Franklyn KWAKYE
ISC Paris - Promo 2019
Spécialisation MMTI

Mémoire de fin d'études

-

La sécurité du système d'information d'entreprise sur le cloud

Référent :

Miguel LIOTTIER

Table des matières

Synthèse :

Mon sujet de mémoire a été pensé suite à un échange avec un intervenant acteur dans le monde la cybersécurité. Les multiples exemples qui racontés sur les problèmes liés aux technologies types cloud avait interpellé ma réflexion sur le sujet.

Chaque entreprise dispose d'un système d'information, mais par souci de réduction des coûts, elle cherchera à avoir une solution la plus rentable possible. À travers mes recherches académiques pour élaborer mon cadre conceptuel, les différents auteurs apportaient des interrogations semblables à celle reçue en cours et mon conforter sur mon choix du sujet à traité et à expertiser sur l'environnement de l'infonuage et sa sécurisation. De plus, mon choix en matière de stage de fin d'études dans un cabinet de conseil en cybersécurité, mais permis d'approfondir mes connaissances sur le sujet, de comprendre les concepts et les enjeux. Partant de la définition de la sécurité dans le dictionnaire Larousse, jusqu'à l'aspect technique des différents modèles de cloud, il était très difficile de ne pas s'éparpiller. La décision a été de répondre au problème en grands thèmes afin d'être certains que chaque concept et chiffre était à leurs places.

Ma problématique était de répondre à l'impact du cloud sur la sécurité des échanges de données en entreprise. Beaucoup d'interrogations ont nourri ma problématique, mais malheureusement beaucoup de frustrations se sont formées durant mes études. Il était difficile d'obtenir des réponses des personnes visées dans le périmètre souhaité : soit le moment était inapproprié ou soit les processus de mise en contact sont souvent longs et fastidieux. Heureusement, une relation durant un stage a suggéré une étude récente sur le sujet de mémoire qui correspondant en majeure partie à aux questions quantitatives posées à l'échantillon souhaiter. Aujourd'hui, l'expertise acquérir n'est pas le plus grand, mais il permet de répondre à des problématiques sur le SI du cloud et valorise le travail fourni dans le cabinet actuel. Le

cloud est une technologie ayant beaucoup d'avenir, mais aussi pas mal d'incertitude en matière de sécurité avec les IoT par exemple. L'ouverture serait de voir comment on pourrait cartographier un ensemble des données avec une emprunte type unique pour être sûr que la donnée existe à l'endroit stocké. Une piste possible à exploiter dans l'avenir avec l'émergence de la 5G comme moyen d'accès plus rapide donc une quantité de données nouvelle à sécuriser et donc à tracer.

Introduction :

Le Cloud Computing est actuellement l'un des sujets les plus chauds des technologies de l'information (IT). Cependant, ce n'est pas tant que le terme " Cloud Computing " désigne une foule de nouvelles technologies, mais plutôt que ces technologies sont combinées et mises à niveau de manière efficace pour permettre de nouveaux services informatiques et de nouveaux modèles économiques. (S. SRINIVASAN 2011)

Avec le Cloud Computing, comme avec beaucoup de nouvelles technologies et de nouveaux services, les questions de sécurité de l'information et de protection des données font l'objet de débats intenses et d'examens beaucoup plus critiques que dans le cas des offres qui existent depuis un certain temps déjà. De nombreuses enquêtes et études révèlent que les préoccupations des clients potentiels en matière de sécurité de l'information et de protection des données font obstacle à un déploiement plus large. La confiance nécessaire doit encore être développée si l'on veut tirer parti du cloud. (SURYATEJA P. 2016)

Le Cloud Computing est donc une solution qui permet de réduire les coûts dans les organisations tout en offrant des ressources à la demande et du calcul sans avoir besoin de créer une infrastructure informatique. Les services, tels que Amazon Web Services (AWS) ou Microsoft Azure, permettent aux entreprises de fournir et de déprovisionner instantanément des machines virtuelles (VM) en fonction de leurs besoins, en payant simplement ce qu'elles utilisent.

Afin de créer l'environnement nécessaire, les fournisseurs de services dans les nuages (CSP) utilisent les technologies de virtualisation pour maximiser la valeur de leurs systèmes. Les serveurs ont toujours eu besoin de fonctionner seuls sur des machines physiques pour éviter que d'autres services n'interfèrent avec eux ; mais l'inconvénient était le gaspillage des ressources.

La virtualisation permet d'utiliser toutes les ressources d'un hôte physique en les partageant entre les systèmes d'exploitation invités. Au travers de l'ensemble des recherches effectuées, un certain nombre d'éléments sont sortis et ont permis d'élaborer un questionnement sur la façon d'aborder le sujet de la sécurité des systèmes d'information d'entreprises sur le cloud. Plusieurs sous-questions ont optimisé ma problématique pour ma question de recherche et la voici :

Quels sont les impacts positif ou négatif de l'usage cloud sur la sécurité des échanges de données ?

Ainsi avec l'ensemble des questions à venir sur le sujet, le sujet des systèmes d'informations dans le cloud et sa sécurisation donne lieu un plan en deux parties : L'approche théorique avec les concepts et les enjeux de l'usage du cloud et en suite un approfondissement et une analyse terrain du sujet.

1- Concept et enjeux de la sécurité et l'usage du cloud

Dans cette partie théorique nous allons essayer de répondre aux différentes questions que pose la problématique générale. Différente sous parties vont articulés les notions et définitions utilisés pour répondre au mieux au concept de la sécurité et à celui qu'est le cloud.

a. La sécurité et la donnée dans le SI

i. La sécurité au sens large

De façon générale, la sécurité se trouve dans tout de types systèmes développer par les êtres vivants. On peut séparer cela en deux grandes catégories en matière de sécurité : le domaine physique et psychique. Physiquement, la sécurité est l'absence de péril d'une situation qui n'est pas soumise à un évènement critique ou à risque. Il existe donc dans ce qui est visible et palpable, une possibilité de réduire le risque via une échelle gradué. Psychiquement, la sécurité est l'état d'esprit d'une personne qui se sent tranquille et confiante. Pour l'individu ou un groupe, c'est le sentiment (bien ou mal fondé) d'être à l'abri de tout danger et risque. Le dictionnaire Larousse donne la définition suivante de la sécurité : « Situation dans lequel quelqu'un, quelque chose n'est exposé à aucun danger, à aucun risque, en particulier d'agression physique, d'accidents, de vol, de détérioration ; Absence ou limitation des risques dans un domaine précis. On observe donc un dénominateur commun au sens large, c'est que la notion de risque qu'on souhaite atténuer et/ou limiter. Il suffit donc d'observer la faune et la flore pour constater que la sécurisation d'un bien ou d'un ensemble propre à soi ou pour un tiers, est une priorité absolue. La sécurité d'une entité (objet, personne, entité politique, juridique, intellectuelle, écologique..., informatique) s'envisage individuellement ou collectivement, soit comme objectif (objectif de sécurité), en tant que droit (droit à la sécurité), en tant que valeur (la sécurité est la première des libertés), en tant qu'état de ce qui est sécurisé, en tant que fonction ou d'activité qui vise à sécuriser cette entité ; face à des risques et/ou à des menaces (ces deux notions n'étant pas

réductibles l'une à l'autre). On cherchera donc en matière de sécurité à obtenir un coup d'avance sur un potentiel danger qui pourrait altérer la quiétude de la réalité protéger. Ainsi, si une situation présentée demande un regard particulier en matière sécurité, c'est fondamentalement pour atténuer et/ou limiter le risque.

Le risque dépend donc de l'environnement ou la posture dans laquelle on se trouve, par exemple le risque opérationnel d'un application critique pour une organisation sous la LDP (Loi de protection militaire) ne sera pas le même que celui de la PME (petites et moyennes entreprises) sur secteur dans le secteur agroalimentaire. Mais à quoi le risque ressemble et comment se définit-il. Un risque c'est un danger éventuel où la probabilité est inhérente à une situation ou une activité. On dit donc que le risque se subit. On ne peut pas prendre le risque pour en faire une réalité tant que notre réalité n'est pas affectée un événement négatif à la situation. Par exemple, le risque de la perte de données dépendant qu'une action négative non prévisible soit subit pour émettre la véracité de la perte de données comme risque potentiel. Ainsi il sera risqué de prendre une clé USB (Universal Serial Bus) trouvé par un employé sur le parking de son entreprise et l'insert dans son poste de travail. C'est l'absence de certitude et de contrôle d'une situation interne ou externe à l'environnement où l'ont ce trouve, qui définit la granularité du risque. Un autre aspect du risque, c'est qu'il peut être affronté dans l'espoir d'en tirer une situation ou une activité positive. L'exemple le plus connu reste celui de la bourse. En vulgarisant le concept de la bourse on pourra dire qu'on prendra un risque financier quand après une analyse du marché, les opportunités que comporte l'action valorisé sera bon. On prendra donc le risque de miser sur cette action plus qu'une autre dans l'espoir de fructifier l'investissement. En matière de contrôle, on pouvoir crée des scénarios de risques potentiels pour répondre un résultat. Un coureur de formule 1 va prendre le risque de d'augmenter sa vitesse dans une trajectoire afin d'obtenir un résultat, dans ce cas positif s'il gagne des seconds

négatifs s'il fait une sortie de route. « *C'est pourquoi, prenant le risque, j'encourageaisv le soulèvement, sans rejeter aucune des influences qui étaient propres à le provoquer* » (De Gaulle, Mém. guerre, 1956, pp. 292). Le risque rattache donc un regard objectif ou subjectif d'une situation donnée dans le but de limiter ou atténuer le danger potentiel. Au sein d'une entreprise, le risque peut être classé de façon pyramidale car il n'atteint pas les mêmes agents de l'organisation. Le risque d'un groupe peut avoir un impact très fort ou mineur selon l'organisation. Un individu, ayant un rôle à responsabilité critique, peut avoir un taux aussi élevé de risque qu'un groupe d'individu de cette même organisation.

Dans un monde incertain, la maîtrise des risques permet de renforcer la pérennité de l'entreprise. Toutefois, la survie d'une organisation ne dépend pas uniquement de sa capacité à maîtriser les risques. Les principaux risques à considérer par l'organisation sont les risques opérationnels quotidiens ; ils nourrissent en permanence le coût du risque de l'entreprise, et peuvent remettre en cause la pérennité de l'organisation en quelques heures.

ii. La donnée et le système d'information

La donnée est un élément essentiel d'un système d'information. La donnée est selon la définition du dictionnaire : « *Quantité connue dans l'énoncé d'un problème et qui sert à trouver la solution* » ; « *Ce qui est connu et admis, et qui sert de base, à un raisonnement, à un examen ou à une recherche.* » ; « *Ensemble des indications enregistrées en machine pour permettre l'analyse et/ou la recherche automatique des informations* ». On retrouve un certain nombre d'éléments permettant de dire permet de traiter un problème, c'est à dire qu'on peut la consulter à l'état brut et la rendre utilisable pour solutionner un besoin. Elle est disponible pour être utiliser comme support à un étude dans un but d'émettre des hypothèses afin de prendre une décision mais aussi automatiser un ensemble d'action programmer pour effectuer des actions à grande échelle, le but étant l'optimisation d'un processus. Ainsi, il y a principalement des

données qualitatives et des données quantitatives. Les premières se réfèrent aux chiffres et la seconde à la qualité. On peut avec des données, dès lors qu'elles sont organisées, émettre une information et transmettre de la connaissance mais pour ce faire, il faudra structurer la donnée via un systèmes de classification en forme de tableau interprétable par un outil ou un programme informatique. Chaque donnée provient d'une source qui doit être vérifiable pour répondre au besoin d'analyse souhaitée.

Dans un système d'information, la donnée est le fondement du système pour répondre au besoin de l'utilisateur. Cependant chaque brique d'un système d'information peut comporter un risque et il faudra donc chercher à le sécuriser. Le système d'information est aujourd'hui un élément central du fonctionnement d'une organisation. Par définition le un système d'information peut être défini comme un ensemble de ressources (personnel, logiciels, processus, données, matériels, équipements informatiques et de télécommunication...) permettant la collecte, le stockage, la structuration, la modélisation, la gestion, la manipulation, l'analyse, le transport, l'échange et la diffusion des informations (textes, images, sons, vidéo...) au sein d'une organisation. (Architecture and Patterns for IT, Charles T. Betz , Morgan Kaufmann, 2011)

Dans l'étude de documents universitaires, la représentation du système d'information peut être sous différente formes. On retrouve un certain nombre d'éléments et le schéma ci-dessous est l'une des formes les plus simple pour notre usage et notre compréhension. Ainsi, Chaque

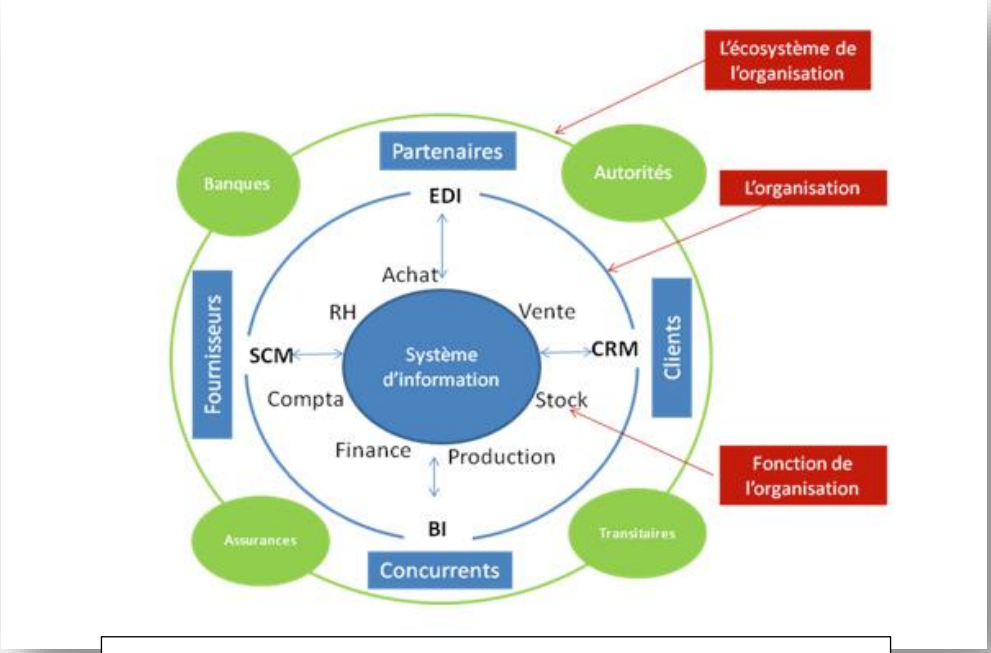

Figure 1 : Représentation d'un SI , Boughzala 2014

dimension d'un système d'organisation comporte au moins 3 couches : l'écosystème de l'organisation. C'est ce qu'on peut aussi nommer l'aspect macro de l'organisation face à son environnement de développement ; l'organisation elle-même qui va regrouper l'ensemble des entités qui permettent le fonctionnement des différents besoins de l'organisation et les fonctions de l'organisation segmentés en blocs de métiers de l'entreprise qu'on appellera des services (Achat, Ventes, Finance, RH, Comptabilité, etc.). Tout élément métier de l'organisation comporte une fonction bien précise dans l'organisation afin interagir avec l'écosystème interne mais aussi à l'écosystème externe de l'organisation. Dans le cadre de notre sujet et dans le monde actuel, où la digitalisation est en constante évolution, il faut observer que le SI (Système d'Information) est un élément capital dans les échanges de données traités avec l'extérieur de l'organisation mais aussi pour les mouvements internes de données brutes dans l'organisation. Quand bien même un système d'information peut avoir plusieurs possibilités d'actions dans

l'entreprise, il faut assurer et maitriser certain risque au vu des multiples échanges et mouvements d'information dans l'organisation. Un danger ou une menace potentiel doit être anticipé et mis dans un cadre particulier qu'on appelle la politique de sécurité. (IRACST, Vol. 1, No. 2, 2011)

iii. Politique de sécurité

La politique de sécurité des systèmes d'information (PSSI) est devenue indispensable au sein des entreprises ayant un système d'information. La PSSI relève d'une vision stratégique de l'organisme et traduit un engagement fort de la direction générale. Elle s'inscrit nécessairement sur le long terme.

- Elle définit le cadre d'utilisation des ressources du système d'information mais
- Elle identifie les techniques de sécurisation à mettre en œuvre dans les différents services de l'organisation
- Elle sensibilise les utilisateurs à la sécurité informatique.

BEIGBEDER J. *PSSI Orientation – ENS – 01/03/2017*).

Comme dans dit dans la partie concernant le système d'information, le traitement de la donnée va satisfaire un ou plusieurs acteurs en fonction de son besoin dans l'instant choisi. Il faudra donc que la politique de sécurité s'associe avec un certain nombre de critère opérationnelle mais aussi réglementaire pour rendre l'usage du système d'information fiable et certain.

La sécurité informatique a pour objectif de maintenir, à un niveau convenable (défini par la direction générale), les garanties suivantes :

- **Disponibilité** : garantie que les entités autorisées ont accès à tout moment aux éléments considérés.

- **Intégrité** : garantie que les ressources sont exactes et complètes (non corrompues).
- **Confidentialité** : garantie que les ressources sont accessibles au moment voulu par les entités autorisées.
- **Traçabilité/Preuve** : garantie que les accès et tentatives d'accès aux ressources sont tracés et que ces traces sont conservées et exploitables.

Ces quatre principes combinés, « DICT » ou « DICP(Preuve) », permettent d'assurer un niveau de sécurité suffisamment élevé pour satisfaire au besoin de sécurité des données de l'entreprise concernée. On va donc utiliser ce qu'on appelle une norme ISO (Organisation internationale de normalisation). L'ISO établit des documents qui définissent des exigences, des spécifications, des lignes directrices ou des caractéristiques à utiliser systématiquement pour assurer l'aptitude à l'emploi des matériaux, produits, processus et services (ISO.2019). Ainsi il existe Il existe plus d'une douzaine de normes dans la famille ISO/IEC 27000. Il existe une autre méthode qui permet d'élaborer une politique de sécurité comme MEHARI (*Method for Harmonized Analysis of Risk*) mais nous n'attarderons pas dessus. Le schéma ci-dessus nous montre comment une politique de sécurité s'érige en mode projet pour répondre aux objectifs fixés par le RSSI (Responsable de la Sécurité des Systèmes d'Information) et les normes.

CRITÈRES	ATTAQUES	IMPACTS
CONFIDENTIALITÉ	**Divulgation, accès** par des tiers non autorisés et **détournement** à des fins délictueuses, de données confidentielles (touchant des travaux confidentiels, des données scientifiques ou technologiques, des données personnelles telles que médicales ou financières…), que ces données soient stockées ou échangées (messagerie)	Pertes du patrimoine scientifique ; pertes d'avance technologique et technique ; pertes financières ; contentieux juridique
DISPONIBILITÉ	**Vol de matériel, émission de malware** (virus, ver, déni de service…) **Sinistres**	Interruption de service ; paralysie ou désorganisation conduisant à l'incapacité opérationnelle de fonctionnement, de décision, de gestion, de sécurisation ; saturation de ressources, de systèmes d'alerte ; perte de données précieuses (scientifiques ou de gestion) par absence ou insuffisance de sauvegarde ; atteinte à la sécurité du personnel, des usagers ; perte d'image de marque
INTÉGRITÉ	**Modification accidentelle ou délibérée** (défiguration de sites Web…), **piégeage**de systèmes d'information, **émission de malware** (bombes logiques, chevaux de Troie, sniffeurs…), **vol** ou **détournement** de moyens informatiques à des fins délictueuses (compromission de serveurs…)	Résultats de fonction incomplets ou incorrects ; expérimentations non crédibles ; prises de décisions inadaptées ; appropriation frauduleuse de biens ; prise de contrôle d'un système physique ; perte du patrimoine scientifique ; perte d'image de marque ; atteinte à des libertés individuelles (cybersurveillance indue…)

Figure 2 : Plan d'action PSSI du CNRS, 2009

L'exemple de la politique de sécurité du CNRS (Centre national de la recherche scientifique) nous montre les actions et impacts en cas le problématique cyber en fonction des besoins de sécurisation. On observe bien que le DCIT est développer pour différents cas d'usages en vue de mesures les impacts mais aussi de porter des actions concrètes.

b. Le cloud computing

i. Définition du cloud computing.

Il existe de nombreuses définitions du "Cloud Computing" données par différents chercheurs. Le RAD de Barkley définit le Cloud Computing comme

Le "*Cloud Computing" désigne à la fois les applications fournies sous forme de services sur Internet et le matériel et les logiciels des systèmes dans les bases de données qui fournissent ces services. Les services eux-mêmes ont longtemps été désignés sous le nom de Software as a Service (SaaS). Le matériel et les logiciels des bases de données sont ce que nous appellerons un "nuage". Lorsqu'un nuage est mis à la disposition du grand public sous forme de paiement à l'utilisation, nous l'appelons nuage public ; le service vendu est l'informatique utilitaire. Nous utilisons le terme "nuage privé" pour désigner les bases de données internes d'une entreprise ou d'une autre organisation, qui ne sont pas mis à la disposition du grand public. Ainsi, le cloud computing est la somme du SaaS et de l'Utility Computing, mais n'inclut pas les nuages privés. Les personnes peuvent être des utilisateurs ou des fournisseurs de SaaS, ou des utilisateurs ou des fournisseurs de services informatiques*". (Armbrust et al., 2009, p6)

Le résumé des caractéristiques du Cloud Computing décrit par Stanoevska-Slabeva et Wozniak est (Stanoevska-Slabeva et Wozniak, 2009, p50) :

- Le "Cloud Computing" est un nouveau paradigme informatique.

- Les ressources d'infrastructure (matériel, stockage et logiciels système) et les applications sont fournis selon le principe du "X-as-a-Service". Lorsque ces services sont proposés par un prestataire indépendant ou à des clients externes, le cloud computing est basé sur des modèles commerciaux de paiement à l'utilisation.

- Les principales caractéristiques des nuages sont la virtualisation et l'évolutivité dynamique à la demande.

- « Utility computing » et le SaaS sont fournis de manière intégrée, même si l'informatique utilitaire peut être consommée séparément.

- Les services dans le nuage sont consommés soit via un navigateur Web, soit via une API définie.

ii. Architecture & modèle déploiements du cloud

Pour aller plus en profondeur nous allons voir les typologies cloud et leurs services.

1. Architecture : modèles et infrastructures

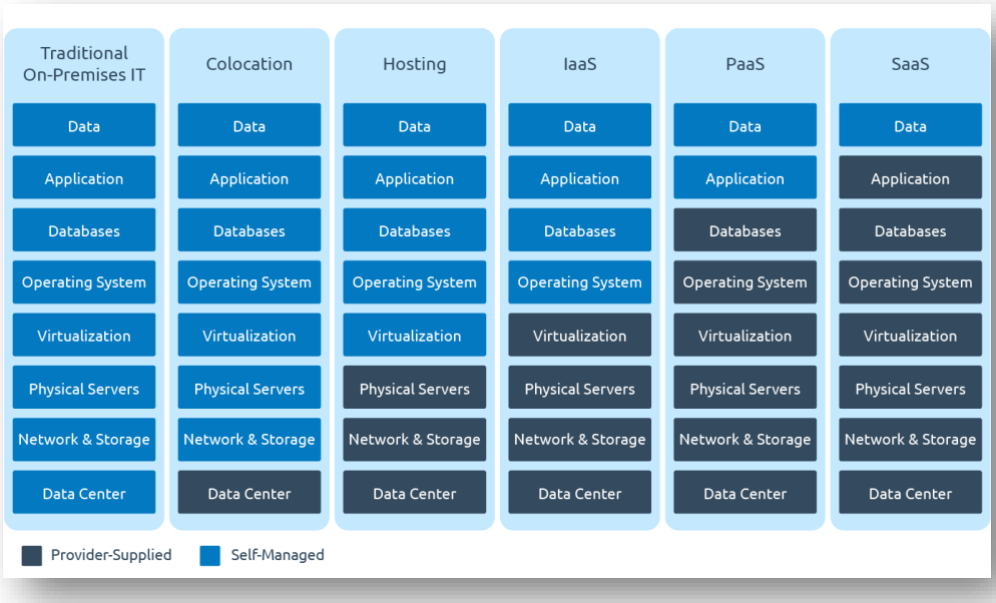

Figure 3 - Modèle de cloud : IaaS PaaS et SaaS

Les modèles d'informatique dans les nuages, comme le montre l'infographie, permettent aux consommateurs d'accéder aux services fournis par les fournisseurs de services en nuage. Celles-ci sont examinées en détail ci-dessous :

On en retrouve 3 principaux :

SaaS (*Software-as-a-Service*) : Dans ce modèle, les consommateurs peuvent utiliser les services applicatifs fournis par les fournisseurs de cloud computing. Il repose essentiellement sur l'accès par un navigateur internet au service. (NIST.2011) En générale, ce service est régi par l'abonnement à ce qu'on appelle des licences ayant pour fonctionnement l'usage de l'abonnement téléphonique. Les utilisateurs vont principalement de voir passé par la plateforme customiser par l'entreprise pour accéder aux informations « stocker » au sein de l'organisation elle-même. Le déploiement, stockage, maintenance, sauvegarde sont du ressort du fournisseur de service. Un bon exemple de SaaS est Office 365 qui propose des applications à la demande du type CRM (customer relationship management) et autres outils de collaborations. Il est donc très facile pour le client de bénéficier d'une application de manière quasi instantanée et à la demande sans aucun frais en immobilisation. Il y a très peu de prérequis, si ce n'est un accès à internet pour utiliser les applications généralement directement via le navigateur. Le déploiement, stockage, maintenance, sauvegarde sont du ressort du fournisseur de service.

PaaS (*Platform as a Service*) compte parmi les trois principales catégories de services informatiques en mode cloud. La capacité offerte au consommateur consiste à déployer sur l'infrastructure en nuage des applications créées ou acquises par le consommateur à l'aide de langages de programmation, de bibliothèques, de services et d'outils pris en charge par le fournisseur. Le consommateur ne gère ni ne contrôle l'infrastructure cloud sous-jacente, y compris le réseau, les serveurs, les systèmes d'exploitation ou le stockage, mais il contrôle les

applications déployées et éventuellement les paramètres de configuration de l'environnement d'hébergement d'applications. (NIST.2011) Parmi les solutions : Windows Azure de Microsoft, App Engine de Google, Amazon Web Services, Salesforce, IBM avec BlueMix.

IaaS (*Infrastructure as a service*) Cela peut se traduire en français par « infrastructure en tant que service ». Il consiste à offrir un accès à un parc informatique virtualisé, c'est-à-dire des machines délocalisées, ne lui appartenant pas, sur lesquelles le consommateur peut installer un système d'exploitation, des applications ou des données. Le consommateur est ainsi dispensé de l'achat de matériel informatique. (Vers quelle sécurité sur le Cloud. Géraud B.2017). Si une entreprise développe un nouveau logiciel, il peut s'avérer plus rentable économiquement d'héberger et de tester cette application en faisant appel à un fournisseur IaaS.

Selon une étude sur les entreprises françaises en juillet 2015 par l'organisme de Markess International, 80% utilisent le SaaS, 28% l'IaaS et 11% le PaaS

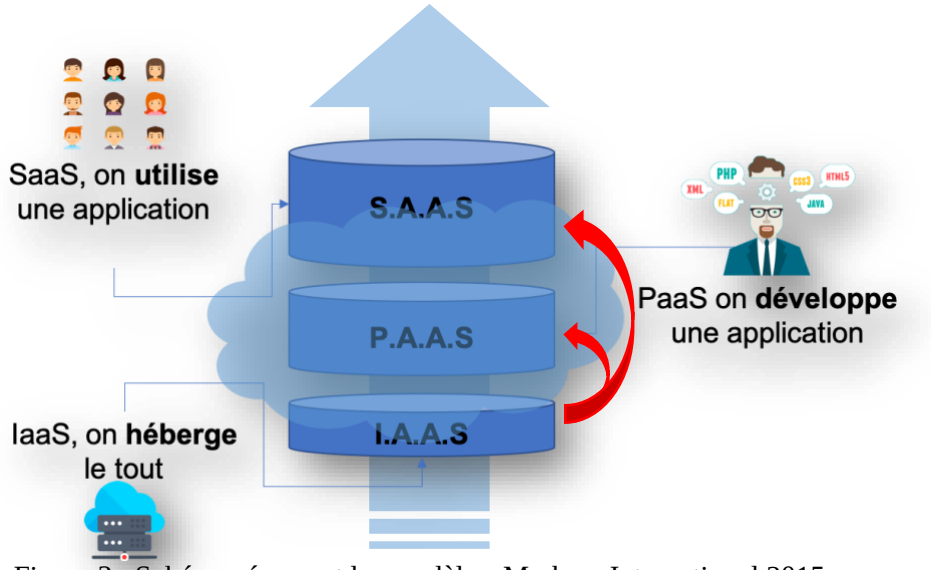

Figure 3 : Schéma résumant les modèles, Markess International 2015

Pour simplifier ces différentes définitions le schéma ci-dessus reprends les éléments cités pour mieux comprendre les différentes couches du cloud. Passons à ce qui permet différents services de cloud en passant par rapidement sur le principe de virtualisation.

2. Modèle de déploiement du cloud

Avant de s'attarder sur le service cloud, il faut distinguer le cloud computing et virtualisation. Il n'y a pas parfois de la confusion car on pense nécessairement que tout ce qui est lié au cloud est virtualiser ou autre. Par définition la virtualisation consiste à créer une représentation virtuelle, basée logicielle, d'un objet ou d'une ressource telle qu'un système d'exploitation, un serveur, un système de stockage ou un réseau. Ces ressources simulées ou émulées sont en tous points identiques à leur version physique. .

L'informatique dans les nuages est un service donnant des ressources informatiques partagées à la demande par Internet, tandis que la virtualisation permet de rendre les espaces informatiques indépendants d'une infrastructure physique. De par cette distinction, il existe principalement 3 types type cloud : public, privée et hybride et une quatrième qui s'émerge de plus en plus : communautaire.

Public : ce type de cloud est rattaché nécessairement à un prestataire de service cloud qui propose les biens matériels et les services aux entreprises en leurs permettant un accès via Internet. Le Cloud public peut être gratuit ou fonctionner selon paiement à la consommation.

Privé : Il existe deux types de cloud privé. On parlera de cloud privé externe quand un ensemble de cloud sont dédiés à une entreprise mais dont la gestion du service cloud se trouve entre les mains d'un fournisseur externe à l'entreprise. L'accès sont régit par un système de réseaux sécurisés type VPN (Virtuale Proctol Network) généralement. Le cloud privé interne est à l'usage de plusieurs consommateurs appartenant à cette seule entreprise qui est propriétaire de l'infrastructure. Elle peut également être partagée ou mutualisée de façon privée avec les filiales. L'architecture est hébergée par l'entreprise. (Nist.2011)

Hybride : Une combinaison de deux ou plusieurs modèles de déploiement de cloud computing, liés de manière à ce que le transfert de données s'effectue entre eux sans s'affecter mutuellement. Ces nuages seraient généralement créés par l'entreprise et les responsabilités de gestion seraient partagées entre l'entreprise et le fournisseur de l'infonuage. Dans ce modèle, une entreprise peut décrire les objectifs et les besoins des services. Un nuage hybride bien construit peut être utile pour fournir des services sécurisés tels que la réception des paiements des clients, ainsi que ceux qui sont secondaires à l'entreprise, comme le traitement de la paie des employés. Le principal inconvénient du nuage hybride est la difficulté de créer et de gérer efficacement une telle solution. Les services provenant de différentes sources doivent être obtenus et fournis comme s'ils provenaient d'un seul endroit, et les interactions entre les composantes privées et publiques peuvent rendre la mise en œuvre encore plus complexe. Il peut s'agir de nuages privés, communautaires ou publics qui sont liés par une technologie propriétaire ou standard qui assure la portabilité des données et des applications entre les nuages qui les composent. Un exemple de nuage hybride comprend Amazon Web Services (AWS).

c. Les impacts du « cloud » sur l'échange de données en entreprise.

i. Le Grid Computing vs Cloud Computing.

Il y a toujours eu un débat sur l'évolution du Cloud Computing et le point le plus important de ce débat est le Grid Computing. Certaines personnes appellent le "Cloud Computing" et le "Grid Computing" les mêmes phénomènes, tandis que d'autres considèrent le "Cloud Computing" comme une extension du "Grid Computing". Pour trouver la vérité, nous devons connaître le Grid Computing (Stanoevska- Slabeva, Wozniak, 2009, p59). Le Grid Computing est un phénomène complexe qui a évolué grâce à des développements antérieurs en matière de calcul parallèle, distribué et HPC (High Performance Computing) (Weishäupl et al.,

2005 et Harms et al. 2006). L'une des définitions du calcul en grille les plus citées au départ est celle de Foster et Kesselman (1998).

"*A computational grid is a hardware and software infrastructure that provides dependable, consistent, pervasive and inexpensive access to high-end computational capabilities.*" (Stanoevska-Slabeva and Wozniak, 2009, p23)

Table 1 – Grid and Cloud Computing Technically Compared (Stanoevska-Slabeva and Wozniak, 2009, p59)

	Grid Computing	**Cloud Computing**
Means of utilization (e.g. Harris 2008)	Allocation of multiple servers onto a single task or job	Virtualization of servers; one server to compute several tasks concurrently
Typical usage pattern (e.g. EGEE 2008)	Typically used for job execution, i.e. the execution of a program for a limited time	More frequently used to support long-running services
Level of abstraction (e.g. Jha et al. 2008)	Expose high level of detail	Provide higher-level abstractions

Par la suite, le développement du partage des ressources informatiques génériques a commencé à être observé comme le véritable problème du Grid Computing. Selon M. Foster, le développement du support pour le partage générique des ressources informatiques a commencé à être considéré comme le véritable problème du Grid,

Le cloud computing concerne également la manière dont les technologies de l'information sont fournies et utilisées et pas seulement les améliorations technologiques des bases de données (Creeger, 2009, p50). Les entreprises doivent prendre en compte les avantages, les inconvénients et les autres effets du cloud computing sur leurs activités et leurs pratiques d'utilisation avant d'adopter et d'utiliser le cloud computing (Khajeh- Hosseini et al., 2010b, p2). Dans les entreprises, l'adoption du Cloud Computing dépend beaucoup de la maturité des processus organisationnels et culturels comme de la technologie en soi (Fellowes,

2008). Certains prédisent que l'adoption du cloud computing ne se fera pas du jour au lendemain, mais qu'il faudra peut-être 10 à 15 ans avant qu'une entreprise typique ne fasse ce choix. Nous sommes actuellement dans une période de transition au cours de laquelle de nombreuses décisions doivent être prises en ce qui concerne l'adoption du Cloud Computing dans l'entreprise.

La décision d'adopter le Cloud Computing est difficile à prendre en raison de toute une série de raisons pratiques et socio-politiques. Il n'est pas possible que toutes les entreprises externalisent l'ensemble de leurs besoins informatiques de base à des fournisseurs de cloud computing ; elles établiront plutôt un environnement informatique hétérogène basé sur des serveurs dédiés, des clouds organisationnels et éventuellement plus d'un fournisseur de cloud computing public. La manière dont l'adoption du cloud computing est gérée ne dépend pas seulement de questions techniques, mais aussi de facteurs socio-techniques (c'est-à-dire le coût, la confidentialité et le contrôle), de l'impact sur les pratiques de travail et des contraintes découlant des modèles commerciaux existants. Par conséquent, les défis que les entreprises doivent relever avant l'adoption du cloud computing sont les suivants : i) fournir des informations précises sur les coûts de l'adoption du cloud computing ; ii) soutenir la gestion des risques ; et iii) veiller à ce que les décideurs puissent faire des compromis éclairés entre les avantages et les risques (Khajeh-Hosseini et al., 2010c, p4).

ii. Les avantages et inconvénients

Dans " Cloud Migration : A Case Study of Migrating an Enterprise IT System to IaaS", Khajeh-Hosseini et autres (2010a) parlent de l'infrastructure en nuage d'une tierce partie. Selon eux, si l'infrastructure en nuage tierce est introduite, elle offre aux entreprises de nombreuses possibilités d'améliorer la gestion des revenus et des dépenses, tant pour le personnel financier que pour les clients. Elle permet également de faciliter la gestion des flux de trésorerie pour le

personnel financier, car le modèle de tarification du cloud a un coût initial et une facturation mensuelle minimes et il réduit également la variabilité des dépenses en électricité. Ce sont là les avantages par rapport au centre de données interne, car il peut être coûteux d'acheter du matériel et la trésorerie peut également être lente et difficile à obtenir des clients. En outre, les coûts énergétiques diminueront également car vous ne gérez pas votre propre centre de données et le cloud tiers en sera responsable. L'infrastructure en nuage est également très utile pour le département financier de l'entreprise afin de réduire la charge administrative. Les solutions d'infrastructure cloud tierces offrent de nouveaux modèles de tarification, qui aident à gérer les revenus des clients, des ventes et du personnel marketing (Khajeh-Hosseini et al., 2010a, p5).

Khajeh-Hosseini et autres (2010a) ont conclu que le Cloud Computing est une technologie perturbatrice qui va changer la façon dont les systèmes informatiques des entreprises sont déployés en raison de sa nature bon marché, simple et évolutive. Le cloud computing peut être nettement moins cher que l'achat et la maintenance d'un centre de données interne, car il élimine les problèmes liés au support car il n'y a pas d'infrastructure physique à entretenir. Toutefois, les entreprises doivent tenir compte de nombreux aspects sociotechniques avant de migrer vers le cloud (Khajeh-Hosseini 2010a, p7).

Mayur et al. (2008) étudient le service de stockage de données S3 d'Amazon pour les applications à forte intensité de données scientifiques. Selon eux, le service S3 regroupe les trois caractéristiques des données, à savoir une grande durabilité, une grande disponibilité et un accès rapide, en une seule méthode de tarification, mais la plupart des applications n'ont pas besoin d'être toutes regroupées. Par exemple, le stockage d'archives, qui a besoin de durabilité mais qui peut survivre avec une disponibilité et des performances d'accès plus faibles. Par conséquent, il est suggéré que S3 fournisse des services par le biais d'un certain nombre de classes limitées de services afin que les utilisateurs puissent choisir la combinaison de

durabilité/disponibilité/performances d'accès qu'ils souhaitent pour un meilleur coût (Mayur et al., 2008, p8). Par conséquent, le coût est plus élevé lorsque les services de stockage regroupent la durabilité, la disponibilité et les performances d'accès.

Dans le rapport "Clearing the Air on Cloud Computing" de McKinsey & Co, ils affirment que le Cloud Computing peut coûter deux fois plus cher que les centres de données internes. Cependant, ce problème ne concerne que les grandes entreprises, mais les petites et moyennes entreprises ne sont pas concernées et elles en tirent des avantages en termes de coûts. Selon eux, "les offres de cloud computing sont actuellement les plus intéressantes pour les petites et moyennes entreprises... et la plupart des clients des clouds sont des petites entreprises" (Lublinsky et Boris, 2009). La raison en est que les petites entreprises n'ont pas la possibilité de se développer en centres de données géants. La variabilité des coûts est un aspect clé du Cloud Computing et lorsque les entreprises optent pour la transparence des coûts, l'évolutivité et la variabilité des coûts, un nouveau défi et une nouvelle opportunité se présentent (Qamar et al., 2010, p2).

En bref, nous pouvons dire que le coût et la sécurité sont les facteurs importants pour toute entreprise qui veut adapter le "cloud computing". Les entreprises ont tendance à choisir les méthodes de paiement pour rémunérer les fournisseurs de cloud computing. Le mode de paiement le plus courant pour les entreprises et les fournisseurs de cloud computing est le "paiement au fur et à mesure". C'est l'une des caractéristiques nouvelles du "cloud computing", qui est moins cher à long terme que d'avoir son propre centre de données. Cependant, le cloud computing est moins cher pour les petites et moyennes entreprises que pour les grandes. L'élasticité est un autre facteur qui permet aux entreprises d'adapter le "cloud computing" car elles peuvent utiliser leurs ressources de manière dynamique. La sécurité des données est la préoccupation la plus importante des entreprises qui adaptent le cloud computing. La plupart

des problèmes de sécurité sont dus au manque de contrôle de l'entreprise sur l'infrastructure physique. Les services web et les navigateurs web sont également une source de préoccupation en ce qui concerne le cloud computing, car la plupart des services en nuage sont accessibles via le web. Les questions de gouvernance comprennent la gouvernance et la gestion des risques d'entreprise, la découverte légale et électronique, la conformité et l'audit, la gestion du cycle de vie des informations, ainsi que la portabilité et l'interopérabilité. Les questions opérationnelles comprennent la sécurité traditionnelle, la continuité des activités et la reprise après sinistre, l'exploitation des centres de données, la réponse aux incidents, la notification et les mesures correctives, la sécurité des applications, le cryptage et la gestion des clés, et la virtualisation.

Outre les problèmes de sécurité, le cloud computing présente également certains avantages en matière de sécurité. Parmi ces avantages, citons l'avantage de l'échelle avec de multiples emplacements, les réseaux de périphérie, le délai de réponse improvisé et la gestion des menaces. Parmi les autres avantages, citons la sécurité en tant que différenciateur du marché, les interfaces standard pour la sécurité gérée

2- Approche terrain

a. Introduction

La gestion de la sécurité est un défi majeur pour les grandes comme pour les petites entreprises. La transition vers l'informatique dans les nuages augmente les défis auxquels ces entreprises sont confrontées en raison des nombreuses inconnues. Un aspect important de la sécurité est la sécurité physique. Une organisation qui possède les ressources informatiques sait comment assurer la sécurité physique. Une organisation qui utilise l'informatique dans les nuages ne sait pas où se trouvent les ressources matérielles et, par conséquent, à condition que cette forme de sécurité soit transférée au fournisseur de services.

b. Méthodologie et résultat

Comme déjà identifié par le sujet et la question de recherche, il est maintenant important de faire correspondre la conception et les méthodes avec l'énoncé du problème et les questions de recherche, en d'autres termes, une stratégie de recherche. La stratégie de recherche est la méthode scientifique qui aide à répondre aux questions de recherche. Il faut d'abord observer une présentation générale de la stratégie, avec les méthodes de recherche, les outils d'analyse de la collecte de données, les outils d'investigation, l'éthique, etc. Comme mentionné, l'identification du type de questions de recherche choisi est une bonne stratégie de recherche.

i. Méthodologie et stratégie de recherche

La méthode est un outil permettant de générer des solutions aux problèmes et d'en tirer de nouvelles connaissances (Lekwall & Wahlbin, 2001). Comme Marshall & Rossman présentent trois conditions pour choisir une stratégie, qu'il s'agisse d'expériences, d'enquêtes, d'analyses d'archives, d'histoire ou d'études de cas, il faut suivre trois conditions, à savoir : a) le type de questions de recherche posées, b) le degré de contrôle qu'un enquêteur exerce sur les événements comportementaux réels et c) le degré de concentration sur les événements contemporains pour choisir ma stratégie (Marshall & Rossman, 1989, p5).

La première chose à considérer était la question de la recherche. Les questions de recherche pouvaient être identifiées avec trois objectifs : explicatif, descriptif ou exploratoire (Marshall & Rossman, 1989, p3). Comme Marshall, Rossman et Yin l'ont dit dans leur littérature respective, les questions "quoi" conduisent à des études exploratoires et les questions "comment" et "pourquoi" conduisent à des études explicatives (Marshall & Rossman, 1989, p3-6). Comme ma question était de trouver la réponse à la question de savoir quels sont les avantages et les inconvénients du "cloud computing", et les facteurs qui poussent les entreprises à passer à la technologie du "cloud computing", l'étude poursuivie est une étude de cas

exploratoire (Marshall & Rossman, 1989, p6). Ayant conscience des variables essentielles du sujet, des phénomènes, du Cloud Computing, des systèmes d'information dans les entreprises, de l'effet de coût, de l'effet de sécurité et de la manière dont ils affectent les entreprises. Les constructions de base répondaient aux questions et rassemblaient autant de données que possible, et donc, permettait d'obtenir une quantité plus importante d'informations. La question a permis à comprendre les phénomènes dans un contexte particulier, le Cloud Computing et les entreprises.

Une fois le processus de collecte des données achevé, l'étape suivante a été l'analyse des données. Il existe de nombreuses méthodes qui rendent l'analyse des données plus significative. Ces techniques pouvaient être utilisées pour gérer le texte de l'entretien, pour comprimer l'entretien sous la forme de quelques phrases courtes afin d'obtenir les points importants dits dans l'entretien. En fonction des méthodes et des outils de collecte de données utilisés, le choix à été l'analyse de l'étude de cas pour analyser mes données. KVALE, S. (1996)

Il était très important, lors de l'analyse, de comprendre les données textuelles. Il faut souligner et comprendre la partie importante d'un texte pour pouvoir en saisir le sens général et ensuite l'interpréter pour lui apporter cohérence et sens. Pour y parvenir, il fallait donc effectuer un processus circulaire, par la compréhension le texte dans son ensemble, puis l'interprétation des parties du texte afin de mieux comprendre l'ensemble, puis je suis revenu aux parties, et ainsi de suite. Dans mon étude, plusieurs études de cas ont été mené afin de confronter les différentes personnes impliquées dans le Cloud Computing. Cela à permis par la suite de faire face à des points de vue contradictoires, incomplets, confus et imprécis sur la question de l'interaction avec le système d'information et la technique du cloud computing. Mais avec cette approche pour donner un sens à l'ensemble, c'est-à-dire la relation entre le système d'information d'une entreprise et le Cloud Computing, cela à aidé à mieux comprendre les

données textuelles. L'objectif de l'analyse de l'étude de cas était de faire une description très précise du cas et de son contexte. Dans mon cas, les effets du Cloud Computing dans les entreprises, les avantages et les inconvénients par rapport au coût que les entreprises doivent payer et la sécurité de leurs données. Après l'étude de toutes les données collectées, il fallait établir un schéma de chaque étape des processus décrits ci-dessus. Dans le cadre de la méthode d'analyse des études de cas, un certain nombre d'outils était disponible :

Interprétation directe : le principe de cet outil était de sélectionner un cas précis, un seul, et d'essayer d'en trouver la signification, sans recoupement ni sources multiples d'aide (Creswell, 2007, p156-157). Dans mon cas, ce processus a aidé à donner un sens plus fort aux questions, en remettant ensemble toute la compréhension repérée.

Ensuite, il fallait établir des modèles entre mes différents cas (Yin, 2002, p26). En trouvant des similitudes et des différences, il fallait déterminer un lien entre mes affaires et les interpréter dans leur ensemble pour créer une connaissance générale de la question. L'interprétation des différentes affaires peut prendre plusieurs sens ; il peut s'agir de différentes personnes interrogées et d'une étude différente des systèmes d'information sur la même question. C'est ainsi qu'il fallait déterminer quelles étaient les affaires, et à l'aide de cette méthode, déterminer qu'elles étaient les liens entre elles.

De plus, il a fallu développer des généralités à partir des données analysées. Il s'agissait d'une généralisation que les cas qui montrent aux autres personnes, afin qu'ils puissent l'apprendre et l'appliquer à un autre ensemble de population (Creswell, 2007, p163). Après une description complète de l'étude et de son contexte, il eut une présentation. Suite à cela, il fallait présenter les questions qui étaient étudiées dans le contexte précis, c'est-à-dire d'après ma compréhension ou d'après les différentes publications trouvées. Ensuite, l'examen de certaines

des questions ont été posés et à ce stade, il fallait commencer à confirmer ou à discréditer les preuves recueillies, afin de pouvoir commencer à les interpréter.

Enfin, la présentation des déclarations et un résumé de la compréhension sur l'étude, l'interprétation, et une conclusion étant réaliste, afin que le lecteur puisse juger par lui-même.

ii. Etudes des cas : résultat

1. Le coût & la sécurité pour l'entreprise FMG

FOX Mobile à Berlin est une entreprise qui utilise le "Cloud Computing" et qui peut donner des réponses sur les avantages et les inconvénients qu'elle obtient en adoptant le "Cloud Computing". Ayant mené quelques entretiens avec un employé responsable du "Cloud Computing" au sein de FMG, le choix a été la fois facile et difficile. Ayant un salarié dans mon réseau s'y trouvant, cela a permis d'avoir un accéder directe aux contacts et aux informations, mais aussi d'obtenir des informations biaisées et des critiques. Cependant, il fallait essayer de maintenir l'équilibre ce qui il est important pour la recherche. D'autre part, il fallait parvenir à trouver un fournisseur de cloud computing et c'est DNS Europe. Les entretiens ont été menés sur les avantages et les inconvénients qu'ils pensent que les entreprises peuvent obtenir avec leur adoption du Cloud Computing.

Selon la personne interrogée, le FMG a commencé à utiliser le Cloud Computing avec le projet de moteur d'acquisition. Il a été développé par une société de logiciels externe et la société a choisi de le déployer dans le nuage d'Amazon et c'était l'exigence de leur stratégie. Cependant, la décision de mettre l'application dans le nuage a été prise par le groupe Fox Mobile. Elle a été déployée dans le nuage dès le début du projet. La personne interrogée a défini le Cloud Computing comme "*Le Cloud Computing est un moyen flexible d'allouer des ressources à partir d'un pool, permettant de consommer de la puissance de traitement en fonction de vos*

besoins. Il facilite la mise en place et le déclassement des instances de serveurs, ce qui permet d'augmenter la taille de votre infrastructure lorsque vous devez faire face à des pics d'activité tout en économisant des coûts lorsque vous n'avez plus besoin de cette puissance supplémentaire. L'utilisation globale d'un nuage conduit à l'optimisation des ressources de sorte qu'au final, elles sont moins chères pour toutes les personnes concernées". Pour ce projet, le FMG utilise l'IaaS (Infrastructure as a Service) car c'est le modèle qui répond le mieux à ses besoins. Ils utilisent le cloud comme une infrastructure où ils déploient leur propre application. Ils utilisent l'IaaS d'Amazon, qui est géré par une société tierce nommée Right Scale. Interrogé sur la raison de choisir le fournisseur de cloud spécifique, l'interviewé a répondu qu'Amazon est un acteur majeur sur ce marché, ce qui en fait évidemment un candidat. Elle a bénéficié de ses propres besoins internes en matière d'évolutivité et de flexibilité de l'infrastructure et elle ne cesse d'élargir son offre. En ce qui concerne la procédure pour commencer à travailler avec le Cloud Computing et les questions contractuelles et juridiques, la personne interrogée a estimé qu'il est assez simple de créer un compte et de mettre en place un serveur. Il existe de nombreuses images de serveurs prêts à l'emploi qui couvrent les besoins, différentes configurations comme le Web, l'application ou le serveur de bases de données. Cela dit, l'équipe qui a créé l'infrastructure a dû écrire un nombre assez important de scripts pour adapter l'environnement.

Avant l'adoption du Cloud Computing, le FMG utilisait exclusivement les services d'un centre de données classique. M. X était d'avis que l'emplacement des données et les exigences de sécurité qui les entourent sont évidemment des questions importantes et que la conformité aux normes des bases de données et les accords de niveau de service (SLA) y répondent. Bien entendu, le déploiement dans le nuage met en quelque sorte l'accent sur la question de la sécurité des données. Mais le cloud ne signifie pas automatiquement des problèmes de sécurité. Nous

sommes en premier lieu responsables de la sécurisation de notre application. Cela dit, nous avons parfois besoin de certaines conformités standardisées au niveau de l'entreprise. Comme nous prévoyons d'en déployer davantage dans le nuage à l'avenir, nous discutons d'un accord d'entreprise avec Amazon. Lorsqu'on leur a demandé comment ils répondaient à la demande quotidienne avant de passer au cloud, la réponse a été assez simple, car il s'agit d'une nouvelle application et de leur première expérience.

Outre les tests, le coût a été l'un des principaux facteurs qui ont incité la FMG à passer au "cloud". Cependant, la personne interrogée a également déclaré que le coût n'était pas le premier facteur à prendre en compte pour l'adoption du cloud computing. La première raison était de donner à l'équipe une autonomie complète sur ses besoins de déploiement, permettant de contrôler tout le cycle de vie de ses activités. Le Cloud Computing est certainement plus rentable mais les coûts n'étaient pas la raison principale dans ce cas. La motivation première était une nouvelle façon de travailler pour l'équipe, un processus visant à la rendre indépendante, notamment en ce qui concerne ses besoins de déploiement et d'évolutivité.

La seconde interview a été menée avec le même employé du groupe Fox Mobile que la première. L'objectif de cette seconde interview était de s'informer sur la sécurité de l'entreprise et sur les effets du "Cloud Computing" sur la sécurité de l'entreprise, c'est-à-dire du groupe Fox Mobile. La première question qui lui a été posée était de savoir si l'entreprise, c'est-à-dire le FMG, avait pensé aux problèmes de sécurité avant de passer au Cloud Computing et si le Cloud Computing est sécurisé pour vous au niveau de l'entreprise. Selon lui, la sécurité est probablement l'une des questions qui inquiètent les nouveaux venus dans le cloud. Son équipe a repris une application qui était déjà déployée dans le nuage. Néanmoins, comme c'était nouveau pour eux, un de leurs ingénieurs en infrastructure a fait une petite enquête sur ce sujet. Ils ont également examiné la documentation fournie par Amazon sur leurs normes de sécurité.

Ils ont conclu que la sécurité dans le cloud dépend principalement de la façon dont vous traitez les problèmes de sécurité au niveau de votre serveur. Le cloud n'est pas une menace plus importante en tant que telle lorsqu'il s'agit de traiter la sécurité au niveau de votre application (c'est-à-dire l'authentification et l'autorisation d'accès) ou de configurer les ports à ouvrir. Au niveau de l'infrastructure, ils s'appuient sur Amazon et ont le sentiment d'avoir une expérience considérable dans ce domaine. La sécurité étant un problème pour l'entreprise, ma question suivante était de savoir si elle mettait en œuvre la sécurité par elle-même dans l'entreprise. Elle n'a pas mis en place la sécurité au niveau de l'entreprise pour certaines applications dans le nuage. En dehors de la sécurité au niveau des applications, leurs équipes de développeurs s'appuient sur leur équipe d'infrastructure pour les questions de sécurité concernant les réseaux, le pare-feu et les protocoles autorisés à accéder aux serveurs ou aux données dans leur centre de données standard. Les données ne sont pas cryptées et il s'inquiétait de l'endroit où les données étaient stockées. En ce qui concerne la connexion cryptée, ils l'ont fait chiffrer. Ils utilisent le HTTPS pour la communication entre leur application frontale déployée dans le nuage et leurs applications API qui sont déployées dans leur centre de données standard. De plus, l'accès à leurs API implique que le client utilise un certificat client SSL (Secure Sockets Layer) qu'ils ont émis.

Le FMG s'appuie sur les protocoles pris en charge par le serveur d'application ou le système d'exploitation sous-jacents. Comme la FMG utilise IaaS du nuage Amazon EC2 et que la sécurité est la responsabilité des deux parties, c'est-à-dire l'entreprise et le fournisseur du nuage, sous la forme de la sécurité physique, de l'infrastructure réseau, des systèmes informatiques et de la sécurité des applications, ils considèrent la sécurité physique comme faisant partie du service et partent donc du principe qu'aucune personne ne peut se connecter du nuage à leur serveur à partir d'une adresse privée, car cela ne devrait être réservé qu'au personnel technique

d'Amazon. Toutefois, ils s'occupent de la sécurité au niveau des systèmes informatiques, c'est-à-dire de la sécurité du web, et prévoient d'en faire plus.

La personne interrogée a décrit le cas du FMG sur le Cloud Computing comme quelque chose à apprendre sur le nuage. Il a déclaré que la sécurité est toujours quelque chose dont il faut tenir compte au niveau de leur application. Une chose est sûre : lorsque vous êtes dans le nuage, vous avez théoriquement moins de contrôle que lorsque vous êtes dans votre propre serveur ou réseau privé. C'est pourquoi il a estimé qu'il est plus de leur devoir de le rendre plus sûr que de dépendre des autres. Ainsi, ils peuvent configurer un pare-feu dans le nuage, limiter l'accès ; par exemple, ils ferment tous les ports sauf 80. Il était d'avis que cela peut être pour le marketing que ce fournisseur de cloud computing dit qu'il est plus sûr, mais il pensait que sa décision d'entreprise et son devoir de prendre et de mettre en œuvre la sécurité du service cloud proposé.

2. Le point de vue fournisseur

Une fois l'entretien avec le FMG, c'est-à-dire les utilisateurs du cloud computing, il était temps de voir l'autre côté de la médaille, c'est-à-dire d'avoir le point de vue du fournisseur de cloud computing. DNS Europe est un fournisseur de services d'informatique en nuage, une interview a été mené concernant ma question de recherche pour savoir ce qu'ils pensent et pour parler aux entreprises des avantages qu'elles peuvent tirer de l'adoption de l'informatique en nuage. Parallèlement, les questions posées sur les inconvénients du cloud computing et sur l'état d'avancement de cette technologie jusqu'à aujourd'hui n'ont pas tout eux des réponses. L'interview a été menée avec un employé de DNS Europe nommé Y. Il est actuellement directeur technique chez le fournisseur de services de cloud computing DNS Europe et est basé à plein temps à Belgrade, en Serbie. l'entretien était par téléphone en raison du problème de

distance. L'objectif de l'entretien était d'avoir le point de vue des fournisseurs de services de Cloud Computing sur ce qu'ils pensent être le Cloud Computing, sur l'état d'avancement de la technologie, sur les avantages qu'ils offrent aux entreprises et sur les inconvénients que présente encore, selon eux, la technologie en termes de coût et de sécurité. Selon la personne interrogée, DNS Europe est une entreprise paneuropéenne de communications IP qui offre à ses clients dans toute l'Europe des services et des solutions Internet sur mesure allant de l'intégration des systèmes des fournisseurs d'accès à Internet au développement de produits et au conseil.

M. Y est d'avis que le "Cloud Computing" dans le monde des affaires est la nouvelle chose sur laquelle tout le monde se concentre et, grâce au "Cloud Computing", tout le monde se concentre aussi sur l'offre et la gestion et la plupart de cette offre et de cette gestion s'articule autour du thème de la sécurité et de la conformité. La sécurité est donc le principal obstacle qui freine de nombreuses entreprises dans le domaine des services traditionnels de "cloud computing". Comme dans le modèle actuel des services de cloud computing, il est très difficile de savoir où leurs données sont physiquement stockées. En d'autres termes, il viole presque toutes les dispositions et exigences de la plupart des auditeurs de sécurité de l'information, à savoir où résident leurs données et qui a accès aux machines physiques. La personne interrogée a également parlé des tendances du marché et de la manière dont les entreprises résolvent leurs problèmes techniques en gardant à l'esprit la technologie du cloud computing. Selon lui, la plupart des entreprises qui contournent les limites du "Cloud Computing" commencent à utiliser des nuages privés. Le nuage privé est exactement le même que celui d'Amazon ou de Google, sauf qu'il est basé sur le matériel que les gens possèdent eux-mêmes. Avec cette approche, on obtient tous les avantages du "Cloud Computing" qui comprennent la virtualisation, l'encapsulation et la possibilité de faire migrer les applications. Ainsi, grâce à cette approche, la politique de sécurité des données de l'entreprise va jusqu'à la couche physique. Par

conséquent, DNS Europe trouve des clients qui manquent de connaissances au niveau des systèmes d'exploitation, des systèmes de grille ou de l'administration des systèmes et qui ont des compétences en développement, puis leur fournit l'administration des systèmes. Un autre avantage du Cloud Computing est que les développeurs n'ont pas à penser à l'administration du système et à d'autres choses et se contentent de coder et de développer. La personne interrogée pense que le cloud computing est très bénéfique pour les petites et moyennes entreprises et qu'il va prospérer, surtout lorsque les différents services en nuage auront une inter-collaboration, par exemple, dans les médias sociaux où Facebook est capable de s'authentifier avec le scintillement et le twitter. Cependant, les grandes entreprises ne sont toujours pas sûres de l'informatique dans les nuages et ont leurs réserves, ce qui rend le nuage privé très intéressant pour elles. Les nuages privés et les centres de données sont essentiellement la même chose, les centres de données étant les sous-ensembles de tous les services de nuage.

c. Étude empirique

i. L'effet coût

Une chose que tout le monde entend avec le "Cloud Computing" est le coût et c'est pourquoi la question de recherche a été conçu pour savoir comment le "Cloud Computing" impact les entreprises. Au cours de mes entretiens avec FMG, le but était de découvrir comment les coûts affectent l'entreprise dans son activité et si le Cloud Computing est vraiment rentable. Comme indiqué dans la partie théorie, selon laquelle l'attrait économique du cloud computing est souvent mentionné comme "*la conversion des dépenses d'investissement en dépenses d'exploitation*" (Armbrust et al. 2009, p12), les entreprises (FMG) considèrent le cloud computing de la même manière. FMG a déclaré que, hormis le fait de donner à l'équipe de développement une autonomie complète, l'autre raison était la rentabilité. Il existe différents modèles de coûts/prix détaillés sur le marché du Cloud Computing (Khajeh-Hosseini et al.,

2010b, p4), c'est-à-dire le paiement au fur et à mesure, la tarification par paliers, la tarification à l'unité et la tarification par abonnement. Le FMG a également adopté l'un des modèles de coût appelé "*pay as you go*", dans lequel le FMG paie pour chaque heure utilisée. Ils achètent donc des heures au fournisseur de "cloud computing", qui sont réparties de manière non uniforme dans le temps dans la communauté du réseau.

DNS Europe est d'accord avec la déclaration selon laquelle la flexibilité et le facteur d'élasticité rendent le Cloud Computing rentable pour les entreprises. L'employé de DNS Europe a déclaré que grâce à l'extensibilité ou à l'élasticité, les entreprises peuvent désormais évoluer en fonction de leurs besoins.

Outre l'élasticité, la taille de l'entreprise est un autre facteur sur lequel le coût du "cloud computing" a une incidence. Dans le rapport "Clearing the Air on Cloud Computing" de McKinsey & Co, ils affirment que le Cloud Computing peut coûter deux fois plus que les centres de données internes. Il y a un autre aspect qui peut s'avérer bénéfique ou désavantageux pour les entreprises. Mayur et ses collaborateurs (2008) ont étudié le service de stockage de données S3 d'Amazon pour les applications scientifiques à forte intensité de données. Selon eux, le service S3 regroupe, selon une méthode de tarification unique, les trois caractéristiques des données, à savoir une grande durabilité, une grande disponibilité et un accès rapide, mais la plupart des applications n'ont pas besoin d'être toutes regroupées (Mayur et al., 2008, p8).

Ainsi en résumé

- Il existe quatre facteurs qui influent sur le facteur coût de toute entreprise. Ils comprennent l'élasticité ou l'extensibilité, la flexibilité, le coût du centre de données, les modèles de tarification et le coût d'administration.

- Le Cloud Computing est rentable pour les entreprises en ce qui concerne ces facteurs et est très avantageux pour les petites et moyennes entreprises.

ii. L'effet sécurité

La deuxième partie de ma question de recherche portait sur les problèmes de sécurité des données du Cloud Computing. Au cours de mon étude empirique, il était question essayer de déterminer si l'adoption du cloud computing en matière de sécurité des données est bénéfique ou si elle constitue un inconvénient pour les entreprises.

La question était très générale, à savoir si le FMG a pensé aux questions de sécurité avant de passer au "Cloud Computing" et si le "Cloud Computing" est suffisamment sûr pour eux. L'employé du FMG a réitéré sa première approche, comme il l'avait dit lors de la première interview, à savoir que c'était la décision de l'entreprise qui avait développé l'application de la déployer dans le Cloud. Comme mentionné dans la partie théorique, la plupart des problèmes de sécurité qui se posent aux entreprises du fait de l'utilisation du cloud computing sont dus à l'absence de contrôle sur l'infrastructure physique. Les entreprises ne savent pas où résident les données ni quel mécanisme de sécurité est appliqué pour les protéger, c'est-à-dire si les données sont cryptées ou non et, si oui, quelle méthode de cryptage est appliquée, si la connexion utilisée pour que les données voyagent dans le nuage est cryptée et comment les clés de cryptage sont gérées (Window Security, 2010).

Conclusion

Dans ce travail de recherche, le sujet abordé les effets du Cloud Computing dans les entreprises. Les domaines spécifiques sur lesquels il fallait faire des recherches au cours de mon étude étaient le coût et la sécurité. Le constat est que le cloud computing est un sujet très brûlant de nos jours et que de nombreuses entreprises s'y intéressent. La plupart des entreprises en ont une idée, mais il existe toujours une certaine confusion quant à la définition réelle du "cloud computing". Cela est compréhensible car cette technologie est encore à ses débuts, mais comme elle a évolué à partir du Grid Computing, la plupart des entreprises qui ont utilisé le Grid Computing sont mieux à même de comprendre le terme "Cloud Computing". Il existe une confusion ou un désaccord sur les limites du "Cloud Computing" car de nombreuses entreprises et même des fournisseurs de cloud computing pensent que le cloud privé fait partie du "Cloud Computing". Toutefois, dans mes recherches, le constat est que *le Cloud Computing est la somme du Software as a Service (SaaS) et de l'Utility Computing, mais n'inclut pas les nuages privés*.

Les entreprises qui sont en train de prendre la décision d'adopter le "Cloud Computing" sont confrontées à un véritable dilemme car elles entendent des avis différents (positifs et négatifs) provenant de sources différentes. La première caractéristique qui pousse les entreprises à envisager le "cloud computing" est l'effet de coût. Une recherche approfondie sur l'effet de coût sur les entreprises. Il existe de nombreux facteurs ou caractéristiques qui influent sur le coût du cloud computing pour les entreprises. Ces facteurs comprennent l'élasticité, la flexibilité, le coût des bases de données, les modèles de tarification et les coûts administratifs. L'élasticité est le facteur le plus important pour rendre le Cloud Computing rentable pour les entreprises et la plupart des entreprises passent au Cloud Computing en raison de cette caractéristique. La conclusion est que les entreprises économisent leur capital en ne construisant pas leur centre de

données et en n'embauchant pas d'employés pour les gérer. En plus de cette flexibilité et des différents modèles de tarification, le cloud computing est plus rentable pour les entreprises. Toutefois, une conclusion importante est que ces avantages ne concernent que les petites et moyennes entreprises. Les grandes entreprises peuvent réduire leurs coûts en construisant un grand centre de données en raison de leur demande et du capital dont elles disposent. En d'autres termes, le cloud privé est une solution parfaite pour les grandes entreprises.

Dans mon étude, il fallait également gérer les résultats concernant la deuxième partie de ma question de recherche, à savoir la sécurité dans le Cloud Computing pour les entreprises. Je voudrais ici mentionner la première réponse de mon entretien avec l'employé de la FMG. Il a clairement indiqué que le bénéfice de la sécurité n'est pas la valeur ajoutée du Cloud Computing. La conclusion est que le Cloud Computing posait de nombreux problèmes de sécurité aux entreprises. Ces problèmes comprennent le manque de contrôle sur les données physiques, la sécurité du navigateur web, les attaques par déni de service distribué, la perte des clés de cryptage, les risques juridiques, les problèmes de réseau et les catastrophes naturelles. Toutefois, outre ces inconvénients, il existe également des avantages pour les entreprises. Ces avantages sont liés à l'échelle, à l'interface standard, à la journalisation, à la gestion des risques et à l'efficacité des mises à jour et des défauts. Toutefois, dans mon étude, la conclusion est que ces avantages ne permettent pas de surmonter les problèmes de sécurité du cloud computing. Par conséquent, les entreprises ne devraient pas adopter le cloud computing en raison d'une meilleure sécurité de leurs données.

Annexes

GUIDE D'ENTRETIEN – ETUDE DE CAS

Guide d'entretien : FMG

Phase introductive

- Présentez-vous ? Quel poste occupez-vous ?
- Quel est le secteur d'activité de votre société ?

Phase de recentrage : Passage au le cloud computing

- Quelle est votre position et vos responsabilités dans l'entreprise ?
- Quels sont les principaux domaines de travail du groupe Fox Mobile ? Quelle est la taille de l'entreprise ? Vous la considérez comme grande, moyenne ou petite ?
- Je suppose que vous utilisez l'informatique en nuage. Quand Fox Mobile a-t-elle adopté l'informatique en nuage ?
- Qui a décidé de passer au cloud computing ?
- Pouvez-vous définir le cloud computing comme ce qu'il est pour vous ?
- Quel service de cloud computing utilisez-vous ? IaaS, PaaS ou SaaS ? Et pourquoi ?
- Quel fournisseur de cloud computing utilisez-vous ?
- Avez-vous une raison particulière de choisir ce fournisseur ?
- Comment avez-vous commencé à utiliser le cloud ? Processus facile ? Procédures juridiques ? Nombre de jours pour commencer à travailler ? Contrat à signer ?
- Comment la Fox traitait-elle ses données, avant l'informatique dématérialisée ? Si centre de données interneQuels étaient les problèmes qu'il contenait ?
- Selon vous, quels étaient les facteurs généraux/principaux pour passer au Cloud ?
- Comment assuriez-vous la restauration avant que la demande quotidienne de l'application ne passe au Cloud ? Avez-vous deviné les heures de pointe ?

Question sur le coût

- Le cloud computing est-il plus rentable et constitue-t-il la principale raison de passer au cloud ?
- Pensez-vous que "le modèle de coût" est bénéfique pour les entreprises et vous en êtes satisfait ?
- Quel modèle de coûts utilisez-vous avec les fournisseurs de services en nuage ? « *Pay as you go* », à plusieurs niveaux, à l'unité, par abonnement ?
- Comme vous êtes une grande entreprise, pourquoi n'avez-vous pas opté pour un nuage privé et des économies à long terme ?
- Voyez-vous des problèmes dans le Cloud computing jusqu'à présent ?
- Connaissez-vous le facteur d'élasticité du nuage ? Qu'en pensez-vous ?
- Avant l'arrivée du cloud Grid sur le marché, pourquoi n'avez-vous pas opté pour cette solution ?

- De nombreux fournisseurs de cloud computing offrent une grande durabilité, une haute disponibilité et un accès rapide, mais certaines applications ne le font pas toutes. Votre application avait-elle besoin de toutes ces caractéristiques ? Si ce n'est pas le cas, quel est le rapport coût-efficacité de l'informatique en nuage ?
- L'administration du système a été réduite par le cloud ? Est-ce que cela rend les choses plus rentables pour les entreprises ?

Question sur la sécurité :

- Avez-vous pensé à la question de la sécurité lors du passage au cloud computing ?
- Pour votre entreprise, le cloud computing est-il sécurisé ou non ?
- Avez-vous mis en place la sécurité par vous-même dans l'entreprise ?
- Savez-vous où vos données sont stockées et cela vous inquiète-t-il ?
- Savez-vous si vos données sont cryptées ? Si oui, quelle est la méthode de cryptage appliqué ?
- La connexion utilisée pour les données de voyage est-elle cryptée ?
- Le https est fait par vous ou le nuage l'a fait ?
- Mettez-vous en œuvre le TLS (Transport Layer Security) ?
- Dans l'IaaS d'Amazon EC2, la sécurité est la responsabilité des deux parties, c'est-à-dire l'entreprise et le fournisseur de cloud, sous la forme de la sécurité physique, de l'infrastructure réseau, des systèmes informatiques et de la sécurité des applications. Comment la gérer ?
- Selon vous, quels sont les avantages de l'informatique en nuage en matière de sécurité ?
- Pensez-vous que la sécurité du cloud computing s'améliore grâce à un facteur de différenciation du marché ?
- Dans quelle mesure l'interface standard des services de sécurité gérés est-elle bénéfique pour les entreprises ?
- Les preuves et l'audit s'améliorent-ils avec le cloud computing, c'est-à-dire la journalisation ?
- L'informatique dans les nuages se caractérise par des mises à jour et des défauts efficaces ; pensez-vous qu'elle rend les données plus sûres ?
- Êtes-vous satisfait de la sécurité fournie par les fournisseurs de services d'informatique en nuage ? Qu'attendez-vous à l'avenir de l'informatique dans les nuages en matière de sécurité ?
- Pouvez-vous penser à des améliorations de la sécurité du Cloud computing de la part des fournisseurs pour que les entreprises se sentent plus en sécurité ?

Phase introductive

- Présentez-vous ? Quel poste occupez-vous ?
- Quel est le secteur d’activité de votre société ?

Phase de recentrage

- Quelle est votre position et vos responsabilités au sein de DNS Europe ?
- Quels sont les principaux domaines de travail de DNS ? Quelle est la taille de l'entreprise ?
- Quelles sont les entreprises dont vous vous occupez ?
- Pouvez-vous définir le cloud computing comme ce qu'il est pour vous ?
- Chez DNS, vous fournissez le nuage privé ou aussi le cloud computing ?

- Quel service de cloud computing fournissez-vous ? IaaS, PaaS ou SaaS ?
- Comment une entreprise peut-elle commencer à utiliser le cloud ? Un processus facile ? Procédures légales ?
- Nombre de jours pour commencer à travailler ? Contrat à signer ?
- Comment différencier un centre de données d'un nuage privé ?
- Pourquoi utilisez-vous le terme "grid computing" sur votre site et non le terme "cloud computing" ?
- Avez-vous une interface pour les utilisateurs ?

Bibliographie

- ARMBRUST M., FOX A., GRIFFITH, R., JOSEPH, A., KATZ, R., KONWINSKI, A., LEE, G., PATTERSON, D., RABKIN, A., STOICA, I. and ZAHARIA, M. (2009). *Above the Clouds: A Berkeley View of Cloud Computing. Technical Report.* University of California at Berkeley.
- BALDING C. *Assessing the Security Benefits of Cloud Computing.* (2008). Cloud Security Blog, Accessed 10th May, 2019.
- BEIGBEDER J. *PSSI Orientation – ENS – 01/03/2017* , Paris 2017
- CHARLES T. BETZ , KAUFMANN. *M Architecture and Patterns for IT*, 2011
- DE GAULLE C, *Mémoires de guerre – L'Unité : 1942-1944 (tome II)*, éd. Plon, Paris, 1956 pp.22
- CREEGER, M. (2009). "*CTO roundtable: cloud computing,"* Comm. of the ACM, vol. 52.
- CRESWELL, J. W. (2007): Qualitative inquiry and research design : choosing among five traditions. 2nd ed., Sage Publications, Thousand Oaks, Calif.
- FELLOWES, W. (2008). Partly Cloudy, Blue-Sky Thinking About Cloud Computing. Whitepaper. 451 Group.
- MARSHALL, C. & ROSSMAN, G.B., (1989), *Designing Qualitative Research, Newbury Park*, California: Sage.
- FOSTER I, KESSELMAN, C, TUECKE S (2001) The Anatomy of the Grid: Enabling Scalable Virtual Organization. International Journal of High-Performance Computing Applications 15(3):200-222
- FOSTER I, KESSELMAN C (1998) Computational Grids. http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.25.9598&rank=1

- HARMS, U., REHM, H-J., RUETER, T., WITTMANN, H. (2006) *Grid Computing für virtualisierte Infrastrukturen.* In: Barth T, Schüll A (eds) Grid Computing: Konzepte, Technologien, Anwendungen, pp. 1-15. Vieweg+Teubner, Wiesbaden
- KHAJEH-HOSSEINI, A., GREENWOOD, D., SOMMERVILLE, I., (2010a). *Cloud Migration: A Case Study of Migrating an Enterprise IT System to IaaS.* Submitted to IEEE CLOUD 2010
- KHAJEH-HOSSEINI, A., SOMMERVILLE, I., SRIRAM, I., (2010b). *Research Challenges for Enterprise Cloud Computing.* Submitted to the 1st ACM Symposium on Cloud Computing, SOCC 2010.
- IRACST - *International Journal of Computer Science and Information Technology & Security* (IJCSITS) Vol. 1, No. 2, December 2011
- KVALE, S. (1996) *Interviews: an introduction to qualitative research interviewing*, SAGE, Thousand Oaks, CA.
- LEKWALL, P., AND WAHLBIN, C. (2001). *Information för Marknadsföringsbeslut* (4th ed.). Göteborg: IHM Förlag.
- LUBLINSKY, BORIS. (2009, April 22). *Cleaning the air on Cloud Computing*. from http://www.infoq.com/news/2009/04/ai
- NIST, *The NIST Definition of Cloud Computing*, 2011 at https://csrc.nist.gov/publications/detail/sp/800-145/final
- MAYUR, P., ADRIANA, L., MATEI, R., AND SIMSON, G., (2008). *Amazon S3 for Science Grids: a Viable Solution?* In Data-Aware Distributed Computing Workshop (DADC).
- MARSHALL, C. & ROSSMAN, G.B., (1989), *Designing Qualitative Research*, Newbury Park, California: Sage.

- QAMAR, S., LAL, N., SINGH, M., (2010). Internet Ware Cloud Computing: Challenges. (IJCSIS) International Journal of Computer Science and Information Security, Vol. 7, No. 3, March 2010.
- STANOEVSKA-SLABEVA, K., WOZNIAK, T. (2009). Grid Basics. In: *Stanoevska-Slabeva, K. Wozniak, T., and Ristol, S., Grid and Cloud Computing A Business Perspective on Technology and Applications.* Springer Berlin Heidelberg, 2009.
- S. SRINIVASAN "*Is Security Realistic In Cloud Computing?"* - Jesse H. Jones School of Business Texas Southern University USA (2011)
- SURYATEJA P. "*Threats and Vulnerabilities of Cloud Computing: A Review*" CSE Dept., Vishnu Institute of Technology, Bhimavaram, India, 2016
- WEISHÄUPL T., DONNO F., SCHIKUTA E., STOCKINGER H., WANEK H. (2005). *Business In the Grid: The BIG Project.* Proceedings of the 2nd International Workshop on Grid Economics and Business Models (GECON 2005).

Résultat Compilatio

Bonjour,
Une partie de votre document Mémoire de Franklyn Final.docx vient d'être analysée !
Le taux de similitude de cette partie est de **1%**
Vous pouvez consulter son rapport, même si l'analyse de votre document n'est pas totalement terminée en vous connectant à votre compte Compilatio puis en cliquant sur le document en cours d'analyse.

Hello,
A part of your document Mémoire de Franklyn Final.docx has been analysed !
The similiraty index of this part is **1%.**
Connect to your Compilatio account and view the corresponding report (eventually the analysis of the whole document is not finished).

Guten Tag,
Ein Teil Ihres Dokument Mémoire de Franklyn Final.docx ist analysiert worden !
Der Prozentsatz an Uebereinstimmungen betraegt **1%.**
Loggen Sie sich in Ihrem Compilatio Konto ein und schauen Sie den passenden Bericht an (die Analyse des vollstaendigem Dokument ist eventuell noch nicht abgeschlossen).

Buongiorno,
Una parte del tuo documento Mémoire de Franklyn Final.docx è appena stata analizzata !
la percentuale di similitudine di questa parte è di **1%**
Puoi consultare il tuo rapporto, anche se l'analisi del tuo documento non è totalmente terminata connettendoti a il tuo conto Compilatio e poi cliccando sul documento in corso di analisi.

Buenos días,
¡Parte de su documento Mémoire de Franklyn Final.docx acaba de ser analizada!
el porcentaje de similitud de esta parte es de **1%**
Puede consultar su informe, aunque el análisis no haya acabado por completo conectándose a su cuenta Compilatio y haciendo un clic en el documento analizándose.

Compilatio.net
LOGICIEL D'AIDE À LA DÉTECTION DE PLAGIAT

Logiciel de détection de plagiat
COMPILATIO.NET, leader francais de la prevention du plagiat
http://www.compilatio.net