République Algérienne Démocratique et Populaire
Ministère de l'enseignement supérieur et de la recherche scientifique
Université Larbi Tébessi - Tébessa
Faculté des Sciences Exactes et des Sciences de la Nature et de la Vie
Département : Mathématiques et Informatique

Mémoire de fin d'études
Pour l'obtention du diplôme de MASTER 2
Domaine : Mathématiques et Informatique
Filière : Informatique
Option : Systèmes d'information

Thème

Vers une coordination transparente entre le Cloud Computing et le Fog Computing

Présenté Par :
HAMDI PACHA Mohammed Tahar

Devant le jury :

Mr LAIMECHE Lakhdar	*MCA*	*Univérsité Larbi Tébessi*	*Président*
Mr MENASSEL Yahia	*MAA*	*Univérsité Larbi Tébessi*	*Examinateur*
Mr METROUH Abdelmalek	*MCB*	*Univérsité Larbi Tébessi*	*Encadreur*

Date de soutenance *: 13/06/2020*

بسم الله الرحمن الرحيم

***J**e dédie ce travail*

À Mes CHERS PARENTS

Pour les sacrifices déployés à mes égards ; pour leur patience Leur amour et leur confiance pour moi. Ils ont tout fait pour mon bonheur et ma réussite. Qu'ils trouvent dans ce modeste travail, le témoignage de mon Profonde affection et de mon attachement indéfectible. Nulle dédicace ne puisse exprimer ce que je leur dois Que dieu leur réserve la bonne santé et une longue vie.

À MA CHERE ET UNIQUE SŒUR DHIKRA QUE J'AIME PROFONDEMENT

Pour ses encouragements, son soutien et aide pendant ma formation.

À MES ONCLES, MES TANTES ET MES COUSINS

En témoignage de mes sincères reconnaissances pour les efforts qu'ils ont consentis pour me soutenir au cours de mes études. Que dieu nous garde toujours unis.

À Toutes les personnes qui m'ont aidée à réaliser mon projet

HAMDI PACHA Mohammed Tahar

Remerciements

*« **S**oyons reconnaissants aux personnes qui nous donnent le bonheur*

*E**lles sont les Charmants jardiniers par qui nous âmes sont fleuries »*

MARCEL PROUST

***C**'est avec un grand plaisir que je réserve ces quelques lignes en signe de gratitude et de profonde reconnaissance à tous ceux qui de près ou de loin, ont contribué à la réalisation et l'aboutissement de ce travail.*

***T**out d'abord, je tiens à remercier **Allah** tout puissant, de m'a permis de mener à bien ce mémoire, et de m'a orienté au chemin du savoir.*

***E**nsuite, je remercie sincèrement Dr. **METROUH Abdelmalek**, MCB au sein du département mathématiques et informatique de la faculté des sciences exactes et sciences de la nature et de la vie à l'université de Tébessa, pour son encadrement, son assistance, son soutien, sa disponibilité et ses précieux conseils.*

***M**es vifs remerciements s'adressent à Dr. **LAIMECHE Lakhdar,** MCA, et Mr. **MENASSEL Yahia,** MAA, au sein du département mathématiques et informatique de la faculté des sciences exactes et sciences de la nature et de la vie à l'université de Tébessa, pour l'honneur qu'ils m'ont accordé en acceptant de juger mon travail.*

***E**nfin, j'adresse mes chaleureux remerciements à mes enseignants pour la qualité de l'enseignement qu'ils ont bien voulu me prodiguer durant mes études afin de me fournir une formation efficiente.*

***M**erci à toutes et tous.*

Résumé

Cloud Computing a été introduit comme une solution optimale afin de réduire les couts, la consommation d'énergie, et assurer la sécurité et les gains de production et du temps. Pour les utilisateurs ; le développement d'internet of things a apporté des nouveaux défis tels que le problème de Cloud qui ne peut pas répondre aux nombreux données générées par les appareils d'IoT en temps réel ; afin de résoudre ce problème le Fog est apparu. Mais le problème que les data centre de Fog sont très limités par rapport aux data centre de Cloud . La solution est la coordination entre le Cloud et le Fog afin de résoudre et éliminer tous les problèmes d'IoT, Nous allons parler dans ce mémoire de fin d'étude sur les modèles de coordination existants et nous allons choisir un modèle de coordination qui est le stockage.

Notre contribution est de réaliser une étude de cas sur la conduite automatique d'une voiture intelligente dont on va proposer des algorithmes pour la conduite automatique.

Mots clés : Cloud Computing -IoT-Fog Computing-voiture intelligente-Conduite automatique - Coordination.

Abstract

Cloud Computing has been introduced as an optimal solution to reduce costs, energy consumption, and ensure security, production and time savings. For users; the development of the internet of things has brought new challenges such as the problem of the Cloud not being able to respond to the large amount of data generated by IoT devices in real time; in order to solve this problem the Fog has appeared. But the problem is that Fog data centers are very limited compared to Cloud data centers. The solution is the coordination between the Cloud and the Fog in order to solve and eliminate all the problems of IoT. We will talk in this final memorandum studies existing coordination models and we will choose a coordination model which is storage.

Our contribution is to carry out a case study on the automatic driving of an intelligent car for which we will propose algorithms for automatic driving.

Keywords: Cloud Computing -IoT-Fog Computing-smart vehicle-Automatic driving - Coordination.

ملخص

أدخلت الحوسبة السحابية كحل مثالي للحد من التكاليف واستهلاك الطاقة و من اجل ضمان الأمن وربح الإنتاج والوقت. بالنسبة للمستخدمين فان تطور الإنترنت أدى إلى تحديات جديدة مثل مشاكل السحابة التي لا يمكنها الإجابة على البيانات الكثيرة التي تولدها أجهزة إنترنت الأشياء في الوقت الحقيقي. ولحل هذه المشكلة نشأت الحوسبة الضبابية. ولكن المشكلة أن مراكز بيانات الضباب محدودة جدا مقارنة بمراكز بيانات السحابة. الحل هو التنسيق بين السحابة والضباب لحل وإزالة جميع مشاكل انترنت الأشياء. سنتحدث في هذه الرسالة عن نماذج التنسيق الموجودة واخترنا نموذج للتنسيق وهو التخزين.

مساهمتنا هي دراسة حالة حول القيادة الآلية للسيارة الذكية ثم اقترحنا خوارزميات للقيادة الآلية.

الكلمات المفتاحية :

الحوسبة السحابية - إنترنت الأشياء - الحوسبة الضبابية - السيارة الذكية - القيادة الآلية - التنسيق

Table des matières

Liste des figures

Liste des tableaux

Introduction Générale

«En informatique, la miniaturisation augmente la puissance de calcul.

On peut être plus petit et plus intelligent.»

Bernard Werber

La demande croissante pour de nouveaux services informatique plus économiques et fiables a permis l'émergence d'une nouvelle technologie qui est le Cloud Computing.

Le Cloud Computing est une technologie qui permet de transférer le traitement et l'espace de stockage de l'ordinateur vers le Cloud, qui est un appareil serveur auquel on accède via Internet, donc les programmes informatiques sont transformés des produits en services, cette technologie contribue à maintenir les problèmes de maintenance et de développement des programmes informatiques des entreprises utilisées pour eux, l'infrastructure de Cloud Computing dépend des centres des données avancés qui offrent un grand espace de stockage aux utilisateurs.

Le Cloud Computing signifie en général les services qui sont fournis via des appareils et des programmes connectés à un réseau des serveurs transportant leurs données dans un Cloud. Une garantie virtuelle qui se connecte en permanence et sans interruption, avec différents appareils (ordinateurs, tablettes, smartphones…etc) après avoir défini un code spécial pour ouvrir le verrou du réseau, et donc accessible depuis n'importe où et à tout moment, et avec le développement de la technologie disponible sur Internet de nombreuses organisations et entreprises ont rendues leurs applications disponibles en ligne grâce au Cloud Computing. Cette technologie a largement profité aux utilisateurs en réduisant les coûts.

Malgré les innombrables points positifs du Cloud, le plus gros obstacle rencontré par le Cloud est le problème de latence car le Cloud est très loin des utilisateurs finaux, ainsi que les nombreuses données générées par les appareils, notamment après l'émergence et l'expansion de l'IoT, ce qui a conduit à penser à une autre structure proche des utilisateurs finaux. Ici une nouvelle structure a été créée qui est le Fog.

Le Fog est une extension du Cloud, il est très proche des utilisateurs ce qui mène à éliminer le problème de latence et répond aux besoins des utilisateurs finaux en temps réelles car il se compose par des nœuds et chaque nœud couvert une zone géographique ce qui signifie que l'analyse et le traitement et la réponse aux données reçues seront dans un temps réel.

Malgré les avantages et l'utilité du Fog mais avec le développement d'IoT et et l'émergence des villes intelligentes, La coordination entre le Cloud et le Fog est devenue essentielle, surtout avec les limitations des serveurs de Fog par rapport au Cloud en particulier coté stockage.

La coordination entre Cloud et Fog élimine tous les problèmes posés dans le Cloud ou le Fog, et participe au succès des villes intelligentes.

Chapitre1 : l'Informatique en nuage (Cloud Computing)

"L'informatique : alliance d'une science inexacte

Et d'une activité humaine faillible."

Luc Fayard

1. Introduction

De nos jours les systèmes d'informations sont constamment à la recherche de nouvelles technologies afin de rendre leurs systèmes informatiques performants, économiques, et écologiques. Des études ont révélées que la plupart des serveurs dans nos salles machines n'utilisent que 10% des capacités de leurs processeurs ; ce qui représentait une grosse perte en termes de ressources financières, humaines, et de stockage.

Pour pallier à ce problème des grandes entreprises comme Amazone, Microsoft... ont décidées de mettre à la disposition des entreprises et des particuliers leurs infrastructures informatiques ce qui a donné naissance au Cloud Computing. Cependant beaucoup d'entreprises au capital réduit peinent à s'introduire dans le domaine et utilisent des technologies obsolètes [34]. Dans ce chapitre nous présenterons le Cloud Computing, ses caractéristiques et ses domaines d'application, ainsi que son architecture et les services qu'il offre, ses défis, ses avantages et ses inconvénients, ses domaines d'applications, sa sécurité et ses acteurs principaux.

2. Définition

2.1. Internet des objets (Internet of Things)

Selon l'Union internationale des télécommunications, l'Internet of things (IoT) est une « infrastructure mondiale pour la société de l'information, qui permet de disposer de services évolués en interconnectant des objets (physiques ou virtuels) grâce aux technologies de l'information et de la communication interopérables existantes ou en évolution ». En réalité, la définition de ce qu'est l'Internet of Things n'est pas figée. Elle recoupe des dimensions d'ordres conceptuel et technique.

D'un point de vue conceptuel, l'IoT caractérise des objets physiques connectés ayant leur propre identité numérique et capables de communiquer les uns avec les autres. Ce réseau crée en quelque sorte une passerelle entre le monde physique et le monde virtuel.

D'un point de vue technique, l'IoT consiste en l'identification numérique directe et normalisée (adresse IP, protocoles smtp, http...) d'un objet physique grâce à un système de communication sans fil qui peut être unepuce RFID, Bluetooth ou Wi-Fi[1].

2.2. Informatique en nuage (Cloud Computing)

Le Cloud Computing est un modèle d'accès, à travers le réseau Internet, à un ensemble de ressources numériques, pouvant être allouées et libérées à la demande et pour lesquelles le fournisseur du service assure l'ensemble des activités de maintenance, de support et d'exploitation. C'est une forme particulière de gestion de l'informatique, dans laquelle l'emplacement et le fonctionnement du nuage ne sont pas portés à la connaissance des clients.

Ce modèle offre des services de différentes natures, allant des services d'infrastructure (location de capacités de stockage ou de calcul), des services de plateforme (location d'environnements de développement pré-configurés) ou de services d'applications (location d'applications). [2]

2.2.1. Historique du l'informatique en nuage (Cloud Computing)

L'idée du Cloud Computing est née en 1960 par des pionniers tels que John McCarthy. Et Joseph Carl était limité au traitement des transactions financières et des données de recensement

- En 1979, le terme Cloud Computing a été utilisé pour la première fois par le professeur de systèmes d'information Chellappa Ramnath
- Le développement actuel du Cloud Computing a commencé en 1999. Salesforce a introduit son site Web pour une application électronique. La société a été la première à utiliser la livraison d'applications d'entreprise.
- En 2002, Amazon a lancé son premier Cloud, appelé Amazon Web Services, avec un ensemble de services basés sur le Cloud.
- En 2006, Amazon a également lancé son deuxième Cloud appelé AC2 en tant que service commercial sur Internet.
- En 2009, le Cloud est devenu Google Cloud, où il a créé des applications basées sur un navigateur.[3]

3. Internet des objets en bref

Il ne fait aucun doute qu'Internet a eu un impact sur la vie des gens et les pratiques des organisations. Agissant comme un middleware de communication fiable, Internet permet de connecter entre eux différents composants matériels et logiciels dans la mesure où la localisation n'est plus un obstacle à la disponibilité des informations et à l'accessibilité des services. Les derniers développements en matière de TIC, tels que l'IoT, visent la commodité en veillant à ce que les choses dans l'environnement des personnes et des organisations soient accessibles et répondent à leurs demandes. Smart home (maison intelligente) est un bonne exemple de cette commodité où des choses comme les appareils électroménagers blancs prennent des mesures au nom des occupants de la maison.

Différentes formes d'informatique contribuent au fonctionnement de l'IoT, y compris l'informatique mobile, et omniprésente , dans la mesure où certaines choses du XXIe siècle sont déjà améliorées par l'informatique, les réseaux et les capacités de stockage

[4]. Malheureusement, l'abondante littérature sur l'IoT n'aide pas à proposer une définition unique de ce qu'est l'IoT. D'une part, Barnaghi et Sheth donnent un bon aperçu des exigences et des défis de l'IoT[5]. Les exigences comprennent la qualité, la latence, la confiance, la disponibilité, la fiabilité et la continuité qui devraient influer sur l'accès et l'utilisation efficaces des données et services IoT. De plus, les défis résultent des écosystèmes actuels de l'IoT, caractérisés par des milliards de choses dynamiques, ce qui rend les techniques et les solutions de recherche, de découverte et d'accès existants. inapproprié pour les données et services IoT. D'un autre côté, Abdmeziem et al. Discutent des caractéristiques de l'IoT et des moyens d'y parvenir. technologies[6]. Les caractéristiques comprennent la distribution et l'interopérabilité, l'évolutivité, la rareté des ressources et la sécurité. Et Les technologies habilitantes comprennent la détection, la communication et l'analyse de l'information et l'actionnement. Ces technologies sont mappées sur une carte à trois couches Architecture de l'IoT comprenant la perception, le réseau et l'application, respectivement. Un guide complet sur les applications, les protocoles et les processus d Les meilleures pratiques de l'IoT sont publiées par le groupe DZone en 2017[7]. Le guide couvre divers aspects pertinents pour l'IoT, tels que la protection de la vie privée, des données importantes, la surveillance, le contexte et l'architecture. Certains les termes qui méritent d'être mentionnés dans le guide sont l'IoT consensuel ce qui signifie que tous les fournisseurs d'IoT doivent respecter et prendre en compte tous les éléments suivants les mesures en leur pouvoir pour protéger la vie privée et la sécurité des utilisateurs, l'informatique omniprésente, ce qui signifie que la prochaine génération des systèmes d'IoT nécessitera un protocole middleware capable de de gérer des dispositifs hétérogènes, en supportant l'évolutivité, assurer la confidentialité et la sécurité, et encourager l'utilité, et le contexte ce qui signifie que le fait d'aborder l'attention des utilisateurs devrait être au bon moment avec le bon message.

4. Caractéristiques de Cloud Computing

Le Cloud Computing se distingue des solutions traditionnelles par les caractéristiques suivantes [2] :

- **Large accessibilité via le réseau** : Les services sont accessibles en ligne et sur tout type de support (ordinateur de bureau, portable, smartphone, tablette). Tout se passe dans le navigateur Internet
- **Mesurabilité du service :** L'utilisation du service par le client est supervisée et mesurée afin de pouvoir suivre le niveau de performance et facturer le client en fonction de sa consommation réelle.
- **Solution multiclient :** Une même instance d'un logiciel est partagée par l'ensemble des clients de façon transparente et indépendante. Tous les clients utilisent la même version du logiciel et bénéficient instantanément des dernières mises à jour. Chaque client dispose d'un paramétrage utilisateur qui lui est propre.
- **Disponibilité à la demande :** Le service peut être souscrit rapidement et rendu opérationnel automatiquement avec un minimum d'interaction avec le fournisseur.
- **Élasticité immédiate des ressources :** Des ressources supplémentaires peuvent être allouées au service pour assurer la continuité du service en cas de pic de charge, ou bien être ré-allouées à un autre service dans le cas inverse.

- **Mutualisation des ressources :** Des ressources utilisées pour exécuter le service sont mutualisées pour servir à de multiples clients. Les multiples serveurs sollicités, totalement inter-connectés, ne forment plus qu'une seule ressource virtuelle puissante et performante.

5. Les fondements technologiques de Cloud Computing

Avant de parler des technologies de base du Cloud, nous allons définir les composants fonctionnels de ce dernier, [22]:

- **Le prestataire de service Cloud** (**CSP pour Cloud Service Provider**) : Il s'agit d'une entité qui gère le serveur de stockage Cloud (**CSS pour Cloud Storage Server**), l'espace de stockage pour préserver les données des clients et la puissance de calcul élevée ;
- **Le Client/propriétaire (Cloud Client/Owner)** : Il s'agit d'une entité, qui a d'une grande quantité de fichiers de données à stocker dans le Cloud et s'appuie sur ce dernier pour la gestion des données et du calcul, il peut être soit un consommateur individuel ou une organisation ;
- **L'utilisateur (Cloud User)**: Il s'agit d'une unité, qui est inscrit sur le propriétaire et utilise les données de celui-ci stockées sur le Cloud. L'utilisateur peut être un propriétaire lui-même.
- **Courtier (CB ou Cloud Broker)** : En général, deux types de Brokers dans le **Cloud** peuvent être distinguées. Tout d'abord, il ya des Brokers qui se concentrent sur la négociation des relations entre les consommateurs et les fournisseurs sans posséder ou gérer l'infrastructure Cloud. Ils fournissent, par exemple, des services de conseil aux consommateurs de Cloud pour déplacer leurs ressources informatiques dans un Cloud approprié. Deuxièmement, il ya des Brokers qui ajoutent des services supplémentaires sur le dessus de l'infrastructure / la plate-forme / le logiciel d'un prestataire de Cloud afin d'améliorer et sécuriser l'environnement Cloud pour les consommateurs. Par exemple, un Broker peut apporter au consommateur un service de gestion d'identité et d'accès au dessus de service de base offert par le fournisseur Cloud**.** À titre d'exemple, le Broker peut développer des API afin de rendre les services Cloud interopérables et portable, [23]; Les technologies et les infrastructures de base nécessaires pour construire un

  Cloud, indépendamment du son type sont:

5.1. Les centres de données « Data Center »

Un Cloud a besoin de serveurs sur un réseau, et ils ont besoin d'une maison (station). Cette maison physique et tout le matériel y faire un centre de données. Le centre de données est un site hébergeant l'ensemble des systèmes nécessaires au fonctionnement des applications informatiques, [24]. Il est toujours constitué de trois composants élémentaires:

- L'infrastructure, c'est à dire l'espace et les équipements nécessaires au support des opérations du data centre. Cela comprend les transformateurs électriques, les alimentations, les générateurs, les armoires de climatisation, les systèmes de distribution électrique, etc.
- Les équipements informatiques comprenant les serveurs, le stockage, le câblage ainsi que les outils de gestion des systèmes et des équipements réseaux.
- Les espaces d'exploitation, c'est-à-dire le personnel d'exploitation qui pilote, entretient et répare les systèmes lorsque cela est nécessaire ;

Le Cloud contient des centres de données avec 10000 ou plus de serveurs sur site, toutes consacrée à l'exécution des applications qui sont construites avec des composants d'infrastructure cohérente (tels que grilles, matériel, OS, réseau et ainsi de suite), [25].

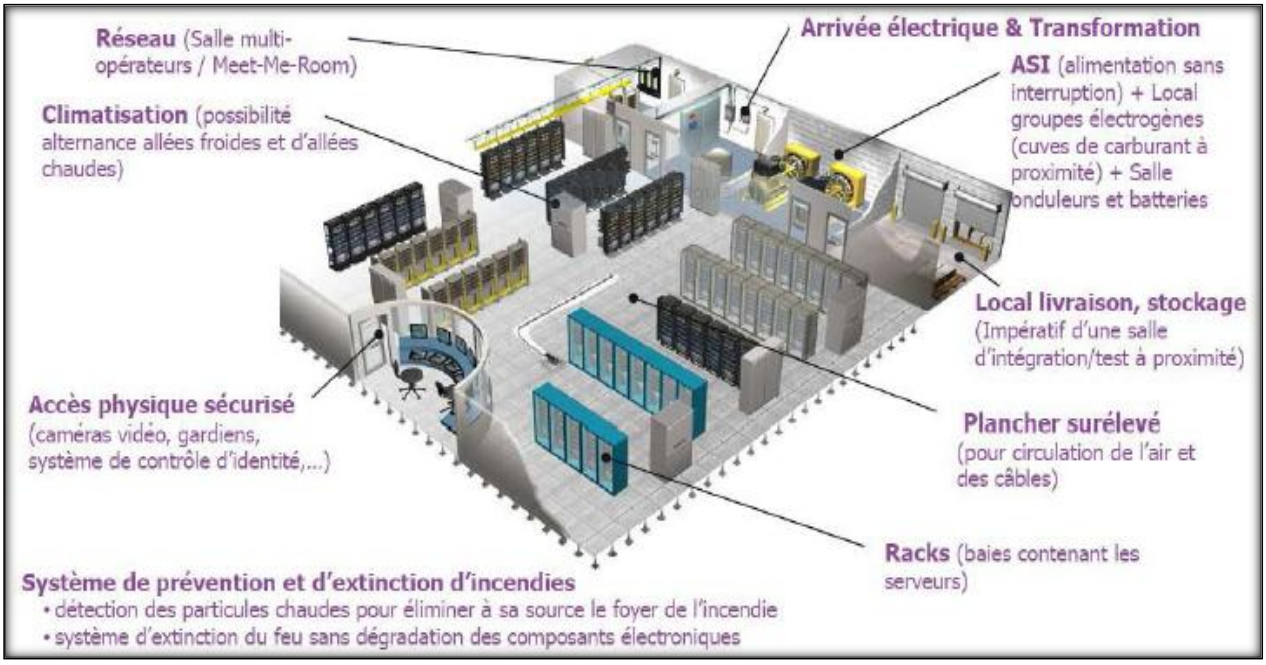

Figure 1 : Une salle d'hébergement de serveurs ou data Center [26]

5.2. La Virtualisation

La virtualisation est une méthode d'exécuter plusieurs systèmes d'exploitation virtuels indépendants sur un seul ordinateur physique. La création et la gestion des machines virtuelles a souvent été appelée virtualisation de plate-forme (platform virtualisation). La Virtualisation de plate-forme est exécutée sur un ordinateur donné (plate-forme matérielle) de logiciel appelé un programme de contrôle. Le programme de contrôle crée un environnement simulé, un ordinateur virtuel, ce qui permet d'utiliser un logiciel hébergé spécifique à l'environnement virtuel, parfois appelé logiciel invité (Guest Software), [27].

La Virtualisation peut être d'une grande utilité pour les systèmes de Cloud comme il peut améliorer la mutualisation des ressources et permettre l'approvisionnement des ressources rapides et élastique. Ces avantages font de réseaux flexibles, agiles menant à d'importantes réductions de coûts. Dans les applications de Cloud typiques, des serveurs, des dispositifs de stockage et réseaux peuvent tous être virtualisés, [28, 29] Certains des principaux avantages de la virtualisation, qui sont indigènes au Cloud, sont les suivants:

- Une facturation basée sur l'utilisation (la tarification des services) et non pas la capacité matérielle fixe ;
- Le déploiement rapide de serveurs supplémentaires ;
- La promotion des économies d'échelle ;
- La séparation de la clientèle des d'emplacements de serveurs physiques ;
- L'utilisation repose sur Service-LevelAgreements (SLA) ;
- La tolérance aux pannes ;
- La mobilité des applications entre les serveurs et les centres de données.

Une **VM** est un conteneur de logiciels totalement isolé, capable d'exécuter ses propres systèmes d'exploitation et applications, à l'instar d'un ordinateur physique. Une machine virtuelle se comporte exactement comme un ordinateur physique. Elle contient un processeur, une mémoire RAM, un disque dur et une carte d'interface réseau virtuels (autrement dit, basés sur des logiciels) qui lui sont propres, [9].

En générale, la **virtualisation** est réalisée par l'utilisation d'un « **Hyperviseur** ». L'**Hyperviseur** est un logiciel qui permet à plusieurs images virtuelles de partager une seule machine physique et d'attribuer et séparer logiquement les ressources physiques. L'**Hyperviseur** permet au matériel informatique d'exécuter plusieurs systèmes d'exploitation invités en même temps. Chacun des systèmes d'exploitation invités est isolé et protégé contre tous les autres fonctionnant sur la même machine physique et n'est pas affecté par des problèmes ou de l'instabilité qui se produisent sur d'autres machines virtuelles.

Plusieurs **Hyperviseurs** puissants incluant **KVM** (**K**ernel-based**V**irtual **M**achine), **Xen**et **QEMU** sont open source. **VMWare** est actuellement le leader du marché dans le domaine de la **virtualisation** et plusieurs de ses produits sont basées sur l'open source.

La figure **1.4** montre une vue de haut niveau d'un **Hyperviseur** où les ressources de la machine hôte sont partagés entre un nombre d'invités, dont chacun peut exécuter des applications et chacun a un accès direct aux ressources physiques sous-jacents

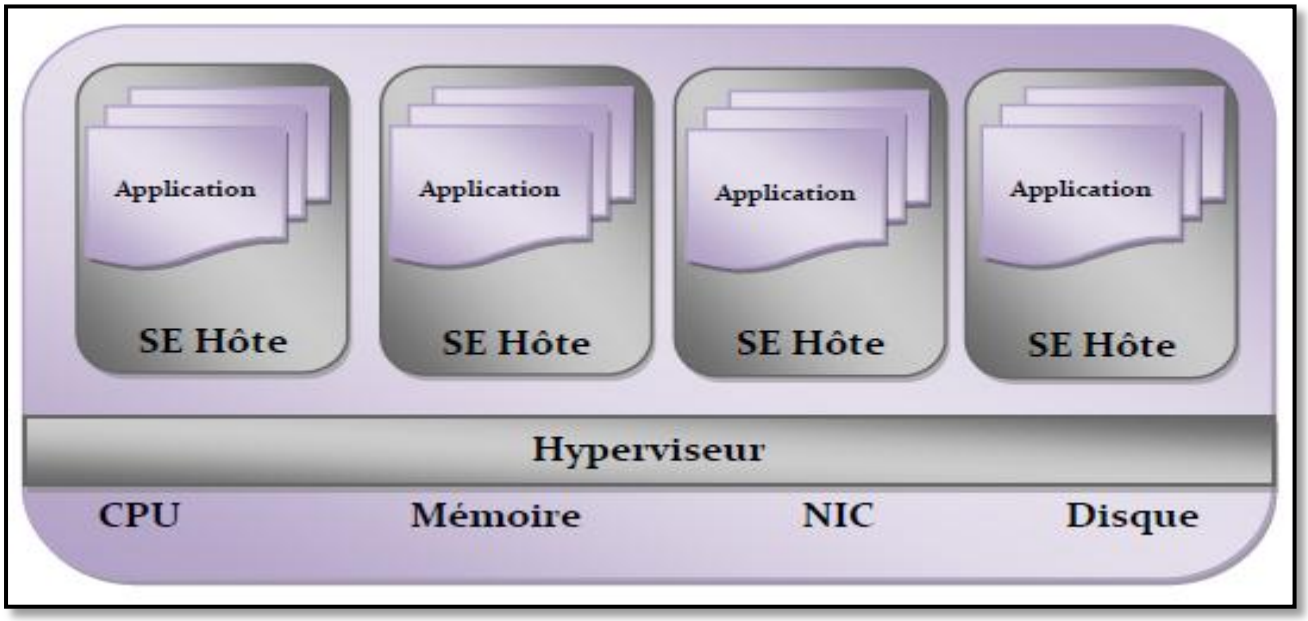

Figure 2 : Hyperviseur

5.3. Les API d'accès

Un Cloud a besoin d'une API d'accès. Les utilisateurs de Cloud ont besoin d'un moyen pour accéder aux nuages, fournir de nouveaux serveurs virtuels, obtenir des données dans et hors de stockage, démarrer et arrêter les applications sur les serveurs et déclasser les serveurs qui ne sont plus nécessaires. Tout cela doit être possible à distance, parce que les utilisateurs de Cloud jamais mis les pieds à l'intérieur du centre de données.

6. Architecture globale du Cloud Computing

L'architecture globale du Cloud Computing comporte essentiellement [8] :

- **Clients :** Un client Cloud se compose de matériel informatique et/ou de logiciels qui s'appuient sur le Cloud Computing pour la livraison des applications, ou qui est spécifiquement conçu pour la fourniture de services Cloud et qui, dans les deux cas, est essentiellement inutile sans elle.
- **Services :** Un service Cloud comprend des produits, des services et des solutions livrés et consommés en temps réel sur Internet. Par exemple, les services Web accessibles par d'autres composants et logiciels de Cloud Computing.

- **Applications :** Une application Cloud exploite le Cloud dans l'architecture logicielle, ce qui élimine souvent la nécessité d'installer et d'exécuter l'application sur son propre ordinateur, Ce qui allège le fardeau de la maintenance logicielle, du fonctionnement continu et du support.
- **plateforme :** Une plateforme Cloud facilite le déploiement d'applications sans coût, la complexité d'achat, de gestion du matériel et des logiciels sous-jacents.
- **Le stockage :** Le stockage dans le Cloud implique la livraison de stockage de données en tant que service, y compris des services de base de données, souvent facturés sur une base de calcul utilitaire.
- **L'infrastructure :** L'infrastructure Cloud, en tant que service, est la fourniture d'infrastructures informatiques, généralement un environnement de visualisation de plates-formes.

7. Services du Cloud Computing

7.1. Modèles de déploiement

Le Cloud Computing peut être déployé en quatre types différents [10] :

➢ **Cloud public**

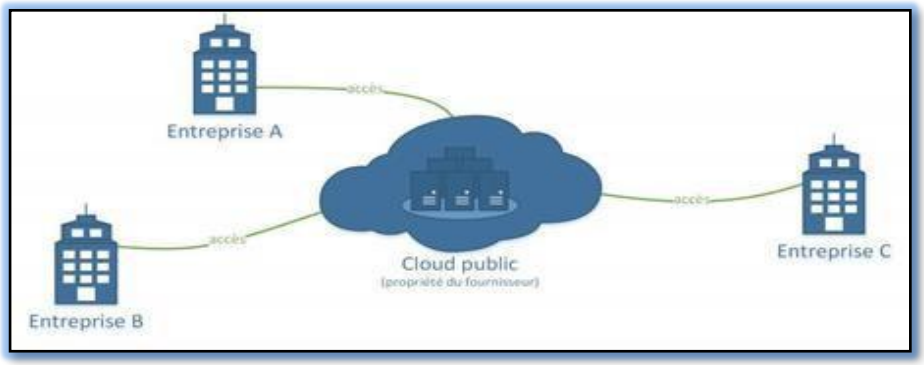

Figure 3: Exemple du Cloud public[10]

Les Clouds publics sont exploités par un fournisseur de services Cloud, qui propose des ressources de calcul, par exemple des serveurs et du stockage, via Internet. Microsoft Azure est un exemple de Cloud public. Dans un Cloud public, tout le matériel, tous les logiciels et toute l'infrastructure sont la propriété du fournisseur du Cloud.

➢ **Cloud privé ou Cloud dédié :**

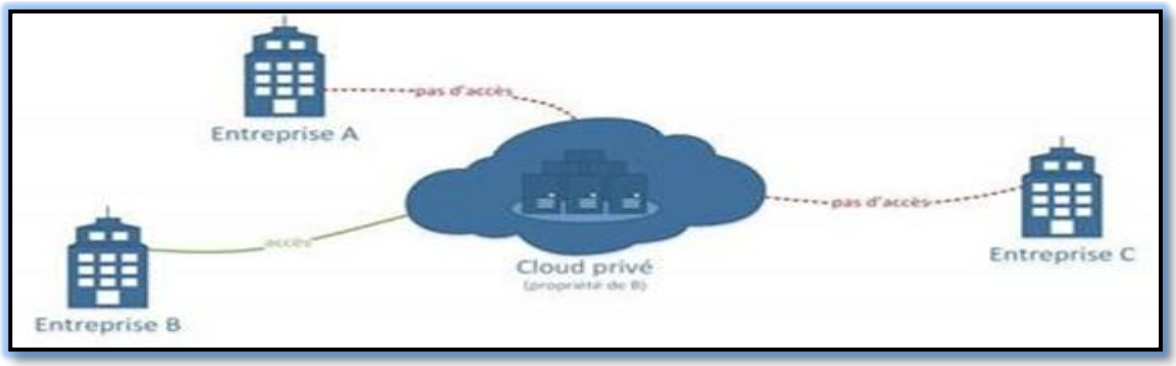

Figure 4 : Exemple du Cloud privé[10]

Le Cloud privé est l'ensemble des ressources de Cloud Computing utilisées

de façon exclusive par une entreprise ou une organisation. Le Cloud privé peut se trouver physiquement dans le centre de données local de l'entreprise. Certaines entreprises paient également des fournisseurs de services pourqu'ils hébergent leur Cloud privé. Le Cloud privé est un Cloud dans lequel les services et l'infrastructure se trouvent sur un réseau privé.

➢ **Cloud communautaire :**

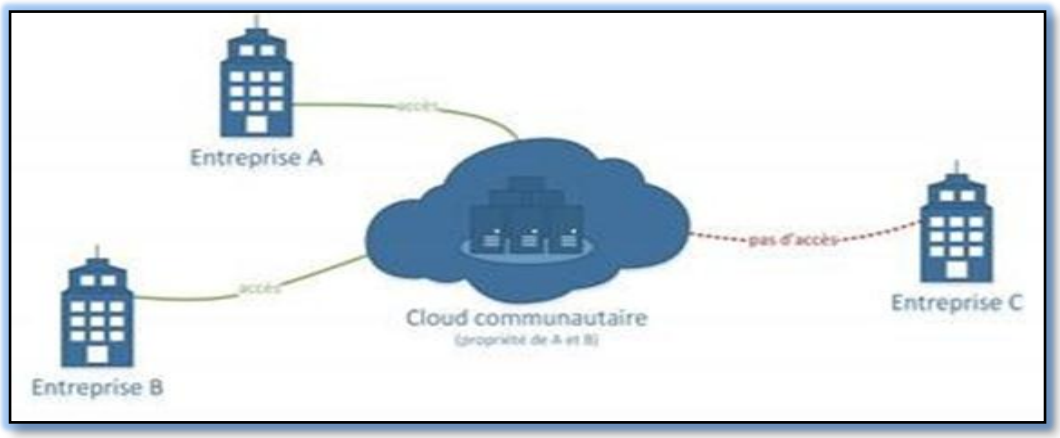

Figure 5: Exemple du Cloud communautaire[10]

Cloud communautaire correspond à un Cloud privé partagé par un groupement d'acteurs. Ce mode de déploiement vise à abaisser la barrière à l'entrée du Cloud privé tout en bénéficiant d'un niveau de service spécifique. Il est adapté à la mutualisation au sein d'un écosystème où la co-gouvernance est envisageable (regroupement de collectivités ou d'acteurs publics, communautés d'universités).

➢ **Cloud hybride :**

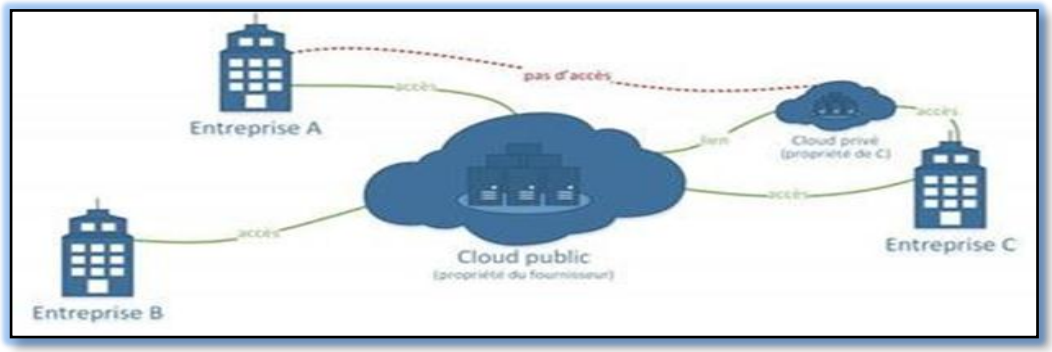

Figure 6: Exemple du Cloud hybride[10]

Le Cloud hybride regroupe des Clouds publics et privés, liés par une

technologie leur permettant de partager des données et des applications. En permettant aux données et aux applications de passer du Cloud privé au Cloud public, le Cloud hybride offre aux entreprises un plus grand niveau de flexibilité et plus d'options de déploiement.

7.2. Modèles de services

Trois grands modèles d'usage du Cloud se dégagent actuellement, tous présentent des caractéristiques différentes comme illustré dans la figure 7 [11] :

- **IaaS (Infrastructure as a Service, des services virtuels disponibles à la demande) :** Il s'agit de l'offre la plus basique dans le portefeuille Cloud Computing correspondant à la location de capacités de calcul et de stockage. Dans un service IaaS, le fournisseur met à disposition et administre les ressources matérielles virtualisées comprenant :
  - La puissance de calcul
  - Les unités de stockage des données
  - Les réseaux
  - Les couches de virtualisation
  - Les systèmes d'exploitation

  Le client prend en charge la gestion et l'exploitation de toutes les couches supérieures, middlewares, bases de données et applications. La souscription à une offre IaaS permet au client d'externaliser son parc matériel serveur et de s'affranchir des compétences de conception et d'exploitation des infrastructures techniques. Les prestataires des solutions IaaS les plus connus sont : Amazone avec Amazone ElasticCompute Cloud (EC2), ou Orange Business Service avec Flexible Computing.

- **PaaS (Platform as a Service, des plateformes de développement prêtes à l'emploi)** : Il s'agit de l'offre intermédiaire dans le portefeuille Cloud Computing. Le fournisseur met à disposition une plateforme middleware opérationnelle, incluant des serveurs d'applications, des bases de données et les

outils permettant au client de développer et de déployer ces propres applications.

Cette configuration est très employée pour disposer de plateformes de développement ou de tests disposant de l'ensemble des outils et middleware nécessaires, en évitant ainsi les tâches de construction et de maintenance de ces plateformes non critiques. Elle se destine donc naturellement avant tout aux développeurs. Des services comme Google App Engine, Bungee Connect et Force.com sont des exemples PaaS. Les principaux fournisseurs de PaaS sont : Microsoft avec Azure, Google avec Google App Engine et Orange Business Services.

➢ **SaaS (Software as a Service, des services métiers à la demande) :** Il s'agit d'une offre « tout compris ». Le prestataire met à disposition une application qu'il administre et configure en majeure partie. Le client externalise ainsi ses applications auxquelles il accède à la demande. Il paie à l'usage, selon le nombre d'utilisateurs et/ou le temps d'utilisation du logiciel. Les prestataires de solutions SaaS les plus connus sont : Google avec Gmail et Youtube ou encore les réseaux sociaux Facebook et Twitter.

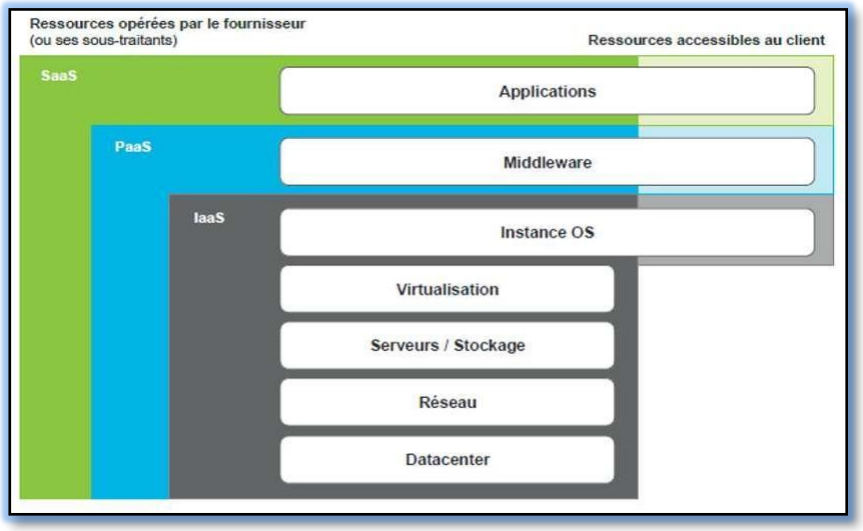

Figure 7 : Catégories d'offres Cloud Computing et couches techniques[11]

8. Les défis de Cloud Computing

Le Cloud Computing présente plusieurs défis [12] :

- **Sécurité:** L'utilisation des réseaux publics, dans le cas du Cloud public, entraîne des risques liés à la sécurité du Cloud. En effet, la connexion entre les postes et les serveurs applicatifs passe par le réseau Internet, et expose à des risques supplémentaires de cyber attaques, et de violation de confidentialité.
- **Disponibilité:** Le client d'un service de Cloud Computing devient très dépendant de la qualité du réseau pour accéder à ce service. Aucun fournisseur de service Cloud ne peut garantir une disponibilité de 100%.
- **Piratage :** Tout comme les logiciels installés localement, les services de Cloud Computing sont utilisables pour lancer des attaques (craquage de mots de passe, déni de service..). En 2009, par exemple, un cheval de Troie a utilisé illégalement un service du Cloud public d'amazone pour infecter des ordinateurs.
- **Cadre légal :** Des questions juridiques peuvent se poser, notamment par l'absence de localisation précise des données du Cloud Computing.
- **Réversibilité:** En cas de rupture de contrat ou de changement de fournisseur, le client doit s'assurer de la récupération et de la destruction de ses données sur l'infrastructure du fournisseur après sa migration.

9. Les avantages et les inconvénients du Cloud Computing

9.1. Les avantages du Cloud Computing: [13]

- **Pas d'investissement initial et Souplesse :** Plus grande flexibilité des outils informatiques (pas d'installation ni de mises à jour, pas de maintenance matérielle, montée en charge automatisée, nombreux connecteurs disponibles…).
- **Réduction des coûts :** Les utilisateurs ne payent que ce qu'ils consomment. Forte économie en coût et énergie notamment dans les cas de besoins non constants ou linéaires.
- **Sécurité :** Diminution du risque de panne matérielle. Les données sont sécurisées et l'informatique est réellement nomade.

- **Mobilité :** L'utilisateur peut à tout moment et à partir de n'importe quel appareil se connecter à ses applications et son workflow.
- **Gain de productivité et de temps**

9.2. Les inconvénients du Cloud Computing : [14]

- Les données seront stockées en dehors du réseau de l'entreprise, peut-être même à l'étranger, ce qui peut enfreindre la réglementation et les lois de votre pays en matière de protection des données. En cas d'instabilité de la connexion Internet, avoir des problèmes d'accès à vos services.
- Des sites comme Facebook et Twitter sont très sujets aux attaques. Le piratage d'un compte d'entreprise pourrait avoir des conséquences néfastes pour la réputation de l'entreprise, tandis que l'utilisation imprudente des sites par un salarié pourrait offrir aux cybercriminels l'opportunité d'entrer dans le réseau et de soustraire des données des clients.
- La sauvegarde automatique des données et des niveaux de sécurité élevés n'étant pas.
- garantis, il convient d'être très attentif.

10. La sécurité dans le Cloud Computing

10.1. La sécurité physique de l'exploitation

Les entités et les mécanismes qui opèrent dans le management d'un Cloud sont les caractéristiques de sécurité essentielles pour une plate-forme dans les nuages.

Les développeurs et administrateurs d'une infrastructure de Cloud ont grâce à leur statut professionnel les privilèges suffisants pour créer et exploiter le service. Les fournisseurs de services développent des mécanismes de contrôles préventifs et réactifs:

-Des accès sécurisés aux données protégées

-Une combinaison de contrôles qui améliore grandement la détection d'activités malveillantes

-Plusieurs niveaux de surveillance (monitoring), d'enregistrement (logging) et de rapports (reporting).

Par ailleurs, les fournisseurs de services pratiquent régulièrement des vérifications sur les antécédents de certains membres du personnel et bride les accès aux applicatifs, aux systèmes et aux LAN en fonction de leurs responsabilités (on peut tout à fait comparer ces principes de sécurité à la gestion d'un aéroport).

Bien évidemment, pour garantir une sécurité optimale, il est nécessaire que l'environnement physique soit aussi sécurisé (accès aux locaux, badges, …). Les Data Centers sont construits pour fonctionner sept jours sur sept et utilisent diverses méthodes contre les coupures électriques, les pannes réseaux et les intrusions physiques. Ces centres de données doivent être conformes aux normes de l'industrie en terme de sécurité physique et de fiabilité. Ils sont gérés, surveillés et administrés par des équipes restreintes dont les informations d'identification changent très régulièrement. [30]

10.2. Quel niveau de sécurité ?

La sécurité absolue n'existe pas. Lorsque l'on évoque la sécurité dans le Cloud, il faut spécifier à quel niveau on souhaite répondre à cette question : au niveau Service, Plate-forme ou Infrastructure.

D'un point de vue applicatif, la sécurité est gérée au sein même du développement de cette application. Que l'on soit sur place ou dans le nuage, la sécurité applicative dépendra des mécanismes internes et de sa conception.

Dans le cas d'une faille de sécurité au niveau système d'exploitation, la question ne se pose pas réellement puisque toutes les infrastructures utilisant ce système seront vulnérables. Un patch pourra résoudre le problème.

Comment peut-on garantir que l'hébergeur assure une sécurité optimale aussi bien au niveau de ses installations physiques, de son personnel et des technologies qu'il utilise ? La sécurité du Cloud n'est pas un nouveau problème.

Comme évoqué dans les parties précédentes, un Cloud public répond à des normes de sécurité « militaires » et globalement les données sont beaucoup mieux protégées au sein du nuage que sur un site dont la sécurité n'est pas la fonction première.

Les architectures dans le nuage proposent des mécanismes cryptographiques permettant d'intégrer de manière autonome et dans ses propres applicatifs la confidentialité de ces données sensibles.

Enfin, si les niveaux de sécurité imposée dans les nuages ne conviennent pas, il sera toujours envisageable de conserver ces informations sur un site de la société avec ces propres dispositions internes. L'applicatif peut se trouver au sein d'un Cloud public alors que les données sont rigoureusement conservées dans un nuage privé, on parlera donc d'une architecture de type Cloud hydride. L'« Information Security Forum » (ISF), qui regroupe plus de 300 membres dont RSSI et Riskmanager, déclare que 91 % de ses membres estiment que le Cloud Computing accroît les menaces de sécurité et qu'ils ne sont donc pas prêts à l'adopter. Cela montre, qu'il y a encore beaucoup de progrès à faire pour convaincre de la sécurité du Cloud auprès des entreprises et des organisations. [30].

11. Aspect économique

11.1. Une économie d'échelle

Le Cloud Computing cumule les points financiers les plus avantageux d'une plate-forme Client/Serveur et des mainframes. La génération des mainframes se caractérisait par d'importantes économies d'échelle du fait du coût d'intégration conséquent et de la complexité à recruter des personnes qualifiées pour la gestion de ces systèmes. A une époque, la puissance de calcul (mesurée en MIPS – million d'instructions par seconde) augmentait de manière exponentielle, alors qu'en parallèle les coûts diminuaient rapidement.

Mais seuls les grands groupes disposaient des moyens nécessaires et enregistraient une demande suffisante pour combler un tel investissement. Etant donné ces coûts conséquents, les entreprises avaient pour priorité la consommation des équipements informatiques plutôt que la réactivité vis à vis des utilisateurs. Les requêtes des utilisateurs étaient mises en file d'attente et le traitement n'intervenait que lorsque les ressources nécessaires étaient disponibles. L'arrivée du modèle client/Serveur, a permis de diminuer les coûts initiaux de ces achats, et d'administrer les ressources beaucoup plus facilement. Cette souplesse a fait baisser de façon notable l'accès aux services IT, d'où une augmentation radicale de l'agilité des utilisateurs. En revanche : les centres de données se développaient de manière tentaculaire avec de nombreux équipements

achetés pour répondre à la demande, mais n'étaient utilisés qu'à hauteur de 5 à 10 % de leur capacité.[31]

Le Cloud Computing n'est pas synonyme d'un retour à l'ère des mainframes, comme certains analystes le laissent croire, loin de là. Il propose aux utilisateurs des économies d'échelle et un rendement dépassant de loin celles des Client/Serveur. La modularité et l'agilité sont également bien supérieures à ce qu'offrait la technologie des mainframes. Fini les compromis ! Les économies d'échelle découlent des domaines suivants :

- Les coûts liés à l'énergie. Les besoins énergétiques ne cessant de croitre, la facture d'électricité est devenue l'élément principal du TCO (Total cost of ownership).[32] Elle en représente aujourd'hui 20 à 25 %. L'indicateur d'efficacité énergétique (PUE - Power Usage Effectiveness) [30] tend à baisser davantage dans les grands sites que dans les petits. Les opérateurs de petits centres de données doivent payer l'électricité au tarif local en vigueur, alors que les gros fournisseurs paient moins en implantant leurs centres de données dans des lieux où l'approvisionnement en électricité est moins coûteux et en signant des contrats d'achat en gros.[32] De plus, l'étude montre qu'un opérateur qui gère plusieurs centres de données peut bénéficier de taux différents en fonction de la position géographique de chaque centre, ce qui allège encore les dépenses énergétiques.
- Les coûts des entités d'administration (personnel de l'infrastructure). Le Cloud Computing restreint considérablement les coûts liés aux équipes opérationnelles à tous les niveaux en automatisant la plupart des tâches d'administration redondantes. Néanmoins, les grandes entreprises y parviennent mieux que les petites. Dans un groupe traditionnel, une même personne peut administrer environ 150 serveurs [33]. Dans un centre de données du Cloud, ce même informaticien a des milliers de machines sous sa responsabilité. Les administrateurs peuvent alors se consacrer à des actions à plus forte valeur ajoutée (développement d'applications ou rajouts de fonctionnalités, par exemple) et répondre aux sollicitations, toujours plus pressantes, des utilisateurs auxquelles le service informatique a à faire.

- Les coûts de Sécurité et de fiabilité. Malgré le fait qu'elle soit souvent citée comme un obstacle à l'adoption d'une solution de Cloud public, la nécessité accrue de sécurité et de fiabilité donne lieu à des économies d'échelle. Pour prétendre à des niveaux acceptables, il faut généralement accepter d'importants investissements. Les principaux fournisseurs commerciaux de Cloud sont souvent mieux armés en la matière. Dotés d'une plus grande expertise qu'un simple service informatique d'entreprise, ils assurent une parfaite sécurité et fiabilité des systèmes du Cloud.
- Les remises quantitatives. Les opérateurs de grands datacenters profitent régulièrement d'importantes remises sur le matériel, de l'ordre de 25-3O% %, par rapport aux acheteurs lambda. Cela est dû à la standardisation d'un nombre limité d'architectures matérielles et logicielles. À l'ère des mainframes, il n'était pas rare de voir coexister plus de 10 architectures différentes. Quant à une topologie client/serveur, elle pouvait regrouper près d'une douzaine de variantes UNIX, le système d'exploitation Windows Server et x86, ainsi que quelques plates-formes RISC. Dans un environnement aussi hétérogène, il était difficile de compter sur des remises quantitatives importantes. Avec le Cloud, l'homogénéité de l'infrastructure permet de réaliser des économies d'échelle.

Dorénavant, beaucoup d'autres économies d'échelle pourront être envisagées, mais nous n'avons pour l'instant pas le recul nécessaire. Les data Centers n'en sont qu'à leur balbutiement et nous voyons aujourd'hui pousser hors de terre des complexes d'une superficie de plusieurs centaines d'hectares **(Tableau 1)**.

Etant donnée l'envergure impressionnante de ces « Méga Centres » de données, la Recherche & Développement ne chômera pas pour maximiser leur rendement et leur exploitation, afin de les rendre encore plus attrayants pour les clients. Les opérateurs de grands centres de données profiteront bien plus de ces avantages que les centres plus petits implantés à l'intérieur des entreprises.

Entreprise	Lieu	Coût (en M)	Taille (en m2)
Internet Village (Jui 09)	Annandale, Ecosse	1600	279 999
National Security Admin.Jui09	Camp Williams, Utah	2000	92900
Microsoft Sept 09	Chicago, Illinois	500	65000
Appel Mai 09	Maiden, C. du Nord	1000	46500
Microsoft Juin 09	Dublin, Irlande	500	N/A
Facebook, Fev 10	Princeville,Oregon	N/A	28500

Tableau 1 : Nouveau projet d'implémentation de data Centers[33].

11.2. La segmentation

La société Brocade a mené une étude sur la plupart des grands groupes internationaux et, 61 % d'entre eux envisagent une migration vers le Cloud Computing d'ici 2012. Les objectifs principaux étant : une réduction des coûts, et une plus grande flexibilité. Sur les 3 prochaines années, l'implantation mondiale du Cloud devrait connaître une progression constante :

- **PaaS :** plus 20 %, ce qui représente 14 milliards $
- **SaaS :** plus 21 %, soit 17,6 milliards $
- **IaaS :** plus 35 %, soit 13,3 milliards $.

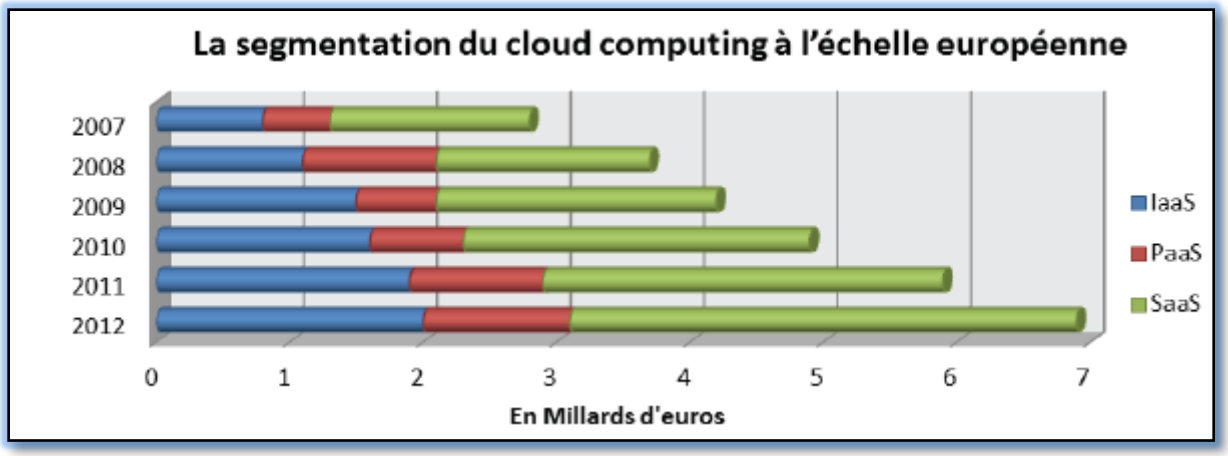

Figure 8 : Segmentation du Cloud Computing à l'échelle européenne[79]

12. Domaines d'application du Cloud Computing

Actuellement et sans que les utilisateurs se rendent compte, de nombreuses applications sont passées dans le Cloud :

- **Domaine militaire :** La technologie employée dans un environnement militaire doit être opérationnelle en toute circonstance. Qu'il s'agisse de garantir l'exécution correcte des opérations quotidiennes, le fonctionnement constant des communications internationales ou la gestion réussie de situation de crise, la solution militaire Camera manager (vidéo protection dans le Cloud) de Panasonic permet de garder un œil constant sur les organisations militaires. Il ne se limite pas à l'enregistrement et l'affichage en temps réel, mais il embarque également de nombreuses fonctions courantes de gestion vidéo-programmation, alarme, utilisation d'une API, gestion des utilisateurs, et est capable de supporter tout ce qu'on fait, quelles que soient les difficultés à surmonter [15].
- **Domaine médical :** Le Cloud a la capacité d'améliorer la collaboration dans l'industrie des soins de santé. En permettant aux professionnels de stocker et accéder aux données à distance. Les professionnels de santé aux quatre coins du monde peuvent accéder aux données des patients et appliquer les soins nécessaires au plus vite. De plus, la téléconférence, les mises à jour des dernières innovations en soins de santé et les conditions du patient en temps réel, permettent d'économiser du temps pour sauver des vies [16].

Followmed est une solution Cloud proposant de multiples fonctionnalités ayant pour objectif de simplifier le quotidien des professionnels de santé, gérez leur activité médicale, innovez leur communication sur le réseau social dédié aux professionnels de la santé, utilisez ce logiciel médical en Cloud pour stocker et Accéder à l'ensemble de leurs données où qu'ils soient.

- **Domaine de l'éducation :** Le Cloud est un excellent levier technologique pour fournir des services collaboratifs extrêmement riches permettant de créer des sessions extrêmement interactives et de réaliser des opérations d'apprentissage à distance qui vont être complémentaires à l'enseignement traditionnel. Par exemple des usages de type blending-learning (ou formation mixte) avec de la vidéo en apprentissage seul, du cours en présentiel et du cours virtuel connecté qui va permettre aux étudiants d'affranchir des limites de l'espace et offrir un panel de possibilité plus important [17]. Virtual ComputingLab (VCL) est une infrastructure Cloud qui fédère des ressources informatiques de plusieurs sites (serveurs, systèmes de stockage, instances de logiciels). Elle permet aux élèves des différents établissements primaires et secondaires de l'Etat ainsi qu'aux étudiants des différents campus de l'université d'accéder, où qu'ils se trouvent (en ce compris chez eux), à un pool de ressources techniques et pédagogiques évoluées et à jour [15].
- **Domaine industriel :** Pour pérenniser la croissance de l'industrie manufacturière, les fabricants doivent sans cesse améliorer la précision et la rapidité de leurs procédés, et optimiser chaque interaction avec les fournisseurs, distributeurs et prestataires de services. On assiste ainsi à la démocratisation des architectures technologiques "just in time" (ou dynamiques), basées sur des Clouds publics et privés, qui aident les fabricants à tenir leurs objectifs et à maintenir leur compétitivité [18]. Salesforce est une plateforme Cloud complète permettant de gérer les interactions entre les fournisseurs et leurs clients, et les aider à prospérer et réussir [19].

13. Les principaux acteurs du Cloud Computing

- **Amazon :** Amazon, au travers « Amazon Web Services » (AWS) met à disposition un Cloud public depuis 2006. Au départ, il s'agissait de rentabiliser leurs énormes infrastructures en place pour absorber les pics de charge lors des fêtes de Noël sur leur boutique en ligne. Aujourd'hui, Amazon propose un service d'IaaS avec « EC2 » (ElasticCompute Cloud) et différents PaaS liés ou non à leur boutique.
- **Google :** Microsoft Azure, anciennement connu sous le nom de Windows Azure, est le nouveau nom de la plateforme Cloud (IaaS et PaaS) de Microsoft. Au départ simple plateforme basée sur Windows Server, Microsoft Azure a gagné en flexibilité et permet désormais aux développeurs d'utiliser n'importe quel langage, infrastructure ou outil pour créer, déployer et gérer des applications. [20]
- **VMware :** La virtualisation est le processus qui consiste à créer une version logicielle (ou virtuelle) d'une entité physique. La virtualisation peut s'appliquer aux applications, aux serveurs, au stockage et aux réseaux. Il s'agit de la manière la plus efficace de réduire les dépenses informatiques tout en stimulant l'efficacité et la flexibilité des entreprises de toute taille. [21]

Conclusion

Le Cloud Computing ou informatique en nuage est une infrastructure dans laquelle la puissance de calcul et de stockage est gérés par des serveurs distants auxquels les usagers se connectent via une liaison Internet sécurisée. L'ordinateur de bureau ou portable, le téléphone mobile, la tablette tactile et autres objets connectés deviennent des points d'accès pour exécuter des applications ou consulter des données qui sont hébergées sur les serveurs. Le Cloud se caractérise également par sa souplesse qui permet aux fournisseurs d'adapter automatiquement la capacité de stockage et la puissance de calcul aux besoins des utilisateurs.

On va présenter dans le prochain chapitre une autre infrastructure qui est le Fog.

Chapitre 2 : Fog Computing (informatique en brouillard)

" Notre cerveau a le don de connecter des faits. Parfois ces connexions conduisent à des découvertes scientifiques, parfois à des œuvres d'art, le plus souvent à des affabulations"

Thierry Crouzet

1. Introduction

Le Cloud Computing est devenu l'un des piliers de l'application et du matériel intelligent. Mais la dépendance croissante à l'égard des dispositifs Internet des objets IoT et applications logicielles a conduit ces petits dispositifs à générer une grande quantité de données et à exiger une très grande capacité d'analyse et de réponse basée sur le Cloud, imposant certaines limitations de Cloud Computing en raison de la lenteur de la vitesse Internet, du stockage et de la récupération de l'information, en particulier dans les applications qui considèrent la vitesse Internet comme très importante, comme les applications médicales, les opérations chirurgicales et la conduite sur route .

L'un des modèles utilisés pour résoudre les problèmes précédents est Fog Computing, où les périphériques effectuent le traitement, le stockage des données et d'autres au lieu du Cloud, puis envoient des informations et des rapports périodiques au Cloud . Cette technologie tire parti de la proximité des périphériques intelligents et les utilise

pour accélérer le stockage et la récupération des informations. Le nom en est dérivé, car le Fog est le plus proche de la Terre et des Smart Devices (IoT), tandis que le est le plus éloigné.

Mais n'oublie pas que le Fog est une extension du Cloud Computing et ne la remplace pas de toute façon. C'est une façon de profiter du matériel et des périphériques à proximité pour équilibrer la charge du Cloud.[59]

2. Nouveaux défis en IoT nécessitent une nouvelle architecture

L'IoT émergent présente de nombreux nouveaux défis qui ne peuvent être résolus de manière adéquate par les modèles actuels de Cloud et d'informatique hôte. Nous discutons ici de plusieurs de ces défis fondamentaux.

2.1. Exigences de latence strictes

De nombreux systèmes de contrôle industriels, tels que les systèmes de fabrication, les réseaux intelligents, les systèmes de pétrole et de gaz et les systèmes d'emballage des marchandises, exigent souvent que les latences de bout en bout entre le capteur et le noeud de contrôle restent à quelques millisecondes [35]. De nombreuses autres applications d'IoT, comme les communications véhicule-véhicule, les communications véhicule-route, les applications de contrôle de vol par drone, les applications de réalité virtuelle, les applications de jeu et les applications de négociation financière en temps réel, peuvent nécessiter des latences inférieures à quelques dizaines de millisecondes. Ces exigences sont loin de ce que les services Cloud classiques peuvent atteindre.

2.2. Contraintes de bande passante réseau

Le nombre important et en croissance rapide de choses connectées crée des données à un rythme exponentiel [36]. Une voiture connectée, par exemple, peut créer des dizaines de mégaoctets de données par seconde. Cela comprendra des données sur :

1) la mobilité de la voiture, comme ses routes et ses vitesses
2) les conditions de fonctionnement de la voiture, comme l'usure et l'usure de ses composants

3) l'environnement environnant de la voiture, comme les conditions routières et météorologiques
4) les vidéos enregistrées par les caméras de sécurité de la voiture. Un véhicule autonome produira encore plus de données, qui ont été estimées à environ un gigaoctet par seconde [37].

Le réseau intelligent américain devrait générer 1000 pétaoctets de données chaque année. En comparaison, la BiblIoThèque du Congrès des États-Unis a généré environ 2,4 pétaoctets de données par mois, Google a fait le trafic d'environ un pétaoctet par mois et le réseau d'AT&T a consommé 200 pétaoctets par an en 2010 [38].

L'envoi de toutes les données au Cloud nécessite une bande passante réseau extrêmement élevée. Il est souvent inutile ou parfois interdit en raison de la réglementation et des préoccupations relatives à la confidentialité des données. Selon la recherche ABI, 90 % des données générées par les points de terminaison seront stockées et traitées localement plutôt que dans le Cloud [36].

2.3. Périphériques limités en ressources

De nombreux appareils IoT auront des ressources très limitées. Par exemple, les capteurs, les collecteurs de données, les actuateurs, les contrôleurs, les caméras de surveillance, les voitures, les trains, les drones et les dispositifs médicaux intégrés aux patients.

De nombreux périphériques à ressources limitées ne pourront pas compter uniquement sur leurs propres ressources limitées pour répondre à tous leurs besoins informatiques. Exiger de tous qu'ils interagissent directement avec le Cloud sera irréaliste et prohibitif, car de telles interactions nécessitent souvent un traitement intensif en ressources et des protocoles complexes. Par exemple, la multitude de micro-ordinateurs sur un véhicule moderne a besoin de mises à jour de micrologiciels, mais il sera difficile d'obtenir des mises à jour de micrologiciels auprès des services Cloud en exigeant que chacun de ces appareils à ressources limitées exécute les opérations cryptographiques lourdes et les procédures sophistiquées requises pour obtenir des mises à jour de micrologiciels.[80]

2.4. Systèmes cyber-physiques

À mesure que de plus en plus de systèmes cyber-physiques sont connectés à l'informatique, le pendule entre la "brique" et le "clic" commence à revenir à la "brique", où les interactions, et souvent les intégrations étroites, entre les systèmes cybernétiques et physiques deviennent de plus en plus importantes et apportent de nouvelles priorités opérationnelles et de nouvelles exigences opérationnelles. Parmi les systèmes cyber-physiques, on peut citer les systèmes de contrôle industriel, les villes intelligentes et les voitures et trains connectés.

Dans ces systèmes, le fonctionnement ininterrompu et sûr est souvent la priorité absolue. La mise hors ligne d'un système, quelle qu'en soit la raison, peut entraîner des pertes importantes pour l'entreprise ou des désagréments intolérables pour les clients, et doit donc être planifiée des jours, des semaines et même des mois à l'avance dans certains cas [39]. Par exemple:

- ➢ Exiger que les voitures soient amenées dans les ateliers de réparation juste pour installer les paquets de mise à jour des logiciels peut causer des inconvénients intolérables et entraîner des coûts élevés pour les propriétaires de voitures et les constructeurs automobiles.
- ➢ Un réacteur nucléaire fonctionne généralement sur des cycles de 18 mois et toute période d'inactivité peut causer des dizaines de milliers de dollars [40].
- ➢ De nombreux autres systèmes de contrôle ou de fabrication industriels, comme les usines d'assemblage de voitures et les générateurs d'énergie électrique dans les réseaux d'énergie, ont des exigences semblables pour des opérations sécuritaires ininterrompues et nécessitent des semaines à des mois de temps de préparation pour planifier les temps d'arrêt du système.

Par conséquent, contrairement aux routeurs, commutateurs, ordinateurs personnels et smartphones dans l'Internet d'aujourd'hui, les délais et les possibilités de mise à jour du matériel et des logiciels dans ces systèmes cyber-physiques peuvent être considérablement limités. De nombreuses applications de contrôle critiques, qui doivent être mises à jour au fil du temps, ne peuvent pas être déplacées vers le Cloud en raison de retards, de bande passante ou d'autres contraintes.

Une nouvelle architecture informatique et de mise en réseau sera donc nécessaire pour réduire les besoins de mise à jour du matériel et des logiciels dans les systèmes critiques.

2.5. Services ininterrompus avec connectivité intermittente au Cloud

Les services Cloud auront de la difficulté à fournir des services ininterrompus aux périphériques et aux systèmes qui ont une connectivité réseau intermittente au Cloud. Ces dispositifs comprennent les véhicules, les drones et les plates-formes pétrolières. Par exemple, une plate-forme pétrolière dans l'océan et loin de la côte peut n'avoir que des canaux de communication par satellite pour se connecter au Cloud.

Ces chaînes par satellite peuvent souffrir de fluctuations importantes de la qualité et de la disponibilité intermittente. Cependant, des applications telles que la collecte de données, l'analyse de données et les contrôles pour la plate-forme pétrolière doivent être disponibles même si la plate-forme ne dispose pas de la connectivité réseau avec le Cloud. Par exemple, lorsqu'une voiture traverse une zone où elle perd la connectivité Internet, de nombreux services et applications pour les appareils et les personnes dans la voiture doivent continuer d'être disponibles. Lorsqu'une voiture tombe en panne dans une telle zone et doit être remplacée par l'un de ses dispositifs de contrôle électronique (ECU) avant de pouvoir recommencer à fonctionner, le nouvel ECU doit être authentifié afin d'empêcher l'installation sur le véhicule de tout ECU non autorisé et potentiellement infecté par des logiciels malveillants. Toutefois, les services d'authentification basés sur le Cloud ne seront pas disponibles dans ce scénario. [80]

2.6. Nouveaux défis de sécurité

Les solutions actuelles de cyber sécurité pour l'Internet d'aujourd'hui, conçues principalement pour protéger les réseaux d'entreprises, les datacenters et l'électronique grand public, se sont concentrées sur la protection de périmètres. En particulier, un système ou un dispositif individuel sous protection est placé derrière des pare-feu qui fonctionnent avec des systèmes de détection et de prévention des

intrusions afin d'empêcher les menaces de sécurité de passer par les périmètres protégés.

Certaines fonctions de sécurité à forte intensité de ressources sont également transférées dans le Cloud. Les services de sécurité existants basés sur le Cloud continuent de mettre l'accent sur la protection basée sur le périmètre, comme la redirection d'email et du trafic Web vers les Cloud pour la détection des menaces et la redirection des demandes de contrôle d'accès vers les Cloud pour le traitement de l'authentification et de l'autorisation. Si les menaces pénètrent dans ces protections, les réactions les plus fréquentes ont été que les opérateurs humains mettent le système hors ligne, nettoient ou remplacent les fichiers et les périphériques compromis, puis le remettent en ligne.

Ce paradigme actuel de sécurité ne sera plus suffisant pour relever de nombreux nouveaux défis en matière de sécurité dans l'IoT. Nous discutons ici de plusieurs de ces défis. [80]

2.7. Tenir à jour les informations d'identification et les logiciels de sécurité sur un grand nombre de périphériques

À mesure que le nombre et la diversité des périphériques connectés augmenteront, un défi croissant sera de savoir comment gérer les informations d'identification de sécurité sur ces périphériques et comment maintenir à jour les informations d'identification et les logiciels de sécurité sur les périphériques. Exiger de chaque périphérique qu'il se connecte au Cloud pour mettre à jour ses informations d'identification et ses logiciels de sécurité sera impossible. [80]

2.8. Protection des périphériques à ressources limitées

De nombreux appareils à ressources limitées dans l'IoT ne disposeront pas de ressources suffisantes pour se protéger adéquatement. Ces périphériques peuvent avoir une très longue durée de vie, et le matériel et les logiciels qu'ils contiennent peuvent être difficiles à mettre à niveau. Pourtant, ces appareils devront rester en sécurité pendant leur longue durée de vie. Par exemple, le remplacement de tout matériel sur

les voitures, qui a déjà été vendu aux consommateurs, peut créer des inconvénients importants pour les propriétaires de véhicules et entraîner des coûts élevés et des dommages de réputation pour les constructeurs automobiles. Cependant, au cours de la longue durée de vie d'une voiture qui dure en moyenne environ 11,4 ans [41], les menaces à la sécurité seront considérablement plus avancées, de nombreuses nouvelles menaces apparaîtront et les mécanismes nécessaires pour lutter contre les menaces croissantes devront être améliorés et améliorés en conséquence. Une question fondamentale se pose donc : Comment protéger un très grand nombre de périphériques limités en ressources contre les attaques de sécurité?

2.9. Évaluation de l'état de sécurité des grands systèmes distribués de manière fiable

IoT supportera de nombreux systèmes distribués de grande taille. Par exemple, un réseau de transport branché peut avoir des milliers d'appareils déployés dans une ville pour contrôler les signaux de circulation et communiquer avec les véhicules. Un grand constructeur automobile devra assurer la sécurité de dizaines de millions de voitures sur la route dans un grand pays comme les États-Unis. Une compagnie pétrolière et gazière peut avoir besoin d'interconnecter des centaines de sites éloignés comme des plates-formes pétrolières, des sites d'exploration, des raffineries et des pipelines. Une grille intelligente comprendra des sous-systèmes de mesure en réseau, de collecte de données, d'agrégation de données, de distribution d'énergie et de réponse à la demande dans de multiples zones géographiques.

Par conséquent, il sera essentiel de pouvoir déterminer de façon fiable si un grand nombre de périphériques et de systèmes distribués fonctionnent en toute sécurité. Toutefois, les approches conventionnelles ont de la difficulté à satisfaire simultanément aux exigences d'évolutivité et de surveillance fiables.

Les systèmes actuels de surveillance de la sécurité et de l'état de santé reposent sur la collecte de messages d'état de sécurité et de données d'enregistrement à partir des appareils. Toutefois, ces systèmes peuvent souvent produire des résultats peu fiables lorsqu'ils sont appliqués à certains systèmes d'IoT . Par exemple:

- ➔ De nombreux appareils fonctionnant dans des environnements physiquement non protégés peuvent être compromis et utilisés pour envoyer de fausses informations [42][43][44]. Les adversaires peuvent aussi facilement utiliser ces dispositifs compromis pour former une majorité locale dans de nombreux scénarios d'IoT. Par exemple, ils peuvent compromettre la majorité des compteurs intelligents d'une maison, d'un bâtiment ou même d'une région entière. En conséquence, les mécanismes existants de détection des fausses informations, qui reposent généralement sur la majorité des sources de données pour être honnêtes (c.-à-d. sans compromis et sans dysfonctionnement), ne seront plus adéquats.
- ➔ Les attaquants peuvent compromettre un système cyber-physique et endommager l'équipement physique tout en conservant les messages à destination et en provenance du système. L'attaque de Stuxnet contre l'installation nucléaire iranienne en est un excellent exemple : le ver Stuxnet a masqué l'attaque en envoyant des messages d'état normaux aux aux administrateurs du système tout en déplaçant le réacteur nucléaire hors de contrôle [45][46][47].

Pour accroître la fiabilité de la surveillance de l'état de sécurité, les mécanismes d'attestation à distance permettent à un dispositif de prouver cryptographiquement sa fiabilité à un vérificateur distant [48][49]. Un périphérique fait une réclamation au vérificateur au sujet de certaines propriétés de son environnement matériel, logiciel ou d'exécution et utilise ses informations d'identification de sécurité (par exemple, une racine matérielle de certificats de confiance et de clés publiques) pour garantir ces propriétés. Le vérificateur vérifie ensuite ces allégations de façon cryptographique.

Toutefois, les méthodes d'attestation à distance existantes ont surtout visé à permettre à un dispositif individuel d'attester de sa propre fiabilité. De nombreux périphériques à ressources limitées dans l'IoT ne pourront pas prendre en charge l'attestation distante à forte intensité de traitement. Même dans la mesure du possible, forcer un grand nombre de périphériques à effectuer une attestation à distance peut entraîner des coûts et une complexité de gestion excessifs.

De plus, la technologie d'attestation à distance existante ne peut à elle seule traiter le cas où un dispositif lui-même n'est pas compromis, mais où son entrée sensorielle est suffisante.

2.10. Répondre aux compromis de sécurité sans causer des perturbations intolérables

Les solutions actuelles de réponse aux incidents reposent principalement sur des mécanismes de force brute tels que l'arrêt d'un système potentiellement compromis, la réinstallation et le redémarrage de son logiciel, ou le remplacement de ses composants et sous-systèmes. De telles réponses extrêmement perturbatrices, qui ignorent en grande partie la gravité des compromis, peuvent provoquer des perturbations intolérables dans les systèmes critiques. Cependant, le maintien d'un fonctionnement ininterrompu et sûr, même lorsque le système est compromis, est souvent la priorité absolue pour les systèmes critiques tels que les systèmes de contrôle industriel, les usines de fabrication, les véhicules connectés, les drones et les réseaux intelligents. Par exemple:

- Un générateur électrique peut être infecté par un malware qui cherche simplement à voler de l'énergie pour une utilisation non autorisée. L'arrêt du générateur pourrait provoquer de graves perturbations du réseau intelligent et des coupures d'électricité excessives.

- Les systèmes de contrôle industriel ont souvent peu de tolérance pour les temps d'arrêt. Les opérations de fabrication peuvent également avoir des répercussions critiques sur la sécurité. Par conséquent, les fabricants accordent habituellement de l'importance à l'exploitation et à la sécurité ininterrompues plutôt qu'à l'intégrité du système. Cela signifie que les mises à jour matérielles et logicielles ne peuvent être installées que pendant les temps d'arrêt programmés d'un système, qui doivent être courts et éloignés, plutôt que chaque fois qu'un compromis de sécurité est détecté.
- Une voiture branchée peut être infectée par des logiciels malveillants qui peuvent devenir actifs pendant que la voiture est en marche. Bien que les

logiciels malveillants puissent causer toute une gamme de dommages au véhicule et mettre le conducteur et les passagers en danger, l'arrêt brusque du moteur chaque fois qu'un malware est détecté pourrait être un moyen encore plus rapide et plus sûr de causer des accidents mortels de la circulation.

- ➢ Si un drone volant en plein air est brusquement éteint simplement parce qu'un compromis de sécurité est détecté, il peut s'écraser du ciel sur des personnes, des maisons et d'autres propriétés pour causer de sérieux dommages. Au lieu de cela, un atterrissage sûr ou des mécanismes de retour en toute sécurité seront essentiels pour répondre à de telles menaces de sécurité qui peuvent compromettre le vol d'un drone.
- ➢ Un serveur d'un data center peut être infecté par un logiciel espion qui cherche à voler des secrets commerciaux. Même si le fait de permettre à un serveur aussi compromis de continuer à fonctionner pourrait donner à l'attaquant l'accès à certaines données sensibles, il se peut que cela n'affecte pas directement les services stratégiques du datacenter. Si nous arrêtons le serveur, ou arrêtons l'exécution des fichiers infectés par des programmes malveillants pour attendre que le programme malveillant soit supprimé, les temps d'inactivité du système pourraient causer des dommages beaucoup plus importants, notamment des pertes économiques importantes pour l'opérateur du datacenter, des perturbations pour ceux qui comptent sur les datacenters pour exploiter leur entreprise et des inconvénients pour les autres utilisateurs du datacenter.

Par conséquent, le paradigme actuel de réaction aux incidents, qui est très perturbateur, ne sera plus suffisant pour assurer la sécurité des nombreux systèmes critiques dans les nouvelles technologies de l'information. [80]

3. L'époque émergente du Fog

Combler les lacunes technologiques dans la prise en charge de l'IoT , il faudra une nouvelle architecture informatique et de mise en réseau (Fog) qui distribue des fonctions de calcul, de contrôle, de stockage et de mise en réseau plus proches des périphériques utilisateur finaux.

Comparé au Cloud, le Fog se distingue par les trois dimensions suivantes :

- ➢ Effectuer une quantité substantielle de stockage de données à l'utilisateur final ou à proximité (plutôt que de stocker les données uniquement dans des data center distants).
- ➢ Effectuer une grande quantité de fonctions de calcul et de contrôle à l'utilisateur final ou à proximité (plutôt que d'exécuter toutes ces fonctions dans des data centers distants et des réseaux cellulaires centraux). Ces fonctions de calcul et de contrôle peuvent comprendre, par exemple,

- Applications pour les utilisateurs finaux et leurs périphériques.
- Fonctions de contrôle et d'exploitation des systèmes d'utilisateurs finaux tels que les systèmes de fabrication, les véhicules, et des grilles intelligentes.
- Services de gestion des réseaux, systèmes et applications des utilisateurs finaux.
- Services de support des applications basées sur le Cloud, tels que la collecte et le prétraitement des données à envoyer au Cloud.

- ➢ Effectuer une quantité considérable de communications et de réseautage à l'utilisateur final ou à proximité (plutôt que de router tout le trafic réseau à travers les réseaux de base). Cela peut comprendre, par exemple, des moyens d'améliorer les performances et l'évolutivité des réseaux locaux peer-to-peer, un contrôle intelligent des réseaux d'accès radio (RAN), l'organisation et la gestion des réseaux locaux mobiles ad hoc et l'intégration des réseaux locaux ad hoc aux réseaux d'infrastructure.

Le Fog est une extension naturelle du Cloud : Le Fog et le Cloud se complètent les uns les autres pour former un continuum de services mutuellement avantageux et interdépendant entre le Cloud et les points de terminaison afin de rendre l'informatique, le stockage, le contrôle et la communication possibles n'importe où dans le continuum.

Fog permet un continuum de services: Par exemple, pour les appareils portables, un téléphone mobile peut devenir un Fog pour fournir des applications de contrôle et d'analyse locales aux appareils portables. Lorsque l'utilisateur se trouve à l'intérieur de

son véhicule, le véhicule peut devenir un Fog pour son téléphone mobile afin de permettre à de nombreuses fonctions de smartphone, telles que l'affichage, l'interface utilisateur, l'audio, l'annuaire téléphonique, d'être déplacé dans le véhicule. L'équipement de contrôle de la circulation routière peut à son tour servir de Fog pour que le véhicule fournisse des renseignements sur la circulation au véhicule.

Fog et Cloud sont interdépendants : Par exemple, les services Cloud peuvent être utilisés pour gérer le Fog. Le Fog peut servir de proxy au Cloud pour fournir des services Cloud aux points de terminaison et agir comme proxy des points de terminaison pour interagir avec le Cloud. De plus, le Fog peut être la tête de plage pour la collecte et l'agrégation de données pour le Cloud.

Fog et Cloud sont mutuellement bénéfiques : Certaines fonctions sont naturellement plus avantageuses pour être exécutées dans le Fog tandis que d'autres dans le Cloud. La détermination des fonctions qui devraient être exercées dans le Fog et de la façon dont le Fog devrait interagir avec le Cloud sera un aspect clé de la recherche et du développement sur le Fog.

Traditionnellement, les services et les applications sont fournis avec de grandes "boîtes" centralisées, coûteuses et difficiles à innover, telles que les passerelles de service (S-GW) et les passerelles de réseau de données de paquets (PDN-GW) dans le coeur LTE, les grands serveurs dans un centre de données et les passerelles et routeurs de base dans un réseau étendu. La vision traditionnelle est que le bord utilise les réseaux et les datacenters de base. La vue Fog indique que le bord fait partie du réseau central et d'un datacenter. [80]

Le tableau 2 présente les principales caractéristiques du Fog par rapport au Cloud.

	Cloud	**Fog**
Emplacement et modèle de calcul	Centralisé dans un petit nombre de grands centres de données.	Souvent répartie dans de nombreux endroits, potentiellement sur de vastes zones géographiques, plus près des utilisateurs le long du continuum Cloud-to-Thing Les noeuds et systèmes de

		Fog distribué peuvent être contrôlés de manière centralisée ou distribuée.
Taille	Les datacenters de Cloud sont de très grande taille, chacun contenant généralement des dizaines de milliers de serveurs.	Un Fog dans chaque emplacement peut être petit (p. ex., un seul noeud de Fog dans une usine de fabrication ou à bord d'un véhicule) ou aussi grand que nécessaire pour répondre aux demandes des clients. Un grand nombre de petits noeuds de Fog peuvent être utilisés pour former un grand système de Fog.
Opération	Exploiter dans des installations et des environnements sélectionnés et entièrement contrôlés par des opérateurs de Cloud. Fonctionnant et géré par des équipes d'experts techniques. Exploité par de grandes entreprises.Exploiter dans des installations et des environnements sélectionnés et entièrement contrôlés par des opérateurs de Cloud. Fonctionnant et géré par des équipes d'experts techniques. Exploité par de grandes entreprises.	Peut fonctionner dans des environnements déterminés principalement par les clients ou leurs besoins. Un système de Fog ne peut être contrôlé ou géré par personne et ne peut être exploité par des experts techniques. Le Fog peut nécessiter peu ou pas d'intervention humaine. Peut être exploité par de grandes et de petites entreprises, selon leur taille.
Applications	Le support prédomine, sinon seulement, des applications de domaine cybernétique. En général, il prend en charge les applications qui peuvent tolérer des retards aller-retour de l'ordre de quelques secondes ou plus.	Peut prendre en charge à la fois les systèmes et les applications cyber-domaines et cyber-physiques. Peut prendre en charge un nombre considérablement plus élevé d'applications critiques qui nécessitent des latences inférieures à des dizaines de millisecondes ou même inférieures.
Configuration requise pour	Exiger des clients qu'ils aient	Les besoins en bande

la connectivité Internet et la bande passante	une connectivité réseau au Cloud pendant toute la durée des services. Les besoins en bande passante réseau long-courrier augmentent avec la quantité totale de données générées par tous les clients.	passante réseau long-courrier augmentent avec la quantité totale de données qui doivent être envoyées au Cloud après avoir été filtrées par le Fog.

Tableau 2 : Principales caractéristiques du Fog par rapport au Cloud[80]

3.1. Avantages de l'architecture de Fog

Un dénominateur commun sous-jacent au Fog est que le Fog distribue les ressources et les services de calcul, de communication, de contrôle et de stockage plus près des utilisateurs. Une architecture Fog peut être entièrement distribuée, la plupart centralisée, ou quelque part entre les deux. L'architecture Fog et les applications qu'elle prend en charge ("Applications Fog") peuvent être virtualisées et implémentées entièrement dans le logiciel. Ils peuvent également être mis en oeuvre dans du matériel et des logiciels dédiés. [80]

Une architecture Fog permettra à la même application de s'exécuter n'importe où, réduisant ainsi le besoin d'applications spécialisées dédiées uniquement au Cloud, uniquement pour les points de terminaison, ou simplement pour les périphériques de bord. Il permettra aux applications de différents fournisseurs de fonctionner sur la même plate-forme physique sans interférence mutuelle. Il fournira un cadre commun de gestion du cycle de vie pour toutes les applications, offrant des capacités de composition, de configuration, de distribution, d'activation et de désactivation, d'ajout et de suppression, ainsi que de mise à jour des applications. Il offrira en outre un environnement d'exécution sécurisé pour les services et les applications Fog. Le Fog s'intégrera à Cloud pour permettre des services de bout en bout transparents.

Les principaux avantages du Fog peuvent se résumer comme suit :

3.1.1. Cognition: Sensibilisation aux objectifs axés sur le client. Une architecture de Fog, consciente des besoins des clients, peut mieux déterminer où effectuer les fonctions de calcul, de stockage et de contrôle le long du continuum Cloud-to-Thing.

Les applications de Fog, étant proches des utilisateurs finaux, peuvent être construites pour mieux connaître et refléter de près les besoins des clients.

3.1.2. Efficacité: Mettre en commun les ressources le long du continuum Cloud-to-Thing. Le Fog peut distribuer des fonctions d'informatique, de stockage et de contrôle n'importe où entre le Cloud et le point de terminaison pour tirer pleinement parti des ressources disponibles le long de ce continuum. Il peut également permettre aux applications de tirer parti des ressources de réseau, de stockage et de calcul autrement inactives disponibles en abondance sur les périphériques réseau et utilisateurs finaux tels que les tablettes, les ordinateurs portables, les appareils électroménagers intelligents, les véhicules et les trains connectés et les routeurs de bord réseau. La proximité plus étroite de Fog avec les points de terminaison lui permettra d'être mieux intégré aux systèmes des utilisateurs finaux afin d'améliorer l'efficacité et les performances globales du système. Ceci est particulièrement important pour les systèmes cyber-physiques critiques en termes de performances.

3.1.3. Agilité : Une innovation rapide et une évolutivité abordable. Il est généralement beaucoup plus rapide et moins cher d'expérimenter avec les périphériques clients et périphériques. Plutôt que d'attendre que les fournisseurs de gros réseaux et de boîtes de Cloud lancent ou adoptent une innovation. Le Fog facilitera la création d'un marché ouvert pour les particuliers et les petites équipes qui utiliseront des API ouvertes (interfaces de programmation d'applications), des SDK ouverts (kits de développement de logiciels) et la prolifération d'appareils mobiles pour innover, développer, déployer et exploiter de nouveaux services.

3.1.4. Latence: Traitement en temps réel et contrôle du système cyber-physique. Le Fog active l'analyse des données à la périphérie du réseau et peut prendre en charge les fonctions de contrôle sensibles au temps pour les systèmes cyber-physiques locaux. Cela est essentiel non seulement pour les applications commerciales, mais aussi pour la vision d'Internet tactile pour permettre aux applications AI intégrées avec des temps de réaction millisecondes.

Ces avantages permettent à leur tour de nouveaux services et modèles d'affaires, et peuvent contribuer à élargir les revenus, à réduire les coûts ou à accélérer le déploiement des produits.

3.2. Le Fog aide à relever les défis liés aux IoT

Le Fog peut fournir des moyens efficaces de surmonter de nombreuses limitations des architectures informatiques existantes qui reposent uniquement sur l'informatique dans le Cloud et sur les périphériques de l'utilisateur final. Le tableau 3 montre, à titre d'exemple, comment le Fog peut aider à relever les défis de l'IoT [80]

Les défis d'IoT	Comment le Fog peut aider
Contraintes de latence	Le Fog , permet d'effectuer l'analyse des données, le contrôle et d'autres tâches sensibles au temps à proximité des utilisateurs finaux, est l'option idéale et souvent la seule pour répondre aux exigences de synchronisation strictes de nombreux systèmes d'IoT.
Contraintes de bande passante réseau	Le Fog permet le traitement hiérarchique des données le long du continuum Cloud-to-Things, permettant ainsi d'effectuer le traitement là où il peut équilibrer les exigences de l'application et les ressources réseau et informatiques disponibles. Cela réduit également la quantité de données à envoyer au Cloud.
Périphériques à ressources limitées	Le Fog peut effectuer des tâches gourmandes en ressources pour le compte de périphériques limités en

	ressources lorsque de telles tâches ne peuvent pas être déplacées dans le Cloud pour une raison quelconque, réduisant ainsi la complexité de ces périphériques, les coûts de leur cycle de vie et leur consommation d'énergie.
Services ininterrompus avec connectivité intermittente au Cloud	Un système de Fog local peut fonctionner de façon autonome pour assurer des services non interrompus même s'il dispose d'une connectivité réseau intermittente avec le Cloud.
Nouveaux défis de sécurité d'IoT	Un système de Fog peut, par exemple, 1) servir de proxy pour les périphériques à ressources limitées afin d'aider à gérer et à mettre à jour les informations d'identification et les logiciels de sécurité sur ces périphériques, 2) exécuter une vaste gamme de fonctions de sécurité, comme l'analyse des programmes malveillants, pour les périphériques à ressources limitées afin de compenser les fonctionnalités de sécurité limitées sur ces périphériques, 3) surveiller l'état de sécurité des périphériques à proximité, et 4) tirer parti des informations locales et du contexte pour détecter les menaces en temps.

Tableau 3 : Comment le Fog peut aider à relever les défis de l'IoT[80]

Les essais de démonstration du concept (PPC) démontrent la valeur commerciale et la nécessité technologique du Fog. Par exemple, fin 2015, Cisco a mené avec succès un PPC à Barcelone, où Fog a rendu les applications de villes intelligentes plus rentables et gérables. Barcelone envisage de déployer des milliers de cabinets routiers dans toute la ville pour optimiser la gestion du trafic, la gestion de l'énergie, la gestion de l'eau et des déchets. Avant de pouvoir concrétiser cette vision, la ville a dû faire face à deux défis majeurs. Premièrement, la façon traditionnelle d'ajouter de nouvelles applications en ajoutant de nouvelles passerelles et de nouveaux serveurs dédiés dans chaque armoire routière n'est plus possible en raison de l'espace limité de l'armoire. Deuxièmement, les applications installées ont utilisé des systèmes de gestion d'applications en mode "siloed", ce qui a rendu le système excessivement coûteux à déployer, à exploiter et à entretenir. Le Fog a fourni une solution. Un noeud Fog unique a fourni une plate-forme commune à chaque armoire pour tous les services et a permis aux applications de différents fournisseurs de coexister sans interférer les unes avec les autres. Il a fourni une plate-forme unifiée pour prendre en charge la mise en réseau, la sécurité et la gestion du cycle de vie de toutes les applications, ce qui a réduit les coûts des systèmes et permis aux fournisseurs d'applications de se concentrer sur le développement d'applications plutôt que de fournir du matériel et des logiciels spécialisés pour héberger et gérer leurs applications.

3.3. Le Fog permet de nouveaux modèles d'entreprise perturbateurs

Le Fog permettra de mettre en place de nouveaux modèles d'entreprise potentiellement très perturbateurs pour l'informatique et la mise en réseau. Par exemple, [80]

- Avec le Fog , les routeurs, les commutateurs, les serveurs d'applications et les serveurs de stockage convergeront en noeuds de Fog . Une telle transformation peut considérablement remodeler le paysage du réseau, des serveurs et du secteur des logiciels.
- Fog-as-a-Service (FaaS) permettra à de nouveaux modèles d'affaires de fournir des services aux clients. Contrairement aux Clouds qui sont principalement exploités par de grandes entreprises qui peuvent se permettre de construire et

d'exploiter d'énormes datacenters, FaaS permettra aux entreprises, grandes et petites, de fournir des services privés ou publics d'informatique, de stockage et de contrôle à différentes échelles pour répondre aux besoins d'une grande variété de clients.

- Fog offre également une nouvelle façon pour les fournisseurs de services de réseau d'ajouter de la valeur aux clients dans un nouveau monde de neutralité du réseau. Prenons, par exemple, l'impact de la décision de la Commission fédérale des communications (FCC) des États-Unis, Titre II. Le vote de la FAC en février 2015 pour classer les services Internet, y compris les services mobiles, comme un "utilitaire" en vertu du mandat réglementaire du titre II, pourrait pousser davantage l'innovation en réseau à la pointe aux États-Unis. Un nouvel environnement réglementaire ne signifie pas que les réseaux ne peuvent plus être conçus et gérés, mais nous avons peut-être besoin de différents points de vue pour contrôler les réseaux : non pas de l'intérieur du réseau, mais de l'ensemble des utilisateurs finaux. Par exemple, aujourd'hui, les opérateurs de réseau peuvent choisir dans quelle voie (WiFi, Macro-cellulaire et Femtocell) un périphérique utilisateur doit se trouver. Étant donné que les différentes voies ont des vitesses différentes et des systèmes de paiement/montant différents, une telle pratique ne peut plus être autorisée aux États-Unis. Au lieu de cela, nous devons améliorer le système de conception où chaque périphérique utilisateur doit choisir la voie à suivre pour lui-même. Le défi résultant de la réglementation du Titre II est une "épée suspensive" qui refroidit le déploiement d'innovations d'infrastructure de réseau, car l'équilibre risque-retour se dirige désormais vers "le maintien du réseau tel quel." Cependant, tant que le gouvernement n'interdit pas les choix des utilisateurs finaux, nous pouvons alors lancer la mise en réseau à partir du bord, via un contrôle/configuration piloté par le client/la maison.

4. Étude de cas sur l'utilisation du Fog

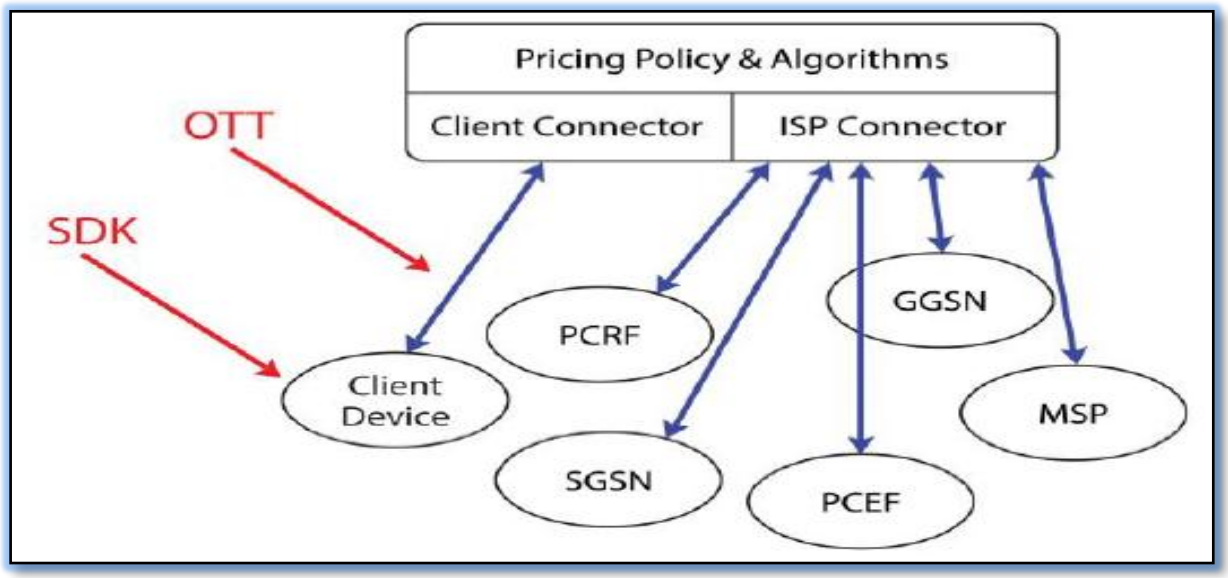

Figure 9: Le SDK installé dans les clients peut permettre l'inférence et la configuration du réseau[80]

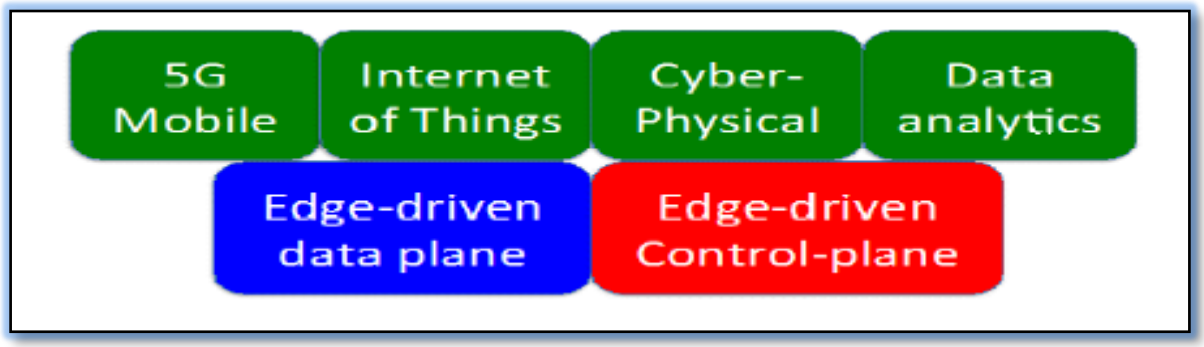

Figure 10: Le plan de données et le plan de contrôle de Fog permettent différentes applications[80]

La R&D architecturale pose la question de savoir "qui fait quoi, à quel moment et comment remettre les modules en place?" En tant qu'architecture, Fog prend en charge une variété d'applications, y compris celles qui sont généralement associées à l'IoT et celles qui sont souvent considérées comme faisant partie du 5G ou de l'analyse des données et de la gestion des données.Le Fog est une architecture pour l'informatique, le stockage, ainsi que pour la mise en réseau. En particulier, l'architecture Fog se compose à la fois du plan de données et du plan de contrôle, chacun avec un nombre

croissant d'exemples de couches de protocole de la couche physique à la couche d'application:

➔ Exemples de plan de données du Fog :

- Mise en commun des ressources informatiques/de stockage/bande passante inutilisées des clients et du contenu local
- Mise en cache de contenu à la périphérie et gestion de la bande passante à la maison
- Formation de faisceaux distribués pilotés par le client
- Communications directes client-client (p. ex. FlashLinQ, LTE Direct, WiFi Direct, AirDrop)
- Cloudlets et micro centres de données

➔ Exemples de plan de contrôle du Fog:

- Gestion du contenu Over the Top (OTT)
- Fog-RAN : Réseau d'accès radio alimenté par les Fogs
- Contrôle HetNets basé sur le client
- Stockage Cloud contrôlé par le client
- Gestion de session et chargement de signalisation à l'extrémité
- Inférence de la détection des foules dans les états de réseau
- Analyses Edge et extraction en temps réel des flux

Le plan de données de Fog a été étudié de façon plus approfondie, p. ex. [50]. Dans ce qui suit, nous soulignons quelques cas particuliers qui illustrent le potentiel et les défis du plan de contrôle du Fog , tels que l'inférence, le contrôle, la configuration et la gestion des réseaux:

Bien que certaines de ces études de cas soient des sujets centraux dans ce que beaucoup de gens imaginent définir en partie "5G:" HetNets/petite cellule/densification, sur le provisionnement des services de haut niveau, la radio cognitive et la détection par la foule, d'autres études de cas mettent l'accent sur la

pensée architecturale pour les services IoT, les questions sur la propriété, le contrôle et la visibilité des réseaux personnels, tels que "Apple Watch et le genre ont leur propre plan de données ?" qui vont aider à équilibrer ? le pouvoir entre les AT&T et les Apple du monde. Si le réseau à l'intérieur ou autour des utilisateurs finaux a une topologie logique qui ressemble à une étoile, avec une passerelle fixe (iPhone, par exemple), la visibilité, le contrôle et la valeur ajoutée par les opérateurs réseau seront radicalement différents de ceux du scénario alternatif où les passerelles sont choisies dynamiquement ou où les objets peuvent parfois avoir des voies de communication directes sans passerelle.

Cas 1: États LTE de détection de foules (en déploiement commercial). Grâce à une combinaison de mesures passives (p. ex., RSRQ), de sondes actives (p. ex., train de paquets), de corrélation du débit d'application et d'exploration de données historiques, une collection de dispositifs clients peut être en mesure, en temps réel et avec une précision utile, de déduire les états d'un eNB, comme le nombre de blocs de ressources utilisés [51].

Cas 2 : approvisionnement du réseau OTT et gestion du contenu (en déploiement commercial). L'approche traditionnelle de l'innovation dans les réseaux consiste à introduire une autre boîte à l'intérieur du réseau, éventuellement une boîte virtualisée, mais une boîte néanmoins. Le Fog exploite directement les "choses" et les téléphones à la place, et supprime complètement la dépendance aux boîtes dans le réseau. Avec les SDK situés derrière les applications sur les appareils clients, les services réseau peuvent être innovants beaucoup plus rapidement grâce à des tâches telles que l'encapsulation des URL, le marquage du contenu, le suivi de la localisation, la surveillance du comportement. Dans ce cas, les SDK clients travaillent collectivement par l'intermédiaire d'un contrôleur (dans le Cloud comme celui hébergé par Amazon, par exemple) mais contournent la majeure partie du réseau central cellulaire (un deuxième type de Cloud).

Cas 3: Contrôle HetNets basé sur le client (normes 3GPP). La coexistence de réseaux hétérogènes (p. ex., LTE, femto, WiFi) est aujourd'hui un élément clé des réseaux cellulaires. Plutôt que de passer par le contrôle de l'opérateur de réseau, chaque client

peut observer ses conditions locales et décider du réseau à rejoindre. Grâce à la randomisation et à l'hystérésis , de telles actions locales peuvent émerger globalement pour converger vers une configuration souhaitable [52]. Dans le cas d'un contrôle hybride de HetNets, l'interface Fog-Cloud permet aux clients eux-mêmes d'effectuer la configuration du réseau en temps réel, tandis que des paramètres à plus long terme comme l'attribut de stabilité RAT ou les valeurs d'hystérésis peuvent passer du Cloud (réseau de base sans fil) aux clients.

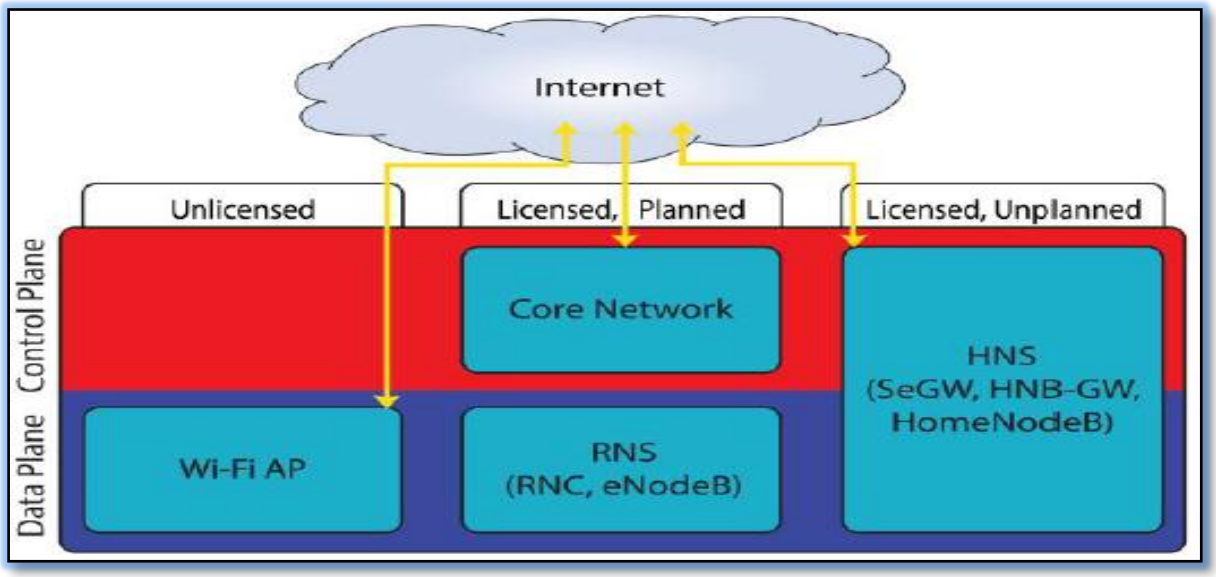

Figure 11 : La coexistence de réseaux hétérogènes peut être gérée en partie par les clients[80]

Cas 4 :"Shred and Spread" - stockage dans le Cloud contrôlé par le client (en phase de test bêta). En découplant le stockage massif et bon marché (dans le Cloud) du contrôle de la vie privée du côté client (dans le Fog), nous pouvons obtenir le meilleur des deux mondes. Par exemple, en déchiquetant un fichier du côté du Fog et en répartissant ensuite les octets d'un fichier donné sur plusieurs Cloud publics, dans une couche de calage client, entre plusieurs fournisseurs de stockage en Cloud , on peut être sûr que la confidentialité des données est maintenue même si la clé de chiffrement est divulguée par un fournisseur de Cloud donné [53].

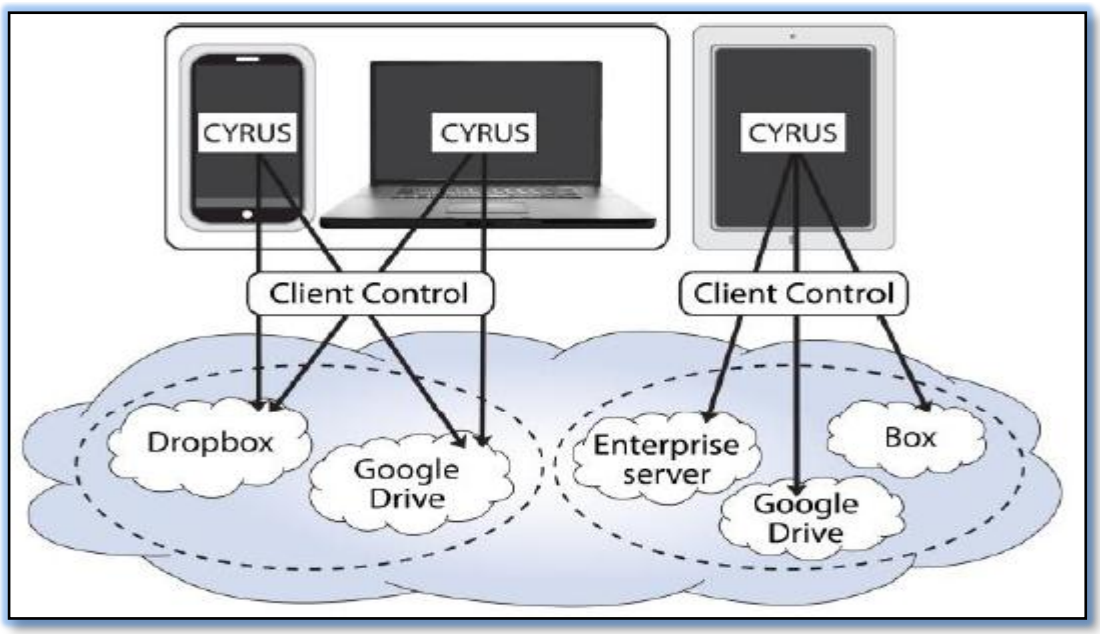

Figure 12 : Shred and Spread (projet CYRUS) stocké dans le Cloud mais contrôle dans le Fog[80]

Cas 5 : Extraction de flux en temps réel pour l'IA intégrée (dans le cadre d'un essai bêta). Examinez les tâches de réalité virtuelle associées à Google Glass. Certaines des tâches de recherche d'informations et de calcul peuvent être effectuées sur le Glass (un "objet portable"), d'autres sur le téléphone associé (un appareil client), d'autres encore sur le stockage à domicile (un appareil périphérique), et le reste dans le Cloud. Une architecture de raffinements successifs peut exploiter tous ces dispositifs en même temps, avec une division intelligente du travail entre eux [54].

Cas 6 : Emprunt de bande passante à des voisins dans D4D (en essai bêta). Lorsque plusieurs appareils appartenant à la même personne, à des parents ou à des employés de la même entreprise sont côte à côte, l'un d'entre eux peut demander aux autres de partager leur bande passante LTE/WiFi en téléchargeant d'autres parties du même fichier et en transmettant, via WiFi Direct, de client à client [55].

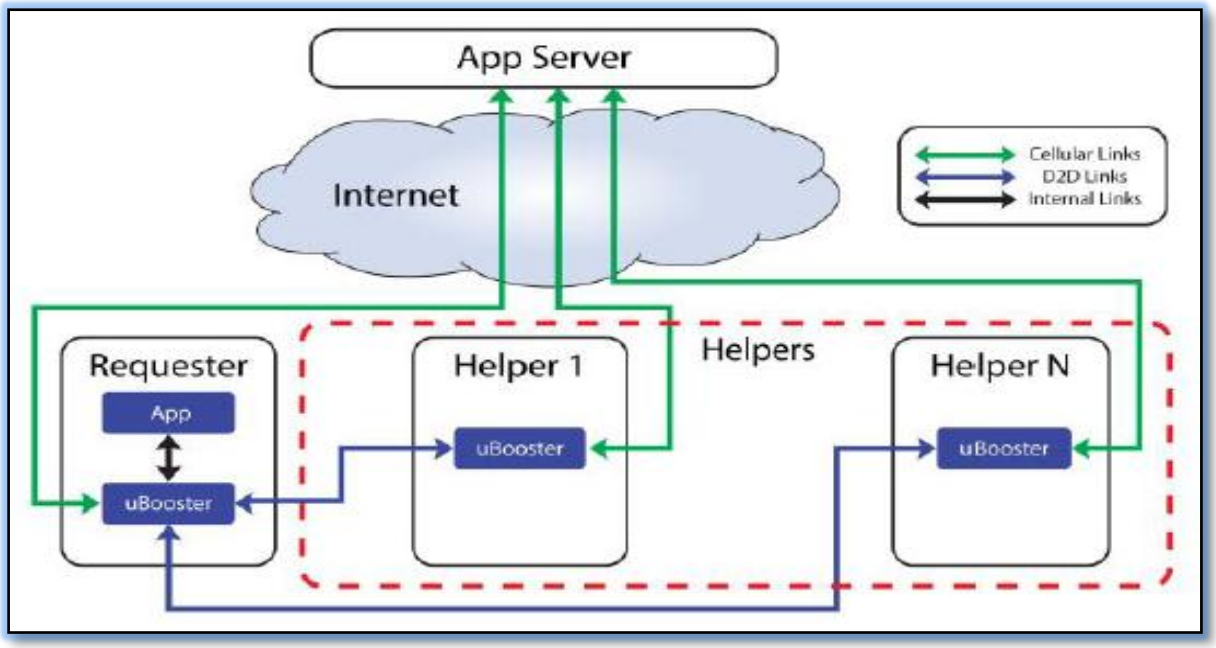

Figure 13 : Les ressources inactives des périphériques clients peuvent être mises en commun dans D4D pour une utilisation plus efficace[80]

Cas 7 : gestion de la bande passante au niveau de la passerelle domestique (en essai bêta). En adaptant le décodeur/passerelle domestique, la capacité limitée de la bande passante est répartie entre les utilisateurs concurrents et les sessions d'application, en fonction de la priorité de chaque session et des préférences individuelles. Un prototype sur un routeur de base démontre un contrôle évolutif, économique et précis de l'allocation de la capacité sur le bord[56].

Cas 8 : Formation de faisceaux distribués (dans le cadre d'une démonstration en laboratoire). Le Fog peut également se produire dans la couche physique, par exemple en exploitant des MIMO multi-utilisateurs pour améliorer le débit et la fiabilité lorsqu'un client peut communiquer avec plusieurs points d'accès WiFi. Pour la liaison montante, nous pouvons utiliser la formation de faisceaux multi-utilisateurs afin que le client puisse envoyer plusieurs flux de données à plusieurs points d'accès simultanément. Pour la liaison descendante, nous pouvons utiliser l'annulation des interférences afin que le client puisse décoder des paquets parallèles provenant de plusieurs points d'accès. Ces opérations peuvent être effectuées entièrement du côté client [57].

5. Questions ouvertes et défis de la recherche

Comme c'est le cas pour tout nouveau domaine de R-D, de nombreux thèmes dans le Fog ne sont pas complètement nouveaux, et sont plutôt des versions évoluées des transformations accumulées au cours des dix ou deux dernières années :

- Comparé aux réseaux peer-to-peer (P2P) du milieu des années 2000, Fog n'est pas seulement une question de partage de contenu (ou de plan de données dans son ensemble), mais aussi de mesure du réseau, de gestion du réseau, d'activation des services et de contrôle en temps réel des systèmes cyber-physiques.

- Comparé à la recherche sur les réseaux mobiles ad hoc (MANET), Fog s'appuiera sur des périphériques, des applications et des réseaux hiérarchiques de bout en bout bien plus puissants, diversifiés et souvent de pointe, grâce à des réseaux sans fil et câblés à large bande.

- Comparé au travail générique de réseautage en bord dans le passé, Fog ajoute une nouvelle couche de signification au principe de bout en bout : en plus d'optimiser entre eux, les périphériques de pointe, qui mesurent et contrôlent collectivement le reste du réseau, collaboreront avec le Cloud pour permettre des services de bout en bout le long du continuum Cloud-to-Thing.

En plus de plusieurs autres thèmes d'architecture de réseau ayant une histoire plus longue, les réseaux centrés sur l'information (ICN), les réseaux définis par les logiciels (SDN), la virtualisation des fonctions de réseau (NFV), Fog revisite les fondements de l'architecture de l'informatique et de la mise en réseau: qui fait quoi et comment les coller ensemble :

- **ICN :** Redéfinir des fonctions (pour fonctionner sur des objets numériques plutôt que sur des octets)
- **SDN :** Séparer le plan de contrôle du plan de données et permettre l'implémentation du plan de contrôle dans le logiciel.

- **NFV :** Virtualiser les fonctions (via un plan de contrôle centralisé).
- **Fog :** Déplacer les fonctions (vers la périphérie du réseau et le long du continuum Cloud-to-Things).

Bien que Fog n'ait pas à s'appuyer sur la virtualisation ou à être centré sur l'information ou défini par un logiciel, on peut envisager un Fog centré sur l'information et virtualisé, car ces branches sont complémentaires les unes des autres et peuvent être des vecteurs de Fog.

Le Fog inclut aussi bien les réseaux mobiles que filaires, et traverse le bord, l'accès et les câbles. La prise en charge de l'informatique de pointe mobile au sein d'un RAN exigera plusieurs des mêmes fonctions d'une architecture Fog de bout en bout pour, par exemple, distribuer, orchestrer, gérer et sécuriser les applications et les plates-formes d'activation d'applications. Le Fog , cependant, est plus large que la simple prise en charge de l'informatique mobile de pointe. Le Fog est une architecture qui permet de distribuer des services informatiques, de stockage, de contrôle et de mise en réseau n'importe où le long du continuum Cloud-to-Thing, sur et à l'intérieur des réseaux sans fil et filaires, et qui prend en charge les applications de réseau mobile et filaire.

Comme dans toute zone émergente de son enfance, il n'y a pas de pénurie de questions stimulantes dans Fog, dont certaines continuent d'être tirées d'une étude antérieure de P2P, MANET et Cloud, tandis que d'autres sont motivées par une confluence des développements récents dans l'ingénierie de réseau, les périphériques utilisateur et l'expérience utilisateur. Ensuite, nous discutons de plusieurs catégories de défis liés à la recherche sur le Fog . [58]

5.1. Interfaces des Fog avec Cloud , autres Fog , things , et les utilisateurs finaux

La question fondamentale de l'architecture est "qui fait quoi, à quel moment, et comment les rassembler ?" Dans le cas de Fog, la question devient :

1) quelles tâches doivent être confiées au Fog (p. ex., celles qui nécessitent un traitement en temps réel, les objectifs de l'utilisateur final ou l'exploitation économique de ressources inactives)
2) qui vont au Cloud (p. ex. stockage massif, calcul lourd ou connectivité à grande distance)
3) qui vont aux objets
4) comment le Fog , le Cloud et les objets doivent interagir entre eux. Les architectures Fog devraient permettre le déplacement dynamique des tâches de calcul, de stockage et de mise en réseau entre le Fog, le Cloud et les ailes.

Par conséquent, les interfaces pour que le Fog interagit avec le Cloud, d'autres Fog , les objets et les utilisateurs, comme l'illustre la figure 14, doivent :

1) faciliter le déplacement souple et, dans certains cas, dynamique des fonctions de calcul, de stockage et de contrôle entre ces différentes entités
2) permettre l'accès pratique des utilisateurs aux services de Fog
3) permettre une gestion efficace du cycle de vie du système et des services.

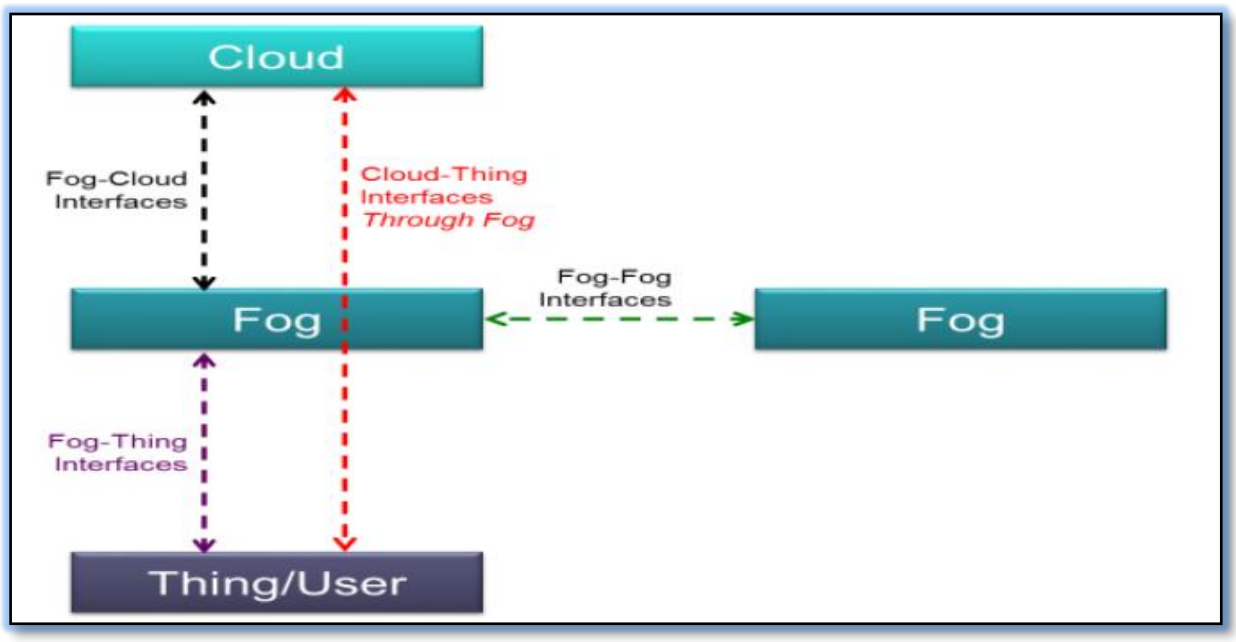

Figure 14 : Les interfaces de Fog

- ➢ **Interfaces Fog-Cloud:** Les interfaces Fog-Cloud seront nécessaires pour appuyer les collaborations Fog-Cloud afin de fournir des services de bout en bout. Il appuiera des fonctions permettant, par exemple:
- Le Fog à gérer à partir du Cloud.
- Le Fog et le Cloud pour s'envoyer des données.
- Cloud pour distribuer les services sur le Fog.
- Services de Cloud à fournir au Fog
- Services de Cloud à fournir par le truchement de Fog to Things et aux utilisateurs finaux.
- Services de Fog à fournir à Cloud.
- Le Fog et le Cloud pour collaborer entre eux afin de fournir des services de bout en bout.

Il est essentiel de déterminer quelles informations doivent être transmises sur l'interface Fog-Cloud, la fréquence et la granularité de ces informations, et comment le Fog et le Cloud devraient réagir à l'information. [58]

- ➢ **Interfaces Fog-to-Fog :** Différents noeuds ou systèmes de Fog peuvent collaborer entre eux pour prendre en charge conjointement une application. Par exemple, plusieurs systèmes Fog peuvent partager les tâches de stockage et de calcul des données pour un ou plusieurs utilisateurs ou applications. Différents noeuds ou systèmes de Fog peuvent également collaborer pour servir de sauvegardes les uns pour les autres. Une question importante est donc de savoir comment concevoir l'interface et les protocoles pour permettre à différents noeuds Fog dans le même système Fog, et différents systèmes Fog, de collaborer.
- ➢ **Interfaces Fog-thing/utilisateur :** Le Fog fournira des services à un large éventail d'utilisateurs finaux et d'appareils dotés de capacités très diverses. L'interface Fog-Thing et l'interface Fog-User seront essentielles pour permettre aux Objets et aux utilisateurs finaux d'accéder aux services Fog de manière conviviale, efficace et sécurisée.

5.2. Le bord de Fog activé et accès de réseautage

Le Fog peut être utilisé pour prendre en charge la mise en réseau au bord. Par exemple, Fog peut fournir des services pour aider les périphériques à la pointe du réseau et les périphériques de l'utilisateur final (par exemple, les véhicules, les drones, les robots industriels et de consommation , les smartphones et les jauges de réalité virtuelle) à former des réseaux locaux , en fournissant des informations de sécurité temporaires à ces périphériques locaux pour les aider à établir des communications fiables, et agir en tant que serveurs d'applications et serveurs de stockage de données locaux pour les réseaux de périphérie. [58]

Certaines fonctions de Fog pour la prise en charge de ce réseau de bord peuvent être implémentées sur les périphériques de l'utilisateur final. Dans de tels cas, la manière dont les fonctions Fog s'interface avec les systèmes d'exploitation et le matériel des périphériques de l'utilisateur final devient essentielle. Au-delà de l'utilisation de D4D pour la mise en commun des ressources de bord inactif, comme indiqué dans les sections précédentes, de nouvelles piles de protocoles pour les périphériques de l'utilisateur final pour la prise en charge de la mise en réseau des bords activés par le Fog peuvent être nécessaires.

5.3. Sécurité

Par rapport au Cloud, le Fog présente de nouveaux défis en sécurité. Les systèmes distribués, tels que le Fog distribué, sont en général plus vulnérables aux attaques que les systèmes centralisés, comme le Cloud . Bien que Cloud opère dans des installations fortement protégées sélectionnées et contrôlées par des opérateurs de Cloud, Fog a souvent besoin d'opérer dans des environnements plus vulnérables - où ils peuvent le mieux répondre aux besoins des clients et souvent où les utilisateurs le souhaitent. De nombreux systèmes de Fog seront beaucoup plus petits que les Cloud (p. ex., un nœud de Cloud sur un véhicule) et, par conséquent, ils ne disposeront peut-être pas autant de ressources que les Cloud pour se protéger. De plus, chaque système de Fog peut ne pas disposer de l'intelligence mondiale nécessaire pour détecter les menaces. [58]

En même temps, cependant, la proximité de Fog avec les utilisateurs finaux et la proximité de la localité sur le bord lui permet de contribuer à relever certains nouveaux défis en matière de sécurité des IoT, comme nous l'avons vu dans les sections précédentes. Le Fog peut, par exemple, servir de premier noeud pour le contrôle d'accès et le chiffrement du trafic, fournir l'intégrité et l'isolement contextuels, servir de point d'agrégation et de contrôle pour les données sensibles à la vie privée avant que les données ne quittent le bord, et agir en tant que proxy des périphériques limités en ressources pour exécuter des fonctions de sécurité sélectionnées pour ces périphériques limités en ressources. [58]

5.4. Incitation à la participation des clients :

Dans certains cas d'utilisation de l'IoT, ce n'est pas trop de clients non fiables qui suscitent des préoccupations, mais trop peu de clients prêts à y participer. Cela peut être le cas lorsque, par exemple, les clients sont tenus de contribuer volontairement à leurs ressources informatiques ou de stockage ou de collaborer entre eux pour prendre en charge les applications. Les systèmes de marché et les mécanismes d'incitation deviendront utiles. [58]

5.5. Convergence et cohérence:

Les interactions locales pourraient conduire à une divergence, une oscillation et une incohérence des états des systèmes mondiaux, qui sont des problèmes typiques des systèmes distribués et peuvent devenir plus aigus dans une foule massive, sous-organisée, peut-être mobile avec des capacités diverses et une réserve virtualisée de ressources partagées de manière imprévisible. Les cas d'utilisation dans l'analyse des arêtes et l'exploration des cours d'eau soulèvent d'autres défis sur ce défi récurrent dans les systèmes distribués. [58]

5.6. Les compromis architecturaux de bout en bout :

Le Fog nous offrira de nouvelles opportunités de concevoir des systèmes de bout en bout pour obtenir de meilleurs compromis entre architectures distribuées et

centralisées, entre ce qui reste local et ce qui devient global, et entre une planification de déploiement prudente et la résilience par la redondance. Les topologies du système de Fog logique, établies de façon statique ou dynamique, sur le même réseau de Fog physique sous-jacent peuvent être utilisées pour prendre en charge un éventail d'architectures allant de la centralisation complète à la distribution complète. [58]

Pour relever ces défis, nous avons besoin des deux

- ➔ recherche fondamentale, à travers la mise en réseau, le matériel et les systèmes d'exploitation des périphériques, la tarification, l'informatique à base de HCI et la science des données .
- ➔ les interactions entre l'industrie et le milieu universitaire, comme l'illustre l'Open Fog Consortium, un consortium mondial sans but lucratif lancé en novembre 2015 avec des membres fondateurs d'ARM, Cisco, Dell, Intel, Microsoft et Princeton University EDGE Lab.

5.7. Quels seront les principaux outils technologiques pour le Fog :

Lorsque nous examinons les avancées importantes de l'informatique et de la mise en réseau, nous pouvons souvent être en mesure de mettre en évidence une ou plusieurs technologies qui constituent les principaux moteurs de ces avancées. Par exemple, les protocoles TCP/IP ont démarré Internet. La virtualisation a alimenté au Cloud Computing. Quel sera le moteur technologique fondamental, ou ce petit ensemble de technologies fondamentales, qui alimentera Fog ?

En effet, Fog commence à remodeler le paysage futur de multiples industries, conduisant l'innovation à travers toute la chaîne alimentaire de l'industrie, notamment les suivantes :

- ➢ Fournisseurs d'expérience utilisateur final (ex. GE, Toyota, ...)
- ➢ opérateurs de réseau (par exemple, AT&T, Verizon, Comcast, ...)
- ➢ Fournisseurs d'équipements réseau (Cisco, Nokia, Ericsson, Huawei, ...)
- ➢ fournisseurs de services Cloud (par exemple, VMWare, Amazon, ...)
- ➢ intégrateurs de systèmes (p. ex. IBM, HP, ...)

- ➢ Fabricants de périphériques Edge (par exemple, Linksys, ...)
- ➢ fabricants de périphériques clients et IoT (par exemple, Dell, Microsoft, Apple, Google, ...)
- ➢ fournisseurs de puces informatiques (par exemple, Intel, ARM, Qualcomm, Broadcom, ...)

2016 est une année intéressante pour commencer à explorer systématiquement à quoi pourrait ressembler Fog et les différences qu'il apportera au monde du réseautage et de l'informatique dans les 15 prochaines années. [58]

Conclusion

Dans ce chapitre, nous avons présenté les nouveaux défis en IoT et l'époque émergente du Fog , puis une comparaison entre le Fog et Cloud , et Les principaux avantages du Fog , ensuite comment le Fog peut aider à relever les défis de l'IoT ? , en outre les nouveaux modèles de Fog , et des études de cas sur l'utilisation du Fog aussi des questions ouvertes et les défis de la recherche , enfin les Interfaces des Fog avec Cloud , de things , et pour les utilisateurs finaux .

Chapitre 3 : La coordination entre le Cloud Computing et le Fog Computing

"On fait la science avec des faits, comme on fait une maison avec des pierres, mais une accumulation de faits n'est pas plus une science qu'un tas de pierres n'est une maison."

Henri POINCARE

1. Introduction

Après avoir parlé et détaillé dans les deux chapitres précédents le Cloud Computing et le Fog Computing, nous allons aborder ce chapitre sur la coordination entre le Cloud et le Fog Computing , qui est devenu dépendant de l'émergence et de l'utilisation des villes intelligentes . Dans ce chapitre on va discuter sur la coordination entre le Cloud et le Fog . Ensuite nous présentons les modèles de coordination existants afin que nous choisissons un modèle de coordination. Enfin nous détaillons le stockage comme modèle choisi et ses différents mécanismes .

2. La coordination entre Cloud et Fog Computing

Les récents progrès de la technologie des services Cloud alimentent une pléthore d'innovations dans les technologies de l'information, notamment le réseautage, le stockage et l'informatique.

Aujourd'hui, diverses saveurs ont évolué de l'IoT, du Cloud Computing et de ce que l'on appelle le Fog Computing , un concept faisant référence aux capacités des périphériques de bord et des utilisateurs pour calculer, stocker et échanger des données entre eux et avec le Cloud . Bien que le rythme rapide de cette évolution ne soit pas facilement prévisible, aujourd'hui chaque élément facilite et permet le déploiement de ce que nous appelons communément un scénario intelligent, y compris les villes intelligentes, les smart véhicules et les maisons intelligentes. La prochaine grande étape dans l'évolution du Cloud Computing et des réseaux, où les services pourraient être exécutés au bord du réseau, à la fois en parallèle et de manière coordonnée, ainsi que soutenu par l'évolution technologique imparable. Au fur et à mesure que les périphériques de pointe deviennent plus riches en fonctionnalités et plus intelligents, intégrant des capacités telles que le stockage ou le traitement, ainsi que de nouvelles fonctionnalités, telles que la collecte de données, et le partage, un réel besoin émerge pour une coordination entre le Cloud et le Fog .

Pour que l'ensemble de l'écosystème Cloud-Fog fonctionne de manière dynamique, collaborative et coordonnée, le contrôle et la gestion sont le principal défi . Par exemple, en cas d'accident de voiture, le flux de travail des actions à exécuter par tous les différents acteurs impliqués dans leurs propres locaux Cloud, tels qu'un gestionnaire de parc de taxis, contrôleur des feux de circulation, gestionnaire de parc de pistes d'ordures, autobus scolaires, trafic global le contrôle dans une ville, les gestionnaires d'ambulance et les pompiers doivent être coordonnés, orchestrés et gérés efficacement pour fournir la réponse en temps réel la plus appropriée. Ainsi, ce qui se passe sans aucun doute dans cette évolution, c'est que le modèle de gestion statique à Cloud unique évolue vers un nouveau modèle, beaucoup plus dynamique et hétérogène, situé dans des locaux de Fog différents, hétérogènes et généralement mobiles, offrant des services qui peuvent être reliés entre eux, ainsi que des capacités

qui peuvent être offertes conjointement. Ainsi, la conception d'une stratégie de gestion coordonnée devient critique et doit relever les défis associés suivants [69] :

- **Identification des Cloud / Fog**

Une capacité de Cloud existante doit être identifiée avant d'être utilisée. Cela signifie qu'une adresse, une étiquette ou un nom doit être lié à cette capacité de Cloud. Cela est particulièrement important lorsque l'on considère les Clouds dynamiques, le temps sur le marché n'étant pas prédéfini, constant ou même garanti.

- **Adaptation sémantique**

Les performances et les capacités attendues sont très différentes selon les caractéristiques du Cloud / Fog. Par conséquent, une taxonomie adéquate doit être définie pour faciliter la cartographie entre les capacités requises par un service et les capacités offertes par une couche Cloud, et ainsi optimiser l'allocation des ressources. Cette taxonomie doit être supportée par un service d'adaptation sémantique, définissant les métriques et les attributs offerts par les couches de Cloud participantes et incluant de nouveaux paramètres, tels que statique / dynamique (ie, infrastructure continue dans le temps ou non), temps sur le marché (combien de temps cette infrastructure est disponible), le temps de partir (le temps jusqu'au démontage prévu), la connectivité, la sauvegarde et la QoS . [70]

- **Orchestration de couche coordonnée**

L'orchestration globale est nécessaire pour générer un flux de travail individuel d'actions pour chaque service, mapper l'action individuelle dans la taxonomie de la couche de Fog la mieux adaptée aux besoins attendus et coordonner les interactions entre les différentes couches impliquées dans l'exécution du service. L'orchestration des services peut être ponctuelle ou prédéfinie, en fonction des pratiques actuelles. Par exemple, dans le cas d'une urgence médicale, il est probable que les flux de travail des services seront prédéfinis comme dans les systèmes d'urgence actuels et fondés sur la politique et la réglementation des soins de santé. [70]

➢ Découverte et allocation des ressources Cloud

L'exécution d'un service exigeant l'interaction entre différents niveaux de Fog exigera d'abord la sélection appropriée et, dans certains cas, la création de ces couches de Fog. Une entité de gestion doit être chargée de découvrir l'ensemble des Fog disponibles (visibles) et de choisir ensuite ceux qui peuvent le mieux répondre aux exigences du service. La visibilité du Fog peut être gérée par une stratégie de publication/d'abonnement (p. ex., une solution fondée sur le concept de marché) ou par un processus d'enregistrement simple basé sur le profil du propriétaire du Cloud [70].

➢ Planification de l'exécution du service

La planification des services est nécessaire pour décider de la façon dont les fonctions individuelles d'un service sont divisées en différentes couches de Fog et de la façon dont chaque couche traite les services. De nombreuses considérations doivent être observées. Par exemple, un système de feux de circulation qui gère le trafic en temps réel doit être robuste face à un changement ad hoc des règles définies, car son impact sur les conditions de trafic réelles est élevé. Une urgence policière ou médicale peut en effet modifier les réglages du feu de circulation, mais un traitement intelligent est nécessaire pour minimiser l'impact de cette décision particulière sur le trafic urbain global. Les préférences, les priorités, les "codes rouges", les alarmes et les avertissements doivent être pris en compte lors de la planification de l'exécution des services [70].

➢ Garanties QoS

Dans le contexte de l'IoT, lorsque des artefacts comme des Cloudlets doivent être fixés dynamiquement, même en mouvement, la qualité du service est difficile à garantir. Par conséquent, les stratégies visant à atteindre le QoS (ou à proximité du QoS) doivent être établies pour garantir cette qualité, notamment :

- ➢ Garanties de disponibilité des ressources en établissant des seuils pour définir la configuration et le dégagement des différentes couches de Fog

- ➢ Réduire au minimum le temps de réponse du service en sélectionnant le nombre de couches le plus court et en générant le flux de travail approprié pour exécuter un service
- ➢ Amélioration de la fiabilité en générant des techniques de "protection" pour gérer adéquatement la tolérance aux défaillances des couches de Fog[70]

- ➢ **Sécurité / confidentialité des données**

La sécurité et la confidentialité sont des défis bien connus et actuellement non résolus dans le domaine du Cloud , et restent comme tels dans F2C. Le déploiement de Fogs exacerbe en fait ces problèmes, et aussi [8] pour les Cloud véhiculaires, principalement en raison du mode d'opération incontrôlé et hors surveillance inhérent à certains dispositifs de bord. Dans le scénario F2C proposé, tout comme dans Fog Computing la sécurité est envisagée comme un problème clé. La réussite commerciale ou non d'une solution F2C dépend d'une solution adéquate de sécurité et de confidentialité des données.

La valeur de tout nouveau cadre et de toute nouvelle architecture de gestion est mieux mesurée par les services qu'elle peut prendre en charge. Contrairement à ce qui a été abordé par les concepts de Fog Computing , où les services sont traditionnellement exécutés séquentiellement dans les locaux du Fog ou du Cloud [7], nous montrons maintenant que le concept de l'informatique F2C peut en fait optimiser les performances. Il existe plusieurs scénarios plus complexes et plus complets où le F2C pourrait être largement déployé (p. ex. navigation en temps réel, résilience urbaine, défaillance ou contrôle de la qualité dans le secteur industriel), mais le cas d'urgence médicale (bien connu, très exigeant, simple et pas loin du scénario de réalité à venir) est simplement considéré comme une preuve de principe pour positionner et mettre en évidence les avantages du F2C.

Supposons qu'un piéton qui se promène dans une ville souffre d'une urgence médicale. Considérons aussi que le piéton intègre un dispositif générant des avertissements de diffusion, demandant une assistance médicale. Les avertissements peuvent être recueillis par n'importe quelle voiture dans les environs immédiats à

travers les couches de Fog (Cloud déployés dans la ville). On peut imaginer que les dispositifs médicaux intégrés et, par exemple, les signaux lumineux peuvent prévoir un changement de lumières pour que la circulation puisse accueillir une équipe d'urgence et se rendre plus rapidement à l'homme en état de besoin médical, ainsi que les services de gestion parallèle des services de contrôle de la ville et de détection et de localisation des services médicaux d'urgence. La première prendra les mesures nécessaires pour garantir un accès rapide et facile à la personne en cas d'urgence médicale, comme l'allumage des feux de circulation, la signalisation des rues et l'utilisation d'un chemin court pour l'ambulance. Ce dernier sera responsable de la localisation de la voiture de service d'urgence la plus proche, l'ambulance la plus proche capable de traiter l'état découvert, de faire rapport à l'hôpital depuis l'ambulance de l'état du patient pendant que l'ambulance se rend à l'hôpital, et ainsi de suite. Cette chaîne d'actions (workflows de services) peut être conçue pour garantir non seulement une réponse rapide à l'urgence, mais aussi la réponse qui correspond le mieux au type particulier d'urgence (blessures personnelles, accident de voiture, etc.). Les différents processus qui définissent ces flux de travail de services sont traités de façon cohérente et coordonnée en parallèle dans les locaux situés près de l'événement, notamment un système de gestion de la ville, un système de gestion des urgences médicales et l'infrastructure de la ville voisine, comme les unités routières (feux de circulation), les Cloud véhiculaire (voitures), etc.

2.1. Les modèles de coordination

Les modèles de coordination entre le Cloud et Fog Computing sont :

- **le stockage :**(On va le détaillè dans le titre suivant)
- **Collecte et traitement des données :**Traditionnellement, lors du traitement de données provenant de différentes sources, qu'elles soient situées dans le centre de données d'une entreprise ou en mode SaaS à la demande, le modèle ETL, qui est Extraire, Transformer et Charger, est souvent appliqué, avant que les données stockées puissent être utilisées dans une analyse plus approfondie. Les données sont d'abord extraites des services et d'autres sources de données et

transférées sur le réseau. Dans l'étape de transformation, il est nettoyé et structuré par un processeur commun avant d'être chargé dans un magasin de données pour un stockage persistant. À partir de là, il peut être traité ultérieurement à l'aide d'outils de reporting [61]. Traitement des données IoT | T. Pfandzelter | Rubriques avancées dans l'IoTEdgeFog Cloud [62-63, 64]. Topologie de calcul Edge et Fog Dans un contexte IoT, le fait d'avoir un seul magasin de données et un processeur commun peut être utile pour l'analyse des données car il permet une vue globale de l'ensemble du système et est une architecture familière. Cependant, lorsque des millions d'appareils IoT tels que des capteurs ou des caméras vidéo envoient constamment des données à un agent de transformation commun, cet agent et le réseau peuvent rapidement devenir un goulot d'étranglement car ils ne peuvent évoluer qu'à un certain niveau [65], [66] . En outre, cette approche est viciée d'une autre manière. Dans l'IoT, la latence est tout. Lorsque chaque point de données doit d'abord être envoyé vers le Cloud pour traitement, il faut au moins le temps d'aller-retour du réseau pour que les commentaires parviennent aux appareils réels, alors qu'en réalité, les appareils peuvent être physiquement proches les uns des autres, par exemple lors de la commutation sur la lumière dans un scénario de maison intelligente. Le Fog Computing peuvent résoudre ces problèmes. L'idée est de rapprocher physiquement certains composants informatiques d'appareils IoT. Il crée une architecture multicouche dans laquelle le traitement peut être réparti entre des passerelles en communication directe avec les appareils, plusieurs nœuds de Fog qui comblent l'écart avec le Cloud, et enfin l'opérateur dans le Cloud, qui peut toujours transformer et charger des données. L'agrégation et le prétraitement des données plus près des appareils réduisent le coût global du réseau et permettent des réponses avec des latences beaucoup plus faibles. Cependant, cela a bien sûr un prix. En s'éloignant du Cloud, ses avantages tels qu'une puissance de calcul flexible et bon marché, des efforts de maintenance réduits ou une disponibilité plus élevée sont sacrifiés [67], [66].

- **le partage :** Les données sont partagées par des protocoles pairs à pairs comme BitTorrent [Legout et al. 2005] peuvent être utilisés entre les nœuds. De cette façon, les données ne sont pas téléchargées d'un seul et unique nœud parent mais de plusieurs nœuds simultanément. Cela permet de réduire le temps de transfert ainsi que la charge des liens réseau tout en augmentant la disponibilité de la donnée. Le protocole BitTorrent fonctionne de la façon suivante. Les données sont découpées en pièces de taille fixe (par exemple 64 Ko). Le nœud voulant télécharger des données, récupère la liste des identifiants des pièces composant la donnée qu'il souhaite télécharger. Un serveur central appelé tracker ou une table de hachage distribuée est interrogée pour connaître la liste des nœuds stockant les pièces demandées. Le client se connecte alors à plusieurs nœuds stockant au moins une pièce et leur transmet la liste des pièces qu'il aimerait recevoir. Les pièces sont envoyées par blocs (par exemple de 512 octets) d'un nœud à l'autre. Au fur et à mesure que le client reçoit les morceaux de pièces dont il a besoin, il transmet des mises à jour de cette liste afin d'éviter de recevoir plusieurs fois les données. En effet, si deux nœuds stockent une même pièce, il est probable que les deux nœuds l'envoient au client puisque ce dernier demande à chaque nœud auquel il est connecté, la liste de toutes les pièces dont il a besoin. Il existe des mécanismes permettant de télécharger en premier les pièces rares, c'est-à-dire les pièces ayant le moins de réplicas et qui sont susceptibles de ne plus être disponibles en cas de panne d'un nœud ou de partitionnement du réseau. Nous noterons que les données dans BitTorrent, identifiées par leur empreinte, sont également immuables et ne peuvent pas être modifiées. Une telle approche est mise en œuvre dans des outils de synchronisation comme BitSync [Farina et al. 2014] ou Syncthing [Borg 2015]. Les protocoles pairs à pairs peuvent être utilisés exclusivement en bordure du réseau, entre les périphériques des utilisateurs [Palazzi et al. 2009] ou bien s'appuyer sur une infrastructure de Fog pour former un réseau de distribution de contenus hybride [Ghareeb et al. 2013 ; Xu et al. 2006] dans lesquels les clients n'interrogent pas directement le serveur de l'infrastructure de Fog mais essaient dans un premier temps de télécharger la donnée voulue depuis l'un de

leurs voisins. Les clients ont également un rôle de serveur de cache, ce qui permet de réduire la charge des serveurs du réseau de diffusion de contenus. Xu et al. [Xu et al. 2006] proposent d'utiliser les serveurs du réseau de contenus pour y placer le tracker nécessaire à l'échange de données entre les clients.

Afin de privilégier l'accès aux réplicas stockés sur des nœuds « proches » de l'utilisateur, plusieurs protocoles existent. Le protocole Vivaldi [Dabek et al. 2004b] permet de créer une « carte du réseau ». Une fois cette carte construite, il est alors possible de privilégier les nœuds situés à une faible distance. L'inconvénient de cette approche est que construire et maintenir la carte, génère une quantité importante de trafic sur le réseau.

Le protocole P4P [Xie et al. 2008 ; Kiesel et al. 2014] est quant à lui constitué d'un serveur central qui est interrogé par les nœuds voulant télécharger des données. Son rôle est de retourner une distance entre deux nœuds spécifiés. La distance peut être calculée de plusieurs façons et prendre en compte de nombreux paramètres tels que la latence réseau, l'homogénéité des débits sur le chemin, la sortie d'un système autonome (AS), etc. Les clients vont ensuite essayer de privilégier de télécharger les données depuis les nœuds ayant une faible distance. Cette approche intéresse fortement les opérateurs afin de confiner le trafic pair à pair au sein de leur réseau, évitant ainsi de toujours déployer des liens d'interconnexion avec les autres opérateurs de plus grandes capacités.

Nous avons choisi un modèle de coordination, qui est le stockage.

2.2. Le Stockage :

2.2.1. Mécanismes de stockage de données distribué : Dans le Fog Computing , le contrôle et le stockage des données sont tous deux centralisés. Cependant, le stockage de tout dans le Cloud n'est pas réaliste en raison :

a) De la latence élevée [71]

b) De la forte demande de traçabilité entre le bord et le Cloud

c) Du coût élevé de stockage.

De plus, la mobilité des dispositifs de Fog ou de bord est un paramètre important à l'étude. En distribuant les données stockées dans la couche de Fog en fonction de divers paramètres, comme la situation géographique des producteurs et des consommateurs, on pourrait remédier aux inconvénients susmentionnés. Cette solution repose sur le contrôle central de Cloud Computing, associé au stockage de données distribué des noeudsFog [72]. En particulier, des techniques d'équilibrage de la charge peuvent être appliquées pour modifier la topologie du réseau au fil du temps en fonction des besoins des consommateurs en matière d'utilisation des données afin d'atteindre une dépendance temporelle. Les mécanismes de stockage des données comprennent divers domaines de recherche tels que la distribution des données, la diffusion des données et la réplication des données.

2.2.1.1. Distribution des données : Dans les réseaux à grande échelle où il y a un grand nombre de dispositifs coopérants, les stratégies de distribution des données sont en mesure d'éliminer les restrictions de stockage des données en diffusant les données de manière équitable sur tous les noeuds. Dans le Fog Computing , les données doivent être distribuées aux noeuds de Fog. À notre connaissance, il y a quelques oeuvres connexes dans Fog Computing à cette fin [73-74].

Les grandes entreprises comme Amazon et Google ont mis en oeuvre leurs propres solutions pour répondre à leurs besoins de stockage dans leurs environnements très exigeants dans des infrastructures complexes. En outre, les systèmes de stockage P2P ont été proposés comme solution de stockage distribué pour l'informatique distribuée dans de nombreux efforts de recherche au cours des dernières années. Pendant ce temps, les techniques de stockage P2P ont été utilisées dans des systèmes spéciaux comme Content Delivery Systems (CDN) [73] et Cloud Computing. Ainsi, les techniques de stockage P2P semblent être un mécanisme de stockage approprié pour manipuler d'énormes informations dans le paradigme de Fog Computing . Ces systèmes peuvent transférer des données entre différents noeudsFog du même fournisseur pour fournir STaaS aux périphériques de bord. En outre, différents fournisseurs peuvent partager leurs ressources de stockage selon un modèle d'entreprise afin de réduire le coût d'installation et de maintenance des noeudsFog supplémentaires et, parallèlement, d'augmenter leurs capacités en cas de forte

demande. Les systèmes P2P sont passés de réseaux P2P non structurés, où les connexions de noeuds ont été établies arbitrairement, à des systèmes P2P structurés où les connexions de noeuds suivent une forme prédéfinie. De nombreux systèmes de cette dernière approche utilisent des mécanismes de routage pour assurer un nombre maximal d'étapes de recherche, ce qui est souhaitable dans le Fog Computing afin de réduire la latence.

2.2.1.2. Diffusion des données :

La diffusion des données est un sujet qui fait l'objet d'une étude approfondie dans les WSN [76-77]. En outre, dans les réseaux à faible bande passante, des algorithmes de diffusion sont appliqués pour déterminer le chemin le plus court. En outre, les algorithmes de diffusion peuvent être adaptés pour déterminer les différentes voies de transmission en fonction de la charge actuelle des connexions réseau. Dans le Fog Computing , les mécanismes de diffusion peuvent être utilisés entre les différents noeuds de Fog pour réduire le trafic global en décidant de la meilleure méthode de transmission. La diffusion des données se fait principalement entre les noeudsFog. Cependant, il est possible que la diffusion des données implique même une interconnexion entre :

a) les noeuds de Cloud et de Fog
b) les noeuds de Fog et les périphériques de bord.

Dans le dernier cas, les périphériques de bord peuvent étendre la couche de Fog en prenant le rôle de chemins de communication pour livrer un paquet [60].

2.2.1.3. Réplication des données :

Les mécanismes de réplication sont importants pour garantir l'intégrité des données; par conséquent, ils sont fortement recommandés dans les infrastructures où les défaillances sont non seulement courantes mais omniprésentes [75]. La perte de données peut se produire pour diverses raisons, telles que les défaillances du système ou le drainage de la batterie. Les défaillances du système sont très susceptibles de se produire dans les noeudsFog. Ainsi, les mécanismes de réplication sont également cruciaux pour la couche de Fog . La réplication peut être appliquée sur des machines

virtuelles entières ainsi que sur des enregistrements de données. Dans le premier cas, les réplicas ne sont utilisés que pour garantir l'intégrité des données. Dans le deuxième cas, les réplicas peuvent être conservés dans un autre emplacement où il est plus probable qu'ils soient interrogés à partir d'un autre périphérique de bord. En outre, il faudrait également tenir compte de la cohérence des données pour s'assurer que toutes les répliques sont mises à jour avant qu'elles ne soient livrées à un périphérique de bord. Les stratégies de réplication sont utilisées pour améliorer l'intégrité des données et augmenter la disponibilité des données avec un temps de latence et de récupération faible [74]. Toutefois, des quantités élevées de redondance des données réduisent la capacité globale de stockage du système et augmentent les coûts de maintenance.

Conclusion

Dans ce chapitre, nous avons discuté la coordination entre le Fog et le Cloud dont le but est de résoudre les problèmes soulevés dans les deux structures. Dans la première partie, nous avons présenté la coordination, la façon dont elle a été créée, ses défis, et ses modèles. Second, nous avons détaillé le modèle de coordination choisi ainsi que ses mécanismes.

Chapitre 4 : La contribution

" Le succès est un mauvais professeur .Il pousse les gens intelligents a croire qu'ils sont infaillibles "

Bill Gates

1. Introduction

Durant ce chapitre, nous allons présenter une étude de cas ; en utilisant le stockage comme modèle de coordination. Pour cela, nous avons choisi la voiture intelligente (voiture autonome) comme un exemple dans les villes intelligentes (smart cities) qui utilise le Fog Computing. Après, le principe de fonctionnement de notre exemple est expliqué avant de proposer des algorithmes pour améliorer le fonctionnement de ce type des voitures.

2. Qu’est-ce qu'une Smart city (ville intelligente) ?

D'après l'Union internationale des télécommunications et la Commission économique des Nations Unies pour l'Europe en 2015 “La Smart City est une ville innovante qui utilise les technologies de l'information et des communications pour améliorer la qualité de vie, l'efficacité des opérations et des services urbains et la capacité de concurrentielle , tout en répondant aux besoins des générations actuelles et futures en ce qui concerne les aspects économiques, sociaux, environnementaux et culturels ’’.

Les villes intelligentes nécessitent une infrastructure de télécommunications stable, sûre, fiable et interopérable pour prendre en charge une grande quantité d'applications et de services basés sur les TIC.

Les récents développements dans l'Internet des objets (IoT), l'intelligence artificielle (AI), les réseaux intelligents et les compteurs intelligents sont tous des moteurs et soutiennent le développement de villes intelligentes durables dans le monde.

Parmi les objets trouvées dans la ville intelligente et connectées avec les autres appareils d’IoT , on trouve les voitures intelligentes .

3. Qu'est-ce qu'une Smart vehicle (voiture intelligente) ?

C’est une voiture autonome équipée d'un système de pilotage automatique qui lui permet de circuler sans intervention humaine dans des conditions de circulation réelles.[81]

La coordination entre le Cloud et Fog Computing joue un rôle très important pour garantir assurer le succès de la conduite et atteindre le point à atteindre sans aucun accident de la circulation grâce à la vitesse de réception des données générées par la voiture ainsi que par d'autres appareils d’IoT situés à proximité de la voiture , ces données seront reçus par le Fog et traités , après il va envoyer les résultats de ces données à la voiture en quelques secondes.

3.1) Comment fonctionne Smart vehicle

La question est : comment fonctionnent les voitures intelligentes ? Comment définir les caractéristiques des rues, définir leur chemin et éviter de se heurter aux voitures ou aux passants ?

Les voitures à conduite automatique explorent le monde à partir d'un ensemble de capteurs, y compris des caméras, des radars et du lidar, une technique similaire à un radar qui utilise des impulsions de lumière non visibles pour créer une carte 3D très précise pour la zone environnante, tout en maintenant des véhicules à conduite automatique sans danger.

Les caméras, le radar et le lidar travaillent ensemble et se complètent, ce qui permet de disposer de suffisamment de données analysées pour créer une image globale de la zone environnante, afin d'éviter les obstacles, les personnes et d'autres choses. Les caméras peuvent voir et identifier les signaux de circulation, mais ils ne peuvent pas mesurer les distances, et le radar peut mesurer la distance et la vitesse, mais il ne peut pas voir les détails précis.

Et le Lidar, qui fournit des détails précis, mais se désintègre et vous donne un salaire en cas de chutes de neige en hiver.

Tous les capteurs envoient les informations à l'ordinateur central de la voiture intelligente qui analyse et traite les informations reçues et donne ensuite à la voiture l'ordre d'arrêter, de marcher ou de ralentir à une vitesse donnée.

La combinaison des trois capteurs dans les voitures intelligentes ne suffit pas en cas de bouchon. Ici, l'intervention de Fog Computing par API Google Maps , qui est installé dans Fog nodes , API Google maps reçoit les informations de bouchon par des capteurs installées dans les rues et les villes pour les analyser et les traiter, puis réalise un résultat qui est une recherche d'autre chemin vers le point de départ (ce chemin il faut être le plus court que les autres chemins) , après il envoie carte qu'elle contient le nouveau chemin vers l'ordinateur central du véhicule intelligent, et ensuite il stocke le résultat dans le data center de Fog , la figure 15 contient les différents composants de fonctionnement de smart véhicule et ses rôles .

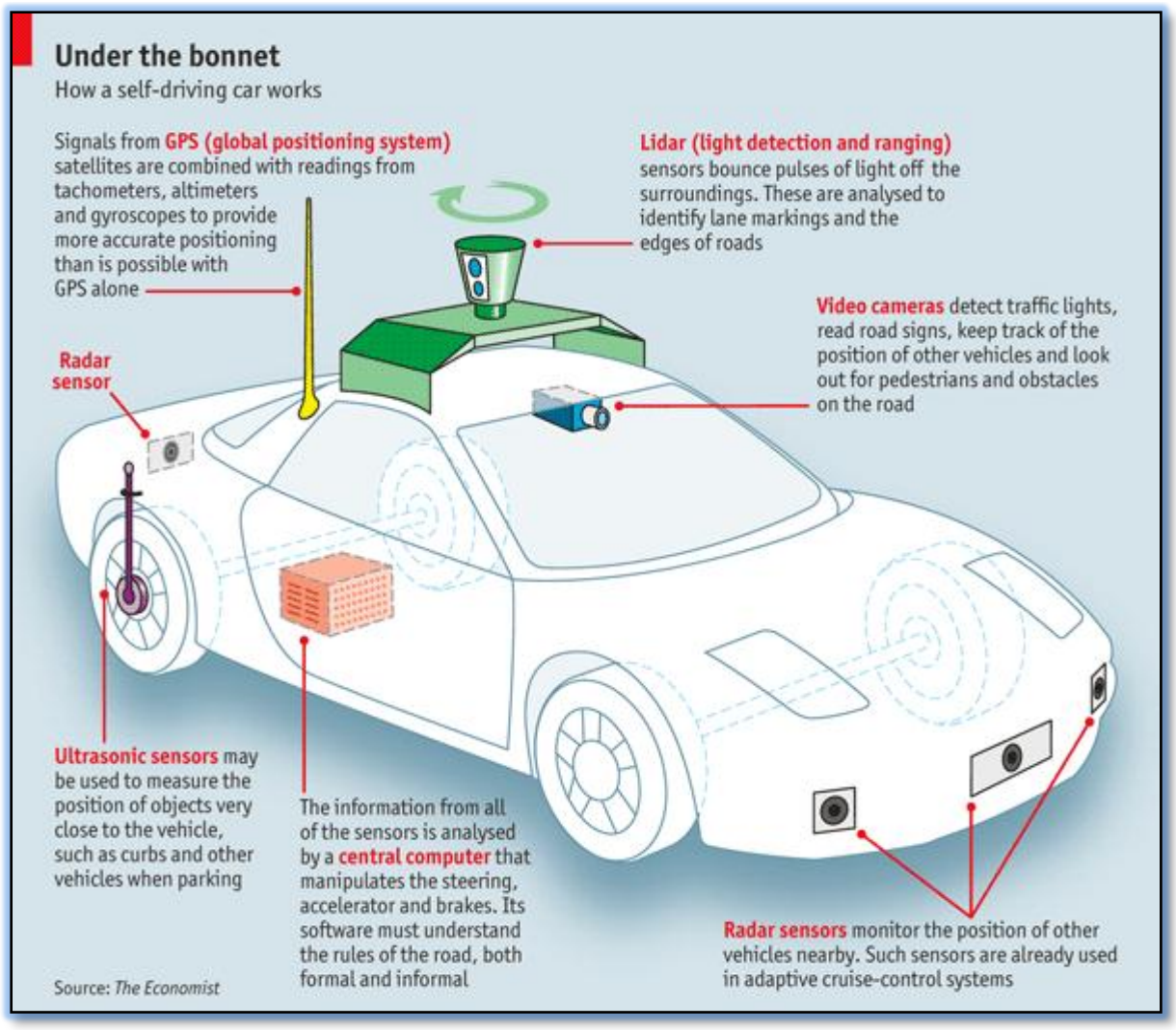

Figure 15 : les différents composants de Smart Véhicule et ses rôles [78]

4. Etude de cas

Dans cette section, on va présenter deux (02) scénarios possibles de déplacement pour une voiture autonome d'une ville intelligente X vers une ville Y. Dans le premier scénario (cas normal), on considère que la voiture traverse son chemin sans aucun obstacle (bouchon dans la route, mauvais temps ou un verglas) et arrive à la ville d'arrivée dans un temps réel. Le deuxième scénario prend en considération les obstacles cités précédemment. Après, nous proposons un algorithme pour chaque scénario.

4.1 Table de description

Symboles	Définitions
X	point de départ
Y	point d'arrivée
SV	Smart vehicle
FN	Fog node(noeud de Fog)
DCF	Data Center Fog
FI	Feu intelligent
PP	Passage piéton
PLV	Plaque de limitation de vitesse
OCSV	Ordinateur central de Smart véhicule
I J K L M N O	des entiers
A B C D E F G	des points dans la route
AGM	API Google Maps
DC	Data Center

Tableau 4 : Description des symboles

4.2. Scénario 1 : Les cas normaux

- ➢ L'utilisateur de SV saisie le point de départ et d'arrivée
- ➢ SV envoie les données vers FN
- ➢ FN analyse et traite les données après ils se comparent avec les données quelles sont stockés dans leur DC
- ➢ FN trouve la carte qu'elle contient ses données stocké dans (DCF)
- ➢ FN envoie la carte vers SV
- ➢ SV installe cette carte dans son computer central
- ➢ SV envoie un message de succès d'installation vers FN
- ➢ FN lance l'api googlemaps (pour faciliter le travail et gagner le temps , google maps travaille avec des capteurs installés dans les routes) .
- ➢ SV active le GPS
- ➢ Api Google maps qu'il se trouve dans les serveurs de FN reçoit la position de SV et continue la suivre

  - ❖ Dans les cas où la SV rencontre un passage piéton, un feu intelligent, un autre véhicule, ou une plaque de limitation de vitesse, le scénario sera comme suit :

Cas de passage piéton :

- ➢ Les radars de SV sont sensibles à la présence d'un obstacle (le passage piéton). Ils mesurent la distance entre l'obstacle et le véhicule et envoient les données vers l'ordinateur central de SV.
- ➢ Les caméras de la voiture identifient l'obstacle et envoient leurs données à l'ordinateur central de SV .
- ➢ Lidar utilise des impulsions de lumière non visibles pour créer une carte 3D précise pour la zone environnante de SV. Après, il envoie la carte vers l'ordinateur central de voiture.
- ➢ L'ordinateur central de SV analyse et traite les données reçus par les capteurs et donne un ordre pour que la voiture s'arrête.

Cas de feu intelligent :

- ➢ Les caméras de SV identifient FI et ses signes et envoie les données vers l'ordinateur central de SV.
  - ❖ Si le feu est vert alors :

    L'ordinateur donne un ordre pour que la voiture traverse le feu.
  - ❖ si le feu rouge :

    L'ordinateur donne un ordre pour que la voiture s'arrête.
  - ❖ Si le feu est orange :
  - ➢ Les radars de SV détectent s'il existe une autre voiture devant ou sur les côtés de SV et envoie les données vers l'ordinateur central.
  - ➢ Les caméras identifient la présence des voiture devant ou sur les côtés de SV et envoient ses données vers SV .
  - ➢ lidar crée une carte 3D précise pour la zone environnante de SV et envoie la carte vers l'ordinateur central de SV .
  - ➢ L'ordinateur central analyse et traite toutes les données des capteurs et fait un résultat après il donne un ordre pour SV pour marcher ou bien continuer l'arrêt.

Cas d'autre véhicule devant SV

- ➢ Les radars de SV détectent s'il existe une autre voiture devant ou sur les côtés de SV et envoie les données vers l'ordinateur central.
- ➢ Les caméras identifient la présence des voiture devant ou sur les côtés de SV et envoient ses données vers SV .
- ➢ lidar crée une carte 3D précise pour la zone environnante de SV et envoie la carte vers l'ordinateur central de SV .
- ➢ L'ordinateur central donne un ordre pour SV pour limiter sa vitesse et laisse une distance entre Sv et l'autre voiture

Cas de plaque de limitation de vitesse

- ➢ Caméras de SV identifient les données de vitesse maximale créée dans la plaque
- ➢ Caméras de SV envoient ses données vers OCSV.
- ➢ Les radars calculent la vitesse de la voiture et envoient ses données vers OCSV.
- ➢ OCSV analyse et traite les données et fait résultat, et envoie ordre a SV pour minimiser la vitesse ou bien rester dans la même vitesse.

4.2.1. Algorithme du premier scénario (les cas normaux)

Début

Fonction passage piéton

Début

Si un PP **Alors**

Les radars de SV captent un obstacle devant le véhicule puis mesurent la distance entre l'obstacle et SVet envoient ses données vers l'ordinateur central de SV

Les caméras identifient l'obstacle qu'il est PP et envoient ses donnée vers l'ordinateur central de SV

Lidar crée une carte 3D précise pour la zone environnante de SV après il envoie la carte vers l'ordinateur central de voiture.

L'ordinateur central de voiture analyse et traite les données reçu par les capteurs

Si une personne traverse PP **Alors**

OCSV envoie message à SV pour s'arrêter

Sinon OCSV envoie message à SV pour continuer le trajet

Fin Si

Fin Si

Fin

Fonction Feu Intelligent

Début

Si FI **Alors**

Les caméras de SV identifient FI et ses signes (rouge, vert, orange) et envoie les données vers l'ordinateur central de SV

Si un feu rouge **Alors**

l'ordinateur central donne ordre pour la voiture pour s'arrêter

Sinon Si un feu orange **Alors**

Les radars de SV sensibles si il y'a une autre voiture devant ou à gauche ou droit de SV et envoie les données vers l'ordinateur central.

les caméras identifient s'il ya des voiture devant ou à gauche ou droit de SV et envoient ses données vers SV .

lidar créer une carte 3D précise pour la zone environnante de SV après il envoie la carte vers l'ordinateur central de SV .

l'ordinateur central analyse et traite tous les données des capteurs et fait un résultat

Si la route est vide **alors**

OCSV donne ordre pour SV pour marcher

Sinon

OCSV donne un ordre à SV pour continuer l'arrêt

Fin Si

Sinon OCSV donne un ordre à SV pour continuer marcher

Fin Si

Fin Si

Fin Si

Fin

Fonction Véhicule devant SV

Début

Si une véhicule devant SV **alors**

Les radars captent l'obstacle et envoient les données vers OCSV

Caméras de véhicule identifient l'obstacle etenvoieent les données vers OCSV

Lidar crée une carte 3d pour la zone de SV et l'envoie vers OCSV

OCSV analyse et traite les données reçus

OCSV donne instruction pour SV pour laisser une distance par rapport l'autre

véhicule

Sinon continuer dans la même vitesse

Fin Si

Fonction Plaque limitation de vitesse
Début
Si PLV **Alors**
Caméras de SV identifient les données de vitesse maximale créée dans la plaque
Caméras de SV envoient ses données vers OCSV.
Les radars calculent la vitesse de voiture et envoient ses données vers OCSV.
OCSV analyse et traite les données et fait résultat, et envoient ordre a SV pour suivre la vitesse maximale.

Fin Si
Fin

Début
Tantque user saisir X et Y dans SV **Faire**
SV envoie les données de S et Y a FN
FN analyse et traite les données et les compare avec les cartes stockés dans DCF
Si carte existe dans DCF **Alors**
FN envoie la carte à SV
SV installe la carte et envoie un message de succès dans son ordinateur central et envoie un message de succès d'installation a FN.
SV active GPS
FN lance API Google Maps
API Google Maps recevoir la position de SV et continue la suivre
Si SV démarre **Alors**
Si passage piéton **alors**
I <- Passage Piéton
Fin Si

Si un feu intelligent **alors**

J <- Feu Intelligent

Fin Si

Si une véhicule devant SV **alors**

K <- Véhicule devant SV

Fin Si

Si PLV **alors**

L <- Plaque limitation de vitesse

Fin Si

Fin Si

Fin Si

Fin Tantque

Fin

Fin

4.3. Scénario 2 : les cas particuliers

- L'utilisateur saisie X et Y
- SV envoie les données vers FN
- FN analyse et traite les données de carte après ils se comparent avec les cartes quelles sont stockés dans leur data center

- **Si la carte est stockée dans DCF les opérations sont :**

- FN envoie la carte vers SV
- SV installe cette carte dans son computer central
- SV envoie message de succès d'installation vers FN
- FN lance l'api google maps (pour faciliter le travail et gagner le temps, google maps travaille avec des capteurs installés dans les routes) .
- SV active GPS
- Api Google maps qu'il se trouve dans les serveurs de FN recevoir la position de SV et continue la suivre

- ❖ Dans les cas particuliers on considère les cas normales (Feu intelligent, passage piéton, véhicule devant SV, plaque limitation de vitesse) + le mauvais temps, le verglas et le bouchon

Cas de passage piéton :

- ➢ Les radars de SV sont sensibles à la présence d'un obstacle (le passage piéton). Ils mesurent la distance entre l'obstacle et le véhicule et envoient les données vers l'ordinateur central de SV.
- ➢ Les caméras de la voiture identifient l'obstacle et envoient leurs données à l'ordinateur central de SV .
- ➢ Lidar utilise des impulsions de lumière non visibles pour créer une carte 3D précise pour la zone environnante de SV. Après, il envoie la carte vers l'ordinateur central de voiture.
- ➢ L'ordinateur central de SV analyse et traite les données reçus par les capteurs et donne un ordre pour que la voiture s'arrête.

Cas de feu intelligent :

- ❖ **Si le feu est orange :**
- ➢ Les radars de SV sensibles si il y'a une autre voiture devant ou à gauche ou droit de SV et envoie les données vers l'ordinateur central .
- ➢ les caméras identifient s'il ya des voitures devant à gauche ou à droit de SV et envoient ses données vers SV .
- ➢ lidar créer une carte 3D précise pour la zone environnante de SV après il envoie la carte vers l'ordinateur central de SV .
- ➢ l'ordinateur central analyse et traite tous les données des capteurs et faire une résultat après il donne un ordre pour SV pour marcher ou bien continue l'arrête ……

- ➢ Les caméras de SV identifient FI et ses signes et envoie les données vers l'ordinateur central de SV.
  - ❖ Si le feu est vert alors :

    L'ordinateur donne un ordre pour que la voiture traverse le feu.

- ❖ si le feu rouge :

  L'ordinateur donne un ordre pour que la voiture s'arrête.
- ❖ Si le feu est orange :

➢ Les radars de SV détectent s'il existe une autre voiture devant ou sur les côtés de SV et envoie les données vers l'ordinateur central.

➢ Les caméras identifient la présence des voiture devant ou sur les côtés de SV et envoient ses données vers SV .

➢ lidar crée une carte 3D précise pour la zone environnante de SV et envoie la carte vers l'ordinateur central de SV .

➢ L'ordinateur central analyse et traite toutes les données des capteurs et fait un résultat après il donne un ordre pour SV pour marcher ou bien continuer l'arrêt.

Cas d'autre véhicule devant SV

➢ Les radars de SV détectent s'il existe une autre voiture devant ou sur les côtés de SV et envoie les données vers l'ordinateur central.

➢ Les caméras identifient la présence des voiture devant ou sur les côtés de SV et envoient ses données vers SV .

➢ lidar crée une carte 3D précise pour la zone environnante de SV et envoie la carte vers l'ordinateur central de SV .

➢ L'ordinateur central donne un ordre pour SV pour limiter sa vitesse et laisse une distance entre Sv et l'autre voiture

Cas de plaque de limitation de vitesse

➢ Caméras de SV identifient les données de vitesse maximale créée dans la plaque

➢ Caméras de SV envoies ses données vers OCSV.

➢ Les radars calcule la vitesse de voiture et envoie ses données vers OCSV.

➢ OCSV analyse et traite les données , fait résultat , et envoie ordre a SV pour minimiser la vitesse ou bien rester dans la même vitesse .

Cas de mauvais temps

Les capteurs de météo au niveau de SV captent l'état de météo et prennent leurs données, et les envoie vers l'ordinateur centrale de SV .les cas de mauvais temps sont :

A) La pluie :

- ➢ OCSV recevoir les données de capteur et l'analyse après les traités , ensuite il faire un résultat
- ➢ OCSV donne un ordre pour SV concernant la météo

  - ❖ **Si la pluie est légère**
  - ➢ l'ordinateur donne un ordre pour SV pour limiter la vitesse
  - ❖ **Sinon si la pluie est forte**
  - ➢ l'ordinateur central envoie ordre pour SV pour limiter la vitesse et ouvrir les fars de pluie, pour que la visibilité de SV devienne claire.

B) La neige :

- ➢ OCSV recevoir les données de capteur et l'analyse après lestraités , ensuite il faire un résultat
- ➢ OCSV donne un ordre pour SV concernant la météo

  - ❖ **Si la neige est légère**
  - ➢ l'ordinateur donne un ordre pour SV pour limiter la vitesse
  - ❖ **Sinon si la neige est forte**
  - ➢ l'ordinateur central envoie ordre pour SV pour limiter la vitesse et ouvrir l'anti brouillard,pour que la visibilité de SV devienne claire.

C) Le vent

- ➢ OCSV recevoir les données de capteur et l'analyse après lestraités, ensuite il faire un résultat
- ➢ OCSV envoie message à SV pour limiter la vitesse à une vitesse donnée

Cas de verglas :

- ➢ Le capteur de température envoie message vers OCSV
- ➢ OCSV recevoir les données de capteur et l'analyse après les traités
- ➢ Si la température est moins de 0 OCSV donne un ordre a SV pour limite sa vitesse à une vitesse donnée

Cas de bouchon

Les capteurs installées au niveau de les routes captent s'il y'a un bouchon (embouteillage des voitures), ils envoient messages vers l'api Google Maps , AGM analyse et traite les données après il choisit un autre itinéraire pour arriver vers le point Y .

dans ce cas on considère le schéma suivant (figure 16) pour apprendre comment AGM choisit autre chemin pour atteindre le but (Y) .

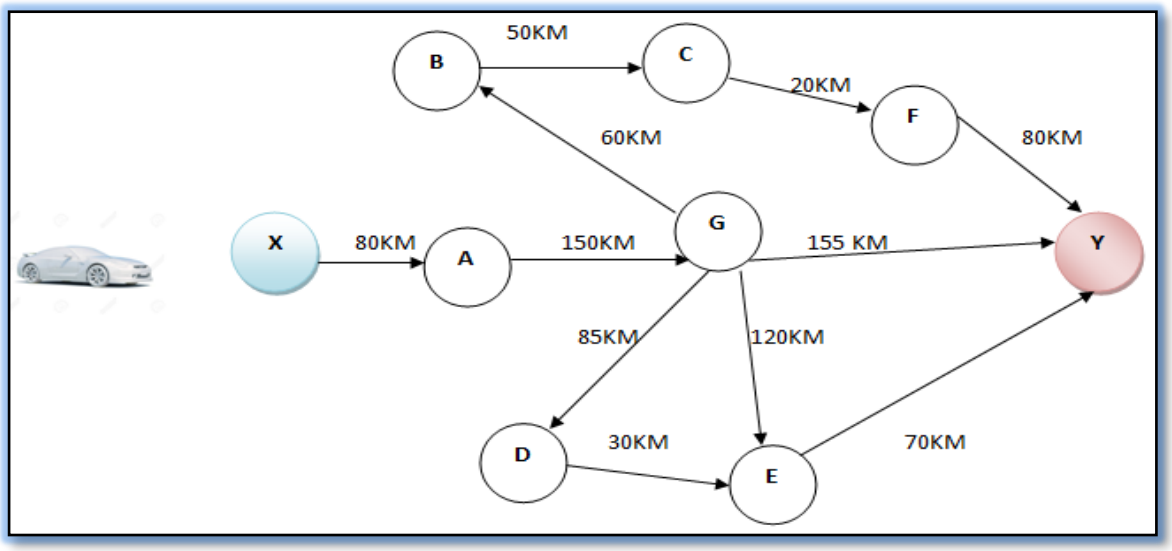

Figure 16 : Schéma pour la route de X vers Y

Le chemin normale de X vers Y est (X A G Y) avec une distance de 385 KM , dans ce cas on considère qu'il y'a un bouchon dans le point G .

AGM utilise l'algorithme de Dijkstra pour calculer l'itinéraire des autres chemins vers Y afin de choisir le plus court chemin

Dans ce cas AGM calcule les distances des chemins de G vers Y pour trouver le plus court chemin.

- ✓ le chemin (G B C F Y) avec une distance de 210KM
- ✓ Le chemin (G D E Y) avec une distance de 185KM
- ✓ Le chemin (G E Y) avec une distance de 190KM

Donc, le chemin (X A G D E Y) est choisi par AGM comme le plus court avec une distance de 395 KM.

NB : Si la carte n'existe pas dans le data center de Fog (DCF), ce dernier transfère les données vers le data center de Cloud (DCC), qu'il les traite afin de trouver la carte. Ensuite, la carte est envoyée au DCF pour la stocker et l'envoyer au SV.

4.3.1 Algorithme du deuxième scénario (les cas particuliers)

Début

Fonction Passage Piéton

Début

Si un PP **Alors**

Les radars de SV captent un obstacle devant le véhicule puis mesurent-la distance entre l'obstacle et SV et envoient leurs données vers l'ordinateur central du SV

Les caméras identifient l'obstacle qu'il est PP et envoient ses donnée vers l'ordinateur central de SV

Lidar crée une carte 3D précise pour la zone environnante de SV après il envoie

la carte vers l'ordinateur central de voiture.

L'ordinateur central de voiture analyse et traite les données reçu par les capteurs

Si une personne traverse PP **Alors**

OCSV envoie message à SV pour s'arrêter

Sinon OCSV envoie message à SV pour continuer le trajet

Fin Si

Fin Si

Fin

Fonction Feu Intelligent

Début

Si FI **Alors**

Les caméras de SV identifient FI et ses signes (rouge,vert,orange) et envoient les données vers l'ordinateur central de SV

Si un feu rouge **Alors**

l'ordinateur central donne ordre pour la voiture pour s'arrêter

Sinon Si un feu orange **Alors**

Les radars de SV sensibles si il y'a une autre voiture devant, à gauche ou à droite de SV et envoie les données vers l'ordinateur central.

les caméras identifient s'il ya des voitures devant ou à gauche ou droit de

SV et envoient ses données vers SV .

lidar créer une carte 3D précise pour la zone environnante de SV après il envoie la carte vers l'ordinateur central de SV .

l'ordinateur central analyse et traite tous les données des capteurs et faire un résultat

Si la route est vide alors

OCSV donne ordre pour SV pour marcher

Sinon

OCSV donne un ordre à SV pour continuer l'arrêt

Fin Si

Sinon OCSV donne un ordre à SV pour continuer marcher

Fin Si

Fin Si

Fin Si

Fin

Fonction Véhicule devant SV

Début

Si un véhicule devant SV **alors**

Les radars captent l'obstacle et envoie les données vers OCSV

Caméras de véhicule identifient l'obstacle et envoie les données vers OCSV

Lidar créer une carte 3d pour la zone de SV et l'envoie vers OCSV

OCSV analyse et traite les données reçus

OCSV donne instruction pour SV pour laisser une distance par rapport l'autre véhicule

Sinon continuer dans la même vitesse

Fin Si

Fin

Fonction Plaque limitation de vitesse

Début

Si PSLV **Alors**

Caméras de SV identifient les données de vitesse maximale créée dans la plaque

Caméras de SV envoies ses données vers OCSV.

Les radars calcule la vitesse de voiture et envoie ses données vers OCSV.

OCSV analyse et traite les données et faire résultat, et envoie ordre a SV pour suivre la vitesse maximale.

Fin Si

Fin

Fonction Mauvais temps

Début

Si un mauvais temps **alors**

Les capteurs de météo captent l'état de météo

Envoie leurs données vers OCSV

Tantque La pluie **alors**

OCSV recevoir les données de capteur

OCSV l'analyse et traite Les données et faire un résultat

OCSV donne un ordre pour SV

Si la pluie est légère **alors**

OCSV donne un ordre pour SV pour limiter la vitesse

Sinon si la pluie est forte

OCSV envoie ordre pour SV pour limiter la vitesse et ouvrir les fars

De pluie

Fin Si

Fin Si

Fin Tantque

Tantque la neige **alors**

OCSV recevoir les données de capteur

OCSV l'analyse et traite Les données et faire un résultat

OCSV donne un ordre pour SV

Si la neige est légère **alors**

OCSV donne ordre pour SV pour limiter la vitesse

Sinon Si la neige est forte **alors**

OCSV envoie ordre pour SV pour limiter la vitesse et ouvrir l'anti brouillard

Fin Si

Fin Si

Fin Tantque

Si un vent alors

OCSV recevoir les données de capteur

OCSV analyse et traite les données et faire un résultat

OCSV envoie message àSV pour limiter la vitesse à une vitesse donnée

Fin Si

Fin Si

Fin

Fonction Verglas

Début

Tantque un verglas **faire**

Si la température est inférieure de **0 alors**

Les capteurs de température de SV envoient leurs données vers OCSV

OCSV analyse et traite les données après faire un résultat

OCSV donne ordre pour SV pour limiter la vitesse à une vitesse donnée

Fin Si

Fin Tantque

Fin

Fonction Bouchon

Début

Si un bouchon **alors**

Les capteurs de la route envoient données pour AGM

AGM recevoir les données

AGM analyse et traite les données

AGM choisit un autre chemin vers Y

Tantque le bouchon dans G **faire**

AGM calcule les distances des autres chemin vers Y

AGM choisit le plus court chemin parmi tous les chemin vers Y

AGM trouve LE plus court chemin (**G D E Y**)

AGM envoie le chemin vers OCSV

SV suivre le chemin

SV arrive vers sa destination Y

Fin Tantque

Fin Si

Fin

Début

Tantque user saisir X et Y dans SV **Faire**

SV envoie les données de S et Y a FN

FN analyse et traite les données et les compare avec les cartes stockés dans DCF

Si carte existe dans DCF **Alors**

FN envoie la carte à SV

SV installe la carte et envoie un message du succès dans son ordinateur central et envoie un message de succès d'installation a FN.

SV active GPS

FN lance API Google Maps

API Google Maps recevoir la position de SV et continue la suivre

Tantque SV démarre **faire**
Si passage piéton **alors**
I <- Passage Piéton
Fin Si

Si un feu intelligent **alors**
J <- Feu Intelligent
Fin Si

Si une véhicule devant SV **alors**
K <- Véhicule devant SV
Fin Si
Si PLV **alors**
L <- Plaque limitation de vitesse
Fin Si

Si mauvais temps **alors**
M<- Mauvais temps
Fin Si

Si un verglas **alors**
N <- Verglas
Fin Si

Si un bouchon **alors**
O <- Bouchon
Fin Si

Fin Tantque
Sinon Si la carte n'existe pas dans DCF **alors**
FN envoie les données de la carte a DCC
DCC Cloud analyse et traite les données et trouve la carte
FN prend une copie de la carte
FN envoie la copie à SV et le stocke dans DCF
SV installe la carte et envoie un message du succès dans son ordinateur central et envoie un message de succès d'installation a FN.
SV active GPS
FN lance API Google Maps
API Google maps recevoir la position de SV et continue la suivre
Tantque SV démarre **faire**

Si passage piéton **alors**
I <- Passage Piéton
Fin Si

Si un feu intelligent **alors**
J <- Feu Intelligent
Fin Si

Si une véhicule devant SV **alors**
K <- Véhicule devant SV
Fin Si
Si PLV **alors**
L <- Plaque limitation de vitesse
Fin Si

Si mauvais temps **alors**
M<- Mauvais temps
Fin Si

Si un verglas **alors**
N <- Verglas
Fin Si

Si un bouchon **alors**
O <- Bouchon
Fin Si

Fin Tantque
Fin Si
Fin Si
Fin Tantque
Fin
Fin

Conclusion

Nous avons réalisé une étude de cas sur les voitures intelligentes en utilisant la coordination entre le Cloud et le Fog Computing dans le coté stockage .Le Fog et le Cloud stockent les cartes que les voiture autonomes ont besoin d'eux .Ensuite on a parlé sur des cas normaux qui nécessitent l'intervention de Fog.

En outre nous avons détaillé les cas particuliers et on a prouvé que la voiture autonome a besoin d'intervention d'API Google Maps en cas de bouchon, et elle nécessite la coordination entre le Cloud et le Fog en cas ou la carte n'existe pas dans les Data Center de Fog.

Enfin on a proposé des algorithmes pour le bon fonctionnement d'une voiture autonome.

Conclusion Générale

«En informatique, la miniaturisation augmente la puissance de calcul.

On peut être plus petit et plus intelligent.»

Bernard Werber

L'objectif de notre travail est de faire le point sur la coordination entre le Cloud et le Fog Computing qui est devenue primordiale après la révolution technologique d'IoT et l'émergence des villes intelligente ainsi que le nombre énorme des données générées par les appareils d'IoT et cela nécessite un traitement des données en temps réel et un espace de stockage massif.

D'abord dans le premier chapitre on a commencé par le Cloud Computing, qui est une récente innovation. Il accroît l'efficacité et la souplesse des sociétés dans la mesure où il permet de travailler à plusieurs sans contrainte (technique, horaire, géographique…), de gérer à la carte les logiciels et donc les fonctionnalités utilisées, de ne plus s'occuper de tâches longues, compliquées et contraignantes liées à la technique, de gagner du temps en limitant les ressaisies et surtout de faire des économies.

Le Cloud a pour objectif de décharger l'utilisateur des problématiques serveur et lui permettre de disposer de ses données et de ses outils où qu'il soit, dès qu'il a une connexion Internet.

Malgré tous les avantages de Cloud mais après l'émergence de l'internet of things et ses défis posés cela oblige à chercher une nouvelle structure , parmi ses défis on a trouvé le problème de latence car les nombreuses données générées par les appareils d'IoT ont besoins des réponses en temps réel , la nouvelle structure est le Fog .

Dans le deuxième chapitre on a abordé le Fog Computing , dont on a détaillé les défis d'IoT qui nécessitent le Fog . Après on a fait une comparaison entre le Fog et le Cloud et aussi les avantages de l'architecture Fog , puis les cas d'utilisations de Fog.

Ensuite dans le troisième chapitre on a parlé sur la coordination entre le Cloud et le Fog Computing, en outre nous avons abordé les modèles de coordination et on a choisis et détaille un modèle de coordination qui est le stockage.

Enfin dans le quatrième chapitre on a fait notre contribution, d'abord par une étude de cas basée sur la coordination entre le Cloud et le Fog qui est la conduite automatique dans une voiture intelligente et après on a proposé des algorithmes afin de garantir une conduite automatique parfaite.

Références Bibliographiques

[1] : https://www.futura-sciences.com/tech/definitions/internet-internet-objets-15158

[2] : Pascal Faure, Gabrielle Gauthey, Marie-Caroline Bonnet-Galzy, Guide sur le Cloud Computing et les Datacentersà l'attention des collectivités locales, (Juillet 2015).

[3] : https://cloudcomputingksu.wordpress.com/2012/05/03

[4] : A.Taivalsaari and T. Mikkonen. 2017. A Roadmap to the Programmable World: Software Challenges in the IoT Era. IEEESoftware34, 1 (2017).

[5] : P.M. Barnaghi and A.P. Sheth. 2016. On Searching the Internet of Things: Requirements and Challenges. IEEE IntelligentSystems31, 6 (2016).

[6] : M.R. Abdmeziem, D. Tandjaoui, and I. Romdhani. 2016. Architecting the Internet of Things: State of the Art. In Robotsand Sensor Clouds, AnisKoubaa and ElhadiShakshuki (Eds.).Springer International Publishing

[7] : DZone. https://dzone.com/guides/iot-applications-protocolsand- best-practices, 2017 (visited in May 2017). The Internet ofThings, Application, Protocls, and Best Practices.Technical Report.

[8] : PujaDhar, Cloud computing and its applications in the world of networking, in IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 1, No 2, (Janvier 2012).

[9] : YousriKouki . Approche dirigée par les contrats de niveaux de service pour la gestion de l'élasticité du "nuage". Laboratoire d'informatique de Nantes-Atlantique (LINA). Mémoire présenté en vue de l'obtention du grade de Docteur. Décembre 2013

[10] : Mickael BARON,Implémentation du modèle mapreduce dans l'environnement distribuehaddop-distribution cloudera , 2014

[11] : Michael Behrendt, Bernard Glasner, Petra Kopp, Robert Dieckmann, Gerd-Breiter, Stefan Pappe, Heather Kreger, Ali Arsanjani, Introduction and Architecture Overview IBM Cloud Computing Reference Architecture 2.0, CCRA.IBMSubmission.02282011.doc, V1.0, Draft,(Février 2011).

[12] : https://fr.wikipedia.org/wiki/Cloud_computing and Applications (consulté le 23/11/2016).

[13] : SIDAA BENAOUDA, Implémentation du modèle mapreduce dans l'environnement distribue, 2015

[14] : PHILIPPE RICHARD, dossier big data : analyse des données intéresse de plus en plus les entreprise ,2012

[15] :http ://business.panasonic.fr/solutions/application/cameramanager-vidoprotection-dans-le-cloud-pour-le-secteur-militaire (consulté le 30 Janvier 2017

[16] : www.lebigdata.fr/soins-de-sante-cloud-1412 (consulté le 27 janvier2017).

[17] : www.orange-business.com/fr/blogs/cloud computing/transformation/lepotentiel-du-cloud-dans-l-educationmstechdays. (Consulté le 29/12/2016)

[18] : www.usine-digitale.fr/article/les-5-grandes-tendances-qui-poussent-lindustrie-manufacturiere-a-adopter-le-cloud.N278476 (Consulté le 29/12/2016).

[19] : www.salesforce.com/fr/crm/what-is-salesforce/ (consulté le 27 janvier2017).

[20] : www.lemagit.fr/definition/Microsoft-Azure-Windows-Azure2016

[21] : www.vmware.com/fr/solutions/virtualization.html 2016

[22] : Sandeep K.Sood. A combined approach to ensure data security in cloud computing .Journal of Network and Computer Applications, pages 1831-1838. 2012. Elsevier

[23] : Sheikh Mahbub Habib, Sascha Hauke, Sebastian Ries, Max Muhlhauser. Trust as a facilitator in cloud computing: a survey. Journal of Cloud Computing: Advances, Systems and Applications, 2012. SPRINGER

[24] : SlaheddineMaaref. Cloud en Afrique: Situation et perspectives. Avril 2012

[25] : Judith Hurwitz, Robin Bloor, Marcia Kaufman, Fern Halper. Cloud computing for dummies. WILEY 2010

[26] : Direction régionale des entreprises, de la concurrence, de la Consommation du travail et de l'emploi. Le Cloud Computing : une nouvelle filière fortement structurante. Septembre 2012

[27] : John W. Rittinghouse, James F. Ransome. Cloud Computing Implementation, Management, and Security. CRC Press 2010

[28] : Richard Hill, Peter Lake, Laurie Hirsch, Siavash Moshiri. Guide to Cloud Computing: Principles and Practice. Springer 2013

[29] : Ronald L. Krutz, Russell Dean Vines. Cloud Security: A Comprehensive Guide to Secure Cloud Computing. WILEY 2010

[30] : Soutenance le 02 Avril 2012, présidée par Mr Neveu , école supérieur de génie informatique , France

[31] : The Economics of Virtualization: Moving Toward an Application-Based Cost Model. IDC. Novembre 2009.

[32] : U.S. Energy Information Administration (juillet 2010) et Microsoft. Le taux commercial moyen aux États-Unis est de 10,15 cents par kilowatt heure. Dans certaines localités, le prix du kilowatt heure peut descendre jusqu'à 2,2 cents.

[33] : James Hamilton, Microsoft Research, 2006

[34] : http://isn.antoine.pagesperso-orange.fr/expose/elie2.pdf

[35] : M. Weiner, M. Jorgovanovic, A. Sahai, and B. Nikoli´c, "Design of a Low-Latency, High-Reliability Wireless Communication System for Control Applications", 2014 IEEE International Conference on Communications (ICC), pp. 3829–3835. IEEE (2014).

[36] : R. Kelly, "Internet of Things Data to Top 1.6 Zettabytes by 2022" <https://campustechnology.com/articles/2015/04/15/internet-of-things-data-to-top-1-6-zettabytes-by-2020.aspx> [Available: April 7, 2016].

[37] : L.Mearian,<http://www.computerworld.com/article/2484219/emerging-technology/self-driving-cars-could-create-1gb-of-data-a-second.html> [Available: April 7, 2016].

[38] : N. Cochrane, "US smart grid to generate 1000 petabytes of data a year" <http://www.itnews.com.au/news/us-smart-grid-to-generate-1000-petabytes-of-data-a-year-170290#ixzz458VaITi6> [Published: March 23, 2010] [Available: April 7, 2016].

[39] : G. Gan, Z. Lu, and J. Jiang, "Internet of Things Security Analysis", 2011 International Conference on Internet Technology and Applications (iTAP), August 16-18, 2011.

[40] : W. Ashford, "Industrial Control Systems: What Are the Security Challenges?", http://www.computerweekly.com/news/2240232680/Industrial-control-systems-What-are-the-security-challenges [Published: October 15, 2014], [Available: January 28, 2016].

[41] : U.S. Department of Transportation, Bureau of Transportation Statistics. http://www.rita.dot.gov/bts/sites/rita.dot.gov.bts/files/publications/national_transportation_statistics/html/table_01_26.html_mfd> [Available: March 2, 2016].

[42] : L. Delgrossi and T. Zhang, "Vehicle Safety Communications: Protocols, Security, and Privacy", published by John Wiley & Sons, 2012, ISBN-10: 1118132726, ISBN-13: 978-1118132722.

[43] : T. Zhang, H. Antunes, and S. Aggarwal, "Defending Connected Vehicles against Malware: Challenges and a Solution Framework", IEEE Internet of Things Journal, Vol. 1, No. 1, February 2014.

[44] : T. Zhang, H. Antunes, and S. Aggarwal, "Securing Connected Vehicles End to End", SAE 2014 World Congress and Exhibition, Detroit, Michigan, USA, April 8 – 10, 2014.

[45] : N. Falliere, L. O Murchu, and E. Chien, "W32.Stuxnet Dossier", Symantec Security Response, Version 1.4, February 2011.

[46] : K. Zetter, "Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon", ISBN-13: 978-0770436179, November 11, 2014.

[47] : https://en.wikipedia.org/wiki/Stuxnet> [Available: March 2. 2016].

[48] : R. Chen, L. Wei, H. Zou, and M. Zhai, "A TCM-Based Remote Anonymous Attestation Protocol for Power Information System", International Power, Electronics and Materials Engineering Conference 2015 (IPEMEC 2015), May 16-17, 2015, Dalian, China.

[49] : A. Francillon, Q. Nguyen, K. B. Rasmussen, and G. Tsudik, "A Minimalist Approach to Remote Attestation", Conference on Design, Automation & Test in Europe (DATE), 2014.

[50] : M. Satyanarayanan, P. Bahl, R. Caceres, and N. Davies, "The case for VM-based Cloudlets in mobile computing," IEEE Transactions on Pervasive Computing, 2009.

[51] : A. Chakraborty, V. Navda, V. N. Padmanabhan and R. Ramjee, "Coordinating cellular background transfers using LoadSense," Mobicom 2013.

[52] : E. Aryafar, A. Keshavarz-Haddard, M. Wang and M. Chiang, "RAT selection games in HetNets," IEEE INFOCOM 2013.

[53] : J. Chong, C. Joe-Wong, S. Ha and M. Chiang, "CYRUS: Toward client-defined Cloud storage," Proceedings of EuroSys 2015.

[54] : L. Canzian and M. van der Schaar, "Real time stream mining: Online knowledge extraction using classifier networks," IEEE Networks Special Issue on Networking for Big Data 2014.

[55] : Z. Zhang, J. Zhang and L. Ying, "Multimedia streaming in cooperative mobile social networks," Preprint.

[56] : F. M. F. Wong, S. Ha, C. Joe-Wong, Z. Liu and M. Chiang, "Mind Your Own Bandwidth: Adaptive Traffic Management on Network Edge," IEEE IWQoS 2015.

[57] : Y. Du, E. Aryafar, J. Camp and M. Chiang, "iBeam: Intelligent client-side multi-user beamforming in wireless networks," Proceedings of IEEE INFOCOM 2014.

[58] : Fog and IoT: An Overview of Research Opportunities Mung Chiang, Fellow, IEEE, and Tao Zhang, Fellow, IEEE

[59] : https://www.syr-res.com/article/12786.html

[60] : L.Gao,T.H.Luan, S.Yu,W. Zhou, andB. Liu, "FogRoute:DTNBased Data Dissemination Model in Fog Computing," IEEE Internet of Things Journal, vol. 4, no. 1, pp. 225–235, 2017.

[61] : D. Fineberg (Intel), "Extract, Transform, and Load Big Data with Apache Hadoop," https://software.intel.com/en-us/articles/extract-transform-and-load-big-data-with-apache-hadoop, Jul. 2013, accessed: 2019-2-11.

[62] : H. Madsen, B. Burtschy, G. Albeanu, and F. Popentiu-Vladicescu, "Reliability in the utility Computing era: Towards reliable Fog Computing," in 2013 20th International Conference on Systems, Signals and Image Processing (IWSSIP), Jul. 2013, pp. 43–46.

[63] : B. Zhang, N. Mor, J. Kolb, D. S. Chan, K. Lutz, E. Allman, J. Wawrzynek, E. A. Lee, and J. Kubiatowicz, "The Cloud is Not Enough: Saving IoT from the Cloud," in 7th USENIX Workshop on Hot Topics in Cloud Computing (HotCloud 15), 2015. [Online]. Available: https://www.usenix.org/system/files/conference/hotCloud15/hotCloud15-zhang.pdf

[64] : N. Govindarajan, Y. Simmhan, N. Jamadagni, and P. Misra, "Event Processing Across Edge and the Cloud for Internet of Things Applications," in Proceedings of the 20th International Conference on Management of Data, ser. COMAD '14. Mumbai, India, India: Computer Society of India, 2014, pp. 101–104

[65] : F. Pisani, J. R. Brunetta, V. M. do Rosario, and E. Borin, "Beyond the Fog: Bringing Cross-Platform Code Execution to Constrained IoT Devices," in 2017 29th

International Symposium on Computer Architecture and High Performance Computing (SBAC-PAD), Oct. 2017, pp. 17–24

[66] : F. Hussain and A. Al-Karkhi, "Big Data and Fog Computing," in Internet of Things, ser. SpringerBriefs in Electrical and Computer Engineering. Springer, Mar. 2017, pp. 27–44.

[67] : P. K. D. Pramanik, P. Choudhury, S. Pal, and A. Brahmachari, "Processing IoT Data: From Cloud to Fog-It's Time to Be Down to Earth," in Applications of Security, Mobile, Analytic and Cloud (SMAC) Technologies for Effective Information Processing and Management. IGI Global, May 2018, pp. 124–148

[68] : I. Stojmenovic and S. Wen, "The Fog Computing Paradigm: Scenarios and Security Issues," Proc. 2014 Federated Conf. Computer Science and Info. Systems, 2014, pp. 1–8.

[69] : XaviMasip-Bruin (xmasip@ac.upc.edu) is an associate professor at UniversitatPolitècnicaCatalunya (UPC). He received his B.Sc., M.Sc., and Ph.D. degrees in telecommunicationsengineering from UPC in 1989, 1997, and 2003,respectively. In 2007, he founded the CRAAX lab at UPC. He has served as Chair and TPC Chair for several conferences as well as Editor and Guest Editor for some journals. His current research interests focus on network management,Cloud and Fog Computing, ITS, and IoT.

[70] : Foggy Clouds and Cloudy Fogs: A real need for coordinated management of Fogto-Cloud Computing systems . Article in IEEE Wireless Communications · October 2016

[71] : W. Ramirez, X. Masip-Bruin, E. Marin-Tordera et al., "Evaluating the benefits of combined and continuous Fog-to-Cloud architectures," Computer Communications, vol. 113, pp. 43–52, 2017.

[72] : O. Salman, I. Elhajj, A. Kayssi, and A. Chehab, "An architecture for the Internet of Things with decentralized data and centralized control," in Proceedings of the 2015

IEEE/ACS 12th International Conference of Computer Systems and Applications (AICCSA), pp. 1–8,Marrakech, Morocco, November 2015.

[73] : M. E. Dick, E. Pacitti, and B. Kemme, "A Highly Robust P2PCDN under Large-Scale and Dynamic Participation," in Proceedings of the 2009 First International Conference on Advances in P2P Systems (AP2PS), pp. 180–185, Sliema, Malta, October 2009.

[74] : L. Pamies-Juarez, M. Sanchez-Artigas, P. Garc´ıa-L´opez, R. Mondejar, and R. Chaabouni, "On the interplay between data redundancy and retrieval times in P2P storage systems," Computer Networks, vol. 59, pp. 1–16, 2014.

[75] : R. Bhagwan,D.Moore, S. Savage, and G.M.Voelker, Replication Strategies for Highly Available Peer-To-Peer Storage Systems, Department of Computer Science and Engineering, University of California, SanDiego, CA, USA, 2002.

[76] : R. S. Carbajo and C. McGoldrick, "Decentralised Peer-to-Peer data dissemination inWireless Sensor Networks," Pervasive and Mobile Computing, vol. 40, pp. 242–266, 2017.

[77] : F. Kangling et al., "Overview of data dissemination strategy in wireless sensor networks," in Proceedings of the 2010 International Conference on E-Health Networking, Digital Ecosystems and Technologies (EDT), pp. 260–263, Shenzhen, China, April 2010.

[78] : www.libelium.com/smart_cars_m2m_accident_prevention

[79] : www.ip-label.nl/wp-content/uploads/2012/10/CloudComputing_Livre_Blanc-fr.pdf

[80] : Fog and IoT: An Overview of Research Opportunities Mung Chiang, Fellow, IEEE, and Tao Zhang, Fellow, IEEE

[81] : https://www.futura-sciences.com/tech/definitions/voiture-voiture-autonome-15601/