

# **Dissertation**

Thème : cloud

Pauline DEVICTOR

Quentin DUBOIS

Vinh FAUCHER

Florian LATAPIE

28 février 2023

## Explication du sujet

Le cloud correspond à l'utilisation de la mémoire et des capacités de calcul des ordinateurs et des serveurs répartis dans le monde entier et liés par le réseau afin d'exécuter des applications. Il existe plusieurs catégories de cloud : les clouds privés, les clouds publics et le cloud hybride.

Le cloud privé correspond au cas où les datacenters, serveurs et infrastructures sont détenues par l'entreprise les utilisant.

Le cloud public désigne ceux détenus par une entreprise différente de celle qui les utilise, on y retrouve par exemple Google Drive, OneDrive, Microsoft Azure, AWS, Google Cloud Platform pour ne citer que les plus connus

Enfin, le cloud hybride consiste en une combinaison du cloud privé et du cloud public. Il permet aux entreprises de rester souveraines des données confidentielles et sensibles ainsi que certaines applications.

Il existe plusieurs modèles de cloud proposés par les fournisseurs. Le premier est le modèle IaaS signifiant *Infrastructure as a Service*. Le fournisseur de cloud met à disposition des clients uniquement les infrastructures et machines souhaitées. Le fournisseur s'occupe de gérer l'ensemble des problématiques associées au matériel tel que le stockage des données, la maintenance, le refroidissement ou l'approvisionnement électrique. Le client doit donc s'occuper de gérer, maintenir et mettre à jour tout le logiciel présent sur les machines, allant du système d'exploitation, des environnements de développement et d'exécution. Il doit également s'occuper du déploiement de ses applications.

Le deuxième modèle est le PaaS pour *Platform as a Service*, ce modèle est un sur-ensemble de l'IaaS. Il fournit les mêmes services que l'IaaS, mais ajoute la prise en charge par le fournisseur du système d'exploitation et les environnements de développement et

d'exécution. Le client n'a plus qu'à importer le code de son application afin de pouvoir offrir ses services.

Le dernier modèle est le SaaS pour *Software as a Service*, ce modèle contient tous les points déjà évoqués précédemment, c'est-à-dire tout ce que contient le PaaS ainsi qu'une application. Le client est simplement utilisateur de cette application et ses données sont stockées sur des serveurs à distance. Ce type de cloud est le plus utilisé par le grand public. Beaucoup d'applications utilisent ce modèle tel qu'Microsoft 365<sup>1</sup>, Google Docs Editors, Google photos, iCloud, Notion ou Canva pour ne citer que les plus connus.

Ces trois modèles sont les plus répandus et aussi les plus anciens. Il existe également deux autres modèles : le CaaS<sup>2</sup> et le FaaS<sup>3</sup>. Nous ne développerons pas ces points, nous les donnons uniquement à titre indicatif afin de faire une description complète des différents modèles de cloud actuellement disponibles.

Ce qui est important à retenir est que le cloud est un terme générique définissant de nombreux concepts différents. La notion de cloud peut avoir un sens un peu différent en fonction du modèle utilisé. Dans le cas général, le cloud correspond à l'hébergement par un fournisseur de machines permettant d'exécuter une application et de stocker les données associées.

---

<sup>1</sup> Anciennement connu sous le nom de « Office 365 »

<sup>2</sup> Containers as a Service

<sup>3</sup> Function as a Service

## Dissertation

Afin d'accélérer et de faciliter les échanges d'informations, nous avons inventé Internet qui fut l'une des plus grandes révolutions technologiques de la fin du siècle dernier. Toutes ces technologies ont permis de répondre à un besoin d'amélioration de nos systèmes de communication, ainsi qu'à l'accessibilité du savoir. C'est dans ce contexte que le cloud public a vu le jour, avec l'apparition des services de messagerie électronique tels que Hotmail en 1996 et Gmail en 2004. Ces services ont été les premiers à proposer un stockage des données en ligne, avant de donner naissance à des solutions plus complètes telles que le *cloud computing* (informatique cloud). Le cloud désigne des serveurs accessibles sur Internet, stockant des données et offrant des services à l'aide de ses données. Les serveurs situés dans le cloud sont hébergés au sein de *datacenters* (centres de données) répartis dans le monde entier. L'utilisation du *cloud computing* permet aux utilisateurs et aux entreprises de s'affranchir de la nécessité de gérer des serveurs physiques eux-mêmes et d'exécuter des applications logicielles sur leurs propres équipements. Cette solution, à l'origine destinée aux entreprises, s'est ouverte ces dernières années aux particuliers. Ce phénomène d'utilisation du cloud s'est d'autant plus répandu lors des multiples confinements ayant eu lieu à la suite de la pandémie de la COVID-19. Les utilisateurs ne sont souvent pas conscients de toutes les données qui les concernent, qu'elles aient été publiées sur le cloud par eux-mêmes ou automatiquement collectées par les services qu'ils utilisent. Il serait intéressant de se demander comment pouvons-nous concilier la nécessité de la présence des données dans le cloud avec les contraintes de confidentialité et de droit à l'oubli, tout en répondant aux enjeux éthiques liés à la collecte et au traitement massif de ces données.

Dans un premier temps, nous évoquerons les avantages liés à l'utilisation du cloud, puis dans un second temps, nous détaillerons les problèmes liés à l'usage du cloud pour les

particuliers. Enfin, nous en concluons sur la pertinence de l'outil en prenant en compte les risques qui y sont associés.

L'avantage principal du cloud est la *scalabilité*, c'est-à-dire pouvoir redimensionner rapidement la taille d'une architecture matérielle : le logiciel étant détaché du matériel, il suffit d'avoir plus de ressources afin d'augmenter le nombre d'utilisateurs auxquels peut répondre notre application. Dans le cloud, l'augmentation de la quantité de stockage, de la quantité de mémoire RAM<sup>4</sup> ou du nombre de processeurs se fait en quelques minutes. C'est l'une des raisons majeures qui pousse la plupart des entreprises à passer d'un cloud privé à un cloud public. Parmi ces entreprises, il y a notamment Air France qui est venue nous parler de cette migration à Polytech lors d'une conférence en octobre 2022. Leur objectif étant de pouvoir ajuster leur architecture matérielle au besoin réel. Ce changement leur permettrait d'éviter de subir les mêmes conséquences que celles pendant la crise du secteur aérien causée par la COVID-19. À cette époque, leur installation informatique n'était que peu utilisée, mais elle engendrait des dépenses considérables. Un autre exemple, plus marquant, est une application qui fait grand bruit ces derniers mois du nom de ChatGPT. Cette intelligence artificielle dédiée à la conversation a réussi à battre le record de croissance en nombre d'utilisateurs en passant en moins de deux mois de 0 à 100 millions d'utilisateurs. Cette performance a été rendue possible grâce à la *scalabilité* de son service basé dans le cloud, sans quoi l'application n'aurait pas pu répondre à une augmentation aussi forte des demandes.

---

<sup>4</sup> Random Access Memory : mémoire vive

Le fait de ne pas être propriétaire de ses propres machines, mais d'être seulement locataire peut consister en un avantage financier. Comme toute location, le client n'a pas besoin d'investir des sommes importantes afin d'acquérir le matériel. Le prix est mensuel et dépend uniquement de l'infrastructure choisie par le client. Ce modèle économique est notamment très avantageux pour les petites et moyennes entreprises (PME), car cela leur permet de pouvoir s'offrir une infrastructure sur-mesure adaptée à leurs besoins, sans avoir de coût d'investissement élevé pour l'achat des machines.

Toujours en lien avec le coût, la maintenance, l'énergie, le refroidissement et les locaux sont également compris. Cela permet aux entreprises d'avoir une bonne estimation de ses dépenses mensuelles pour leurs infrastructures.

Les fournisseurs proposent des niveaux de disponibilité de services approchant les 99,9 %, un chiffre bien supérieur à ce que peuvent généralement offrir les PME qui possèdent leurs propres serveurs. Par exemple, si un problème survient sur une machine le week-end, il est souvent nécessaire d'attendre jusqu'au lundi pour que le problème soit réparé. Cela s'explique par le fait que ces entreprises ne peuvent pas se permettre de payer une équipe de maintenance le week-end en plus de la semaine.

Le cloud permet de pouvoir accéder à ses données indépendamment de sa position géographique sur le globe. Le cloud facilite donc le télétravail pour les entreprises. Récemment, cet avantage a aidé bon nombre d'entreprises durant la pandémie de la COVID-19, leur permettant de pouvoir continuer à exercer leur activité à distance.

Le cloud public présente un autre avantage en permettant le partage de fichiers entre plusieurs utilisateurs. Étant stockés de manière unique sur un serveur distant, il est possible de présenter un fichier à plusieurs personnes simultanément, à l'instar d'une page web. Cette facilité de partage facilite la collaboration entre les utilisateurs, ce qui peut être très bénéfique dans le cadre de projets impliquant plusieurs personnes.

Les particuliers peuvent utiliser le cloud via des applications pour accéder à des services de domotique de type *smart home*<sup>5</sup>. Par exemple, il est possible d'augmenter la température de sa maison avant de rentrer du travail ou de consulter ce qui s'est passé chez soi pendant les vacances loin de la maison.

Le cloud public, sous forme d'application, permet d'offrir de nouveaux services à des particuliers qui ont souvent peu ou pas de connaissances dans ce domaine, élargissant ainsi l'accès à ces services pour un plus grand nombre de personnes.

Cependant, malgré les nombreux avantages du cloud, il ne faut pas négliger l'autre face de la même pièce, avantages et inconvénients sont indissociables.

Il convient de commencer par évoquer le problème le plus important, à savoir celui de la confidentialité des données et de leur propriété. L'accessibilité des données en ligne peut favoriser la divulgation de données vulnérables. Des personnes non autorisées peuvent consulter les données, dans le cas où la gestion des droits d'accès est mal configurée.

---

<sup>5</sup> Maison intelligente

De plus, les données peuvent être stockées sur des serveurs partagés avec d'autres clients, ce qui peut également augmenter le risque de violation de la confidentialité.

Bien évidemment, le problème de la confidentialité est étroitement lié au problème de sécurité.

Par ailleurs, nous ne pouvons parler de connexion internet sans évoquer la question de la sécurité. Nous pouvons ainsi nous demander si le cloud que l'on utilise est réellement sécurisé. En effet, nous ne voulons pas que n'importe qui puisse accéder à nos données personnelles selon leur envie. Ce qui implique une sécurité au moment de l'envoi et de la réception des données, puis d'une sécurité au niveau du stockage des données. Cependant, n'ayant pas la main à ce niveau, nous ne pouvons pas en tant qu'utilisateur nous assurer de cette sécurité, il convient alors aux entreprises gérant le cloud d'informer leurs utilisateurs des possibles problèmes rencontrés. Afin d'éviter de passer ceci sous secret, il existe des lois obligeant les entreprises à informer leurs clients en cas de violation de données personnelles telle que la loi du 6 janvier 1978 ou encore le décret du 30 mars 2012. Néanmoins, certaines entreprises peuvent essayer de ne pas respecter ces lois dans le but d'éviter d'entacher leur réputation. En effet, nous pouvons citer le cas Uber dans lequel l'ex-responsable de la sécurité a caché une faille ultra-massive. En 2016, Uber a été victime d'un piratage informatique et le hacker est parvenu à télécharger les données personnelles de 57 millions d'utilisateurs et de chauffeurs Uber. Il est donc légitime de se demander s'il s'agit d'un cas isolé ou bien de quelque chose de plus répandu qu'il n'y paraît.

Cependant, une sécurité accrue peut engendrer un autre problème : celui de la surveillance constante. Les entreprises responsables de la gestion du cloud doivent non seulement garantir la confidentialité des données stockées, mais également s'assurer qu'elles ne



représentent aucun danger pour le cloud ou les autres utilisateurs. Pour cela, elles doivent procéder à une vérification minutieuse des données envoyées par les utilisateurs, ce qui nécessite une surveillance continue. Cette surveillance est particulièrement essentielle pour les hébergeurs de contenu tels que YouTube et Twitch, pour ne citer que les plus grands.

En raison de la redondance souvent présente dans le cloud, se pose la problématique de la souveraineté des données pour les utilisateurs, étant donné que celles-ci peuvent exister sous forme de plusieurs copies. S'il n'existe pas de copies de nos données, alors il y a un risque de perte si les serveurs sont détruits. L'incendie chez OVH en mars 2021 a entraîné des pertes de données pour les clients dépendant de ce datacenter. La perte fut totale pour certains mais partielle pour d'autres. Cependant, un des arguments de vente du cloud est justement la persistance des données que nous stockons, il peut donc être intéressant d'avoir des sauvegardes afin de pouvoir restaurer les données en cas de problèmes. Néanmoins, si ces sauvegardes existent réellement, elles sont généralement effectuées sans que l'utilisateur en ait connaissance. Ainsi, elles peuvent être utilisées et exploitées sans l'accord préalable de l'utilisateur qui ne serait pas forcément en accord avec cette décision. De plus, cela va à l'encontre du droit à l'oubli. Ce dernier a été établi pour la première fois en mai 2014 dans l'Union Européenne et permet à un individu de demander l'effacement d'une information en ligne qui le concerne. Cependant, si nous n'avons pas connaissance de l'existence d'une information, il nous est difficile de demander son effacement.

De plus, nous pouvons nous interroger sur la question de la propriété de nos données. Étant stockées sur des serveurs distants que nous ne possédons pas, il est difficile de se dire qu'on les possède réellement. Nous pouvons faire un comparatif à notre système bancaire, nous

ne possédons pas réellement notre argent. Toutefois, tout cela est basé sur un système de confiance qui nous assure que si nous en avons besoin, nous pouvons l'utiliser sans en avoir la propriété matérielle. Malheureusement, si un jour ce système s'effondre, nous ne disposerions plus des preuves de l'argent que nous possédons. En outre, le cloud tente de nous inspirer une confiance similaire à celle que nous avons avec notre propre système de stockage de données. Il nous permet d'y accéder à tout moment, à condition d'avoir une connexion internet, même si nous ne possédons pas physiquement nos données. Cependant, le même problème subsiste toujours, si les serveurs sont détruits alors nos données seront tout de même perdues. Il est peut-être préférable de conserver nos données de manière matérielle sur un support externe, tel qu'un disque dur.

Il est souvent difficile pour un utilisateur moyen, qui n'a pas une connaissance particulière des lois régissant le stockage de données sur le cloud, de comprendre où et comment ses informations sont stockées. En outre, en naviguant sur Internet, nous sommes fréquemment confrontés à des demandes d'acceptation de cookies qui peuvent contenir des informations personnelles. Cela soulève la question de savoir comment il est possible de prendre connaissance de toutes les informations stockées à notre sujet.

En conclusion, le cloud offre de nombreux avantages tels que la scalabilité, la réduction des coûts, la facilitation du télétravail et de la collaboration, ainsi que l'accès à de nouveaux services pour les particuliers. Cependant, il est important de prendre en compte les problèmes de confidentialité des données et de leur propriété. Malgré cela, le cloud continue de s'imposer comme une solution incontournable pour les entreprises et les particuliers dans la gestion et le stockage de leurs données. Il faudrait développer des technologies qui permettent de garantir une meilleure protection des données et de la vie privée des utilisateurs. Il est également

important de sensibiliser les utilisateurs sur les risques liés à l'utilisation du cloud et de les encourager à prendre des mesures pour protéger leurs données personnelles. Enfin, il est nécessaire de poursuivre la recherche et le développement de solutions innovantes pour améliorer la sécurité des données stockées dans le cloud.

## Glossaire

- **Cloud** : utilisation de la mémoire et des capacités de calcul des ordinateurs et des serveurs répartis dans le monde entier et liés par un réseau.
- **Cloud computing** : prestation de services informatiques (comme des logiciels, des bases de données, des serveurs et des réseaux) sur Internet.
- **Datacenter** : centre de données
- **Infrastructure-as-a-Service (IaaS)** : services d'infrastructure cloud, est une forme de cloud computing où l'infrastructure informatique est fournie aux utilisateurs finaux sur Internet
- **Function as a Service (FaaS)** : service de cloud computing qui permet aux développeurs de créer, de calculer, d'exécuter et de gérer des paquets d'application en tant que fonctions, sans avoir à assurer la maintenance de leur propre infrastructure.
- **Software as a Service (SaaS)** : service basé sur le cloud où, au lieu de télécharger un logiciel que votre PC de bureau ou votre réseau professionnel peut exécuter et mettre à jour, vous accédez à une application via un navigateur internet.
- **Container as a Service (CaaS)** : service cloud qui permet la gestion et le déploiement des applications au moyen d'une abstraction basée sur les conteneurs.
- **Platform as a Service (PaaS)** : type d'offre de cloud computing dans lequel un fournisseur de services fournit une plateforme à ses clients, leur permettant de développer, d'exécuter et de gérer des applications commerciales sans avoir à construire et à maintenir l'infrastructure que ces processus de développement de logiciels requièrent généralement.

## Références

- [1] «Qu'est-ce qu'un PaaS ?», [En ligne]. Available: <https://www.oracle.com/fr/cloud/definition-paas/>.
- [2] Red Hat, «Le CaaS, qu'est-ce que c'est ?», 22 janvier 2020. [En ligne]. Available: <https://www.redhat.com/fr/topics/cloud-computing/what-is-caas>.
- [3] «Cloud computing | CNIL», [En ligne]. Available: <https://www.cnil.fr/fr/definition/cloud-computing>.
- [4] S. Rahmoune, «ChatGPT : le nombre d'utilisateurs du chatbot atteint des sommets», 2 février 2023. [En ligne]. Available: <https://www.clubic.com/technologies-d-avenir/intelligence-artificielle/actualite-456000-chatgpt-le-nombre-d-utilisateurs-du-chatbot-atteint-des-sommets.html>.
- [5] «LE CLOUD : AVANTAGES ET INCONVÉNIENTS PAR RAPPORT À UNE INFRASTRUCTURE ON PREMISE», [En ligne]. Available: <https://www.compufirst.com/compufirst-lab/cloud/cloud-avantages-inconvenients/main.do?appTreeId=45695>.
- [6] M. Rochefort, «Uber : comment l'ex-responsable de la sécurité a caché une faille ultra-massive», 6 octobre 2022. [En ligne]. Available: <https://www.clubic.com/uber/actualite-440781-uber-comment-l-ex-responsable-de-la-securite-a-cache-une-faille-ultra-massive.html>.