:7900:283::4b21
Connexion à download.01.org (download.01.org)|23.10.68.237|:443… connecté.
requête HTTP transmise, en attente de la réponse… 200 OK
Taille : 181 [text/plain]
Enregistre : «./SHA256SUM_prebuilt_2.6.txt»

SHA256SUM_prebuilt_ 100%[===================>]     181  --.-KB/s    ds 0s

2021-04-25 01:36:01 (5,16 MB/s) - «./SHA256SUM_prebuilt_2.6.txt» enregistré [181
/181]

/opt/intel/linux-sgx /opt/intel/linux-sgx
prebuilt_ae_2.6.tar.gz: Réussi
optimized_libs_2.6.tar.gz: Réussi
/opt/intel/linux-sgx
root@ubuntu:/opt/intel/linux-sgx#
```

Figure 33: Installation des piles SGX

Téléchargé le drive du pilote lunix

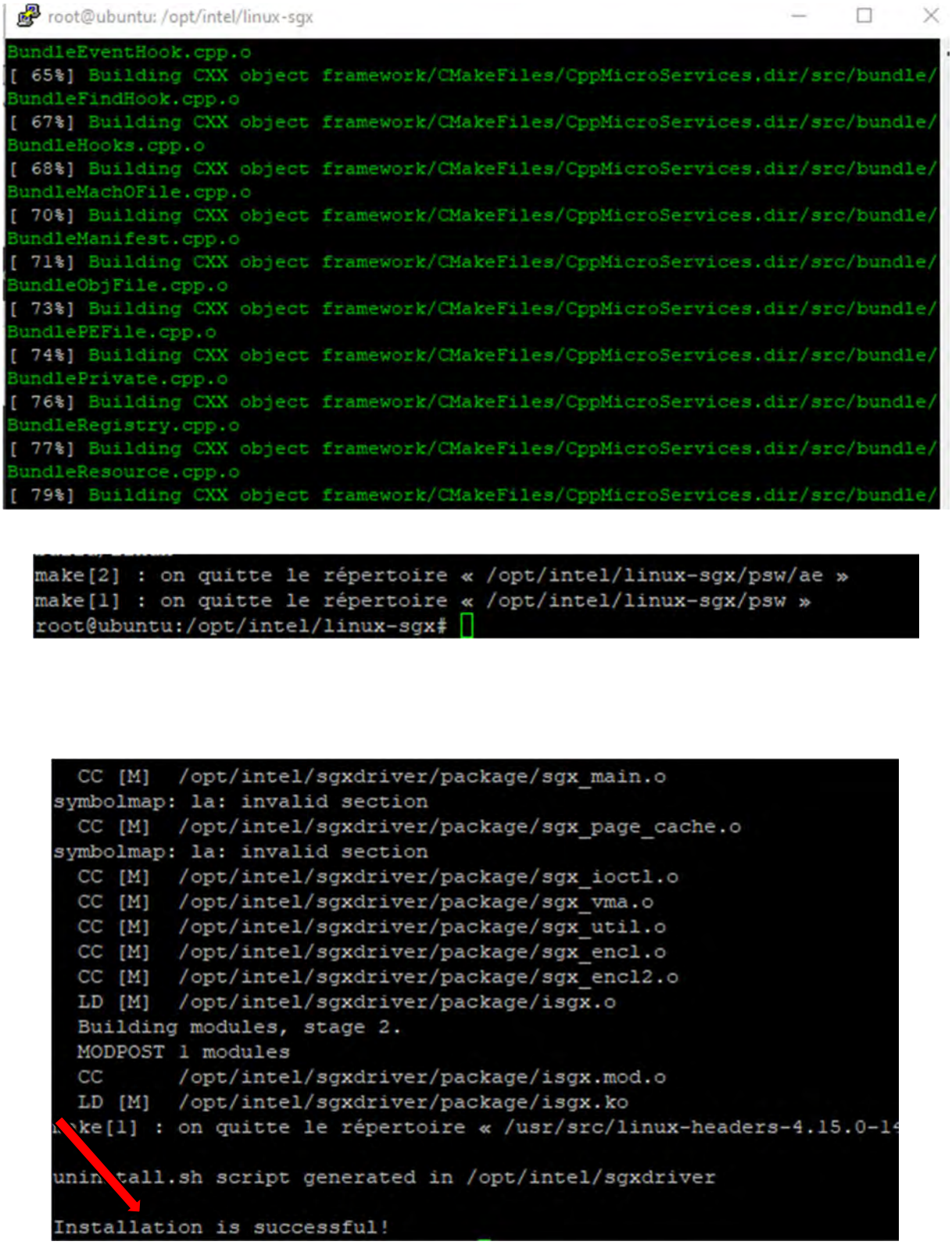

Figure 34: Installation du drive

Redémarrer pour finir l'installation

Utiliser un modèle d'application pour valider l'installation

```
BASE_DIR=/opt/intel
cd $BASE_DIR/sgxsdk/SampleCode/LocalAttestation/
source $BASE_DIR/sgxsdk/environment
make SGX_DEBUG=0 SGX_MODE=HW SGX_PRERELEASE=1
```

Figure 35: Modèle d'application de tester

Créez une application avec un des modèles fournis :

```
</EnclaveConfiguration>
tcs_num 1, tcs_max_num 1, tcs_min_pool 1
The required memory is 2158592B.
The required memory is 0x20f000, 2108 KB.
Succeed.
SIGN =>  libenclave3.so
GEN  =>  Enclave1/Enclave1_u.h
CC   <=  Enclave1/Enclave1_u.c
GEN  =>  Enclave2/Enclave2_u.h
CC   <=  Enclave2/Enclave2_u.c
GEN  =>  Enclave3/Enclave3_u.h
CC   <=  Enclave3/Enclave3_u.c
```

Figure 36: création des enclaves

Exécutez-la

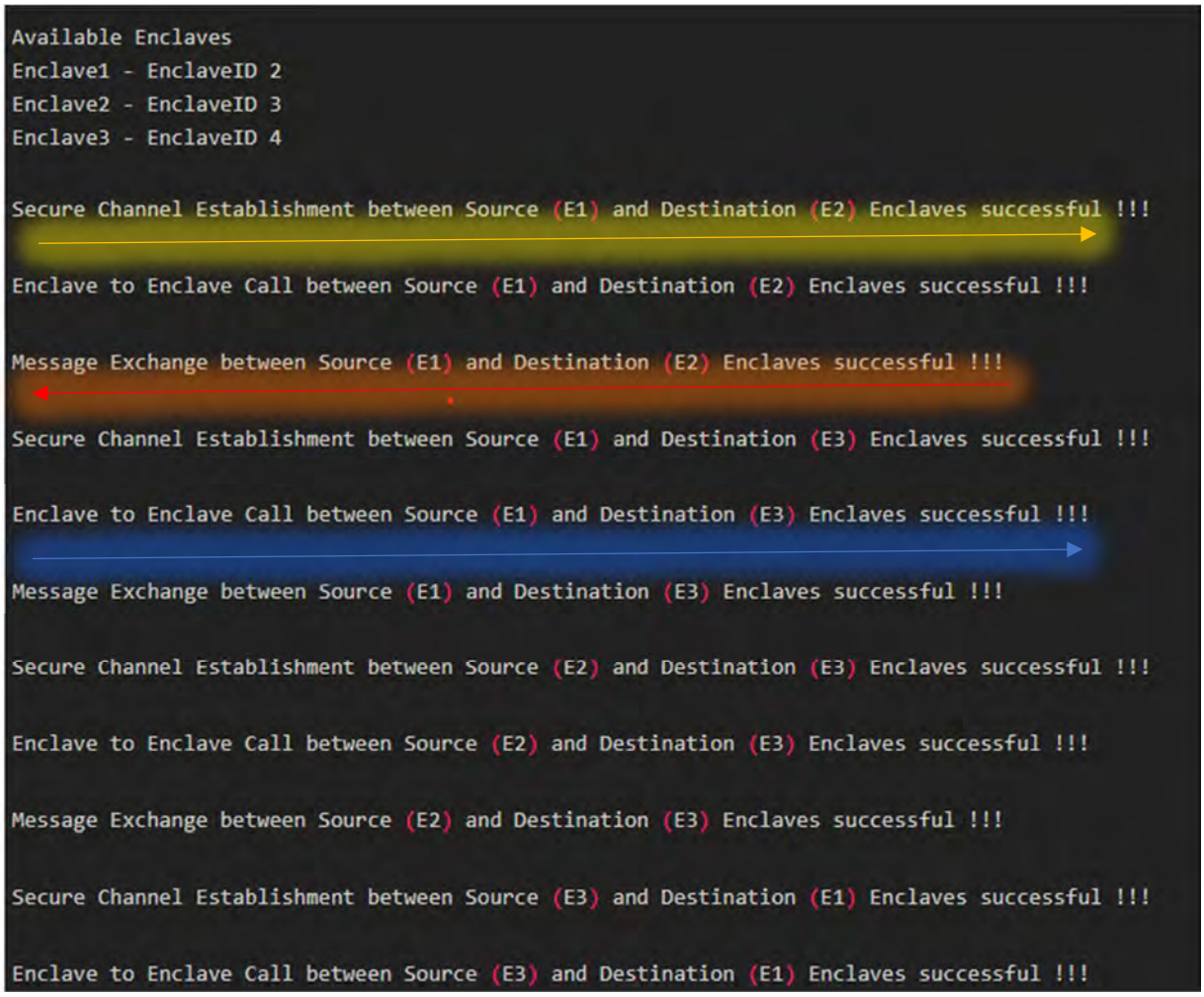

Figure 37: Exécution des enclaves

Les enclaves sont maintenant crées avec succès. Rappelons qu'ils s'agitent des zones protèges dont les données sensibles doivent être stockes.

On souhaitera visualise l'application dans une interface web dans l'avenir et permettant ainsi aux utilisateurs de stockes leurs données en toute sécurité en garantissant leurs confidentialités.

Chapitre 5 : Conclusion Générale et Perspectives

En conclusion, le travail de recherche effectuée dans le cadre de notre mémoire, aborde principalement ***l'étude de la sécurité du Cloud Computing et Mise en place d'une solution de confidentialité.***

Nous avons donné une idée générale sur le Cloud Computing, son architecture et ses différents services et modèles de déploiements.

Nous avons fait par la suite une étude sur la sécurité du Cloud Computing en présentant d'abord les classes de vulnérabilités, ensuite les menaces de sécurité et leurs techniques d'atténuations et enfin les différentes attaques existentielles et leurs défenses.

Nous avons aussi faite l'étude et la comparaison des différentes solutions de confidentialités dans le Cloud Computing.

L'études faite précédemment nous a permis de choisir la solution Software Guard Extensions (Intel SGX) pour la partie mise en œuvre.

Dans la solution proposée, nous avons activer la technologie Intel SGX sur notre noyau KVM côte fournisseur pour s'assurer l'intégrité et la confidentialité des données.

Nous avons aussi installé la pile applicative SDK côte utilisation pour permettre l'utilisation des applications du fournisseur de services.

Notons également que ce mémoire nous a permis de savoir que l'instruction et le savoir de l'homme passent par le travail, la recherche, le sacrifice et le plaisir d'apprendre.

Cependant, nous nous sommes limités à la création des enclaves. Et pour les travaux futurs, nous comptons mettre en place des applications réelles sur les enclaves permettant ainsi aux utilisateurs de manipuler leurs données en toute sécurité dans le Cloud Computing en garantissant l'intégrité et la confidentialité des données.

BIBLIOGRAPHIE

[1] : Deloitte Confidentialité des données dans le nuage Explorer le nouveau régime de protection de la vie privée dans l'environnement infonuagique Consulté le 25/11/2020 à 12h

[2] : Sophos L'ÉTAT DE LA SÉCURITÉ DU CLOUD 2020 Résultats d'une enquête indépendante menée auprès de 5 000 responsables informatiques hébergeant des données et des ressources dans le Cloud public, Juillet 2020 Consulté le 25/03/2021 à 12h

[3] : Mémoire de monitoring d'une infrastructure informatique avec un système de détection et de prévention d'intrusion. Cas d'une entreprise, Ecole Centrale Des Logiciels Libres et de Télécommunications (EC2LT), 2018-2019, 74 pages. Consulté le 23/04/2021 à 12h

[4] : Gens. New IDC IT Cloud Services Survey : Top Benefits and Challenges. A partir de : http://blogs.idc.com/ie/?p=730. Décembre 2009. Consulté le 02/11/2021 à 11h.

[5]: Nicolas GREVET, Le Cloud Computing : Evolution ou Révolution ? M2IRT 2009, 128 pages. Consulté le 12/02/2021 à 12h

[6] : Cloud Computing, Sécurité, stratégie d'entreprise et panorama du marché », Guillaume Plouin, Edition DUNOD, 2013 Consulté le 03/03/2021 à 12h

[7] : Wygwam, Le Cloud Computing : Réelle révolution ou simple évolution ? ,83 pages. Consulté le 25/02/2021 à 15h

[8] : Khalid El Makkaoui 1 · Abdellah Ezzati 1 · AbderrahimBeni - Hssane 2 · Slimane Ouhmad 1, Schémas homomorphiques Fast Cloud – Paillier pour protéger la confidentialité des données sensibles dans le cloud computing ,05 mai 2019 Consulté le 13/04/2021 à 08h

[9] : Mémoire sur La gestion de la confidentialité dans le Cloud Computing, Présentée et soutenue par Salheddine KABOU, en 2017 Consulté le 05/04/2021 à 19h

[10] : https://fr.wikipedia.org/wiki/S%C3%A9curit%C3%A9_du_cloud Consulté le 18/01/2021 à 23h

[11] : Mervat Adib Bamiah et al. / (UAEST) International Journal Of Advanced Engineering Sciences And Technologies Vol No, 9, Issue No, 1,087-090 https://www.academia.edu/4877213/Seven_Deadly_Threats_and_Vulnerabilities_in_Cloud_ Computing Consulte le 12/02/2021 à 09h

[12] : Security Attacks on Cloud Computing With Possible Solution Priyanka C houhan, Rajendra Singh Jaipur Engineering College, Kukas, Jaipur, Rajasthan, India, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 6, Issue 1, January 2016 Consulté le 27/02/2021 à 18h

[13] : Menaces et attaques de sécurité du cloud computing avec leurs techniques d'atténuation, Naseer Amara, Huang Zhiqui, Awais Ali, Conférence internationale 2017 sur l'informatique distribuée et la découverte de connaissances basées sur le cyber Consulté le 27/03/2021 à 18h

[14] : Mémoire sur La gestion de la confidentialité dans le Cloud Computing, Présentée et soutenue par Salheddine KABOU, en 2017 Consulté le 05/04/2021 à 19h

[15] : SS Manikandasaran, L. Arockiam, PD Sheba Kezia Malarchelvi, MONcrypt : une technique pour assurer la confidentialité des données externalisées dans le stockage cloud, Int. J. Information et sécurité informatique, vol. 11, n ° 1, 2019 Consulté le 06/04/2021 à 23h

[16] : DP Zegzhda, ES Usov, AV Nikol'skii et E. Yu. Pavlenko, Utilisation d'Intel SGX pour garantir la confidentialité des données des utilisateurs du cloud, Contrôle automatique et informatique, 2017, Vol. 51, n ° 8, pp. 848–854. Allerton Press, Inc., 2017 : Consulté le 09/04/2021 à 14h

WEBOGRAPHIE

[1w] : https://www.portableone.com/uncategorized/what-is-cloud-computing-2 Consulté le 21/10/2020 à 10h

[2w] : https://exeisconseil.com/article/cloud-computing Consulté le 5/10/2020 à 21h

[3w] : https://steemit.com/turorial/@barthegabi/qu-est-ce-que-le-cloud-computing Consulté le 22/10/2020 à 08h

[4w] :https://www.cloudflare.com/fr-fr/learning/cloud/what-is-a-virtual-private-cloud/ Consulté le 28/10/2020 à 17h

[5w] :https://www.alibabacloud.com/fr/knowledge/what-is-hybrid-cloud Consulté le 12/12/2020 à 22h

[6w] :https://www.hebergeurcloud.com/definition-cloud-computing-selon-nist/ Consulte le 15/12/2020 à 07h

[7w] :https://www.pngkey.com/png/detail/117-1175344_popular-cloud-computing-services-cloud-computing-service-infrastructure.png Consulte le 16/12/2020 à 16h

[8w] :https://blog.iron.io/what-is-iaas-infrastructure-as-a-service/ Consulte le 01/01/2021 à 09h

[9w] : https://quintagroup.com/services/service-images/paas-development-1.png Consulté le 12/01/2021 à 19h

[10w] : https://www.smartdatacollective.com/wp-content/uploads/2018/01/big-data-and-SaaS-startups.jpg Consulté le 15/01/2021 à 11h

[11w] : https://steemit.com/turorial/@barthegabi/qu-est-ce-que-le-cloud-computing Consulté le 18/01/2021 à 23h

[12w] : https://projets-ima.plil.fr/mediawiki/images/f/f2/DoSAttacks.jpg Consulté le 10/02/2021 à 09h

[13w] : https://geekflare.com/wp-content/uploads/2020/02/LDAP-injection.jpg Consulté le 12/02/2021 à 12h

[14w] : https://i.ytimg.com/vi/2-zQp26nbY8/maxresdefault.jpg Consulté le 15/02/2021 à 13h

[15w] : https://upload.wikimedia.org/wikipedia/commons/3/3f/Auth-Forte-b.png Consulté le 18/02/2021 à 08h

[16w] : https://www.malekal.com/wp-content/uploads/MITM-man-in-the-middle-schema.jpg Consulté le 20/02/2021 à 14h

[17w] : https://www.javatpoint.com/cyber-security-goals Consulté le 12/03/2021 à 14h

[18w] : https://talium.fr/protection-donnees-avec-enclave-intel-sgx/ Consulté le 18/03/2021 à 23h

[19w] : https://datatracker.ietf.org/meeting/102/materials/slides-102-teep-recommendations-for-teep-support-of-intel-sgx-technology Consulté le 25/03/2021 à 10h