الجـــــــــــــــــمـهـوريـــــة الجـــــــــــــزائـريـة الديمـــــــقـراطيـة الـشـــــــــعبيـة

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

وزارة التـــــــــــــــــــــــــعـليـم العـــــــالي و البـــــــــحث العـــــلـمـــي

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

جـــــــــــــامعة أبي بكـــر بـلـقـايد – تـلمســـــــــــــان –

Université Aboubakr Belkaïd – Tlemcen –

Faculté de TECHNOLOGIE

THESE

Présentée pour l'obtention du **grade** de **DOCTEUR EN SCIENCES**

En : Télécommunication

Par : Djilali MOUSSAOUI

Sujet

Réseaux véhiculaires en cloud: gestion de la sécurité

Soutenue publiquement, en 19 Octobre 2019, devant le jury composé de :

ABDERRAHIM Mohammed Amine	MCA	Univ. Tlemcen	Président
FEHAM Mohammed	Professeur	Univ. Tlemcen	Directeur
AMAR BENSABER Boucif	Professeur	UQTR Canada	Co- Directeur
LABRAOUI Nabila	MCA	Univ. Tlemcen	Examinateur 1
MERAD Lotfi	Professeur	ESSAT	Examinateur 2

Résumé

Les réseaux modernes se développent selon deux axes. La première est la mobilité, c'est pour assurer la disponibilité du réseau aux entités connectées en mouvement. Sous cet axe, on trouve différents types de réseaux tels que MANET (Mobile Ad hoc NETwork), VANET (Vehicular Ad hoc NETwork) et WSN (Wireless Sensor Network). Le deuxième axe est la disponibilité des ressources en types (informatique, stockage, logiciels) et en volume. Les réseaux les plus utilisés sont le calcul parallèle, le calcul en grille et le cloud computing. Vehicular Cloud Network (VCN) ou Vehicular Cloud Computing (VCC) est le réseau qui assure la mobilité et la disponibilité des ressources permettant de nouveaux services et applications. La sécurité dans le VCC est un grand défi, où les exigences de sécurité doivent être garanties. Les exigences de sécurité les plus importantes sont l'authentification, l'intégrité, la vie privée, la confidentialité et la traçabilité. Dans la littérature, la solution qui répond à ces exigences pour les réseaux câblés est la PKI (Public Key Infrastructure) renforcée par des mécanismes de sécurité pour assurer la confidentialité. Pour cette raison, deux variantes de solutions basées sur la PKI sont proposées : VCPKI (Vehicular Cloud Public Key Infrastructure) et BC-PKI (BlcokChain based PKI) en environnement centralisé et décentralisé

Mots Clés : Réseaux véhiculaire en cloud, PKI, cloud computing, VANET

Abstract

Modern networks are developed along two axes. The first one is mobility, this is to ensure the network availability to the connected entities in motion. Under this axis, we can find different types of networks such as MANET (Mobile Ad hoc NETwork), VANET (Vehicular Ad hoc NETwork) and WSN (Wireless Sensor Network). The second axis is the resources availability in types (computing, storage, software) and volume. The most used networks are parallel computing, grid computing and cloud computing. Vehicular Cloud Network (VCN) or Vehicular Cloud Computing (VCC) is the network that ensures the mobility and availability of resources allowing new services and applications. Security in VCC is a big challenge, where security requirements must be guaranteed. The most important security requirements are authentication, integrity, privacy, confidentiality and traceability. In literature, the solution that satisfies these requirements for wired networks is the PKI (Public Key Infrastructure) enhanced with security mechanisms to ensure privacy. For this reason, two variant of PKI based solutions are proposed: VCPKI (Vehicular Cloud Public Key Infrastructure) and BC-PKI (BlcokChain based PKI) in centralized and decentralized environment.

Keywords: Vehicular Cloud Computing, PKI, cloud computing, VANET

ملخص

يتم تطوير الشبكات الحديثة على طول محورين. الأول هو التنقل ، وهذا لضمان توفر الشبكة للكيانات المتصلة في الحركة. تحت هذا المحور ، يمكننا أن نجد أنواعًا مختلفة من الشبكات مثل MANET (Mobile Ad hoc NETwork) و VANET (شبكة المركبات) و WSN شبكة الاستشعار اللاسلكية. المحور الثاني هو توفر الموارد في الأنواع (الحوسبة ، التخزين ، البرامج) والحجم. أكثر الشبكات المستخدمة هي الحوسبة المتوازية والحوسبة الشبكية والحوسبة السحابية. الشبكة السحابية للمركبات (VCN) أو الحوسبة السحابية للمركبات (VCC) هي الشبكة التي تضمن تنقل وتوافر الموارد التي تتيح خدمات وتطبيقات جديدة. يمثل الأمان في VCC تحديًا كبيرًا ، حيث يجب ضمان متطلبات الأمان. أهم متطلبات الأمان هي المصادقة والنزاهة والخصوصية والسرية والتتبع. في البحوث السابقة ، فإن الحل الذي يلبي هذه المتطلبات للشبكات السلكية هو البنية التحتية للمفاتيح العمومية (PKI) المعززة بآليات الأمان لضمان الخصوصية. لهذا السبب ، يُقترح حلان مختلفان للحلول القائمة علىVCPKI PKI البنية التحتية للمفتاح السحابي العام للمركبات و BC-PKI المستندة إلى BlcokChain في البيئة المركزية واللامركزية

كلمات البحث الشبكة السحابية للمركبات، البنية التحتية للمفاتيح العمومية، الحوسبة السحابية، شبكة المركبات

Remerciements

En tout premier lieu, je remercie le bon Dieu, tout puissant, de m'avoir donné la force pour survivre, ainsi que l'audace pour dépasser toutes les difficultés

J'adresse mes remerciements aux personnes qui m'ont aidé dans la réalisation de ce mémoire, en premier lieu remercie le directeur de these Monsieur *Mohammed FEHAM*, Professeur à l'Université Abou-Bekr Belkaïd de Tlemcen pour sa patience, sa disponibilité, aussi pour l'autonomie qu'il m'a accordée, et ses précieux conseils qui m'ont permis de mener à bien ce travail.

J'adresse aussi mes remerciements à mon co-directeur de la thèse *Pr. Boucif AMAR BENSABER* , Professeur à l'université UQTR Canada, pour sa patience, sa disponibilité et surtout ses judicieux conseils, qui ont contribué à alimenter ma réflexion.

Je remercie également Monsieur Dr. *Mohammed Amine ABDERAHIM*, Maitre de conférence à l'Université Abou-Bekr Belkaïd de Tlemcen, qui malgré un emploi de temps fort chargé, a accepté de juger ce travail et d'avoir accepté de présider le jury de cette thèse.

Je remercie sincèrement Mme *Nabila LABRAOUI*, Maitre de conférence à l'université Abou-Bekr Belkaïd de Tlemcen, Monsieur *Lotfi* MERAD, Professeur à l'Ecole Supérieure en Sciences Appliquées de Tlemcen, d'avoir accepté de rapporter cette thèse, pour l'intérêt qu'ils ont bien voulu porter à ce travail en acceptant de faire partie du jury et d'avoir consacré une partie de leurs temps pour juger et évaluer le travail de cette thèse.

Il me serait impossible de terminer sans adresser une pensée chaleureuse à toute ma famille et, plus particulièrement, à ma femme.

Djilali MOUSSAOUI

Table des matières

Chapitre II : Le Cloud Computing

Chapitre III : Le réseau véhiculaire en cloud

Chapitre IV: La sécurisation du réseau véhiculaire en cloud

Liste des figures

Introduction générale

Chapitre I : Les réseaux VANET

Chapitre II : Le Cloud Computing

Chapitre III : Le réseau véhiculaire en cloud

Chapitre IV: La sécurisation du réseau véhiculaire en cloud

Liste des tableaux

Glossaire

A

AODV *: Ad hoc On-Demand Distance Vector*

AU *: Application unit*

B

BC-PKI *: Blockchain PKI*

C

CA *: Autorité de certification*

CLA *: Cloud Authority*

D

DDoS *: Déni de Service Distribué*

Distributed Hash Table *: Distributed Hash Table*

DLP *: Data Leakage Prevention*

DNS *: Domain Name System*

DoS *: Déni de Service*

DSDV *: Dynamic Destination-Sequenced Distance Vector*

DSR *: Dynamic Source Routing*

DSRC *: Dedicated Short-Range Communications*

DV-CAST *: Distributed Vehicular Broadcast Protocol*

D-VCSP *: Distributed Vehicular Cloud Service Provider*

E

ECC *: la cryptographie par courbe elliptique*

ECMP *: Equal Cost Multi-Path*

ECN *: Electronic Chassis Number*

EDGE *: Enhanced Data Rates for GSM Evolution*

ELP *: Electronic License Plate*

F

FDMA *: Frequency Division Multiple Access*

FSR : Fisheye State Routing

G

GAB *: Guichet automatique bancaire*

GPRS *: General Packet Radio Service*

GPS *: Global Positioning System*

GPSR *: Greedy Perimeter Stateless Routing*

GSM *: Global System for Mobile Communications*

H

HLAR *: Hybrid Location-Based Ad Hoc Routing Protocol*

L

LTCA *: Long-Term Certificate Authority*

M

MANET *: Mobile Adhoc NETwork, : Mobile Ad hoc NETwork*

MCC *: Mobile Cloud Computing*

MOVE *: MOtion VEctor Routing Algorithm*

N

NIP *: numéro d'identification personnel*

NIST *: National Institute of Standards and Technology*

O

OBU *: On Board Unit*

P

PBC *: Pseudonym BlockChain*

PB-PKI *: 8.3.1.2 Privacy-Aware Blockchain-Based PKI*

PCA : Pseudonym Certificate Authority

PKI : Public Key Infrastructure

PRBC *: Pseudonym Revocation BlockChain*

PTVC *: Trust-Based Verifiable Vehicular Cloud Computing*

Q

QoS *: qualité de service*

R

RA *: autorité d'enregistrement*

RIRP *: Reliability-Improving Position-Based Routing*

Root CA *: Root CA*

RSU *: RoadSide Unit*

S

SCPKI *: Smart Contract-based PKI and Identity System*

STI *: Systèmes de Transport Intelligent*

T

TDMA *: time division multiple access*

TPA *: Third party auditor*

U

UMTS *: 'Universal Mobile Telecommunications System*

V

V2I *: Vehicle To Infrastructure*

V2V *: Vehicle-to-Vehicle*

VA *: autorité centrale de validation*

VANET *: Vehicular Ad hoc NETwork*

VCC *: Vehicular Cloud Computing*

VCN *: Vehicular Cloud Network*

VC-PKI *: Vehicular Cloud PKI*

VC-RSU : Vehicular Cloud RSU

VCSP *: Vehicular Cloud Service Provider*

VM *: machines virtuelles*

VPKI *: Vehicular PKI*

W

WAVE *: Wireless Access in Vehicular Environments*

Wi-Fi *: Wireless Fidelity*

WiMAX *: Worldwide Interoperability for Microwave Access*

WLAN *: réseau local sans fil*

WoT *: Web of Trust*

WSN *: Wireless Sensor Network*

Z

ZRP *: Zone Routing Protocol*

Liste des publications

D. Moussaoui, M. Feham, B. A. Bensaber, and B. Kadri, “Securing vehicular cloud networks,” *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 9, no. 5, pp. 4154–4162, 2019.

Introduction générale

Les réseaux modernes se développent selon deux axes. Le premier est la mobilité, qui assure la disponibilité du réseau pour les entités connectées en mouvement, sous cet axe nous pouvons trouver différents types de réseaux MANET (Mobile Ad hoc NETwork), WSN (Wireless Sensor Network) et les réseaux VANET (Vehicular Ad hoc NETwork). Ces derniers ont connu des changements révolutionnaires ces derniers temps, en investissant dans l'incorporation de plus de caractéristiques technologiques dans les véhicules, ainsi que dans l'amélioration de l'efficacité énergétique. permettre aux conducteurs d'accéder à des véhicules intelligents sophistiqués pour un usage quotidien. N'importe quel véhicule actuel est considéré comme un ordinateur sur roues parce qu'il est équipé avec un ordinateur de bord puissant, un dispositif de stockage de grande capacité, des émetteurs-récepteurs radio sensibles, des radars de collision et un appareil GPS.

Le deuxième axe est la disponibilité des ressources en types (informatique, stockage, logiciels) et en volume, les réseaux les plus utilisés sont : Parallel computing, grid computing et cloud computing. Cloud Computing a présenté des progrès rapides qui lui ont permis de prendre en charge les clouds dynamiques construits dans les environnements mobiles. La flexibilité que le cloud a introduite pour la fourniture à la demande de ressources et de services sur Internet lui a permis d'être reconnu comme un service public. Par exemple, Amazon Elastic Compute Cloud (Amazon EC2) est devenu le plus grand fournisseur de capacité de calcul dynamique dans le Cloud. Cette croissance se justifie par l'intérêt croissant des entreprises pour la location élastique et évolutive de services, plates-formes ou logiciels en cloud au lieu de construire et maintenir leurs data centers. Par conséquent, ces intérêts alliés font avancer le développement du Cloud Computing, qui introduit un système de paiement à l'utilisation, l'évolutivité, les ressources à la demande, la technologie de virtualisation et la qualité de service (QoS) sont ses principales caractéristiques. L'intérêt accéléré pour sa polyvalence a fait du cloud computing la principale tendance technologique en IT, avec des investissements massifs et les efforts des entreprises pour migrer leur activité vers ce nouveau paradigme.

Le réseau cloud véhiculaire (Vehicular Cloud Computing -VCC- ou Vehicular Cloud Network-VCN-) est évolution du réseau qui assure la mobilité et la disponibilité des ressources, permettant de nouveaux services et applications. L'idée de base est d'exploiter les ressources sous-utilisées du véhicule, telles que la connectivité réseau, la puissance de calcul, le stockage et la capacité de détection, qui peuvent être partagées avec les propriétaires de véhicules. En outre, ce cadre devrait permettre aux modèles économiques de regrouper les ressources et de les louer à des consommateurs potentiels, à l'instar de l'infrastructure Cloud traditionnelle.

Issu du réseau VANET (Vehicular Ad-Hoc Network), le (VCC) fait l'objet d'une attention croissante. Le VCC est un outil très attrayant en raison de ses caractéristiques et de ses capacités à prendre en charge une série d'applications nouvelles et pertinentes. De plus, les VCC sont conçus pour initier des objectifs qui correspondent directement aux besoins quotidiens en matière de transport, comme la prestation de services computationnels à faible coût pour les utilisateurs autorisés, la réduction de la congestion routière et la mise en œuvre de services visant à améliorer la sécurité routière.

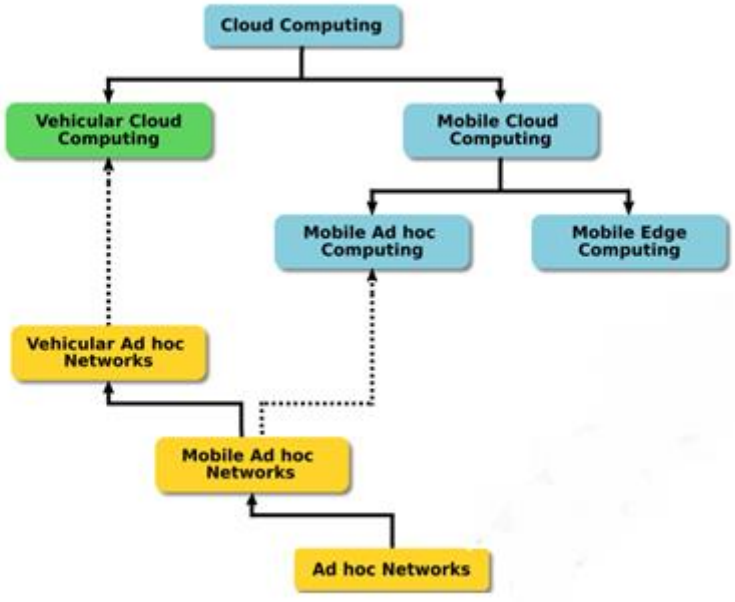

Figure 1 : Évolution du paradigme vers le Vehicular Cloud Computing [1]

Comme le montre la figure 1, les techniques existantes sont classées en fonction de leur contribution à la construction du « Vehicular Cloud Computing ». Ces techniques sont identifiées comme une agrégation de deux paradigmes : Réseaux VANET et Cloud Computing. Les VANET se développent principalement à partir des réseaux adhoc mobile (Mobile Adhoc

NETwork - MANET), dans lesquels la véritable communication entre les nœuds de réseau est basée sur un ou plusieurs sauts. En outre, le VCC est issu du Mobile Cloud Computing (MCC), où la principal préoccupation consiste à atteindre les services Cloud traditionnels qui sont fournis par l'intermédiaire d'une infrastructure, semblable à l'accès aux télécommunications et à d'autres services de transmission de données.

Objectif

La sécurité est un aspect primordial pour les réseaux véhiculaire en cloud, notre objectif est de renforcer la sécurité, pour cela notre démarche s'articule sur trois étapes ; la première est de définir le contexte global et détaillé les différentes parties du réseau véhiculaire en cloud (les réseaux vanet et le cloud computing), la deuxième étape est l'étude de sécurité, où nous avons essayé de mettre en évidence l'impact des attaques sur les exigences de sécurité et les services cloud. A la lumière de cette étude, nous définissons la faiblesse de sécurité du réseau. La troisième étape consiste à proposer une solution qui couvre les faiblesses de sécurité et renforce la robustesse du réseau.

Contribution

Notre contribution est une solution qui prend en considération les caractéristiques du réseaux, il s'agit d'un protocole qui définit en premier lieu l'architecture qui regroupe l'ensembles des éléments des trois composantes de base qui sont les réseaux VANET, le cloud computing et l'infrastructure de la plate-forme de sécurité PKI, par la suite nous passons à présenter le fonctionnement globale du système avec les différents cas de figure et les différent messages échangés, suivit par des tests et des analyses de sécurité pour mettre en évidence la valeur ajoutée de notre proposition par rapport au renforcement de sécurité des réseaux cloud véhiculaire.

Organisation de la thèse

Pour atteindre notre objectif qui est la sécurisation du réseau véhiculaire en cloud, nous avons organisé la thèse comme suit :

Chapitre I : les réseaux vanet. C'est une partie essentielle dans les réseaux véhiculaire en cloud, où nous avons fait un survol global qui s'articule sur deux axes, le premier aspect est les réseaux vanet, où nous avons parlé de la définition des réseaux vanet et son architecture en passant par les mode de communication et les caractéristiques et les protocoles de routage. Nous avons parlé aussi des applications des réseaux vanet, qui rendent ces réseaux intéressants.

Le deuxième aspect est la sécurité dans les réseaux vanet cette partie d'étude commence par définir les exigences de la sécurité pour les vanets en arrivant aux différentes attaques sur ce type de réseau.

Chapitre II : Le coud computing . Ce concept peut être une partie du réseau véhiculaire en cloud dans le cas où la partie vanet a un accès vers le cloud computing via une passerelle, comme in peut etre une caractéristique dans le cas où le cloud computing est composé des véhicules. De ce fait il important d'englober l'ensemble des concepts du cloud computing, pour cela nous avons commencé le chapitre par une définition du cloud computing, nous avons parlé des caractériels, de l'architecture cloud, les composants et les modes de déploiement. Le concept incontournable en étudiant le cloud computing comme une partie de VCC, est le cloud computing mobile (Mobile Cloud Computing MCC).

Puisque notre objectif global est la gestion de sécurité dans les réseaux VCC, nous avons fait un tour sur la sécurité pour le cloud computing qui se résume par définir les exigences de la sécurité, et les différentes attaques possibles sur le cloud computing.

Chapitre III : Réseaux véhiculaire en cloud. Dans ce chapitre nous avons regrouper l'ensemble des notions relatifs au VCC où nous avons commencer par une revue de la littérature sur le commencement de ces réseaux, en passant par l'architecture, la taxonomie, les modèles du réseau et les applications possibles. La sécurité est plus présente dans ce chapitre, où nous avons parlé des exigences de la sécurité, et une classification des attaques en étudiant l'impact des différentes attaques sur les exigences de la sécurité, pour dédiure par la suite quels les exigences les plus touchés par l'ensemble de attaques. Cela ne mène à déduire les points de faible pour la sécurité pour les VCC et proposé l'orientation générale pour proposer une amélioration.

Chapitre IV : La sécurisation du réseau véhiculaire en cloud. D'après l'étude réaliser en chapitre III, nous avons déduit qu'une basé sur la cryptographie améliore la sécurité dans les réseaux VCC, c'est la raison pour laquelle nous commencé notre chapitre par une revue de littérature sur l'utilisation des solutions cryptographique pour améliorer la sécurité dans les réseaux mobile d'une manière générale. La solution la plus complète pour les réseaux internet est le PKI. Pour cela nous avons pensé à adapter le système PKI pour les réseaux VCC.

Une partie de ce chapitre est consacré pour introduire les notions de base pour comprendre le fonctionnement du PKI. En suite nous passons à détailler notre solution VC-PKI où nous supposons qu'il y a un accès vers le réseau internet, de ce fait une centralisation des autorités

est possible. Nous avons décrit en détail le fonctionnement du protocole, nous avons aussi réaliser une implémentation du VC-PKI sur le simulateur OMNET++ pour voir l'impact de notre protocole sur les performances du réseau, et nous l'avons suivi par une analyse de sécurité.

Nous avons aussi adapté la solution PKI pour le cas où le réseau n'a pas d'accès vers le réseau internet, dans ce cas une centralisation des autorités n'est pas possible. Nous avons proposé une décentralisation de la gestion des pseudonymes à l'aide de la technologie blockchain, où nous avons consacré une revue de littérature sur combinaison du PKI et la blockchain. La solution proposée est BC-PKI où nous avons introduit deux blockchain (registres) pour les pseudonymes et leur révocation.

Chapitre I

Les réseaux VANET

1 Introduction

Depuis la dernière décennie, les techniques de communication mobile ont transformé l'industrie automobile en permettant une communication à tout moment et en tout lieu entre différents appareils. Cette facilité de communication permet l'échange d'informations précieuses entre les appareils en déplacement. L'échange transparent d'informations sur des bases de données en temps réel est devenu un nouveau paradigme dans l'industrie. En conséquence, les progrès de la technologie de l'information et de la communication ont facilement soutenu l'idée d'une communication entre appareils mobiles. Parmi ces avancées, le concept de Vehicular Ad-hoc NETworks (VANET) est apparu sous les feux de la rampe et a ouvert de nouvelles possibilités pour l'utilisation des applications de sécurité. VANET se réfère à un réseau créé de manière ad hoc où différents véhicules en mouvement et autres dispositifs de connexion entrent en contact sur un support sans fil et échangent des informations utiles les uns avec les autres. Un petit réseau est créé au même moment avec les véhicules et autres dispositifs qui se comportent comme des nœuds dans le réseau. Toutes les informations que les nœuds possèdent sont transférées à tous les autres nœuds. De même, tous les nœuds, après avoir transféré leur ensemble de données, reçoivent les données transmises par d'autres nœuds. Après avoir accumulé l'ensemble de ces données, les nœuds s'efforcent de générer des informations utiles à partir de ces données, puis de les transmettre à d'autres dispositifs. La communication entre les appareils se développe de telle sorte que les nœuds sont libres de rejoindre et de quitter le réseau, c'est-à-dire qu'il s'agit d'un réseau ouvert. Les nouveaux véhicules lancés sur le marché sont désormais équipés de capteurs embarqués qui permettent au véhicule de s'intégrer et de fusionner facilement dans le réseau et de tirer parti des avantages de VANET.VANET est une variation de MANET (Mobile Ad-hoc NETwork). MANET se compose de nœuds qui communiquent sans réseau central et où les nœuds sont équipés de capacités de mise en réseau. De l'autre côté, VANET s'est révélé être une classe ou une variante de MANET plus difficile et plus responsable. La liberté des nœuds d'entrer ou de sortir du réseau dans VANET nécessite des protocoles de routage différents de ceux de MANET. Cette communication entre véhicules conduit à la transmission et à la réception d'informations afin d'augmenter l'efficacité du trafic, de détecter les conditions routières, de diminuer les collisions, de détecter les situations d'urgence et d'augmenter globalement l'efficience du réseau. VANET transfère également l'information vers des appareils distants à l'aide de multi-saut.

2 Définition

Le réseau ad hoc véhiculaire (VANET) est une forme de réseau ad hoc mobile (MANET), où les nœuds sont des véhicules. Chaque véhicule reçoit et envoie des informations, il joue également le rôle de routeur en transférant des données vers la destination. Dans VANET, la communication peut s'effectuer entre véhicules (véhicule à véhicule) ou entre infrastructure et véhicules (infrastructure à véhicule)[2].

3 Architecture VANET

3.1 Véhicule intelligent

Un véhicule intelligent, intègre essentiellement, un ensemble de capteurs (radar avant, radar de recul, etc.). On trouve aussi un système de positionnement comme le GPS (Global Positioning System) par exemple, qui est essentiel pour localiser et aider à la conduite.

Un véhicule intelligent est équipé d'un système de communication (qui peut être multi-interface), d'un système informatique, d'un dispositif d'enregistrement d'événements dont le fonctionnement est similaire à celui de la boîte noire d'un avion.

Pour des raisons de sécurité, un véhicule intelligent doit être équipé d'un ELP (Electronic License Plate) ou d'un ECN (Electronic Chassis Number) qui indiquent l'identité électronique du véhicule au lieu de l'identification conventionnelle par plaques d'immatriculation. La terminologie actuelle des Systèmes de Transport Intelligent (STI) comprend certaines caractéristiques telles que l'émetteur-récepteur, l'affichage et l'interaction avec le conducteur dans une seule unité appelée OBU (On Board Unit) . La figure I.1 2 montre les différents composants qui peuvent être intégrés dans un véhicule intelligent[3].

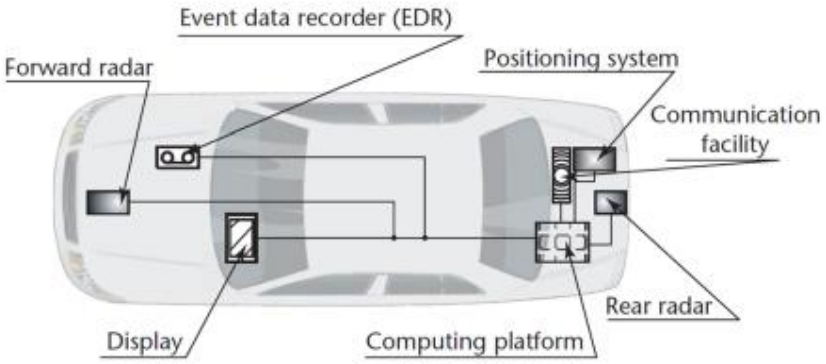

Figure I.1: Véhicule intelligent [3].

3.2 On board unit (OBU):

Ce sont les unités intégrées dans les véhicules intelligents, elles comprennent un ensemble de composants matériels et logiciels de haute technologie (GPS, radar, caméras, divers capteurs). Leurs rôles est d'assurés localisation, calcul, stockage et échange de données sur le réseau. Ce sont des émetteurs-récepteurs qui connectent le véhicule au réseau [4] [5].

Figure I.2: OnBoard Unit (OBU) [6]

3.3 Application unit (AU)

L'UA est l'appareil équipé dans le véhicule qui utilise les applications fournies par le fournisseur en utilisant les capacités de communication de l'OBU. L'AU peut être un périphérique dédié aux différents types d'applications (sécurité routière, applications de confort etc). Il peut être connecté à l'OBU via une connexion filaire ou sans fil comme il peut être regrouper avec l'OBU dans une même unité physique[4].

3.4 RoadSide Unit (RSU)

Le RSU est un dispositif de communication sans fil, il est généralement fixé au bord de la route ou à des emplacements spécifiques, tels que des intersections ou des espaces de stationnement. Le RSU est équipé d'un périphérique réseau pour une communication dédiée à courte portée. Il peut également être équipé d'autres périphériques réseau afin de pouvoir être utilisé à des fins de communication dans le réseau infrastructurel. Selon les principales fonctions et procédures associées à RSU sont[4]:

- Extension de la portée de communication du réseau VANET en redistribuant les informations à d'autres OBU et en les transmettant à d'autres RSU afin d'atteindre d'autres OBUs.
- Exécution d'applications de sécurité telles qu'un avertissement d'accident ou une zone de travail.
- Fournir une connectivité Internet aux OBUs.

Figure I.3: RoadSide Unit (RSU) [7]

4 Mode de communication

4.1 Vehicle-to-Vehicle (V2V)

Les communications de véhicule à véhicule (V2V) sont des communications entre véhicules en mode ad hoc. Dans ce mode, un véhicule peut recevoir, transmettre ou échanger avec d'autres véhicules des informations routières telles que les conditions de circulation et les accidents de la route [8].

4.2 Vehicle To Infrastructure (V2I)

Utilisé pour diffuser entre l'infrastructure du réseau et les véhicules, et pour l'échange d'informations utiles sur les conditions routières et les mesures de sécurité à prendre en compte. Dans ce mode, un véhicule établit une connexion avec le RSU pour se connecter et communiquer avec des réseaux externes tels que l'Internet. Les liaisons V2I sont moins vulnérables aux attaques et nécessitent plus de bande passante que les liaisons V2V[8].

5 Technologie d'accès sans fil dans VANET

5.1 Système cellulaire

Système cellulaire consiste à réutiliser la fréquence limitée disponible pour le service. Le GSM est l'un des systèmes cellulaires offrant un débit maximal de 9,6 kbps. Le GSM utilise les schémas FDMA et TDMA. Le GPRS est un service général de radiocommunication par paquets qui permet la transmission de données avec une bande passante élevée avec efficacité. Des débits de données élevés sont nécessaires pour transmettre des données multimédia. UMTS est

donc utilisé à cette fin. L'évolution améliorée du débit de données (EDGE), qui est la version avancée du GSM, est utilisée à cet effet et fournit également un débit de données de pointe[9].

5.2 WiFi/WLAN

Un réseau local sans fil (WLAN) ou Wireless Fidelity (Wi-Fi) peuvent fournir un accès sans fil pour permettre la communication V2V ou la communication V2I à l'aide de la norme IEEE 802.11.Cette dernière fonctionne à 5 GHz et fournit un débit de données de 54 Mbps avec une portée de communication d'au moins 38 m à l'intérieur et une portée de 140 m à l'extérieur [9].

5.3 WiMax

WiMAX ou IEEE 802.16e est un amendement à Worldwide Interoperability for Microwave Access, offrant un débit binaire élevé et couvrant une large plage de transmission avec des communications fiables et une haute qualité de service (QoS), adaptées au multimédia, à la vidéo et à la voix sur Internet (VoIP). WiMAX atteint un débit de données élevé pouvant atteindre 35 Mbps en utilisant plusieurs entrées et plusieurs sorties (MIMO), avec un multiplexage par répartition orthogonale de la fréquence (OFDM)[9].

Figure I.4: WiMax

5.4 DSRC/WAVE

Dedicated Short-Range Communications sont des canaux de communication sans fil unidirectionnels à courte portée ou à moyenne portée, spécialement conçus pour une utilisation dans le secteur automobile. DSRC sont les technologies clés essentielles pour le marché émergent des systèmes de transport intelligents (ITS). L'accès sans fil dans les environnements de véhicules (Wireless Access in Vehicular Environments WAVE) est très différent des environnements de réseau sans fil Wi-Fi et cellulaire. Les spécifications définies par

IEEE802.11P et IEEE1609 représentent l'ensemble de normes le plus abouti en matière de Réseaux DSRC / WAVE [10]

6 Caractéristiques des réseaux VANET

6.1 Mobilité prévisible

Dans VANET, les véhicules se déplacent selon un schéma de mobilité contraint par les routes, les rues, les autoroutes et par le code de la route (éclairage, limitation de vitesse)[9].

6.2 Conduite Sécurisée

Les réseaux VANET permettent des communications directes entre véhicules en mouvement, permettant ainsi à un ensemble d'applications d'exiger une communication directe entre les nœuds sur le réseau. De telles applications peuvent donner aux conducteurs qui voyagent dans la même direction des messages d'avertissement sur les accidents ou sur la nécessité de freiner brusquement, Ces notifications aident le conducteur à construire une image plus large de la route. De plus, d'autres types d'applications pourraient être appliquées via ce type de réseau afin d'améliorer le confort des passagers et l'efficacité du trafic en diffusant des informations sur la météo, la circulation et les points d'intérêt (stations-service, centres commerciaux et fast food)[9].

6.3 Autonomie énergétique

L'énergie n'est pas un défi majeur dans les VANET comme les réseaux MANET, car les véhicules sont capables d'utiliser l'énergie en continu en utilisant la batterie longue durée[9].

6.4 Densité variable du réseau

La densité du réseau dans VANET dépend de la nature des routes (autoroute, rurale, centre-ville) et de la densité du trafic, qui peut être très élevée ou très faible[9].

6.5 Topologie Dynamique

En raison de la grande mobilité des véhicules et donc de la nature irrégulière, la topologie VANET évolue rapidement. Ce changement rapide de la topologie du réseau facilite l'attaque de l'ensemble du réseau VANET et rend difficile la détection des véhicules malveillants[9].

6.6 Réseau à grande échelle

L'échelle du réseau est variable, elle pourrait être grande dans les zones urbaines denses telles que le centre-ville, les autoroutes et à l'entrée des grandes villes[9].

6.7 Haute capacité de calcul

Puisque les nœuds du réseau VANET sont des véhicules, ils peuvent être équipés d'une ressource informatique, comprenant des processeurs, une capacité de mémoire à grande vitesse, une capacité de stockage et différents types de capteurs. Ces ressources augmentent la capacité de calcul du véhicule, qui offre plus d'applications et de services que MANET[9].

7 Applications de VANET

7.1 Applications de sécurité

Les applications de sécurité ont pour but de rendre la conduite plus sure, et cela par rendre l'information sur la route disponible et en temps réel (l'état de la route, en cas d'accident ...). Les applications de sécurité routière peuvent être classées comme suit :

7.1.1 Trafic en temps réel

Cette application est basée sur le RSU, où les données de trafic en temps réel sont rassemblées et mises à la disposition des véhicules chaque fois que nécessaire. Le but de ce type d'applications est d'éviter les embouteillages[11].

7.1.2 Transfert coopératif de messages

Dans VANET, les messages contenant des informations différentes sont échangés de manière permanente. Parmi ces informations, vous trouverez des informations sur le freinage d'urgence, les actes mal conduits du conducteur, etc. Cette application nécessitait un puissant algorithme de diffusion et un réseau très efficace pour réduire les délais[11][4].

7.1.3 Notification post-collision

En cas de collision, les véhicules impliqués informent les autres véhicules en envoyant des notifications. Ces notifications contiennent des informations sur la collision comme la position et l'heure. Ces notifications sont utiles pour que les véhicules prennent une décision[11].

7.1.4 Avertissement de collision coopérative

Cette application alerte les véhicules de la possibilité d'un accident s'ils conservent le même mode de déplacement. Cela peut être fait par un nœud centralisé (RSU), où le RSU envoie les avertissements qui contiennent des recommandations (changer de voie, réduire la vitesse, etc)[11][12].

7.2 Les applications commerciales

Les applications commerciales fourniront au conducteur le divertissement et les services sous forme d'accès Web, de transmission audio et vidéo en continu. Les applications commerciales peuvent être classées comme suit :

7.2.1 Accès Internet

Dans VANET, les véhicules peuvent avoir un accès Internet facilement via le RSU. Ce peut être un service payant[11].

7.2.2 Téléchargement de carte numérique

Les conducteurs peuvent télécharger et mettre à jour des cartes là où c'est nécessaire. Ce service contient les cartes et les bases de données actualisées sur la région (informations telles que restaurants, hôpitaux, cafés, etc.)[11].

7.2.3 Replay vidéo en temps réel

Le conducteur peut demander la lecture de ses vidéos préférées. C'est un service à bord où les vidéos peuvent être adaptées aux situations de conduite[11].

7.2.4 Annonces on-board

Les fournisseurs de services peuvent présenter leurs services ou produits aux conducteurs pour attirer plus de clients dans leurs magasins. Les publicités peuvent concerner des stations de service, des restaurants d'autoroute. Ces annonces sont présentées sur la base de la position GPS des véhicules[11].

7.3 Applications de commodité

Les applications de commodité concernent principalement la gestion du trafic dans le but d'améliorer l'efficacité du trafic en améliorant le degré de commodité des conducteurs. Les applications de confort peuvent être classées comme suit :

7.3.1 Collection de péage électronique

C'est un système dont l'objectif est d'accroître l'efficacité du paiement du péage. Ce système basé sur deux partie, la première est installée dans le péage, la seconde partie est installée sur l'OBU du véhicule. Par la communication entre les deux parties, le paiement est effectué et il est basé sur l'odomètre du véhicule[11].

7.3.2 Disponibilité du stationnement

Cette application aide à trouver des places disponibles dans les parkings dans une zone géographique donnée. Lorsque le conducteur demande une place dans un parking, il commence à recevoir une notification concernant les places libres les plus proches [11].

7.3.3 Prévision active (de la route)

Cette application assiste le conducteur en anticipant la topographie routière à venir. Ce type d'assistance aide le conducteur à optimiser sa consommation de carburant en régulant sa vitesse de croisière avant de commencer une descente ou une montée[11].

8 Les protocoles de routage

L'objectif principal du protocole de routage est de fournir des chemins optimaux entre les nœuds du réseau avec un temps système minimal. Beaucoup des protocoles de routage ont été développés pour les réseaux VANET, qui peuvent être classés de différentes manières, selon différents aspects ; tels que: caractéristiques des protocoles, techniques utilisées, informations de routage, qualité des services, structures de réseau, algorithmes de routage, etc.

La classification des protocoles de routage VANET est essentiellement basée sur : la topologie la position, géocast, diffusion et cluster, cette classification est basée sur des caractéristiques des et techniques utilisées dans des VANETs.

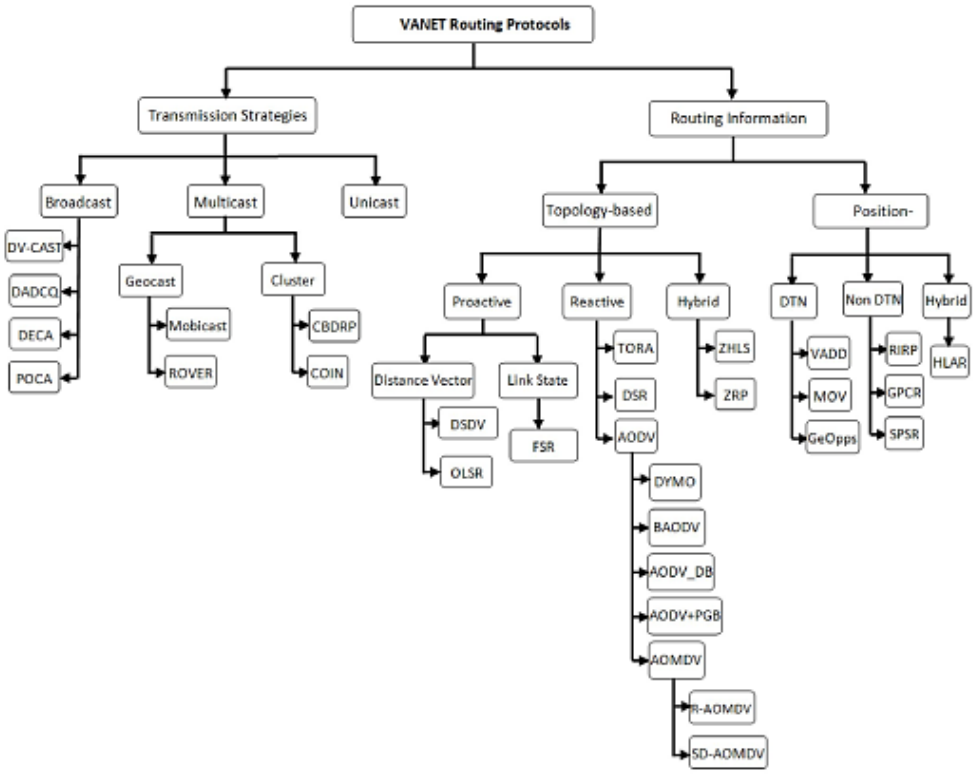

Figure I.5: La classification des protocoles de routage VANET [13]

8.1 Les protocoles basés sur l'information de routage

Cette classe est divisée en deux sous-classes : protocoles de routage basés sur la topologie et basés sur la position. Dans le routage basé sur la topologie, chaque nœud doit connaître la structure du réseau et doit également pouvoir transférer les paquets en utilisant des informations sur les nœuds et les liaisons disponibles sur le réseau. En revanche, le routage basé sur la position, chaque nœud doit connaître les emplacements des autres nœuds avant la transmission de paquets [13].

8.2 Les protocoles de routage basés sur la topologie

L'ordre dans lequel les nœuds sont organisés dans un réseau est appelé topologie. Dans cette catégorie de protocoles de routage VANET, il utilise les informations de liaison présentes sur le réseau pour transférer des données d'un nœud source à un nœud de destination. Les protocoles basés sur la topologie peuvent être soit : proactif, réactif ou hybrides.

8.2.1 Protocoles proactifs

Le principe de base des protocoles proactifs est de maintenir à jour les tables de routage. Ces protocoles sont basés essentiellement sur les protocoles de routage classique (vector distance, link state). Les tables de routage sont maintenues grâce à un échange continu de paquets de contrôle. Le choix des routes s'effectue en se basant sur une métrique (le nombre de sauts, la bande passante ou la route). L'avantage principal de ces protocoles est qu'ils permettent d'assurer un routage optimal, mais l'échange permanent des tables de routage consomme considérablement la bande passante du réseau.

- *DSDV (Dynamic Destination-Sequenced Distance Vector)*

Ce protocole utilise l'algorithme du plus court chemin. Chaque nœud stock les chemins vers toutes les destinations possibles dans une table de routage. La métrique de base pour trouver le plus court chemin est le nombre de saut. Lorsqu'il y a un changement de topologie du réseau, les tables de routage sont mises à jour en les échangeant avec les nœuds voisins. Les chemins cycliques ne sont pas autorisés dans le protocole de routage DSDV[14].

- *FSR (Fisheye State Routing)*

Il est similaire au protocole LSR (Link State Routing Protocol). Chaque nœud gère une table de topologie basée sur les dernières informations reçues des nœuds de voisinage. Il utilise différentes périodes d'échange pour différentes entrées dans la table de routage afin de réduire la taille des messages de contrôle dans les grands réseaux.

L'inconvénient du routage FSR est que la taille de la table de routage augmente avec la taille du réseau. La découverte de l'itinéraire peut échouer si le nœud de destination se situe en dehors de la portée du nœud source. En raison de la grande mobilité dans VANET, les itinéraires vers une destination éloignée deviennent moins précis [2].

8.2.2 Protocoles réactifs

Ces protocoles sont appelés protocoles de routage à la demande car ils mettent à jour périodiquement la table de routage, lorsque certaines données doivent être envoyées. Mais ces protocoles utilisent le processus d'inondation pour la découverte d'itinéraire, ce qui augmente le temps système nécessaire au routage et consomme la bande passante.

- *AODV (Ad hoc On-Demand Distance Vector)*

Est un protocole de routage initié par la source et utilise les messages HELLO pour identifier ses voisins. Le nœud source diffuse une requête de route (route-request) à ses voisins, ces derniers vont diffuser cette requête pour atteindre la destination. Ensuite, la destination envoie un paquet de réponse de route (route-replay) à l'expéditeur[2].

AODV est protocole de routage qui est utilisé à la base pour les réseaux MANET (Mobile Ad hoc NETwork), et des améliorations sont proposée pour répondre aux exigences du VANET où on site :

- Enhancing AOMDV Routing Protocol for V2V Communication (SD-AOMDV)[15]
- A Cross-layer AOMDV Routing Protocol for V2V Communication in Urban VANET (R-AOMDV)[15]

- *DSR (Dynamic Source Routing)*

Il utilise le routage source au lieu de dépendre de la table de routage du nœud intermédiaire. Le routage source consiste à ce que la source détermine un chemin et envoie dans chaque paquet de données tous les nœuds à traverser pour atteindre la destination. Chaque nœud intermédiaire retire son adresse du paquet avant de le retransmettre. Cette technique nécessite la connaissance de la route à utiliser de la part de la source. Cette connaissance des routes est obtenue par une table de routage maintenue dans chaque nœud. Il faut donc dans un premier temps découvrir les routes, puis les conserver tant qu'elles existent[2].

8.2.3 Les protocoles hybrides

Les protocoles hybrides combinent les approches réactive et proactive. Le principe est de connaître le voisinage de manière proactive jusqu''a une certaine distance (par exemple trois ou quatre sauts), et si jamais une station cherche à envoyer quelque chose à un nœud qui n'est pas dans cette zone, une recherche réactive est effectuée à l'extérieur. Selon le type de trafic et les routes demandées, ce type de protocole hybride peut cependant combiner les désavantages des deux méthodes : échange de paquets de contrôle réguliers et inondation de l'ensemble de réseau pour chercher une route vers un nœud éloigné.

- *ZRP (Zone Routing Protocol)*

ZRP est le premier protocole développé en tant que protocole de routage hybride (proactifs, réactifs), il permet à un nœud de réseau de diviser le réseau en zones en fonction de nombreux facteurs comme : puissance de transmission, force du signal, vitesse et d'autres facteurs.

La zone à l'intérieur de la zone est la zone de portée d'acheminement pour le nœud et inversement pour la zone extérieure. ZRP utilise les schémas de routage réactif pour la zone extérieur, et les schémas de routage proactifs pour la zone intérieur.

8.2.4 Protocoles de routage base sur la position

Les protocoles de routage basés sur la position géographique s'appuient sur les informations de position dans le processus de routage ; où la source envoie un paquet à la destination en utilisant sa position géographique plutôt qu'en utilisant l'adresse réseau. Ces protocoles nécessitaient que chaque nœud puisse décider de son emplacement et de celui de ses voisins grâce à l'assistance du système de positionnement géographique (GPS). Le nœud identifie son voisin en tant que nœud situé dans la portée radio du nœud. Lorsque la source a besoin d'envoyer un paquet, elle stocke généralement la position de la destination dans l'en-tête du paquet, ce qui facilite le transfert du paquet vers la destination sans nécessiter de découverte d'itinéraire, de maintenance d'itinéraire ou même de connaissance de la topologie du réseau. Ainsi, les protocoles de routage de position sont considérés comme plus stables et plus adaptés aux réseaux VANET à environnement de grande mobilité, par rapport aux protocoles de routage basés sur la topologie. Les protocoles de routage géographique sont généralement classés en trois classes : protocoles de réseau tolérant le retard (DTN), protocoles de réseau non tolérants de retard (Non DTN) et hybride.

a. DTN (Delay Tolerant Network Protocols)

DTN est un réseau sans fil conçu pour fonctionner efficacement dans les réseaux présentant certaines caractéristiques comme coupure de communication fréquente, réseau à grande échelle, les délais inévitables, largeur de bande limitée. Dans ce type de réseau, tous les nœuds s'entraident pour transférer des paquets. Ces nœuds peuvent avoir une portée de transmission réduite. La transmission des paquets prendra donc beaucoup de temps. Généralement, le nœud DTN est un nœud mobile. Il établit donc des itinéraires vers les autres nœuds lorsqu'ils atteignent sa plage de transmission.

- *MOVE (MOtion VEctor Routing Algorithm)*

L'algorithme MOVE est conçu pour les réseaux légers, en particulier pour la communication entre véhicules en bordure de route. Ce protocole suppose que chaque nœud dispose d'informations sur les localisations globales, outre la connaissance de la vitesse d'un routeur mobile et de la vitesse de ses nœuds voisins. À partir de ces informations, le nœud peut estimer les nœuds qui se trouvent à la distance la plus proche de la destination. Le routage basé sur la

position non-DTN pourrait offrir de meilleures performances uniquement si les routes sont stables et cohérentes[15].

- *VADD (Vehicle-Assisted Data Delivery In VANET)*

Protocole conçu pour gérer les réseaux de véhicules fréquemment déconnectés et les problèmes de forte mobilité. Il implémente le système de stockage et de transfert pendant qu'un nœud est en mouvement, il stocke le paquet jusqu'à ce qu'un nouveau nœud arrive dans sa plage de zones, puis il transfère le paquet stocké à ce nouveau nœud. Ce protocole prédit la mobilité des nœuds en fonction de deux facteurs : le trafic du réseau routier et le type de route[16].

b. Non DTN (Non Delay Tolerant Network Protocols)

Les protocoles non-DTN sont des protocoles de routage géographiques, mais il ne considère pas un problème de dis-connectivité, cela suppose qu'il existe toujours un certain nombre de nœuds pour réussir la communication. Ce protocole ne convient donc que pour les réseaux à haute densité. Dans les protocoles Non-DTN, le nœud transmet son paquet au voisin le plus proche de la destination, mais cette approche peut échouer s'il n'y a pas de voisin le plus proche de la destination plutôt que le nœud actuel lui-même. De nombreux protocoles de routage non-DTN gèrent cette défaillance.

- *GPSR (Greedy Perimeter Stateless Routing)*

GPSR est un protocole de routage glouton réputé dans les VANET. Dans ce protocole, chaque nœud transfère les paquets à d'autres nœuds intermédiaires toujours plus proches de la destination du paquet (transfert glouton), jusqu'à ce que le paquet atteigne sa destination finale. S'il n'y a pas de nœud voisin à proximité de la destination, il utilise le transfert de périmètre pour décider à quel nœud il va livrer le paquet. GPSR est un protocole sans état qui conserve des informations sur les positions de son voisin de premier saut, ce qui pourrait accroître davantage l'évolutivité des protocoles que les protocoles de routage ad hoc les plus courts[15].

- *RIRP (Reliability-Improving Position-Based Routing)*

RIPR est un algorithme de routage basé sur la position conçu pour les VANET. Il vise à résoudre les problèmes d'échec de liaison rencontrés dans un routage basé sur la position qui apparaissent en raison du stockage d'anciennes informations sur un nœud intermédiaire obsolète. RIPR prédit la vitesse des véhicules et leur direction de déplacement, ainsi que les caractéristiques de la route de la ville. Dans ce protocole, l'expéditeur sélectionne un nœud

intermédiaire pour transmettre son paquet en fonction de l'estimation de la mobilité des nœuds voisins effectuée en déterminant initialement si un nœud voisin existe ou non[15].

c. Routage Hybride

Aucun protocole de routage existant ne fonctionne donc efficacement dans toutes les circonstances. Par conséquent, de nombreux chercheurs ont développé des protocoles hybrides, ils fusionnent les caractéristiques de deux ou plusieurs protocoles de routage basés sur la position (non-DTN et DTN), parfois ils fusionnent un ou plusieurs protocoles de routage de topologie (réactif, proactif et hybride) avec un routage basé sur la position.

- *HLAR (Hybrid Location-Based Ad Hoc Routing Protocol)*

HLAR est un protocole de routage de position hybride conçu pour utiliser efficacement toutes les informations de localisation disponibles et minimiser les couts de contrôle de routage. Ce protocole est prévu pour basculer vers le routage à la demande lorsque suffisamment d'informations de localisation est indisponible ou limitée, il résout également le problème de l'absence de plus proche voisin de la destination (régions vides), ce qui en fait presque un protocole évolutif. HLAR fonctionne comme un protocole réactif dans le processus de découverte d'itinéraire[15].

8.2.5 Stratégies de transmission utilisées dans le transfert de paquets

La transmission d'informations d'une source à une destination peut être classée en quatre types: unicast, multicast, braodcast et géocast, toutefois, la multicast et la géocast peuvent être fusionnées dans une classe, car la géocast est généralement un type spécial de transmission par multicast.

8.2.5.1 Protocoles de routage unicast

Le routage de unicast fait référence à la transmission d'informations d'une source unique vers une destination unique en utilisant, où les nœuds intermédiaires sont utilisés pour transférer les données de la source à la destination. C'est la classe la plus largement utilisée dans les réseaux ad hoc généraux. Il existe de nombreux protocoles de routage unicast proposés pour les VANET; la plupart des protocoles de routage basés sur la topologie appartiennent à une classe de unicast tels que VADD, AODV, DSR[15].

8.2.5.2 Protocoles de routage broadcast

Le routage de diffusion (broadcast) est basé sur l'inondation vers tous les nœuds disponibles dans le domaine de diffusion. Le routage de diffusion est largement utilisé dans les réseaux

VANET. Il est principalement utilisé dans le processus de découverte d'itinéraire, certains protocoles (comme l'AODV) permettent aux nœuds de rediffuser les paquets reçus. Les protocoles de routage basés sur la diffusion consomment la bande passante du réseau[15].

- *DV-CAST (Distributed Vehicular Broadcast Protocol)*

DV-CAST est un protocole de routage de diffusion utilisant un schéma à sauts multiples. Dans ce protocole, chaque nœud surveille en permanence l'état de la connectivité voisine afin de leur diffuser des informations. DV-CAST traite différentes classes selon de nombreux aspects tels que : état du trafic, état de la connectivité avec les nœuds voisins. Il utilise les messages périodiques des balises pour obtenir des informations sur la topologie du réseau.

Dans un groupe réduit de nœuds connectés, le nœud peut utiliser la rediffusion avec les nœuds se déplaçant de la même manière. Dans le cas des nœuds voisins sont déconnectés, le nœud source doit utiliser le schéma de stockage et de retransmission, il stocke le paquet de diffusion jusqu'à ce qu'il trouve un autre nœud qui se déplace dans son domaine de diffusion, mais s'il n'y a pas de nœud, il supprimera le paquet une fois la durée de vie du paquet terminée[15].

8.2.6 Protocoles de routage multicast

Les protocoles de routage multicast (multidiffusion) ont pour but de communiquer des messages à de nombreuses destinations en tant que communication de groupe de véhicules. Les protocoles de routage multicast peuvent être classés en deux sous-classes : le protocole de routage géocast et le protocole basé sur un cluster.

a. Les protocoles de routage géocast

Un protocole de routage géocast utilise des métriques d'emplacement géographique pour définir la destination. Par conséquent, dans ce type de protocole, la source enverra un message à plusieurs destinations ayant un point commun, à savoir la position géographique[16].

- *IVG (Inter-Vehicle Geocast Protocol)*

C'est un protocole de routage multicast adapté aux trafics routiers et de sécurité. L'idée principale de ce protocole est de notifier aux véhicules le danger d'accident ou d'autres obstacles. Ce protocole proposé introduit un nouveau concept appelé zone à risque. Ce dernier est défini en fonction des informations de position géographique et de la direction des véhicules. Le groupe de multidiffusion contient des véhicules situés dans la zone. Ce protocole suppose que tous les véhicules sont équipés d'un GPS, afin de collecter les informations nécessaires lors de l'exécution de l'algorithme[16].

b. Les protocoles de routage basés sur les clusters

Ce type de protocole est lié à l'approche de clustering. L'idée principale de cette technique est de diviser le réseau en groupes appelés clusters, en fonction de plusieurs mesures et critères. Pour chaque cluster, l'un des membres joue le rôle de chef de cluster. Il est responsable de la communication à l'intérieur du cluster et à l'extérieur entre les différents clusters.

- *COIN: Clustering for Open IVC Network*

COIN est un mécanisme de regroupement conçu pour améliorer l'évolutivité du réseau. Il divise le réseau en clusters. Mais contrairement aux autres protocoles de cluster classiques, COIN sélectionne les clusters en fonction de trois paramètres : la mobilité des nœuds, la position des nœuds et le comportement des nœuds. Le protocole fournit une période de vie à chaque cluster. Le protocole de routage inter véhicules (IVC) gère les distances instables entre véhicules. Pour permettre à un chef de cluster et au nœud membre du cluster de continuer à communiquer efficacement pendant leur mobilité[2].

9 Sécurité dans les réseaux VANET

9.1 Les exigences de sécurité

- ***L'authentification***

C'est l'une des principales exigences de tout système de sécurité. Dans les réseaux VANET, il est très important de disposer de certaines informations concernant le nœud émetteur telles que son identification et celle de l'expéditeur du message comme ses propriétés et de son emplacement. Il est important d'authentifier tous les utilisateurs et les messages transitant par le réseau. Les contrôles d'authentification les niveaux d'autorisation des véhicules.

Dans les VANET, l'authentification empêche les attaques Sybil en attribuant une identité spécifique à chaque véhicule. Par exemple, éviter les embouteillages peut empêcher une seule voiture de prétendre être un ensemble de cent véhicules afin de donner l'illusion d'une route encombrée[17].

- ***L'intégrité***

L'intégrité garantit qu'un message n'a pas été modifié entre le moment où il a été envoyé et reçu car le message reçu doit correspondre au message envoyé. Le destinataire sera alors en mesure de confirmer l'identité de l'expéditeur au cours de la transaction. L'intégrité protège contre la création, la destruction ou l'altération non autorisées de données. Si un message corrompu est

accepté, la propriété d'intégrité est violée et le protocole serait considéré comme défectueux. Pour assurer l'intégrité du système, le système doit empêcher les attaquants de modifier les messages, car leur contenu doit être sécurisé[17].

- ***La confidentialité***

Lors de la communication entre entités (véhicule ou infrastructure), les entités extérieures ne sont pas en mesure de comprendre les informations confidentielles relatives à chaque entité du réseau. Ceci peut être réalisé grâce à un cryptage des messages protégeant les informations confidentielles de chaque conducteur telles que les profils d'utilisation et l'identité des utilisateurs. La confidentialité des messages dans les VANET dépend du scénario d'application spécifique. Par exemple, les messages relatifs à la sécurité ne contiennent pas d'informations sensibles. Leur cryptage est donc inutile. Cependant, certaines applications comme les paiements de péage, les véhicules vont utiliser un service Internet de RSU, les informations doivent rester confidentiels au moyen de systèmes de cryptage[17].

- ***La disponibilité***

Le réseau et les applications doivent rester opérationnels même en présence de pannes ou de conditions malveillantes. Cela nécessite non seulement une conception sécurisée mais également tolérante aux pannes, une résilience aux attaques, ainsi que des protocoles viables, qui reprennent leurs activités normales après le retour au fonctionnement régulier du réseau. Un protocole de routage adéquat est nécessaire pour atteindre tous les destinataires requis qui peuvent être inconnus de l'expéditeur[17].

- ***La non-répudiation***

La non-répudiation facilitera l'identification des attaquants, même après l'attaque. Toutes les informations relatives à la voiture telles que : l'itinéraire, la vitesse, le temps, toute violation seront stockées dans un équipement appelé TPD (Temper Proof Device), toute entité a une autorisation officielle (exp. La police) pourra récupérer ces données[18].

- ***Temps réel***

Les véhicules se déplacent avec une vitesse importante, cela nécessitera une réaction en temps réel dans certaines situations. Pour satisfaire cette contrainte les réseaux VANET reposent sur la norme émergente pour les communications dédiées à courte portée (DSRC), basée sur une extension de la technologie IEEE 802.11[18].

- ***L'intimité (Privacy)***

C’est de garder les informations des conducteurs à l’abri des observateurs non autorisés, telles que l’identité réelle, le trajet, la vitesse, etc. L'intimité peut être obtenue en utilisant des clés temporaires (pseudonymes). Ces clés seront changées fréquemment, chaque clé pouvant être utilisée uniquement une fois et expire après utilisation, toutes les clés seront stockées dans le TPD (Tamper Proof Device) et seront rechargées à nouveau lors de la prochaine vérification officielle du véhicule[18].

9.2 Entités impliquées dans la sécurité de VANETs

I.1.1.a Le conducteur

Le conducteur est l'élément le plus important de la chaîne de sécurité de VANET parce qu'il est omniprésent et qu'il doit prendre des décisions essentielles. En outre, tous les cas d'utilisation actuellement prévus pour les applications VANET font du conducteur un interlocuteur interactif avec les systèmes d'aide à la conduite[3].

I.1.1.b Le véhicule (OBU)

Bien qu'il ne reflète pas la réalité, l'OBU fait référence au conducteur et au véhicule à l'époque dans la littérature. Dans un réseau VANET, on peut distinguer deux types de véhicules : les véhicules ordinaires qui existent parmi les nœuds du réseau et qui fonctionnent normalement, et les véhicules malveillants[3].

I.1.1.c Unité d'accompagnement routier (RSU RoadSide Unit)

Comme dans le cas de l'OBU, on distingue les terminaux RSU normaux, qui fonctionnent de manière normale, et les terminaux RSU malveillants [3].

I.1.1.d Tiers

Les tiers (de confiance ou de semi-confiance), tous les équivalents numériques des parties prenantes d'une manière directe dans le système de transport intelligent. Parmi ces tiers, nous citons : le régulateur des transports, les constructeurs automobiles, la police de la circulation et les juges [3].

I.1.1.e L'attaquant

Dans le contexte de la sécurité de VANET, l'attaquant est une (ou plusieurs) entité(s) de compromis qui veut violer avec succès la sécurité des véhicules légitimes en utilisant plusieurs

techniques pour atteindre son but. Un attaquant peut aussi être un groupe de véhicules qui coopèrent ensemble [3].

9.3 Les types des véhicules malveillants

Dans les réseaux VANET, les véhicules malveillants lancent des attaques sur des véhicules légitimes de plusieurs manières. Les véhicules malveillants ou attaquants sont classés comme suit :

9.3.1 Interne vs Externe

Les nœuds externes sont des nœuds qui n'appartiennent pas aux réseaux VANET car ils ne sont pas authentifiés sur le réseau. Il est assez difficile pour un nœud externe de faire une attaque. Les attaques montées par les nœuds internes sont difficiles à détecter, car un nœud interne est un membre légitime du réseau. Il y a deux types des nœuds malveillants internes :

Un nœud authentifié, membre à part entière du réseau, et titulaire d'une clé publique authentifiée. Il a accès à tous les détails relatifs aux connaissances disponibles sur le réseau. Ce type de nœuds a la possibilité de commettre toutes sortes d'attaques sur le réseau.

L'autre type du nœud malveillant interne est l'industriel qui peut être des unités mécaniques ou des entités de la chaîne de montage de l'industrie automobile dotées de la capacité de mettre à jour le firmware du véhicule. Cela pourrait leur donner la possibilité d'injecter un programme malveillant dans le système commis par des étrangers [19].

9.3.2 Malveillant vs Rationnel

Un attaquant malveillant utilise diverses méthodes pour endommager les nœuds membres et créer un dysfonctionnement global du réseau sans rechercher son avantage personnel. Au contraire, un attaquant rationnel cherche un avantage personnel des attaques[19].

9.3.3 Actif vs Passif

Un nœud actif est celui qui peut envoyer, modifier ou supprimer des messages pour endommager d'autres nœuds ou à une partie du réseau. Généralement, cet attaquant est autorisé à opérer sur le réseau. De plus, les nœuds actifs ayant le statut d'un nœud interne peuvent commettre presque n'importe quel type d'attaque sur le réseau VANET.

En outre, les nœuds passifs écoutent simplement les communications entre les autres nœuds du réseau. Ce type d'attaquant n'a pas besoin d'être membre du réseau. Il surveillera le réseau et essaiera de trouver des informations sur le réseau. Bien que cela ne puisse pas endommager

directement le réseau, les informations rassemblées pourraient être utilisées pour de futures attaques. En général, les nœuds passifs sont également des nœuds externes[17].

9.4 Les attaques sur les réseaux VANET

On va présenter les attaques par rapport à leur impact sur les exigences de la sécurité dans les réseaux VANET.

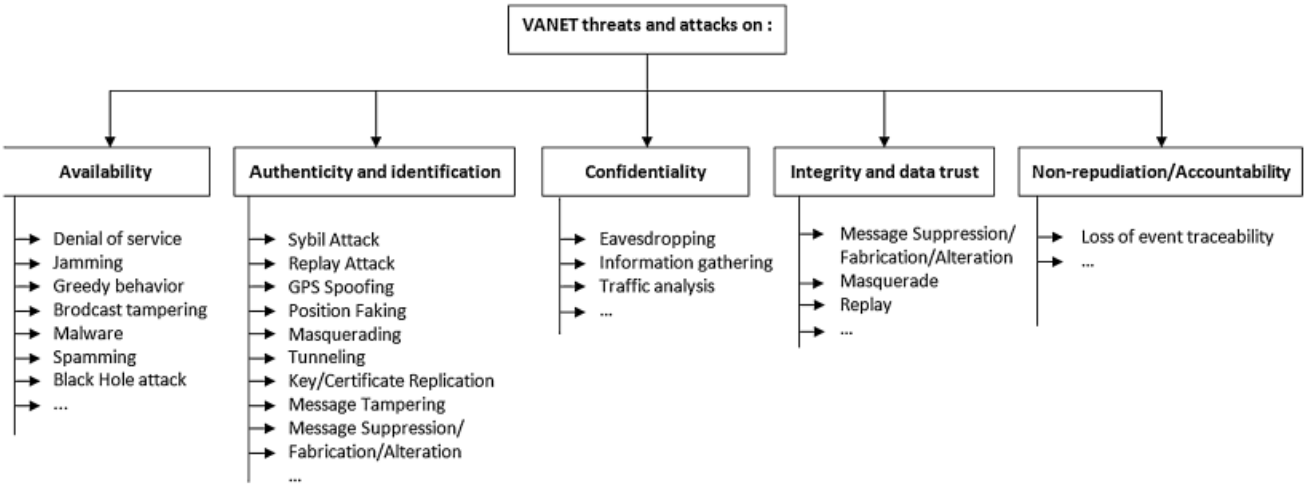

Figure I.6:Les attaques sur les réseaux VANET [18]

9.4.1 Les attaques sur la disponibilité

- *DoS (Déni de Service)*

Cette attaque se produit lorsque l'attaquant prend le contrôle des ressources d'un véhicule ou bloque le canal de communication utilisé par le réseau de véhicules, empêchant ainsi les informations critiques d'arriver. Cela augmente également le danger pour le conducteur s'il doit dépendre des informations de l'application[18].

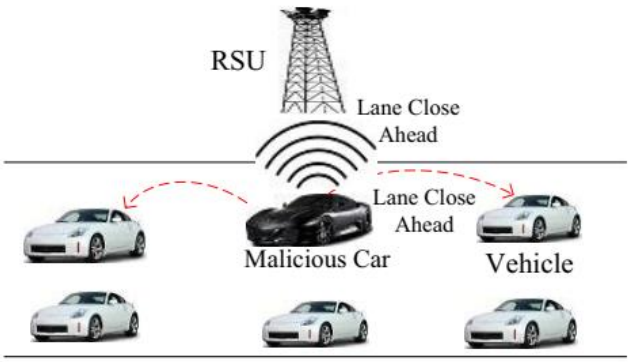

Figure I.7: Déni de Service

- *DDoS (Déni de Service Distribué)*

L'attaque DDOS est générée en gérant l'attaque DOS de manière distribuée. Dans l'attaque DDOS, l'attaquant multiple cible un ou plusieurs services à partir de plusieurs emplacements pour créer un dysfonctionnement dans le réseau. Dans cette attaque, un plus grand nombre de nœuds malveillants bloquent l'accès des autres utilisateurs légitimes aux services. Les attaquants augmentent la latence de transmission inutile du réseau en envoyant des messages spam sur le réseau[20].

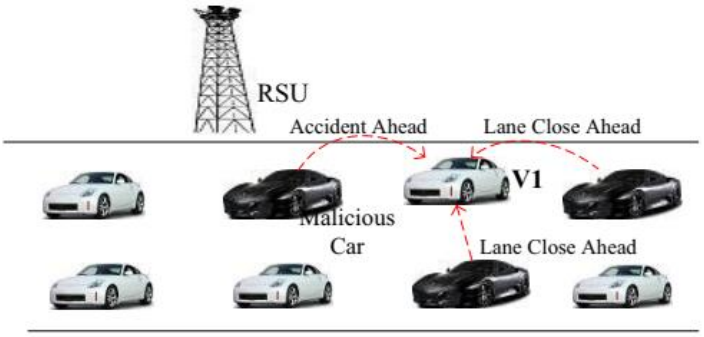

Figure I.8: Déni de Service Distribué

- *L'attaque de trou noir (Blackhole attack)*

Un trou noir est une zone du réseau où le trafic réseau est redirigé. Toutefois, soit il n'y a pas de nœud dans cette zone, soit les nœuds résident dans cette zone refusent de participer au réseau. Cela entraîne la perte de paquets de données. La figureI.9 illustre une attaque de trou noir où le trou noir est formé par un certain nombre de nœuds malveillants, qui refuse de transmettre les messages reçus des voitures légitimes C et D aux voitures E et F[21].

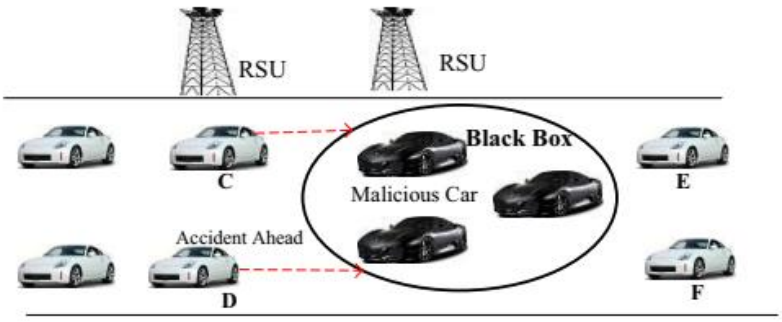

Figure I.9: L'attaque de trou noir

- *L'attaque du trou de ver (Wormhole attack)*

C'est aussi le type d'attaque de routage dans lequel le nœud malveillant de l'attaquant reçoit des paquets de données de l'utilisateur légitime à n'importe quel point du réseau et les achemine vers l'autre point du réseau, puis les tunnelise. Le tunnel créé entre deux nœuds malveillants s'appelle une attaque par trou de ver. La figure I.10 montre l'attaque de trou de ver dans VANET.

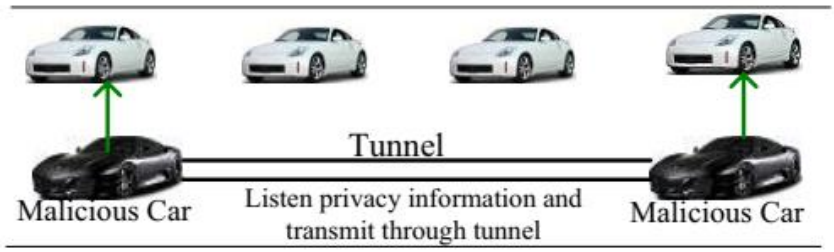

Figure I.10: L'attaque du trou de ver

- *Malware et spam (Malware attack)*

Les attaques de logiciels malveillants et de spam, tels que les virus et le spam, peuvent provoquer de graves perturbations dans les opérations normales de VANETs. Les attaques de logiciels malveillants et de Spam sont normalement exécutées par des membres de l'équipe malveillante plutôt que par des personnes malveillantes[19].

- *L'attaque de brouillage (Jamming attack)*

L'attaque de brouillage est un niveau physique d'attaque de déni de service. Le brouillage dans sa définition de base est la transmission d'un signal pour perturber le canal de communication, il est généralement intentionnel. Cela réduit le rapport signal/bruit (SNR : Signal to Noise Ratio) du récepteur. Le brouillage non intentionnel est appelé " interférence " et se produit lorsqu'une transmission est effectuée dans une bande de fréquences qui est déjà utilisée et opérationnelle. Pour une attaque de brouillage adaptative réussie, le brouilleur doit agir en même temps que le signal utile au brouillage. Il doit également choisir le modèle de transmission de signal le plus efficace qui fusionne le mieux le récepteur[3].

- *L'attaque de comportements gourmands (Greedy behavior attack)*

C'est une attaque sur la fonctionnalité de la couche MAC selon l'architecture du modèle OSI. Le nœud gourmand ne respecte pas la méthode d'accès au canal et essaie toujours de se connecter au média. Le but principal est d'interdire à d'autres nœuds d'utiliser le support et les

services. Un nœud au comportement gourmand tente également de minimiser son temps d'attente pour un accès plus rapide au canal et de pénaliser les autres nœuds non compromis. Un comportement gourmand provoque des problèmes de surcharge et de collision sur le support de transmission, ce qui entraîne des retards dans les services aux utilisateurs autorisés[3].

- *L'attaque de trou gris (Grayhole attack)*

Cette attaque consiste à ne supprimer que les paquets de données de certaines applications qui sont vulnérables à la perte de paquets. Cette attaque est considérée comme une variante de l'attaque de trou noir [3].

- *L'attaque par l'évier (Sinkhole attack)*

Cette attaque consiste à ce que le nœud malveillant attire les nœuds voisins pour que leurs paquets passent par lui, ce qui permet d'éliminer ou de modifier les paquets reçus avant de les retransmettre éventuellement. L'attaque de l'évier peut être utilisée pour monter d'autres attaques comme Trou Gris et Trou Noir [3].

- *L'attaque de sabotage de diffusion (Broadcast tampering attack)*

Dans ce type d'attaque, l'attaquant tente de créer et d'injecter de faux messages d'alerte de sécurité dans le réseau. Cela peut cacher les vrais messages de sécurité aux utilisateurs légitimes, cela peut aussi causer des accidents et affecter sérieusement la sécurité globale du réseau. En général, ce type d'attaque est possible pour un nœud légitime[3].

I.1.1.f Les attaques sur l'authenticité

- *Attaque Sybil (Sybil attack)*

Dans une attaque Sybil, l'attaquant crée de multiples identités de nœuds qui diffusent les mauvaises informations dans le réseau. Dans ce type d'attaque, les données sont diffusées avec une identité falsifiée. Ce type d'attaque mise en œuvre par le véhicule attaquant sur un autre véhicule légitime pour obtenir les différents avantages. Dans cette attaque, le véhicule attaquant créer des identités multiples et envoyer les messages à l'utilisateur légitime comme si il y a un plus grand trafic sur la route sélectionné afin de changer l'itinéraire[20].

- *Global Positioning System (GPS) Spoofing*

Le satellite GPS maintient une table de localisation avec l'emplacement géographique et l'identité des véhicules dans le réseau. Un attaquant peut produire de fausses lectures dans le système de positionnement GPS pour tromper les véhicules et leur faire croire qu'ils se trouvent

à un autre endroit. Les attaquants utilisent le simulateur de satellite GPS pour générer des signaux qui sont plus forts que ceux générés par le système de satellite actuel [19].

- *L'attaque d'usurpation d'identité (Node impersonation attack)*

Chaque véhicule possède un identifiant réseau qui permet de le distinguer des autres nœuds du réseau VANET. Cet identifiant devient particulièrement important en cas de problèmes. Dans l'attaque d'usurpation d'identité, l'attaquant obtient une pièce d'identité valide et passe pour un autre véhicule légitime sur le réseau. Ceci constitue une violation du processus d'authentification dans le réseau[3].

- *L'attaque par tunnel (Tunnelling attack)*

Dans cette attaque, les attaquants utilisent le même réseau pour établir une connexion privée (tunnel). L'attaque par tunnel relie deux parties distantes du réseau de véhicules en utilisant un canal de communication supplémentaire comme un tunnel. Ainsi, les victimes de deux parties distantes du réseau peuvent communiquer en tant que voisins [3].

- *L'attaque de réplication de clé et/ou de certificat (Key and/or Certificate Replication attack)*

L'attaque consiste à utiliser des doubles de clés et/ou de certificats qui servent de preuve d'identification et à créer une ambiguïté qui rend plus difficile l'identification d'un véhicule par les autorités, en particulier en cas de litige[3].

I.1.1.g Les attaques sur la confidentialité

- *Attaque par écoute (Eavesdropping attack)*

Dans les réseaux sans fil tels que les VANET, l'écoute des médias est une attaque facile à réaliser. De plus, elle est passive et la victime n'est pas au courant de la collection. Une attaque par écoute est une attaque sur la confidentialité, elle est sans impact imminent sur le réseau. Cette attaque permet de recueillir plusieurs types d'informations utiles, telles que des données de localisation qui peuvent être utilisées pour le suivi des véhicules [3].

- *Attaque par analyse de trafic (Traffic analysis attack)*

Dans un réseau VANET, l'attaque d'analyse de trafic est une menace passive sérieuse contre la confidentialité et la vie privée des utilisateurs. L'attaquant analyse les informations collectées après une phase d'écoute du réseau, il tente d'extraire le maximum d'informations utiles à ses propres fins [3].

I.1.1.h Les attaques sur l'intégrité

- *L'attaque déguisée (Masquerading attack)*

Un véhicule simule son identité et se fait passer pour un autre véhicule à son propre avantage. Elle est réalisée par la création, la modification et la relecture des messages. Par exemple, un véhicule malveillant ou un agresseur peut faire semblant d'être une ambulance pour escroquer d'autres véhicules afin de les ralentir[19].

- *Attaque par rediffusion (Replay attack)*

Il s'agit d'une attaque classique, elle consiste à rediffuser un message déjà envoyé pour en bénéficier au moment de sa soumission. Par conséquent, l'attaquant l'injecte à nouveau dans les paquets réseau reçus précédemment. Cette attaque peut être utilisée par exemple pour rediffuser des trames de balises, afin que l'attaquant puisse manipuler la position et les tables de routage des nœuds. Contrairement à d'autres attaques, l'attaque de rediffusion peut être effectuée par des utilisateurs non légitimes[3].

- *Falsification/suppression /Fabrication/ modification des messages (Message Tampering/Suppression/Fabrication/Alteration)*

Comme son nom l'indique, cette attaque contre l'intégrité consiste à modifier, supprimer, construire ou altérer des données existantes. Elle peut se produire en modifiant une partie spécifique du message à envoyer. Par exemple, l'attaquant falsifie les données reçues indiquant que l'itinéraire est encombré et les modifie pour tromper les utilisateurs, ce qui indique qu'il n'y a pas de congestion et que la circulation sur la route est normale. Dans cette attaque, l'attaquant peut également supprimer une partie du message, modifier ou créer de nouveaux messages qui l'aident à atteindre son but prévu de l'attaque[3].

Les attaques déguisées, la retransmission, la falsification/suppression/fabrication/ modification et l'illusion de messages peuvent également être considérés comme des attaques contre l'authenticité et l'identification.

I.1.1.i Les attaques sur la non-répudiation

- *Perte de traçabilité des événements (Loss of events traceability)*

La traçabilité consiste à identifier les acteurs et les actions, notamment en matière de sécurité. L'attaque consiste à supprimer les traces d'actions pour créer une confusion pour l'entité d'audit, l'attaquant après des actions malveillantes ou l'attaque efface toutes les traces [21].

I.1.1.j Les attaques sur la vie privée

- *Suivi de localisation (Location Trailing)*

Cette attaque viole la propriété privée. Dans ce cas, l'attaquant traque le véhicule et obtient les informations confidentielles sur le conducteur en suivant illégalement la position ou l'itinéraire suivi par la voiture.

Les attaques sur la confidentialité peuvent toucher la vie privée des utilisateurs du réseau VANET [21].

I.1.1.k Autres attaques

- *Timing Attack*

Transmettre des données au bon moment d'un véhicule à un autre véhicule est très important pour assurer l'intégrité et la sécurité des données. Dans les attaques de timing, chaque fois que des véhicules malveillants reçoivent un message d'urgence, ils ne le transmettent pas aux véhicules voisins au bon moment, mais ils ajoutent des intervalles de temps au message original pour créer un délai. Ainsi, les véhicules voisins des attaquants reçoivent le message après qu'ils en aient réellement besoin [19].

- *Fausse information*

Les attaquants peuvent transmettre des informations incorrectes ou bidon dans le réseau pour leur avantage. Par exemple, un attaquant peut transmettre des informations erronées sur les conditions de circulation afin de faciliter ses déplacements sur la route. Cette attaque est liée aux exigences de sécurité de l'authentification [19].

- *L'attaque du l'homme du milieu (Man in the Middle Attack MiMA)*

L'attaque du l'homme du milieu peut être atteint dans plusieurs contextes. Comme son nom l'indique, l'attaquant est inséré entre l'émetteur et le récepteur. Dans le cas des VANETs, l'attaquant est un véhicule qui est inséré entre deux véhicules qui communiquent. L'agresseur contrôle la communication entre les deux victimes, alors qu'elles pensent qu'elles sont en communication directe l'une avec l'autre. Dans la littérature, l'homme au milieu de l'attaque est utilisé pour violer les mécanismes d'authentification et/ou d'intégrité et de non-répudiation [21].

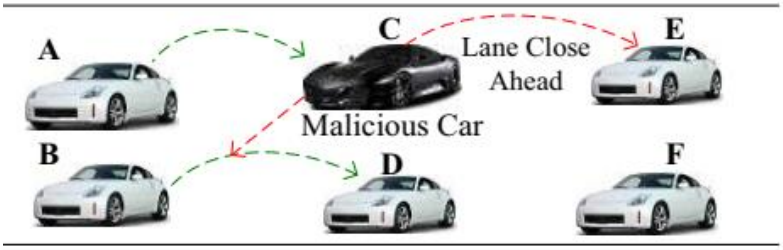

Figure I.11: L'attaque du l'homme du milieu

10 Conclusion

L'invention de réseaux ad hoc de véhicules constitue des véhicules, appelés ici nœuds capables d'établir une communication sans fil avec d'autres nœuds, transformant ainsi le réseau en un maillage auto-organisé et partagé. Ce réseau ouvert de véhicules est appelé VANET, ce qui donne de nombreuses applications pour rendre l'expérience de la route plus efficace, plus sûre, plus convaincante, plus efficace, plus facile et plus agréable en réduisant le temps de déplacement, la congestion routière, en augmentant la capacité routière, en évitant les zones congestionnées et les situations d'urgence etc.

Ce chapitre donne un aperçu générale les réseaux VANET, où nous avons commencé par une présentation d'une manière générale du réseau, ensuite nous avons enchainé avec les protocoles de routage suivi par un survol sur les aspects de la sécurité.

Les réseaux vanet sont la première composante du réseau véhiculaire en cloud, le chapitre suivant va être consacré à la deuxième composante du réseau véhiculaire en cloud, qui est le cloud computing.

Chapitre II

Le Cloud Computing

1 Introduction

Aujourd'hui, dans un monde interconnecté, toute entreprise a besoin d'une politique de sécurité bien pensée. La croissance rapide de l'ère de l'information a considérablement modifié la nature de l'informatique et donne lieu à un nouvel ensemble de préoccupations et de problèmes de sécurité. Selon le National Institute of Standards and Technology (NIST), la politique de sécurité est définie comme " l'ensemble des directives, règlements, règles et pratiques ". qui prescrit la façon dont une organisation gère, protège et distribue l'information Pour la réalisation technologique du Cloud Computing, l'objectif d'un est de protéger les personnes et l'information, d'établir des règles pour le comportement attendu des utilisateurs, de minimiser les risques et de surveiller la conformité aux règlements. Considérant le fait que, ces derniers temps, tous ceux qui s'intéressent aux technologies de l'information sont tombés sur le terme Cloud Computing, il est vraiment important d'examiner sérieusement les questions de sécurité dans le Cloud Computing : Existe-t-il des menaces de sécurité dans le Cloud Computing qui n'apparaissent pas dans les systèmes non Cloud ? Le Cloud est-il sûr et sécurisé pour les utilisateurs ? Alors que le Cloud Computing gagne en popularité, nous tentons de démystifier les risques de sécurité et de protection de la vie privée qui sont introduits, en raison de sa nature transformationnelle. Le succès d'une politique de sécurité dans le Cloud dépend vraiment de la façon dont les contenus de sécurité sont adressés.

Comme la plupart des technologies, le Cloud Computing a évolué à partir d'un besoin. Le la formidable croissance du Web a donné naissance à une nouvelle classe de "Web-scale". Comme la quantité de plus en plus grande d'information disponible dans les bases de données de l'Internet ou la création d'un espace de stockage plus grand dans les serveurs et l'utilisation d'un plus grand nombre d'applications cloudbased stockage sur de longues distances.

2 Définition

La définition de l'informatique en nuage « Cloud Computing » évolue avec l'évolution de la technologie et de ses services. Aucune définition standard pour l'informatique en nuage n'a encore été convenue, d'autant plus qu'elle englobe tant de modèles différents et de marchés potentiels, selon les fournisseurs et les services.

La définition la plus simple de « Cloud Computing » est essentiellement l'informatique basée sur Internet. Le terme "nuage" est utilisé comme une métaphore pour l'Internet, et est venu du dessin de nuage bien connu qui a été utilisé dans les diagrammes de réseau pour représenter l'infrastructure de réseau sous-jacente d'Internet. Le calcul dans l'Internet est fait par des

groupes de serveurs partagés qui fournissent à la demande des ressources matérielles, des données et des logiciels aux appareils connectés au réseau [22].

L'Institut national des normes et de la technologie NIST (The National Institute of Standards and Technology), donne une définition plus formelle: «le Cloud Computing est un modèle pour permettre un accès réseau pratique et à la demande à un réseau partagé de ressources informatiques configurables (par exemple, réseaux, serveurs..) qui peuvent être rapidement provisionnés et libérés avec un effort de gestion minimal ou une interaction entre les prestataires de services» [23]

3 Technologies connexes

Le paradigme de l'informatique dans les nuages à la contribution de nombreuses technologies telles que le calcul parallèle, le calcul en grille, le calcul utilitaire, la virtualisation, l'informatique autonome, l'informatique omniprésente, le logiciel en tant que service, le Web 2.0, l'informatique distribuée et le Web 2.0. Nous expliquerons quelques-unes des technologies liées à l'informatique dans les nuages.

3.1 Le Calcul parallèle

Le concept du calcul parallèle consiste à diviser le problème de calcul qui est un problème scientifique en de nombreuses petites tâches, et à les exécuter en même temps sur un ordinateur parallèle. Généralement, le calcul parallèle est utilisé chaque fois que l'on a besoin d'une puissance de calcul élevée, par exemple dans le domaine de l'exploration énergétique, militaire, médicale et biotechnologique. Un ordinateur parallèle est un ensemble d'unités de traitement homogènes, capables de résoudre plus rapidement de gros problèmes de calcul grâce à la collaboration et à la communication [24].

3.2 Calcul distribué (Grid Computing)

La grille est la technique utilisée pour déplacer la surcharge de travail vers l'endroit qui nécessite l'utilisation de ressources informatiques distantes et immédiatement disponibles. Elle est divisée en plusieurs sous-tâches à exécuter en parallèle, des applications sont également requises par la grille pour vérifier les interfaces logicielles de la grille [24].

3.3 L'informatique utilitaire (Utility Computing)

Il fournit les ressources en fonction de la demande du client et les charge en fonction de l'utilisation. Elle utilise un système de tarification entièrement fondé sur les services publics

pour facturer des frais raisonnables à ses clients. Grâce à la capacité de fournir les ressources à la demande et à un schéma entièrement basé sur la tarification, l'informatique utilitaire maximise l'utilisation des ressources et minimise le coût de la fourniture des ressources [24].

3.4 Virtualisation (Virtualization)

La technologie de virtualisation est présentée depuis 40 ans en arrière, mais il y avait une limitation pour l'application de la virtualisation par les technologies, la limitation a été exposée à dépendre du cloud computing comme une technologie majeure. La virtualisation est une technologie qui sépare le matériel physique sous-jacent et fournit des ressources virtualisées aux applications. Un serveur typique est capable d'héberger un certain nombre d'instances de machines virtuelles, donnant ainsi la possibilité de personnaliser le logiciel à la demande. Il s'agit donc de la technologie qui consiste à fournir le serveur virtuel au client à la demande comme VMware, vCloud, Amazon EC2 et d'autres... La virtualisation est la base de l'informatique en nuage, car elle permet la mise en commun des ressources informatiques à partir d'un groupe de serveurs qui sont des clusters et affecte dynamiquement les ressources virtuelles au client selon les besoins et les réassigne une fois non nécessaires. La virtualisation est une technologie attrayante en raison de la capacité d'isolement et de personnalisation des environnements avec peu d'impact sur les performances [24].

3.5 L'informatique autonome (Autonomic Computing)

Présenté en 2001 par IBM, il est construit de nombreux systèmes informatiques pour leur permettre de faire de l'autogestion tels que des observations automatiques à l'externe et à l'interne et agissant sans aucune interaction humaine. Le but principal de l'informatique autonome est de contrôler la complexité des systèmes informatiques. L'informatique dans les nuages possède également une autre caractéristique puissante qui est l'approvisionnement automatique des ressources afin de réduire le coût des ressources plutôt que de diminuer la complexité du système [24].

3.6 L'informatique omniprésente (Ubiquitous Computing)

L'idée de l'informatique omniprésente a été présentée par Mark Weiser en 1988 et a prédit que cette méthode serait omniprésente. En 1990, les gens ont reçu une grande attention au concept de l'informatique omniprésente et se sont passionnés petit à petit pour l'idée de l'informatique omniprésente. Officiellement, le concept a été proposé par IBM en 1999. En 1999, la première session a été organisée par IBM. En 2000, la première conférence internationale sur

l'informatique omniprésente a eu lieu. De plus, la revue IEEE Pervasive Computing est fondée en 2002. L'un des nombreux objectifs importants de l'informatique omniprésente est de permettre à l'équipement informatique de sentir les changements dans l'environnement et de modifier ses comportements en fonction de ces changements. La technologie des réseaux radio a été utilisée dans l'informatique omniprésente afin de permettre aux utilisateurs d'accéder à l'information sans aucune limitation de lieu et de temps [24].

3.7 Logiciel en tant que service (Software as a Service)

Il s'agit d'une application logicielle basée sur le Web qui fournit un logiciel aux abonnés, SaaS est un modèle d'attribution de logiciel dans lequel les applications ont été conçues pour être fournies par le réseau. Ce modèle a presque le prix d'un forfait tel que le paiement mensuel, ce paiement mensuel couvrira le coût de maintenance des applications, les frais de licence et le coût du support technique. Le modèle SaaS peut être considéré comme la meilleure option pour utiliser les technologies avancées pour les petites et moyennes entreprises [24].

4 Caractéristiques du Cloud Computing

Une autre façon de définir l'informatique dans les nuages est d'examiner ses caractéristiques :

• ***Ressources partagées (Shared resources)***: u ce que le NIST appelle le partage de ressources, où aucune ressource n'est dédiée à un utilisateur mais sont plutôt mises en commun pour servir plusieurs consommateurs [23].

• ***Libre-service à la demande (On-demand self-service)***: Les utilisateurs peuvent s'attribuer des ressources supplémentaires telles que la puissance de stockage ou de traitement automatiquement et sans intervention humaine. C'est comparable à l'informatique autonome où le système informatique est capable de s'autogérer [24].

• ***Élasticité (Elasticity):*** avec l'auto-approvisionnement des ressources, le cloud computing se caractérise par la capacité de localiser et de libérer rapidement les ressources. Cela permettra aux consommateurs d'augmenter à tout moment les ressources dont ils ont besoin pour faire face aux charges lourdes et aux pics d'utilisation, puis de les réduire en retournant les ressources dans le regroupement une fois terminées [24].

• ***Le paiement au fur et à mesure (Pay as you go):*** Appelé aussi le service mesuré. Le cloud computing est proposé comme un service public pour lequel les utilisateurs paient sur la base de la consommation, un peu comme n'importe quel autre service public payant comme l'électricité, le gaz et l'eau [24].

Large accès au reseau (Broad Network Access): Les ressources du Cloud Computing sont accessibles et livrables via le réseau et sont utilisées par de nombreuses applications clientes avec différents types de plates-formes (telles que les téléphones mobiles et les PDA) [24].

Le regroupement des ressources (Resource Pooling): Les ressources du fournisseur sont collectées pour être utilisées par plusieurs clients en utilisant un type multi-locataires, avec différentes ressources qui sont affectées et réaffectées dynamiquement selon l'ordre du client[24].

5 L'architecture du Cloud Computing

5.1 Le modèle en couche du cloud computing

Comme le montre la figure II.1, le cloud computing comprend une architecture à quatre couches, chaque couche de l'architecture cloud ayant la souplesse nécessaire pour coopérer avec les couches supérieures et inférieures. Nous les illustrerons tous comme suit :

5.1.1 La couche application

La couche application est responsable de l'exécution des applications de cloud sur le PC du client. Les applications de cette couche peuvent atteindre la mise à l'échelle automatique pour obtenir une performance maximale. Les exemples de fournisseurs sont force.com, Microsoft et IBM [24].

5.1.2 Couche de plate-forme

Cette couche se réfère au système d'exploitation et aux logiciels. par ce service, le client peut s'assurer qu'il peut obtenir une plate-forme appropriée pour son application pour faire son travail comme le déploiement, le développement, l'hébergement d'application web, et faire des tests. L'objectif principal de la couche plate-forme est de diminuer la charge de déploiement de l'application directement sur les conteneurs VM [24].

5.1.3 Couche infrastructure :

Il est responsable de fournir à l'utilisateur du matériel et des logiciels tels que la capacité du disque dur, la taille de la RAM, le CPU et autres. Grâce à la virtualisation.

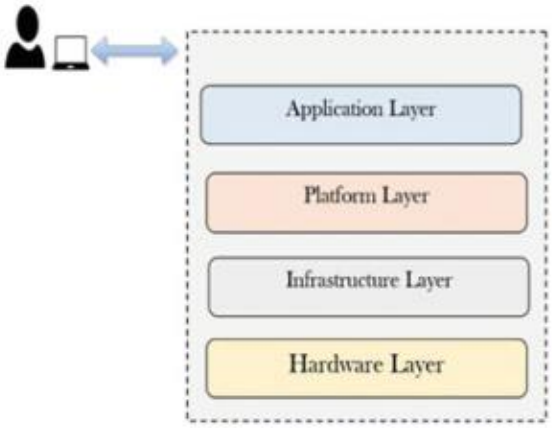

Figure II.1: Le modèle en couche du cloud computing[24]

5.2 Modèles de services de Cloud Computing

Les services fournis par le cloud computing peuvent être classés en trois modèles de services :

Software as à Service (SaaS), Platform as a Service (PaaS) et Infrastructure as a Service (IaaaS). Ces trois modèles sont souvent abrégés en tant que Service SPI (SPI est l'abréviation de Software, Platform and Infrastructure) et constituent la base de tous les services fournis par le cloud computing :

5.2.1 Software as a Service (SaaS)

Dans ce modèle, le logiciel est fourni par le fournisseur sur le réseau sous la forme d'un modèle un-à-plusieurs (une seule instance, architecture multi-locataires) en remplacement du modèle un-à-un typique. Au lieu d'acheter le logiciel et de l'installer sur leur système, les utilisateurs louent le logiciel en payant à l'utilisation ou un abonnement [22].

Exemples : Google Docs et Salesforce.com

5.2.2 Platform as a Service (PaaS)

La technologie est nécessaire à la création d'un logiciel pouvant fonctionner dans le cloud oblige les fournisseurs à créer un environnement ou une plate-forme de développement sur laquelle ces applications peuvent être exécutées. Le deuxième service fourni dans le cloud est l'utilisation de l'environnement de développement lui-même [22].

Exemples : Google Apps Engine et la plate-forme Azure de Microsoft.

5.2.3 Infrastructure as a Service (IaaS)

Dans le troisième service, les utilisateurs ont accès à des éléments de l'infrastructure de calcul elle-même. Grâce aux technologies Internet, les utilisateurs peuvent utiliser la puissance de traitement, les supports de stockage et les composants réseau nécessaires fournis par le fournisseur [22].

Exemples : Amazon.com, EC2 et S3.

6 Composants du Cloud Computing

Les trois principales composantes de l'informatique dans les nuages sont : Clients, centre de données et serveurs distribués comme indiqué à la figure II.2. Chaque composante a une finalité et un rôle précis. Nous allons illustrer chacun d'entre eux comme suit :

6.1 Les acteurs

L'architecture de référence du NIST (National Institute of Standards and Technology) pour le cloud computing définit cinq acteurs majeurs : le consommateur, le fournisseur, l'opérateur, l'auditeur et le courtier du cloud computing. Chaque acteur est une entité (une personne ou une organisation) qui participe à une transaction ou à un processus et effectue des tâches dans le Cloud Computing [25].

Le tableau II.1 énumère brièvement les acteurs définis dans l'architecture de référence du NIST pour le cloud computing

Tableau II.1 : Les acteurs du cloud computing

Acteur	Définition
Le consommateur	Une personne ou une organisation qui a une relation d'affaires avec les fournisseurs de cloud computing pour utiliser les services de ces derniers.
Le fournisseur	Personne, organisation ou entité chargée de mettre un service à la disposition des parties intéressées.
L'auditeur	Une entité qui peut effectuer une évaluation indépendante des services cloud, de l'exploitation du système d'information, de la performance et de la sécurité de la mise en œuvre du cloud.

Le courtier	Une entité qui gère l'utilisation, la performance et la livraison des services cloud et négocie les relations entre les fournisseurs de Cloud et les consommateurs de Cloud.
L'opérateur	Un intermédiaire qui assure la connectivité et le transport des services cloud des fournisseurs de Cloud aux consommateurs du Cloud.

6.2 Centre de données

Les applications qui sont utilisées par les clients du cloud computing sont hébergées dans de nombreux serveurs, il peut s'agir d'un immeuble ou d'une salle dont il n'est pas nécessaire de se trouver sur place mais qui doit être accessible par l'Internet. Plusieurs machines virtuelles (VM) peuvent être exécutées ensemble sur un seul serveur physique connu sous le nom d'hôte, le nombre de VM sera limité par de nombreux facteurs tels que le type des applications qui sont exécutés sur serveur virtuel, la vitesse et la taille du serveur physique [24].

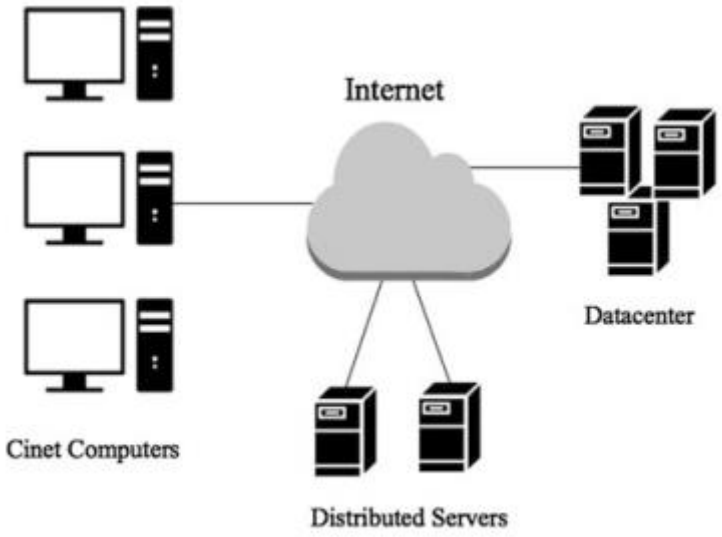

Figure II.2: Les composantes du cloud computing [24]

6.3 Serveurs distribués

Afin d'assurer la fiabilité et la disponibilité des serveurs, le cloud a réparti les serveurs dans les différentes zones géographiques. En cas de défaillance du serveur spécifique, un autre serveur prendra l'action, d'autre part, pour augmenter la scalabilité quand un serveur supplémentaire est nécessaire, un nouveau serveur sera ajouté.

7 Modèles de déploiement

7.1 Cloud privé

L'infrastructure en cloud est fournie pour l'usage exclusif d'une seule organisation comprenant plusieurs consommateurs (p. ex., des unités d'affaires). Il peut appartenir à l'organisation, à un tiers ou à une combinaison des trois, et être géré et exploité par l'organisation, et il peut exister sur le site ou hors site [25].

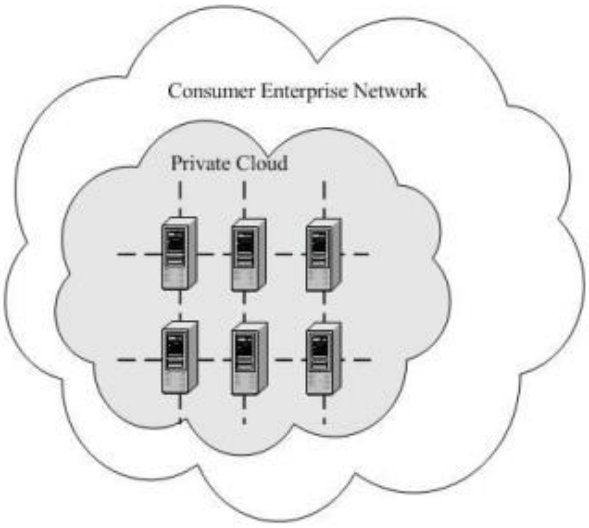

Figure II.3: Le cloud privé [25]

7.2 Le cloud communautaire

L'infrastructure dans ce type de cloud est fournie pour l'usage exclusif d'une communauté spécifique de consommateurs provenant des organisations qui ont des préoccupations communes. Il peut appartenir à un ou plusieurs organismes de la collectivité, à un tiers-partie ou à une combinaison de ces organismes, et il peut être géré et exploité par les organisations de la collectivité [25].

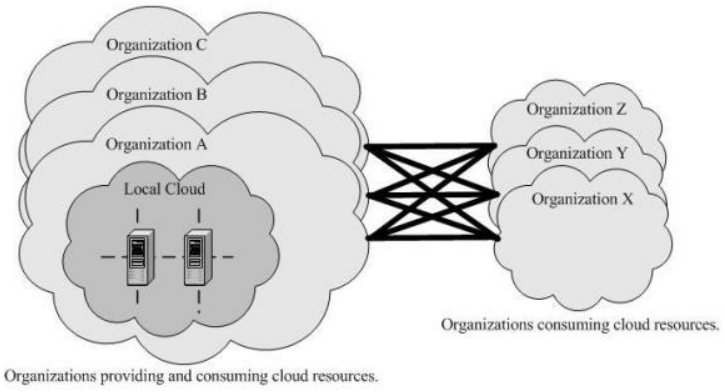

Figure II.4: Le cloud communautaire [25]

7.3 Le cloud publique

L'infrastructure du cloud publique est mise à la disposition du grand public pour une utilisation libre. Elle peut être la propriété d'une entreprise, d'un établissement d'enseignement ou d'un organisme gouvernemental, ou d'une combinaison de ceux-ci [25].

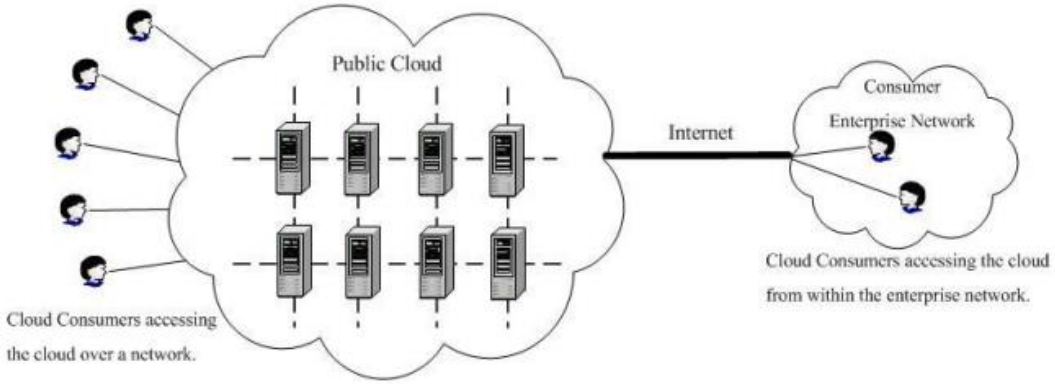

Figure II.5: Le cloud publique [25]

7.4 Cloud hybride

L'infrastructure du cloud publique est une composition de deux ou plusieurs infrastructures distinctes (privées, communautaires ou publiques) qui demeurent des entités uniques, mais qui sont liées entre elles par une technologie normalisée ou exclusive qui permet la portabilité des données et des applications [25].

8 Architectures de centres de données

Le regroupement des serveurs dans les centres de données d'aujourd'hui dépasse les 100 000 hôtes et environ 70 % de toutes les communications sont effectuées en interne. Cela crée un défi dans la conception de l'architecture de réseau interconnecté et de l'ensemble des protocoles de communication.

Étant donné l'échelle d'un centre de données, l'infrastructure réseau hiérarchique conventionnelle devient souvent un point de blocage en raison des limitations physiques et financières de l'équipement réseau utilisé. Plus précisément, la disponibilité des composants 10 Gigabit Ethernet (GE) et leur prix ont défini l'évolution des architectures des centres de données [26].

8.1 L'architecture à deux niveaux

Suivant la structure illustrée à la figure II.6, les serveurs de calcul (S) physiquement disposés en racks forment le réseau de niveau 1. Sur le réseau de niveau 2, les commutateurs de niveau 3 (L3) fournissent une connectivité à maillage complet à l'aide de liaisons 10 GE.

Le routage ECMP (Equal Cost Multi-Path) est utilisé comme technologie d'équilibrage de charge pour optimiser les flux de données sur plusieurs chemins. Il applique l'équilibrage de charge sur les paquets TCP et UDP sur une base de flux par flux en utilisant des techniques de hachage express ne nécessitant pratiquement aucun traitement à partir du processeur d'un commutateur. D'autres trafics, tels que ICMP, ne sont généralement pas traités par ECMP et transmis sur un seul chemin prédéfini.

L'architecture à deux niveaux a bien fonctionné pour les premiers centres de données avec un nombre limité de serveurs de calcul. Selon le type de commutateurs utilisés dans le réseau d'accès, les centres de données à deux niveaux peuvent prendre en charge jusqu'à 5500 nœuds. Le nombre de commutateurs centraux et la capacité des liens centraux définissent la largeur de bande réseau maximale allouée par serveur de calcul[26].

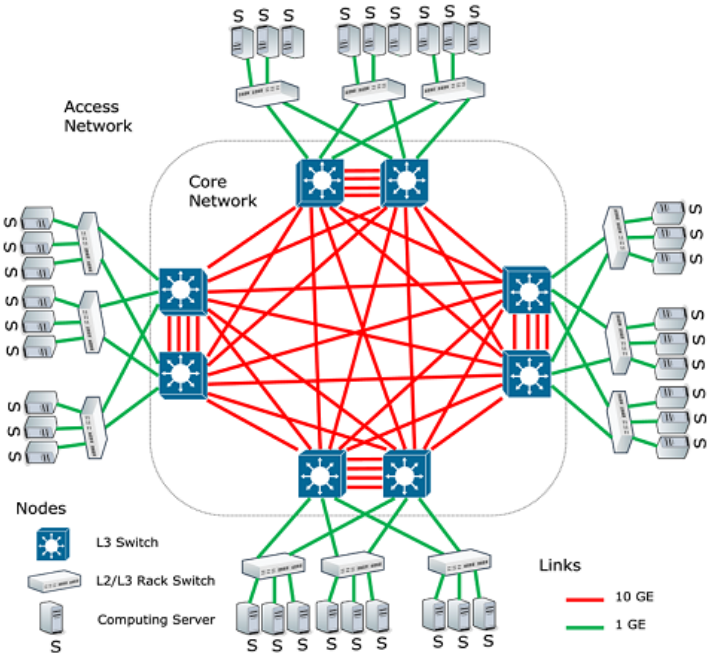

Figure II.6: L'architecture à deux niveaux [26]

8.2 L'architecture à trois niveaux

C'est l'architecture la plus courantes de nos jours. Ils incluent : (a) l'accès, (b) l'agrégation et (c) les couches centrales comme le montre la figure II.7. La disponibilité de la couche d'agrégation facilite l'augmentation du nombre de nœuds de serveurs (à plus de 10 000 serveurs) tout en conservant des commutateurs de couche 2 (L2) peu coûteux dans le réseau d'accès, ce qui fournit une topologie sans boucle.

Étant donné que le nombre maximum de chemins ECMP autorisés est de huit, une architecture typique à trois niveaux se compose de huit commutateurs centraux (seuls quatre sont présentés à la figure II.7).

Une telle architecture met en œuvre un ECMP à 8 voies qui comprend des Groupes d'agrégation de ligne (Line Aggregation Groups -LAG), qui permettent à un client réseau d'adresser plusieurs liens et ports réseau avec une seule adresse MAC.

Bien que la technologie LAG est une excellente méthodologie pour augmenter les capacités de liaison, son utilisation présente plusieurs inconvénients fondamentaux qui limitent la flexibilité et les performances du réseau. Les LAG rendent difficile la planification de la capacité pour les grands débits et la rendent imprévisible en cas de défaillance d'une liaison. En outre, plusieurs types de modèles de trafic, tels que la CIPD et la radiodiffusion, sont généralement acheminés par une seule liaison[26].

De plus, la connectivité full mesh au cœur du réseau nécessite un nombre considérable de câblages.

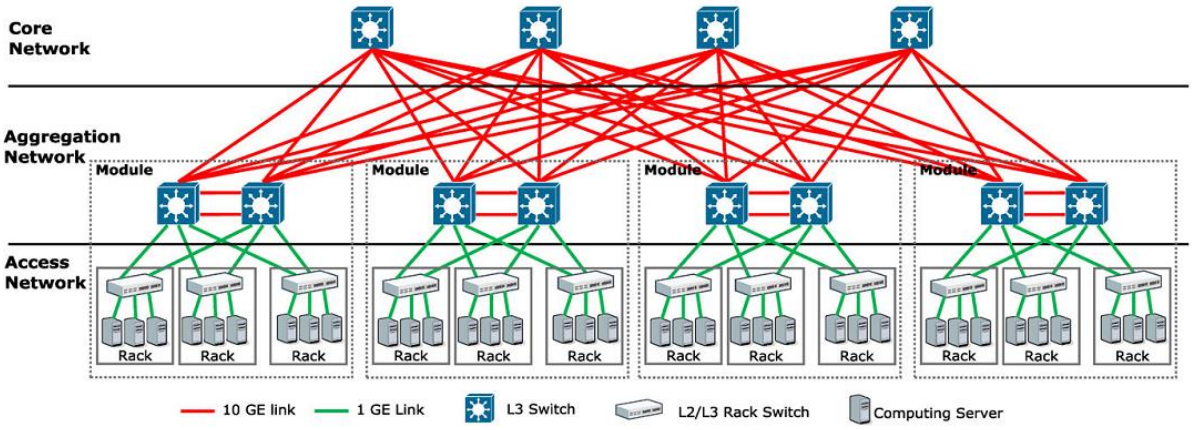

Figure II.7: L'architecture à trois niveaux [26]

8.3 Les approches de la fédération du cloud computing

La fédération du cloud se réfère à un maillage de fournisseurs de cloud qui sont interconnectés sur la base de standards ouverts pour fournir un environnement de calcul décentralisé et universel où tout est régi par des contraintes et des accords dans une infrastructure omniprésente et multi-fournisseurs. Jusqu'à présent, l'écosystème du cloud s'est caractérisé par l'émergence constante de centaines de fournisseurs indépendants et hétérogènes, qui offrent une variété de services à leurs clients. Dans cette sous-section, nous allons présenter les approches fédératives pertinentes que l'on trouve dans la littérature[27].

8.3.1 La vision InterCloud

C'est un ensemble de systèmes IaaS fédérés orientés services publics capables de prédire le comportement des services applicatifs pour des infrastructures intelligentes de down et up-scaling [28]. Cette forme de cloud est caractérisée par

- Une flexibilité de service
- Une qualité de service centré sur l'utilisateur
- L'intégration facile avec les système interne des entreprises
- Une surveillance modulable des composants du système

La figure montre un exemple d'une configuration intercloud

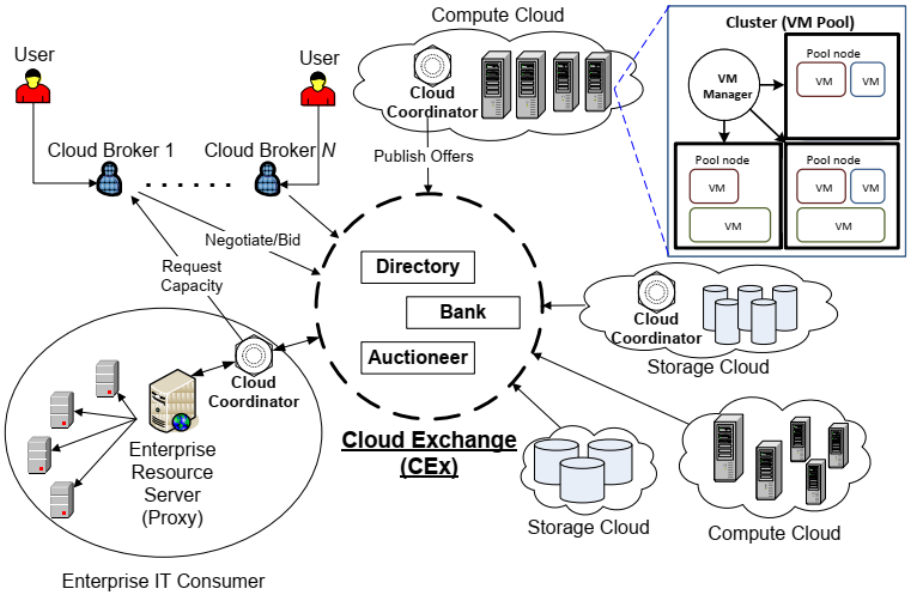

Figure II.8: Exemple d'une configuration intercloud[28]

8.3.2 Approche de fédération Cross-Cloud

C'est une approche de fédération de cloud générique, elle est basée sur une composante logicielle qui réalise la fédération du cloud en sur trois phases [29]:

- La phase de découverte au cours de laquelle l'information sur d'autres nuages est reçue et envoyée.
- La phase du rapprochement en effectuant le meilleur choix du fournisseur selon une mesure d'utilité
- La phase d'authentification pour la création d'un canal sécurisé entre les clouds fédérés

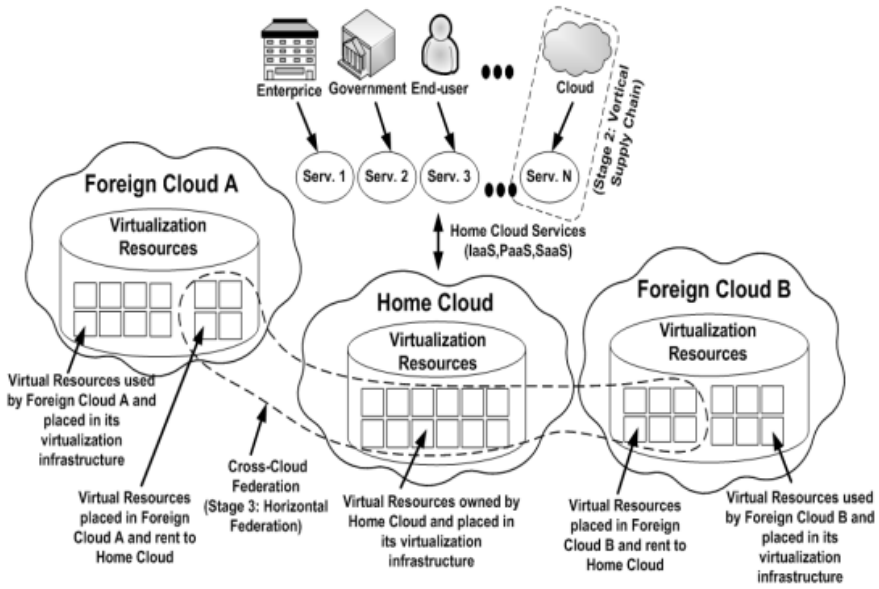

Figure II. 9: La fédération Cross-Cloud[29]

8.3.3 L'approche Multi-Cloud

Dans cette approche, l'ensembles des sous-systèmes (cloud) fonctionnent indépendamment est la fédération consiste à créer une interopérabilité à l'aide d'un protocole de communication [30].

8.3.4 Gestion fédérée du Cloud

Dans la solution fédérée (Federated Cloud Management FCM), l'interopérabilité est réalisée par un courtier de haut niveau plutôt que par la location de ressources bilatérales, comme le montre la figure II.10. Une telle fédération peut être activée sans l'application d'une pile logicielle supplémentaire pour fournir des interfaces de gestion de bas niveau. La logique de la gestion fédérée est déplacée vers des niveaux supérieurs et il n'est pas nécessaire d'adapter les normes d'interopérabilité par les fournisseurs d'infrastructure participants [31].

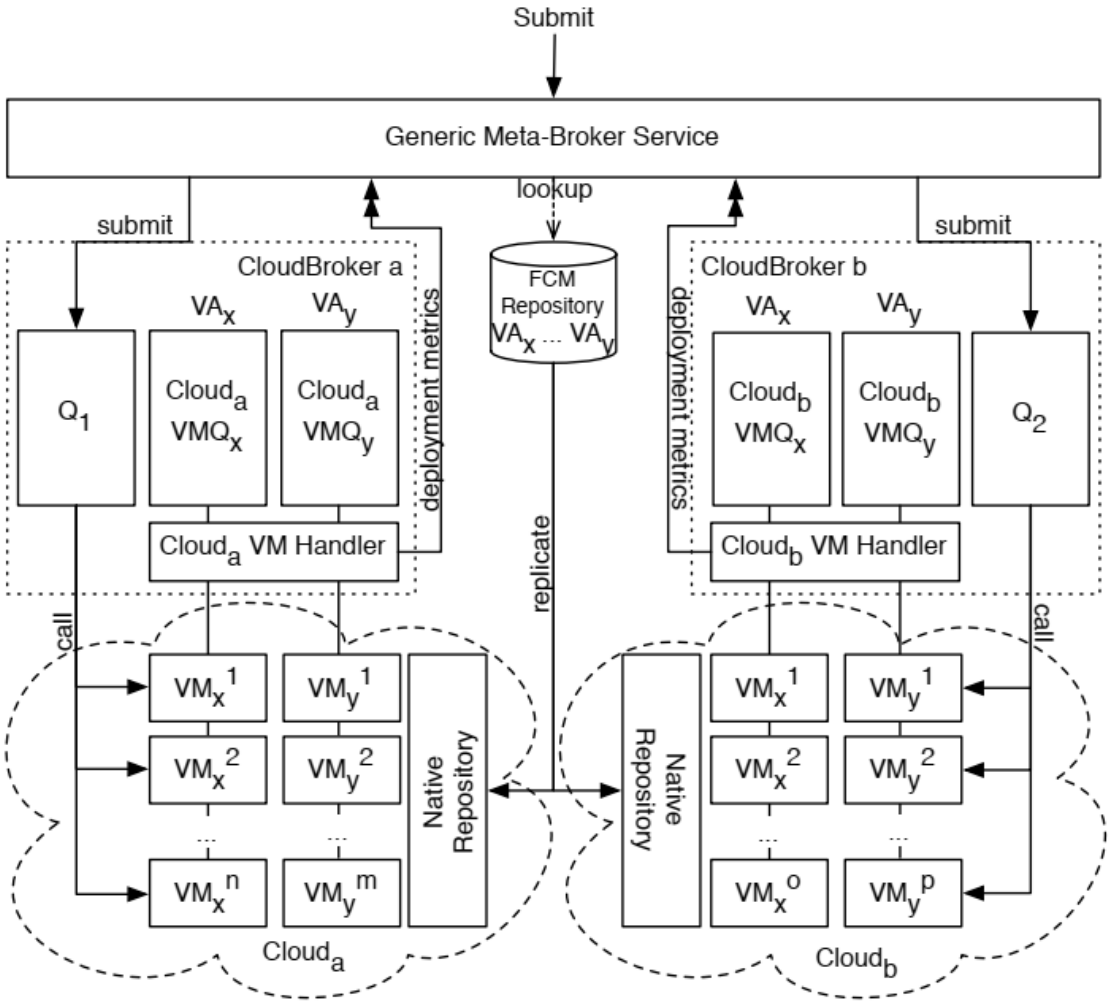

Figure II.10: Gestion fédérée du Cloud [31]

9 Mobile Cloud Computing

9.1 Définition

Le forum Mobile Cloud Computing (MCC) définit le MCC comme suit : Le Mobile Cloud Computing, dans sa forme la plus simple, se réfère à une infrastructure où le stockage et le traitement des données se déroulent à l'extérieur de l'appareil mobile. Les applications Mobile Cloud déplacent la puissance de calcul et le stockage de données des téléphones mobiles vers le Cloud, ce qui fait que les applications et MC ne sont pas seulement destinées aux utilisateurs de smartphones mais à un nombre beaucoup plus grand d'abonnés mobiles [32].

Aepona[33] décrit le MCC comme un nouveau paradigme pour les applications mobiles où le traitement et le stockage des données sont déplacés de l'appareil mobile vers des plateformes informatiques puissantes et centralisées situées dans les clouds. Ces applications centralisées sont ensuite accessibles via la connexion sans fil à partir d'un client léger ou d'un navigateur Web sur les appareils mobiles.

On peut aussi définir le MCC comme une combinaison du web mobile et du Cloud Computing [34] [35] , qui est l'outil le plus populaire pour les utilisateurs mobiles pour accéder aux applications et services sur Internet.

En résumé, MCC fournit aux utilisateurs mobiles les services de traitement et de stockage de données dans les clouds. Les appareils mobiles n'ont pas besoin d'une configuration puissante (par exemple, la vitesse du CPU et la capacité de mémoire) car tous les modules informatiques complexes peuvent être traités dans les clouds.

9.2 Motivation : le besoin d'un cloud mobile

- *Traitement d'images* : GOCR est un programme de reconnaissance optique de caractères (OCR) qui peut être utilisé sur une collection d'appareils mobiles. Dans un scénario réel, cela serait utile dans le cas d'un voyageur étranger qui prend l'image d'un panneau de rue, effectue une OCR pour extraire les mots et traduit les mots dans une langue connue [36].

- *Traitement du langage naturel* : La traduction des langues est une application possible, c'est un outil utile pour les voyageurs étrangers pour communiquer avec les gens du pays [36].

- *Informatique de foule (Crowd computing):* Les enregistrements vidéo de plusieurs appareils mobiles peuvent être assemblés pour créer une seule vidéo qui couvre l'ensemble de l'événement sous différents angles et perspectives [36].

- *Partage de données GPS/Internet* : Il est plus efficace de partager des données entre un groupe d'appareils mobiles qui sont proches les uns des autres, via des réseaux locaux ou peer-to-peer. C'est moins cher et plus rapide [36].

- *Applications de données de capteurs* : Comme la plupart des téléphones mobiles sont aujourd'hui équipés de capteurs, les lectures de capteurs tels que GPS, accéléromètre, capteur de lumière, microphone, thermomètre, horloge et boussole peuvent être estampillées et reliées aux autres lectures des téléphones [36].

- *Recherche multimédia* : Les appareils mobiles stockent de nombreux types de contenu multimédia tels que des vidéos, des photos et de la musique. Par exemple, Shazam est un service d'identification de musique pour téléphones portables, qui recherche des chansons similaires dans une base de données centrale. Dans le contexte du cloud mobile, la recherche peut être effectuée sur le contenu des téléphones voisins[36].

- *Réseaux sociaux* : Le partage de contenu utilisateur étant un moyen populaire d'interagir avec des amis sur les réseaux sociaux tels que Facebook.

9.3 Architecture du cloud computing mobile

A partir du concept de MCC, l'architecture générale du MCC peut être présentée dans la figure II. 11 . Dans la figure II. 4, les appareils mobiles sont reliés aux réseaux mobiles par l'intermédiaire de stations de base (p. ex. station de base de l'émetteur-récepteur, point d'accès ou satellite) qui établissent et contrôlent les connexions (liaisons hertziennes) et les interfaces fonctionnelles entre les réseaux et les appareils mobiles. Les demandes et les informations des utilisateurs mobiles (par ex. ID et localisation) sont transmises aux processeurs centraux qui sont connectés aux serveurs fournissant les services du réseau mobile. Les opérateurs de réseaux mobiles peuvent fournir aux utilisateurs des services d'authentification, gestion d'accès et de comptabilité basés sur les données de l'agent local et des abonnés stockées dans les bases de données. Ensuite, les demandes des abonnés sont acheminées vers le cloud via Internet. Dans le cloud, les contrôleurs de cloud traitent les demandes pour fournir aux utilisateurs mobiles les services cloud correspondants. Ces services sont développés avec les concepts d'informatique utilitaire, de virtualisation et d'architecture orientée services (p. ex., serveurs Web, d'applications et de bases de données) [32].

.

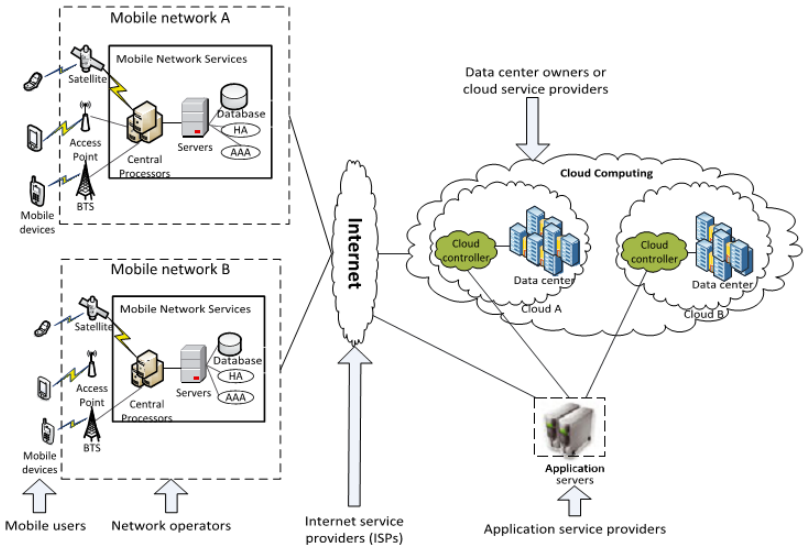

Figure II. 11:L'architecture du cloud computing mobile [32]

9.4 Applications du Mobile Cloud Computing

- *Commerce mobile* : Le commerce mobile (m-commerce) est un modèle de commerce utilisant des appareils mobiles. Les applications de m-commerce remplissent généralement certaines tâches qui nécessitent de la mobilité (par exemple, les transactions et paiements mobiles, la messagerie mobile et la billetterie mobile) [32].

- *Apprentissage mobile* : L'apprentissage mobile (m-learning) est conçu sur la base de l'apprentissage électronique (e-learning) et de la mobilité. Cependant, les applications traditionnelles de m-learning ont des limites en termes de coût élevé des appareils et du réseau, de faible taux de transmission du réseau et de ressources éducatives limitées.

Des applications de m-learning basées sur le cloud sont introduites pour résoudre ces limitations. Par exemple, l'utilisation d'un cloud avec une grande capacité de stockage et une puissante capacité de traitement, les applications offrent aux apprenants des services beaucoup plus riches en termes de taille des données (informations), de vitesse de traitement plus rapide et d'autonomie de la batterie [32].

- *Soins de santé mobiles* : Le but de l'application du MCC dans les applications médicales est de minimiser les limites du traitement médical traditionnel (p. ex. petit stockage physique, sécurité et confidentialité). Les soins de santé mobiles (m-healthcare) fournissent aux utilisateurs mobiles des aides pratiques pour accéder facilement et efficacement aux ressources (par exemple, les dossiers médicaux des patients).

En outre, m-healthcare offre aux hôpitaux et aux organisations de soins de santé une variété de services à la demande sur le cloud plutôt que de posséder des applications autonomes sur des serveurs locaux [32].

Il existe cinq principales applications de soins de santé mobiles du MCC dans le domaine de la santé [37].

- Des services complets de surveillance de la santé permettent aux patients d'être surveillés à tout moment et en tout lieu grâce à des communications sans fil .

- Un système intelligent de gestion des urgences permet de gérer et de coordonner efficacement et à temps le parc de véhicules d'urgence lors de la réception d'appels en cas d'accident ou d'incident.

- Les appareils mobiles de santé détectent le rythme cardiaque, la tension artérielle et le taux d'alcoolémie pour alerter le système de soins de santé d'urgence.

- L'accès permanent à l'information médicale permet aux patients ou aux soignants d'accéder à l'information médicale actuelle et passée.

- La gestion incitative généralisée du mode de vie peut être utilisée pour payer les dépenses de santé et gérer automatiquement les autres frais connexes.

- Le système de gestion des dossiers médicaux des patients affiche les informations concernant l'état des patients, les signaux biologiques associés et le contenu des images via l'interface de l'application.

- La prise en charge de l'affichage des images permet aux utilisateurs mobiles de décoder les fichiers d'images volumineux à différents niveaux de résolution en fonction de la disponibilité et de la qualité du réseau.

- Mobile gaming : Le jeu mobile (m-game) est un marché potentiel générant des revenus pour les fournisseurs de services. M-game peut décharger complètement le moteur de jeu qui nécessite de grandes ressources informatiques (par exemple, le rendu graphique) sur le serveur dans le cloud, et les joueurs interagissent uniquement avec l'interface écran sur leurs appareils.

10 Sécurité dans le Cloud Computing

10.1 Exigences de sécurité

10.1.1 Disponibilité

Le Service Level Agreement (SLA) est un accord de confiance entre le fournisseur et le consommateur pour définir la durée maximale pendant laquelle les ressources ou les applications peuvent ne pas être disponibles pour utilisation. Parce que cet accord formalise la relation entre les utilisateurs et le fournisseur de services dans le cloud, il doit s'organiser très soigneusement. Un moyen idéal de réduire l'indisponibilité des ressources en raison d'une panne ou d'une attaque est d'avoir des sauvegardes pour protéger les informations critiques. De cette façon, l'information du consommateur est disponible hors ligne [38].

10.1.2 Intégrité

La protection des données contre la suppression, la modification ou la production sans autorisation est possible grâce à la réponse aux défaillances et aux mesures correctives, la tolérance aux pannes, la reprise après panne et la reprise après sinistre.

De plus, la signature numérique est capable de vérifier l'intégrité des données et de se remettre de de leur altération[38].

10.1.3 Confidentialité

La revendication de la confidentialité des données des utilisateurs permet d'appliquer des protocoles de sécurité et des techniques de chiffrement appropriées aux différentes couches des applications dans le cloud. Les clients peuvent également chiffrer leurs données avant de les transférer sur le cloud. Comme la confidentialité est corrélée à l'authentification, protéger le compte d'un utilisateur équivaut à contrôler l'accès aux objets dans le cloud. En outre, les fonctions d'authentification biométrique peuvent se connecter aux fonctions antivols et de protection de l'identité dans le cadre de la sécurité dans le cloud [38].

10.1.4 Locations multiples

Pour fournir une multilocation sécurisée, il devrait y avoir un isolement entre les données des locataires ainsi qu'une transparence de l'emplacement où les locataires peuvent ne pas avoir la localisation des données afin d'éviter les attaques internes ou externes [38].

10.1.5 Élasticité

Pour les fournisseurs, l'augmentation et la diminution de l'échelle des ressources des consommateurs donne la possibilité à d'autres consommateurs d'utiliser les ressources qui leur ont été attribuées précédemment, ce qui peut entraîner des problèmes de confidentialité [38].

10.1.6 Vie privée

Des mécanismes de protection de la vie privée doivent être intégrés à toutes les solutions de sécurité. Pour l'utilisation du processus de cryptage, de stocker les clés de seulement côté fournisseur ou côté consommateur améliore la sécurité, en outre, le client peut crypter ses informations avant le chargement dans le cloud. Le cloud présente de nombreux défis juridiques en ce qui concerne les questions de protection de la vie privée liées aux données stockées dans des emplacements différents. En raison de l'évolution des exigences légales selon le pays qui héberge les serveurs, les organisations doivent savoir à tout moment où se trouvent leurs données. Les opérations de gestion de la sécurité devraient englober toutes les exigences en matière de sécurité[38].

10.1.7 Audit

Le processus d'audit comprend l'analyse des journaux la gestion d'accès et l'authentifications pour vérifier si les normes et politiques de sécurité sont respectées. Trois attributs principaux devraient faire l'objet d'une vérification : les événements, les registres et la surveillance devraient permettre de s'assurer qu'il n'y a pas de brèches de sécurité dans le système. L'auditeur tiers (Third party auditor TPA) vérifie l'intégrité des données dans le cloud au nom du client cloud et fournit aux utilisateurs la garantie de l'intégrité de leurs données[38].

10.1.8 Confiance

Dans un environnement de cloud computing, la confiance dépend principalement du modèle de déploiement choisi en fonction de l'audit des données et les applications sont sous-traitées [38].

10.1.9 Non-répudiation

Le fournisseur de services dans le cloud doit garantir la mise en œuvre du protocole de sécurité assure la non-répudiation afin que les interlocuteurs connectés ne puissent participer aux transactions [38].

10.1.10 Perte de données

Lors d'un transfert vers un cloud, les données seront stockées loin de la machine locale du client ou les données passent d'un environnement à un seul propriétaire vers un environnement à plusieurs propriétaires. Ces changements peuvent entraîner une perte ou une disparition de données. Pour diminuer les effets d'un tel problème, les applications de prévention des fuites de données (Data Leakage Prevention DLP) devraient être utilisées pour protéger les données sensibles. De plus, l'utilisation de contrôles d'accès avec cryptage fort aux données des consommateurs assure la sécurité même si les données sont conservées [38].

10.2 Attaques contre le Cloud Computing

10.2.1 Attaque de zombie

Par le biais d'Internet, un attaquant tente d'inonder la victime en envoyant des requêtes provenant d'hôtes innocents sur le réseau. Ces types d'hôtes sont appelés zombies. Dans le Cloud, les demandes de machines virtuelles (VM) sont accessibles par chaque utilisateur via Internet. Un attaquant peut inonder le grand nombre de requêtes via des zombies. Une telle attaque interrompt le comportement normal du Cloud affectant la disponibilité des services Cloud. Le Cloud peut être saturé pour répondre à des requêtes car il est épuisé, ce qui peut provoquer un DoS (Denial of Service) ou DDoS (distributed denial of service) sur les serveurs [39].

Une meilleure authentification et une meilleure gestion d'accès peuvent fournir une protection contre une telle attaque.

10.2.2 Attaque par injection de service

Le système Cloud est responsable de la détermination et éventuellement de l'instanciation d'un service demandé. L'adresse pour accéder à cette nouvelle instance doit être communiquée à l'utilisateur. Un attaquant tente d'injecter un service malveillant ou une nouvelle machine virtuelle dans le système cloud et peut fournir un service malveillant aux utilisateurs. Les programmes malveillants dans le cloud affectent les services du cloud en modifiant (ou en bloquant) les fonctionnalités du cloud. Prenons le cas d'un attaquant qui crée ses services malveillants comme SaaS, PaaS ou IaaS et l'ajoute au système du cloud. Si un attaquant y parvient, les requêtes valides sont automatiquement redirigées vers les services malveillants. Pour se défendre contre ce type d'attaque, un module de vérification de l'intégrité du service

devrait être implémenté. Une forte isolation entre les machines virtuelles peut empêcher l'attaquant d'injecter du code malveillant dans la machine virtuelle du voisin [39].

10.2.3 Attaques sur la virtualisation

Il existe principalement deux types d'attaques exécutées sur la virtualisation : VM Escape et Rootkit dans l'hyperviseur.

VM Escape : Dans ce type d'attaque, le programme d'un attaquant s'exécutant dans une machine virtuelle (VM) brise la couche d'isolation afin de fonctionner avec les privilèges root de l'hyperviseur au lieu des privilèges machine virtuelle (VM). Cela permet à un attaquant d'interagir directement avec l'hyperviseur. Par conséquent, machine virtuelle echape de l'isolation qui est fournie par la couche virtuelle. Par VM Escape, un attaquant accède à l'OS hôte et aux autres machines virtuelles fonctionnant sur la machine physique.

Rootkit dans l'hyperviseur : Les rootkits basés sur les machines virtuelles déclenchent un hyperviseur qui compromet l'OS hôte existant vers une machine virtuelle. Le nouvel OS invité suppose qu'il fonctionne en tant qu'OS hôte avec le contrôle correspondant sur les ressources, cependant, en réalité cet hôte n'existe pas. L'hyperviseur crée également un canal secret pour exécuter du code non autorisé dans le système. Cela permet à un attaquant de contrôler n'importe quelle machine virtuelle fonctionnant sur la machine hôte et de manipuler les activités sur le système [39].

10.2.4 Attaque de l'homme du milieu

Si la couche de socket sécurisée (SSL) n'est pas correctement configurée, n'importe quel attaquant peut accéder à l'échange de données entre deux parties. Dans le cloud, un attaquant est capable d'accéder à la communication de données entre les centres de données. Une configuration SSL appropriée et des tests de communication de données entre les parties autorisées peuvent être utiles pour réduire le risque d'attaque par un homme au milieu[39].

10.2.5 Attaque par usurpation de métadonnées

Dans ce type d'attaque, un adversaire modifie ou change le fichier WSDL (Web Services Description Language) du service où sont stockées les descriptions des instances de service. Si l'adversaire réussit à interrompre le code d'invocation de service du fichier WSDL au moment de la livraison, alors cette attaque peut être possible. Pour surmonter une telle attaque, les informations sur les services et les applications doivent être conservées sous forme cryptée.

L'authentification forte le contrôle d'accès devraient être appliquées pour accéder à ces informations critiques [39].

10.2.6 Attaque d'hameçonnage

Les attaques d'hameçonnage sont bien connues pour manipuler un lien Web et rediriger un utilisateur vers un faux lien pour obtenir des données sensibles. Dans le cloud, il est possible qu'un attaquant utilise le service cloud pour héberger un site d'attaque d'hameçonnage pour pirater les comptes et services des autres utilisateurs dans le cloud [39].

10.2.7 Attaque par la porte arrière d'un canal

Il s'agit d'une attaque passive, qui permet aux attaquants d'accéder à distance au système compromis. À l'aide de canaux détournés, les attaquants peuvent contrôler les ressources de la victime et en faire un zombie pour avoir tenté une attaque DDoS. Il peut également être utilisé pour divulguer les données confidentielles de la victime. Une meilleure authentification et une meilleure isolation entre les machines virtuelles peuvent offrir une protection contre de telles attaques [39].

11 Conclusion

Le Cloud Computing est une technologie très prometteuse qui aide les entreprises à réduire leurs émissions de tout en augmentant l'efficacité. Même si le Cloud Computing a été déployée et utilisée dans les environnements de production.

Dans ce chapitre nous avons fait une présentation du cloud computing en tenant en considération qu'il est la deuxième composante du réseaux véhiculaires en cloud. De ce fait, nous avons commencé par une présentation du réseau et ces caractéristiques, une vue architecturale des centres de donnée est importante. Un coup d'œil sur le mobile cloud computing est nécessaire car il y a une certaine ressemblance entre le MCC et le VCC. La sécurité est aussi présente par une présentation des exigences de la sécurité et les attaques sur le réseau cloud computing.

Dans le chapitre suivant nous allons présenter le réseau véhiculaire en cloud avec une vision complète qui englobe le cloud computing et les réseaux vanet.

Chapitre III

Les réseaux véhiculaires en cloud

1 Introduction

Le « Vehicular Cloud Computing » est une nouvelle évolution technologique qui bénéficie de cloud computing pour servir les conducteurs de VANETs avec un modèle payant à l'utilisation. Ainsi, les objectifs du VCC sont de fournir plusieurs services de calcul à faible coût pour les conducteurs de véhicules, de minimiser les embouteillages, les accidents, le temps de déplacement et la pollution de l'environnement, et d'assurer l'utilisation de services en temps réel et à faible consommation d'énergie des logiciels, plates-formes et infrastructures avec qualité de service pour les conducteurs.

Le VCC peut répondre à la convergence des STI et aux énormes capacités de calcul et de stockage du MCC. En outre, le VCC fournit une intégration techniquement réalisable de la détection omniprésente du WSN, des STI et du MCC pour une meilleure sécurité routière et des systèmes de circulation urbaine intelligents sécurisés.

Ce chapitre va s'articuler sur deux aspects, le premier c'est les réseaux cloud véhiculaire, ou nous allons parler du commencement de ce réseau, ces composants, les types, et l'architecture. Aussi nous allons parler des services des réseaux cloud véhiculaire, et les applications qui touches les différents domaines, et qui rendent ce réseau très intéressant.

Le deuxième aspect est la sécurité qui un aspect important pour n'importe quel type de réseau. Nous allons parler des exigences de la sécurité pour les réseaux cloud véhiculaire et aussi les attaques sur ces réseaux. Pour déduire les points de faible pour la sécurité de ces réseaux nous allons étudier l'impact des attaques sur les exigences de la sécurité. A la fin de ce chapitre nous allons déduire la solution d'une manière générale qui permet de renforcer la sécurité dans les réseaux cloud véhiculaires.

2 Cloud véhiculaire – Le commencement

En 2010, inspirés par le succès et les promesses des clouds conventionnels, un certain nombre de travaux ont introduit le concept de « Vehicular Cloud », (VC, en abrégé) , une extension non triviale, selon plusieurs dimensions, du paradigme Cloud Computing classique. Les VC ont été poussés par la conviction que les véhicules actuels et futurs sont équipés d'ordinateurs, d'émetteurs-récepteurs et de dispositifs de détection puissants. Ces ressources sont généralement sous-utilisées et leur utilisation judicieuse a des répercussions économiques et environnementales convaincantes.

Les premiers chercheurs qui ont introduit le concept VC sont Eltoweissy et al[40], Olariu et al[41], [42]. Leurs premiers articles ont défini diverses versions possibles VC, leurs diverses applications et les défis de la recherche. Plus précisément, les clouds autonomes, précurseur des VC, ont été proposés pour la première fois par Olariu et al[41] où ils ont également donné un aperçu d'un certain nombre d'applications importantes et de défis de recherche. Plus tard, Florin et al[43] ont étendu le modèle VC d'Eltoweissy et al[40] pour répondre aux besoins informatiques des déploiements militaires et des missions tactiques.

L'idée qui a mené à la création du VC était qu'en offrant des opportunités financières et des encouragements, les conducteurs et les propriétaires de véhicules peuvent louer leurs ressources informatiques et de stockage excédentaires aux clients. Cette approche est semblable à celle des grandes entreprises et des sociétés qui louent leurs ressources excédentaires en échange d'avantages financiers. Par exemple, Arif & al [44] ont suggéré que dans un proche avenir, les voyageurs aériens se gareront et brancheront leurs véhicules dans les stationnements pour une longue durée des aéroports. En échange d'un stationnement gratuit et d'autres avantages, ils permettront à leurs véhicules de participer, en leur absence, au centre de données de l'aéroport.

Un certain nombre de chercheurs ont souligné que même dans l'état actuel de la pratique, de nombreuses mises en œuvre de VC sont à la fois technologiquement réalisables et économiquement viables[41], [42], [45], [46]. Étant donné leur large éventail d'applications, il est raisonnable de s'attendre à ce qu'une fois adoptées, les sociétés de VC constituent le prochain changement de paradigme, avec un impact technologique et sociétal durable[47]. Il est un peu étonnant qu'en dépit d'un grand nombre d'articles théoriques, aucune tentative crédible de mise en œuvre de VC n'ait été rapportée dans la littérature. Les seules exceptions notables sont les travaux de Lu et al[48] et Florin et al[49].

L'une des différences fondamentales entre les VCs et les clouds conventionnels est la propriété des ressources. Dans les VC, la propriété des ressources informatiques est répartie entre plusieurs propriétaires, contrairement à un propriétaire unique comme c'est le cas pour les clouds classiques gérés par des sociétés comme Amazon, Google et IBM.

Gu et al[50] ont publié un papier dans lequel ils ont revu les principaux enjeux du VC, notamment son architecture, ses caractéristiques inhérentes, la taxonomie des services et ses applications potentielles[46].

Arif et al[51] ont été les premiers à étudier la faisabilité de centres de données fonctionnant sur les véhicules stationnés dans un grand aéroport. Étant donné que les taux d'arrivée et de départ

varient dans le temps, ils ont proposé un modèle stochastique prédisant l'occupation du stationnement. Plus précisément, ils ont proposé un modèle de répartition en fonction du temps pour la répartition de l'occupation des parkings, en fonction de la variance et du nombre de véhicules. En plus des résultats analytiques, ils ont obtenu une série de résultats empiriques qui confirment l'exactitude de leurs calculs analytiques et la faisabilité de ces datacenters

Olariu et al[47] ont fourni d'autres motivations pour étudier les réseaux de VC et leurs applications[47], suggérant que ces derniers constituent le prochain changement de paradigme, menant les réseaux véhiculaires à un niveau supérieur de pertinence et d'innovation. Depuis la publication de[47], de nombreux articles ont montré comment les VCs peuvent améliorer la solution à de nombreux problèmes dans les domaines de la sécurité et de la vie privée, la fiabilité et la disponibilité, les systèmes de transport intelligent et autres.

3 Clouds véhiculaires Vehicular Clouds – Hypothèses génériques du système

L'objectif de cette section est de fournir un aperçu des hypothèses sur les capacités des véhicules, la virtualisation, la migration des machines virtuelles et les stratégies de réplication des données nécessaires à l'exécution d'une grande variété de tâches utilisateur.

3.1 Modèle du véhicule

Au cours de la dernière décennie, les réseaux de véhicules et les systèmes de transport intelligents (STI), avec leurs nombreuses applications potentielles, ont connu des progrès importants et un intérêt croissant. L'amélioration de la disponibilité de l'Internet sans fil dans les véhicules a favorisé l'apparition d'applications et de services innovants liés à la gestion du trafic et à la sécurité routière. En même temps, nous avons été témoins d'une tendance indubitable vers le développement de véhicules intelligents et l'amélioration de la sécurité et du confort pour les déplacements dans nos villes[52].

Un véhicule typique est habituellement équipé de plusieurs dispositifs et capacités tels que les capteurs et les émetteurs-récepteurs, le GPS, les dispositifs de suivi, la caméra, les ordinateurs embarqués puissants et le stockage[53].

3.2 La virtualisation

La machine virtuelle (VM) est l'un des piliers de la Cloud Computing conventionnelle[54]–[56]. Le même concept reste fondamental en VC. Bien que le type de service fourni par le VC

soit en grande partie immatériel, pour fixer les idées, nous supposons dans la discussion suivante que le VC offre des services IaaS cloud, les utilisateurs peuvent acquérir des ressources informatiques virtualisées. Ils peuvent choisir un système d'exploitation et recevoir une VM avec une instance installée du système d'exploitation de leur choix. Comme l'illustre la figure.II.1, le VC offre à l'utilisateur une instance virtualisée de la plate-forme matérielle et du système d'exploitation souhaités regroupés sous forme de VM et d'OS invité. Pour des raisons de tolérance aux pannes, chaque tâche utilisateur est affectée à plusieurs voitures. Lorsque un job exécuter sur un véhicule est terminé, le résultat est transféré vers le datacenter.

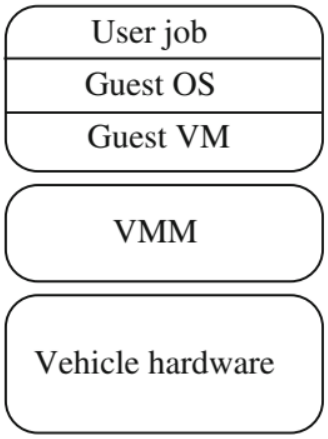

Figure III.1: Modèle de virtualisation [16]

3.3 Migration des machines virtuelles et réplication des données

Une fois qu'un véhicule est prêt à quitter le VC, un certain nombre d'actions doivent être prises. D'abord et avant tout, si le véhicule héberge une VM , la VM et toutes les données intermédiaires stockées par le véhicule partant doivent être migrées vers un véhicule disponible dans la VC. Il existe plusieurs stratégies connues pour la migration des VMs [57][58][59][60].

Malgré son importance fondamentale, il est peu étonnant de constater que seuls quelques auteurs se sont intéressés à la migration des VMs dans les VCs comme Baron et al[57], Refaat et al[60] et Florin et al[49].

3.4 VC statiques et dynamiques

Eltoweissy et al[40] et Olariu et al[42] ont fait remarquer que dans un avenir proche, les véhicules ont la capacité d'utiliser leurs ressources informatiques de manière coopérative pour s'organiser en VCs pour résoudre un certain nombre de problèmes fondamentaux. Bien que le VC stationnaire et statique peut imiter le comportement d'une CC conventionnelle, il ne faut

pas oublier que les véhicules n'ont pas un caractère statique absolu et qu'ils sont impliqués dans plusieurs situations dynamiques ainsi que dans des circonstances imprévues telles que des accidents et des embouteillages.

4 Architecture du réseau véhiculaire en cloud [61]

L'architecture du Vehicular Cloud Computing est basée sur trois couches

4.1 Couche interne du véhicule

Qui est responsable de la collecte et du traitement des informations du véhicule et du conducteur (humeur, pression, température, etc.) en utilisant les différents types de capteurs disponibles dans le véhicule .

Les informations recueillies sont utilisées pour étudier le comportement du conducteur. En cas de mauvaise conduite, un message d'alerte est envoyé aux voisins [61].

4.2 Couche de communication

Cette couche définit les deux modes de communication dans le réseau :

- *La communication véhicule-véhicule (V2V):* les véhicules échangent des messages (l'émetteur et le récepteur sont des véhicules), ce type de communication est utile dans de nombreuses applications telles que les messages d'alerte d'urgence, les avertissements de collision, les avertissements de changement de voie..etc.

- *Communication véhicule-infrastructure (V2I) :* dans ce type de communication, l'information est échangée entre le véhicule et le réseau de l'infrastructure. Il est utilisé dans plusieurs applications comme l'amélioration du niveau de sécurité en évitant les retards de collision et il offre également un accès aux ITS (Intelligent Transport Systems) [61].

4.3 La couche de cloud

Il offre les différents services cloud (informatique, stockage, applications...) ; il est constitué de trois couches internes : application, infrastructure cloud, et plate-forme cloud (Figure III.2)

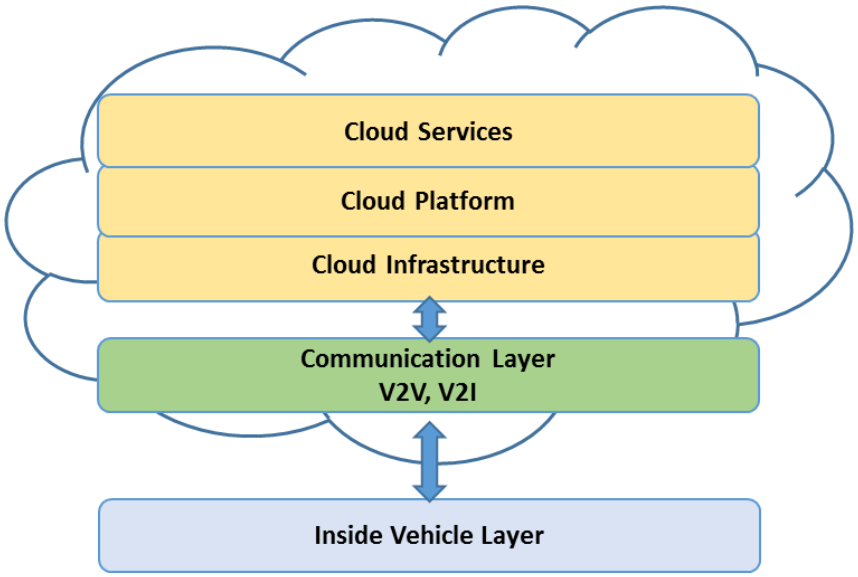

Figure III.2: L'architecture du VCC

5 Taxonomie du Cloud Véhiculaire [62]

Le cloud véhiculaire est divisé en trois grandes catégories : Clouds véhiculaires (VC), Vehicles utilisant les Clouds (VuC), et les Clouds Hybrid (HC).

5.1 Clouds véhiculaires (VC):

Le réseau n'est formé que par des véhicules et en ce qui concerne les mouvements des véhicules, il existe [62] :

- Clouds véhiculaires statiques : Le réseau contient des véhicules à l'arrêt, l'idée principale est d'utiliser les ressources des voitures garées pour former un super ordinateur avec de grandes capacités (calcul, stockage, communication...)

Dans ce type de réseau de véhicules, la contrainte énergétique se pose car les voitures stationnées utilisent principalement l'énergie de la batterie, ce qui réduit l'autonomie.

- Clouds dynamiques : sont formés à la demande de manière ad hoc par des véhicules en mouvement.

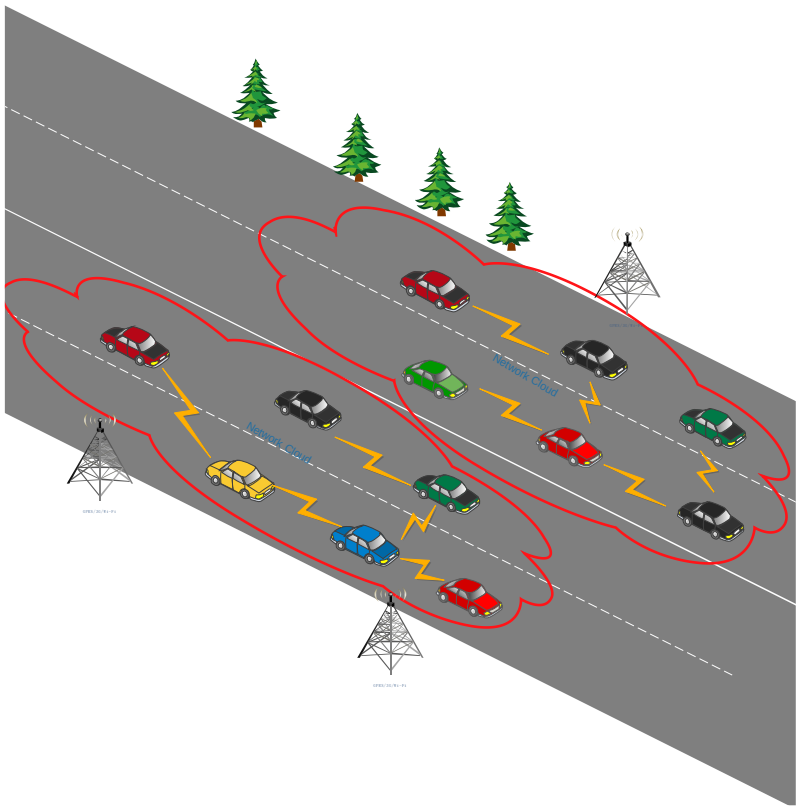

Figure III.3 : Vehicular Clouds (VC) [62]

5.2 Véhicules utilisant le Cloud

Connecte le VANET aux cloud traditionnels où les utilisateurs de VANET peuvent utiliser les services cloud en déplacement [62].

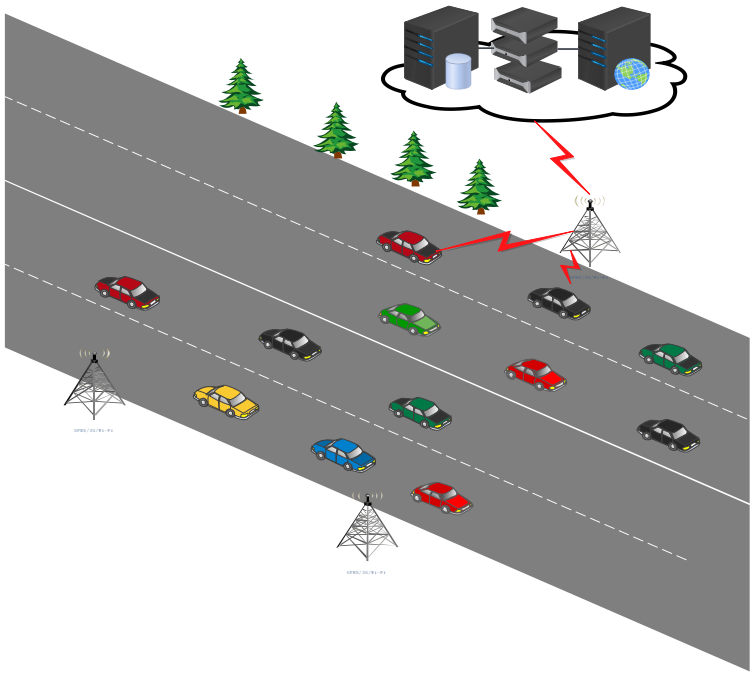

Figure III.4 : Vehicles using Cloud (VuC) [62]

5.3 Hybrid Cloud (cloud inter véhicules)

Les clouds véhiculaires interagiront avec le cloud traditionnel pour l'échange de services. Les véhicules et les RSU serviront de passerelles sur la partie VANET, communiquant ainsi avec les passerelles des clouds traditionnels [62].

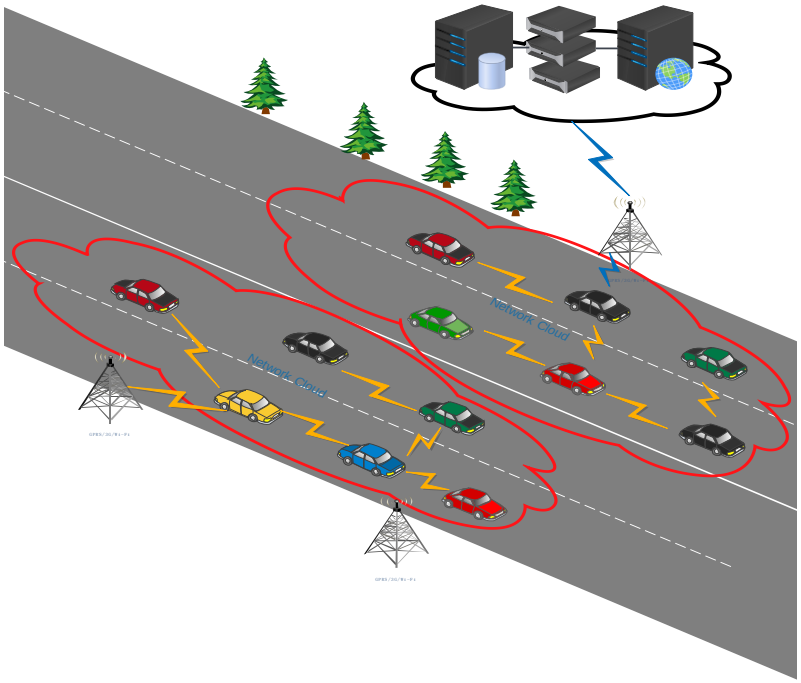

Figure III.5 : Hybrid Cloud [62]

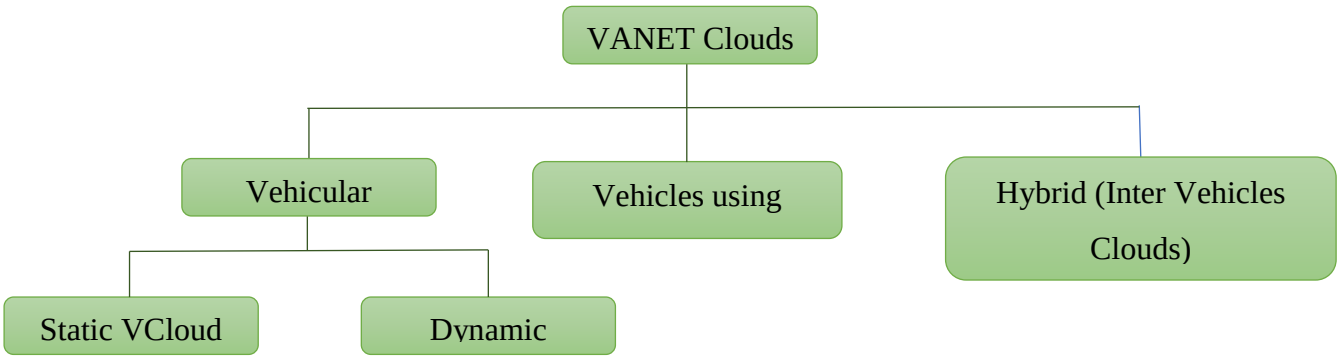

Figure III.2: Taxonomie du réseau véhiculaire en cloud

6 Modèle basé sur les services cloud en cloud Véhiculaire

6.1 Services de base

6.1.1 Infrastructure en tant que service (Infrastructure as a Service -IaaS)

Il met à disposition des ressources cloud (matériel de stockage, réseau, serveurs...). Ces ressources sont virtualisées et fournies en tant que service. La plupart des services offerts sont dérivés de cette couche

6.1.2 Plate-forme en tant que service (Platform as a Service -PaaS)

Dans ce service, la gestion de base de données,le système d'exploitation est rendue disponible, aussi des outils de cloud sont fournis comme l'environnement pour le stockage distribué, les programmes parallèles, le système de fichiers distribué (DFS). Cette couche s'adresse en premier lieu aux développeurs de programmes.

6.1.3 Logiciel en tant que service (Software as a Service -SaaS)

Cette couche offre le logiciel pour les utilisateurs finaux. Il contient des fonctionnalités applicatives (analytique, interactive, transactionnelle, navigation...). Ces applications permettent l'utilisation de différents logiciels disponibles dans le cloud et utiles pour le cloud véhiculaire..

6.2 Services dérivés(secondaires)

6.2.1 Réseau en tant que service (Network as a service -NaaS)

Assurer la connectivité constitue un défi majeur et complexe en milieu urbain. Les réseaux de véhicules réduisent le problème grâce à l'utilisation de points d'accès routiers fixes (AP) et d'utilisateurs mobiles de véhicules. Des initiatives récentes en faveur du NaaS se sont concentrées sur l'utilisation de la communication V2V et V2I pour permettre la connectivité et le transfert de données vers et depuis le Cloud[1].

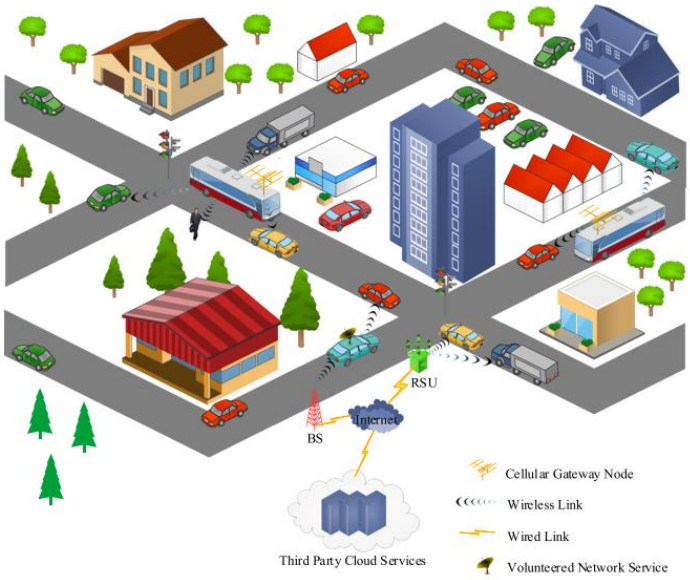

Figure III.6: Réseau en tant que service [63]

6.2.2 Stockage en tant que service (Storage as a service -STaaS)

Chaque véhicule moderne est supposé être équipé d'une grande capacité de stockage car la technologie a permis aux supports de stockage d'atteindre des petites tailles et des coûts réduits. De tels progrès ont motivé les auteurs du travail [64] de détermination des paramètres qui conditionnent la conception et la mise en œuvre d'un centre de données dans le parking d'un aéroport international. Le centre de données exploite la disponibilité des ressources embarquées des véhicules stationnés. Ce travail suppose que les véhicules sont connectés à des sources d'énergie de sorte qu'il n'y a aucune restriction de la consommation d'énergie et de l'autonomie de la batterie. Le travail envisage également un modèle commercial pour encourager les voyageurs aériens à contribuer par le biais de bénéfices sur le stationnement gratuit ou les services automobiles ; dans ce cas, cette approche suppose que les propriétaires de véhicules sont motivés à partager les ressources non utilisées pour construire le cloud véhiculaire [65].

Figure III.7:Stockage en tant que service[63]

6.2.3 Coopération en tant que service (Cooperation as a service - CaaS)

Les réseaux de véhicules offrent une variété de nouveaux services, tels que la sécurité des conducteurs, l'information routière, les avertissements d'embouteillages, les accidents de sable, les conditions météorologiques ou routières, la disponibilité des stationnements et la publicité. Récemment, des réseaux 3G,4G ou 5G et les STI sophistiqués ont été utilisés pour offrir de tels services, mais ces services ont un coût au niveau du matériel et du réseau. Les auteur de [61]envisage une forme de service communautaire appelée CaaS. Il permet aux conducteurs d'obtenir des services en utilisant une infrastructure très minimale. CaaS utilise l'appareil où l'abonné indique ses préférences pour un service, et les voitures souscrites pour le même service aideront à donner à l'abonné des informations importantes sur le service ou en annonçant des informations au réseau. CaaS peut diviser le réseau en clusters, comme dans Content-Based Routing pour les communications intra-cluster [51]

6.2.4 Calcul en tant que service (Computing as a service)

il gère l'agrégation des ressources de calcul disponibles et inutilisées des véhicules, en les rendant accessibles aux utilisateurs autorisés par le biais d'un service. Le Vehicular Cloud Computing est un concept très récent qui traite d'un contexte très sensible et complexe : l'exploration des ressources de calcul dans un environnement très mobile. L'étude menée dans[51] peut servir à estimer les capacités de calcul possibles dans un parc de stationnement, où les véhicules restent immobiles pendant une durée prévisible. Le défi dans cette situation est de définir un modèle approprié qui permette une migration efficace des tâches à l'intérieur et à

partir des véhicules stationnés, en redistribuant les tâches lorsque les véhicules quittent ou arrivent sur le parking [66] [67]. Dans ce cas, le modèle doit tenir compte de la charge de migration, qui implique la suspension des tâches, la sauvegarde de leur état d'exécution, l'identification de nouveaux hôtes et le transfert de tâches ; tous ces facteurs sont essentiels pour déterminer la faisabilité du transfert de tâches dans des scénarios aussi dynamiques[69].

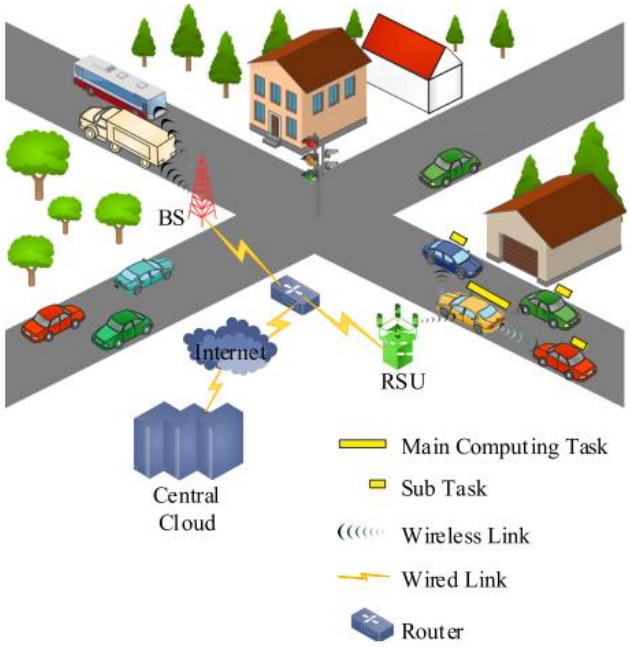

Figure III.8: Calcul en tant que service[63]

6.2.5 Photos sur une roue en tant que service (Pictures on a wheel as a service)

Les auteurs de [68] ont décrit les services de VCC comme une image sur une roue où les images peuvent être livrées sur demande au citoyen en utilisant les caméras embarquées dans la voiture. Ceci pourrait être utilisé car les applications d'enquête exploitant la mobilité des véhicules étendent la couverture au-delà de la portée des capteurs statiques. Les téléphones portables peuvent être utilisés comme source de ce service. Cependant, la batterie et les ressources sont limitées et il y a un risque de problèmes de sécurité et d'exposition. D'un autre côté, pour le VCC, il n'y a aucune préoccupation au sujet de la puissance et des ressources et il n'y a pas tant de problèmes de sécurité ou d'exposition. Le service Pics-on-Wheels sélectionne un groupe de véhicules pour prendre des photos ou des vidéos d'un paysage urbain donné pour une durée limitée, à la demande du client. Pour participer à ce service, les véhicules doivent s'inscrire auprès du gestionnaire de cloud centralisé. Ils téléchargent également périodiquement leur propre position GPS dans le gestionnaire de cloud. Le système de navigation embarqué de chaque véhicule conserve la trace du véhicule pendant une période de temps prédéfinie. Ensuite,

la principale préoccupation est de sélectionner le véhicule pour la prise de vue. Après une évaluation appropriée et minutieuse, le véhicule sera choisi. Dans le cas où aucun véhicule ne se trouve dans la zone cible ou que la demande de service soit refusée, ce service ne sera pas disponible. Ils proposent un algorithme de sélection du meilleur véhicule pour la prise de vue. Au moment d'un accident, ce service peut vous aider dans le cadre d'une expertise médico-légale ou d'une demande de règlement d'assurance.

6.2.6 La détection en tant que service (Sensing-as-a-Service)

Pour garantir la sécurité de conduite, de nombreux capteurs, pour le véhicule lui-même ou l'environnement ambiant, ont été intégrés dans les véhicules. L'une des caractéristiques distinctives des capteurs installés sur les véhicules est de pouvoir profiter de la mobilité des véhicules pour améliorer la couverture de détection. De plus, en agrégeant les données de détection provenant de véhicules géographiquement distribués, il est possible d'acquérir des données de détection bien au-delà de ce qui était possible jusqu'à présent. Il n'est même pas nécessaire d'investir dans le déploiement de réseaux de capteurs. La détection en tant que service devient ainsi une option intéressante à la détection urbaine et attire beaucoup d'attention dans le monde entier[69].

La littérature. Yu et al[70] étudient une approche coopérative de détection et de compression des données pour la surveillance de l'environnement urbain dans les réseaux de capteurs de véhicules (VSNs). Eckhoff et al[71] proposent l'utilisation de voitures stationnées pour détecter les véhicules qui ne sont pas en visibilité directe afin d'améliorer la sécurité. Liu et al[16] développent un système appelé POVA pour la détection des feux de circulation dans les grandes zones urbaines. Ma et al[72] ont proposé un système de transport en cloud piloté par l'utilisateur (Cloud Transportation System-CTS) qui utilise un système de crowdsourcing orienté utilisateur pour collecter des données sur les utilisateurs et prédire la congestion, en collectant, filtrant et modélisant des données, puis calculant intelligemment les trafics et les rendant publics. Yang et al[73] proposent deux mécanismes incitatifs pour le modèle basé sur la plate-forme et le modèle basé sur l'utilisateur, afin de recruter des utilisateurs de smartphones pour fournir des services de détection.

6.3 La relation entre les services basic secondaire dans VCN

	IaaS	*PaaS*	*SaaS*
Network as a service(NaaS)	***X***		
Storage as a service (STaaS)	***X***		
Cooperation as a service (CaaS)	***X***	***X***	
Computing as a service	***X***	***X***	***X***
Pictures on a wheel as a service	***X***	***X***	
Sensing-as-a-Service	***X***	***X***	

7 Applications de cloud computing véhiculaire

Dans cette section, plusieurs scénarios de mise en œuvre possibles et les résultats de l'application du VCC sont examinés[61]

7.1 Un aéroport comme centre de données

Bien que certaines voitures soient stationnées pendant plusieurs jours dans le parking à long terme d'un aéroport principal, ce parc de voitures peut servir de base à un centre de données à l'aéroport. Les voitures qui participent au cloud véhiculaire doivent être branchées dans une prise de courant standard et connectées à Internet par câble. Cependant, le principal problème est de planifier les ressources et d'assigner des tâches de calcul aux divers véhicules dans le cloud véhiculaire, en tenant compte de la nature variable dans le temps des taux d'arrivée et de départ. Arif et ses collaborateurs [51] ont été les premiers à s'attaquer à ce problème en proposant un modèle d'occupation des parkings en fonction du temps basé sur le système informatique en cloud libre « Eucalyptus » [74]. Le modèle Eucalyptus implique une API côté client d'un côté du réseau qui communique avec un contrôleur cloud qui est chargé de gérer plusieurs contrôleurs de cluster. Arif et ses collaborateurs [51] ont considéré un gestionnaire de centre de données comme un contrôleur de cloud computing pour créer une relation avec le monde extérieur, qui comprend quatre composantes (figure III.8) : *(1) coutier (broker)* : négocie avec divers clients potentiels qui ont besoin du service cloud et a l'autorité d'accepter d'éventuelles demandes, *(2) agent de virtualisation* : est responsable de configurer les ressources cloud disponibles pour respecter au mieux les engagements pris par le courtier, *(3)*

gestionnaire des ressource (resource manager) : qui découvre et gère les ressources dynamiques du cloud en fonction des taux d'arrivée et de départ des véhicules, *(4) le planificateur de tâches (task scheduler)* : il est chargé d'allouer les tâches de calcul à chaque cluster - qui interface avec les véhicules - ou même aux véhicules individuels d'un cluster en fonction du volume des ressources disponibles.

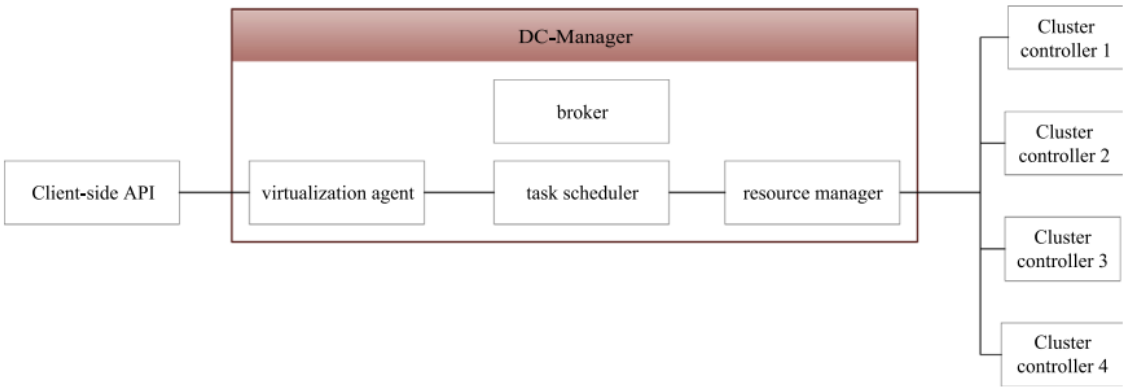

Figure III.9: Gestionnaire de centre de données [61]

7.2 Cloud de données sur les parkings

Des statistiques récentes révèlent que le parc de véhicules mondial est plus de 1,8 Millard [75], et la plupart de ces véhicules passent plusieurs heures par jour stationnés dans des garages, des stationnements ou des rues. Les ressources informatiques et de stockage de ces véhicules sont encore inutilisées et les possibilités d'utilisation sont inexploitées [51].

7.3 Centre de données d'un centre commercial

Des statistiques américaines montrent que les clients des centres commerciaux passent des heures à magasiner tous les jours, avec des pics pendant les week-ends ou pendant la période des fêtes. Une étude récente menée auprès d'adolescents qui fréquentent les centres commerciaux a montré que 95 % des acheteurs passaient plus d'une heure au centre commercial, tandis que 68 % d'entre eux y passaient plus de deux heures. Ainsi, des milliers de clients visitent différents centres commerciaux chaque jour, stationnent leur voiture dans le garage ou le parking du centre commercial et passent quelques heures à faire leurs courses tout en laissant leurs ressources informatiques dans leur véhicule au repos[61].

La direction du centre commercial peut utiliser ce matériel inutilisé en autorisant un service payant prépayé pour les ressources informatiques via Internet. La direction du magasin peut faire des offres intéressantes pour que les clients partagent les ressources du véhicule stationné, par exemple, des réductions au centre commercial, un parking gratuit ou des facilités de

stationnement similaires ailleurs. Cependant, l'un des grands défis du stationnement à court terme en tant que centre de données est sa nature dynamique en raison du taux élevé d'arrivée et de départ et des limites de temps par voiture[61].

7.4 Gestion dynamique des feux tricolores

Aujourd'hui, en raison de l'augmentation du nombre de véhicules sur les routes, le trafic devient un phénomène quotidien qui gaspille le temps et l'énergie humaine, menace la santé des citoyens et nécessite le grand effort computationnel pour être résolu. L'une des meilleures solutions pour surmonter ce problème est d'allouer la bonne quantité de ressources plutôt que de pré-affecter d'énormes ressources comme base pour la pire situation. Prenons l'exemple d'un événement comme un match de football auquel assistent des milliers de personnes, où un embouteillage peut se produire à la fin du match [61].

Bien qu'un certain nombre d'études ont été menées pour résoudre ce problème en tirant parti des VANET et des ITS, ils ne sont pas en mesure de signaler rapidement les problèmes de circulation et ne peuvent généralement pas fournir un plan d'atténuation du trafic. Le VCC est en mesure de présenter un moyen plus efficace et plus économique de résoudre la congestion en fournissant les ressources nécessaires à partir des véhicules disponibles participant au trafic et en les impliquant dans la recherche d'une solution autonome sans attendre la réaction des autorités [40].

7.5 Optimisation de la signalisation routière

Les feux de signalisation règlent la longueur du cycle du signal et la longueur de la phase verte. L'optimisation du système de signalisation se fait actuellement hors ligne, soit à l'intersection isolée, soit au niveau du couloir. Les périodes de temps sont définies par les plans de temps pour certaines périodes, telles que les heures de pointe du matin ou de l'après-midi en semaine. L'un des inconvénients de cette méthode est qu'elle nécessite des données sur les mouvements de trafic qui sont régulièrement collectées pour s'assurer que les plans de synchronisation des signaux sont adaptés aux conditions actuelles du volume de trafic. Un autre inconvénient est que ce système ne s'adapte pas bien aux changements incertains de la situation du trafic. Ainsi, les VC peuvent maximiser les performances du système de signalisation en utilisant dynamiquement un réseau de véhicules [61].

Les auteurs de [76]ont proposé un Navigator Assisted Vehicular route Optimizer (NAVOPT) basé sur le cloud véhiculaire et le cloud sur Internet dans lequel le cloud véhiculaire mesure la

congestion du trafic en segmentant l'heure, les coordonnées GPS et la destination finale sur un navigateur de véhicule à bord, sur le serveur de navigation. Le serveur de navigation - qui est implémenté dans le Cloud sur Internet - est en charge de calculer les itinéraires optimaux en construisant la carte de charge de trafic et la matrice des modèles de trafic et en estimant les charges et retards des segments routiers. Enfin, le serveur renvoie les itinéraires optimisés aux véhicules.

7.6 Les voies réservées aux véhicules à occupation multiple (VOM) auto-organisés

Pour des temps de parcours précis et prédéfinis, les voies réservées aux véhicules à occupation multiple véhiculant un grand nombre de voitures, qui transportent de nombreux passagers, surtout pendant les périodes de forte congestion routière. Cependant, les autorités sont au courant de la congestion et ont le pouvoir officiel d'aménager des voies réservées aux véhicules à occupation multiple, mais elles ne disposent pas des ressources suffisantes pour calculer et évaluer la situation afin d'établir le délai d'utilisation de la voie réservée pour atténuer les effets des embouteillages [61].

VC pourrait mettre en place des voies réservées aux VMO de façon dynamique en stimulant la circulation et en réduisant le temps de déplacement des voies réservées aux VMO. VC peut fournir la solution de manière dynamique en collectant des données à partir de capteurs embarqués dans les véhicules, et ce type de solution n'est pas possible avec la technologie actuelle [77].

7.7 La gestion de l'évacuation

La modélisation du trafic à forte intensité de calcul permet de mesurer les évacuations à partir d'une zone métropolitaine. Les organismes de transport élaborent souvent des simulations pour déterminer les stratégies possibles de contrôle de la circulation en cas d'évacuation. Ainsi, les événements d'évacuation peuvent être subdivisés en cas de notification préalable d'un événement imminent [61].

Les véhicules auto-organisés participant à la procédure d'évacuation formeront un ou plusieurs clouds de véhicules, qui travailleront en étroite collaboration avec le bureau des secours d'urgence. L'équipe de gestion des urgences télécharge les dernières informations concernant les abris ouverts, la nourriture et l'eau sur l'ordinateur du serveur principal.

Les auteurs de [78] ont proposé un système intelligent de gestion des catastrophes en exploitant le système de transport intelligent, le réseau ad hoc de véhicules et la technologie mobile et de cloud computing. Traditionnellement, l'information sur la circulation routière n'est disponible qu'au moyen de boucles inductives, de caméras, de capteurs routiers et d'enquêtes.

7.8 Message de sécurité routière

Les nouvelles voitures sont équipées de dispositifs de détection intégrés pour un fonctionnement sûr et efficace. Les caméras aident le conducteur en suivant les lignes sur la route et l'aident à rester dans la voie. De ce fait, les voitures ont un capteur de nœud, et un VC peut se former dynamiquement avec un grand réseau de capteurs sans fil. Les véhicules interrogent les capteurs des autres voitures qui se trouvent à proximité afin d'augmenter la fidélité et d'obtenir une évaluation des dangers potentiels de la route, de l'état de la route, des ralentisseurs et des trous, de la glace noire et de la vitesse. Cependant, la conception actuelle de VANET ne nous donnera pas la coordination des mesures de sécurité et une solution plus rapide [77] .

7.9 Alléger la congestion fréquente

Peu de conducteurs recherchent des itinéraires de déviation et des itinéraires alternatifs empruntant les routes locales. Il est difficile de prendre des décisions en conduisant, surtout lorsque plusieurs voitures essaient de se diriger vers la même route et que la capacité de la route locale est dépassée, ce qui entraîne des impasses.

Le système consultatif de la circulation et le système ITS contemporain sont tous les deux lents à résoudre les embouteillages et ils ne disposent d'aucun plan de réduction de la circulation. Les véhicules formant un cloud à proximité pourront calculer l'impact de la route locale et la cause de la congestion du trafic et déterminer le goulot des embouteillages [77].

7.10 Gestion des parcs de stationnement

Trouver une place de stationnement convenable à proximité de l'université ou dans les grandes villes bénéficierait de l'aide d'un service de gestion de stationnement automatisé. Récemment, les solutions connues basées sur un modèle unifié de garages individuels et de parcmètres ont été combinées et diffusées à la communauté. Aujourd'hui, les automobilistes peuvent trouver une place de stationnement à l'aide de leurs applications smartphone (Smartpark, ParkMe et ParkMate, par exemple). Cependant, ces applications présentent certains inconvénients qui

n'ont pas été abordés, tels que : la couverture du point limité du monde et le besoin d'accéder à Internet.

En outre, de nombreuses études sur les systèmes de stationnement basés sur VANET ont été proposées ces dernières années [79] qui peuvent être améliorées en utilisant des services VC.

La figure III.12 montre les différents types de scénarios d'application du VCC. Les scénarios d'application du VCC sont divisés en trois types : VCC dynamique, VCC statique et VCC statique/dynamique

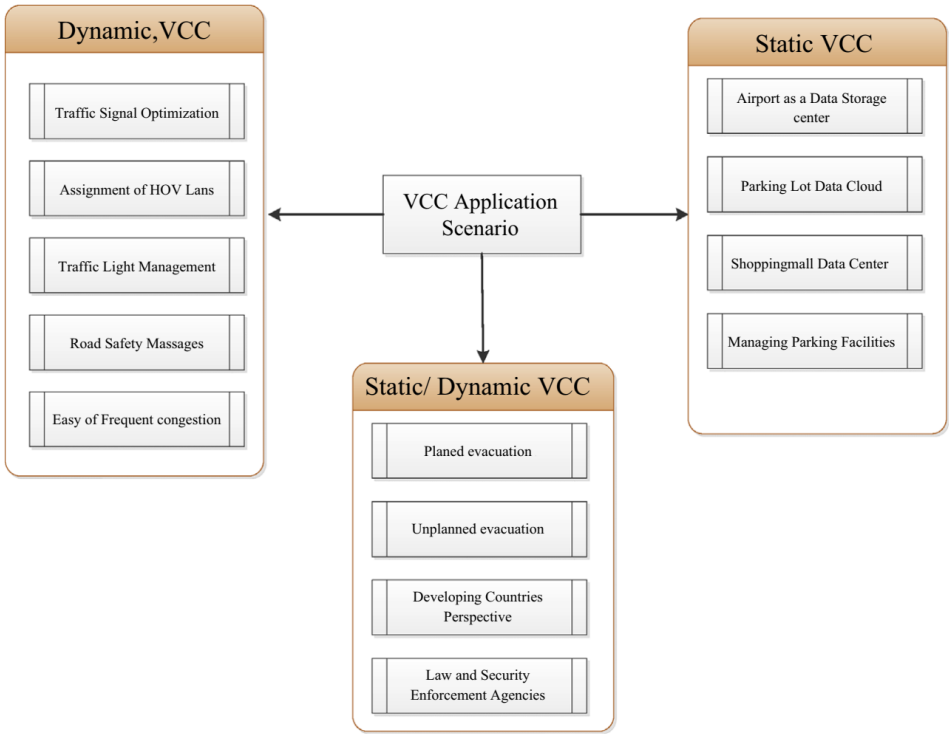

Figure III.10:Les scénarios d'application du VCC [61]

8 Sécurité des réseaux en cloud véhiculaire

8.1 Exigences de sécurité pour les réseaux de VCC

8.1.1 Confidentialité

Dans un environnement de VCC, les attaquants peuvent facilement extorquer des informations personnelles sensibles telles que les détails du véhicule ou l'adresse e-mail du conducteur, son numéro de téléphone ou son adresse résidentielle en utilisant des attaques MITM (Man-in-the-middle). En effet, les informations propres à un véhicule ou les informations privées sont utilisées pour les services applicatifs. Par conséquent, ces informations doivent être cryptées pour protéger les données contre les attaques MITM [80].

8.1.2 L'authentification

L'authentification garantit que le message est généré par l'utilisateur légitime. Il protège les éléments de communication (messages et entités). L'authentification dans le VCC est basée sur trois facteurs principaux. Le premier est le facteur de connaissance "quelque chose que l'utilisateur sait", comme le mot de passe, le code d'identification personnel (PIN), le mot de passe. Le second est celui des facteurs de propriété "quelque chose que l'utilisateur possède", comme la carte d'identité, le jeton de sécurité, le téléphone portable, la RFID. Le troisième est le facteur d'inhérence "quelque chose que l'utilisateur est ou fait", comme l'identifiant biométrique (utilisateur), le numéro de châssis (véhicule), etc [80]**.**

8.1.3 Intégrité

L'intégrité doit être assurée pour les informations transmises dans un environnement VCC. Si l'intégrité des informations d'identification personnelle du conducteur, des informations de paiement ou des informations de localisation est altérée par un message falsifié ou une attaque de falsification, cela pourrait causer des dommages financiers à l'utilisateur ou entraîner la mort en cas d'urgence. Pour se défendre contre les attaques contre l'intégrité des données, l'intégrité des données importantes devrait être garantie par des fonctions de hachage et des signatures numériques [80].

8.1.4 Disponibilité

Dans la communication VANET, un réseau sans fil est utilisé pour communiquer entre les véhicules. Dans le cas du routage en cluster (CBR), un véhicule d'en-tête et des véhicules adjacents forment un cluster pour la communication mutuelle, et parmi ces véhicules, un utilisateur malveillant pourrait interrompre ou arrêter le service du véhicule cible avec un déni

de service (DoS) ou une attaque DDoS (Distributed Denial of Service) comme une inondation ou un blocage [80].

De plus, une attaque contre la disponibilité pourrait se produire si un utilisateur malveillant entrave le routage du réseau du véhicule par une attaque de trou noir [14-16]. Pour garantir la disponibilité, un véhicule doit être authentifié par un mécanisme d'authentification, et seul le véhicule authentifié doit pouvoir accéder à l'objet correspondant.

8.1.5 Vie privée

Comme diverses applications sont maintenant offertes à l'intérieur du véhicule, des atteintes à la vie privée peuvent se produire. Lorsque les données de la boîte noire à l'intérieur du véhicule sont exposées, la vie privée est exposée. De plus, en raison de la divulgation de renseignements personnels, de renseignements sur l'emplacement des véhicules et de l'itinéraire des véhicules fournis par le service de navigation, il y a atteinte à la vie privée. Pour prévenir les atteintes à la vie privée, le chiffrement devrait être appliqué aux renseignements importants. En outre, pour l'identification ou l'authentification d'un véhicule ou d'un utilisateur, au lieu d'utiliser un identifiant unique, un identifiant aléatoire devrait être utilisé pour assurer l'anonymat [80].

8.1.6 Traceability and revocability

To protect user information, the identity must be hidden, and also it is important to use a system component (trace manager) to obtain the real identity where it is needed. [81]

8.1.7 Non-répudiation

Dans le VCC et dans les situations d'urgence comme les accidents, les interventions ou les changements doivent être associés à un véhicule unique (conducteur). En outre, les services dans le Cloud sont offerts pour plusieurs locataires, la non-répudiation est importante pour identifier la participation du locataire dans toute transaction argumentée[81] [82]

8.1.8 Contraintes temps réel

Le facteur temps réel est important car la topologie du réseau change dynamiquement, et certaines applications VCC sont très sensibles au retard comme l'avertissement de collision, le message de sécurité routière, l'état du trafic routier[61].

8.1.9 Multilocation

En raison de la nature des services cloud, les ressources sont allouées pour plusieurs locataires en utilisant la virtualisation.Le locataire ne doit pas avoir accès à d'autres ressources locatives, ni à des informations critiques [82].

8.2 Classification des attaques

Comme le montre la figure III.10, l'architecture du VCC peut être classée en trois couches : le réseau, le canal de communication sans fil et le cloud computing. La première couche est responsable de la collecte des informations et des événements de l'environnement. Ensuite, ces informations sont transférées dans le cloud en utilisant le canal de communication sans fil. Par conséquent, la sécurité des réseaux de véhicules dépend de la sécurité de ces trois couches [61].

1. Sécurité de la couche réseau (VANET, WSN).

2. Sécurité de la couche de transmission (canal de communication sans fil).

3. Sécurité du cloud computing

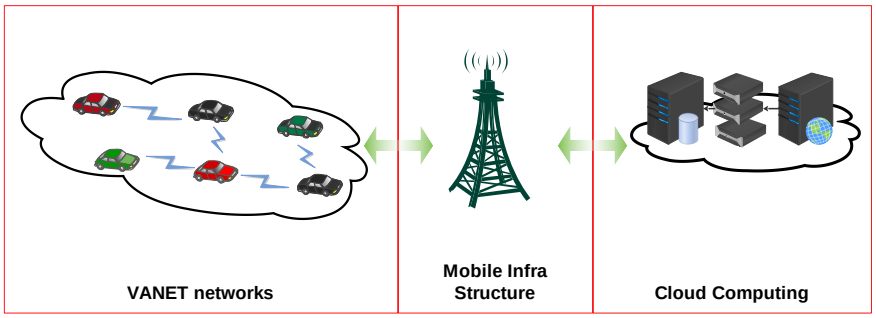

Figure III.11: L'architecture du VCC [61]

Dans le tableau suivant, nous avons regroupé classées les attaques sur le VCC par couches.

Tableau III.1 : les attaques sur les réseaux VCC par couche

La couche réseau	*La couche cloud*	*La couche de transmission*
• Denial of Service attacks (DoS) [10] • Greedy behavior attack [10] • Blackhole attack [32] • Grayhole attack [11] • Sinkhole attack [10] • Wormhole attack [12] [13] [14] • Malware attack [15] [16] • Broadcast tampering attack [34] • Sybil attack [17] • Node impersonation [18] [23] • Tunnelling attack [19] [33] • Key and/or Certificate Replication attack [20] • Eavesdropping attack [10] • Traffic analysis attack [10] • Masquerading attack [33] • Replay attack [33] • MessageTampering/ Suppression /Fabrication/ Alteration [34] • Loss of events traceability [33]	• Zombie attack [21] • Service injection attack [21] • Attacks on virtualization [21] • Man-in-the Middle [21] • Metadata spoofing [21] • Phishing attack [21] • Backdoor channel [21]	• Jamming attack [7]

Le tableau III.1 contient un résumé des attaques sur le VCN regroupées par couches de VCN. Il est clair que la majorité des attaques affectent essentiellement la couche réseau, comme le montrent le tableau II et la figure III.1. Cette couche est la plus touchée car c'est la ligne de front pour accéder aux autres composants VCN.

Tableau III.2 : Résumé des attaques sur les réseaux VCC par couche

	Attacks	***Percentage (%)***
Cloud Layer	7	26,92
Network layer	18	69,23
Transmission layer	1	3,85

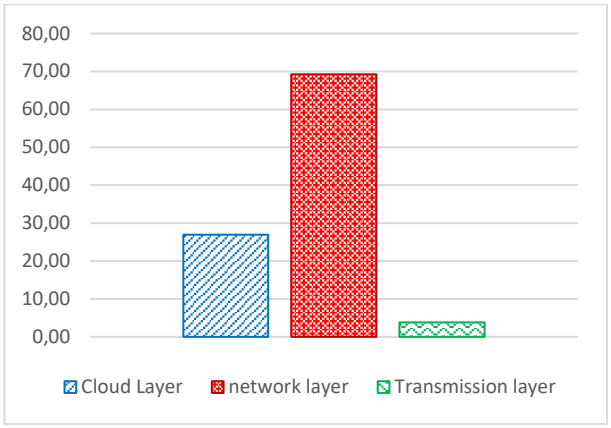

Figure III.12: Les attaques sur les réseaux VCC par couche

8.2.1 Impact des attaques sur le modèle basé sur les services cloud dans VCN

Le VC est un VANET doté de services cloud, donc ce réseau est exposé à un grand nombre d'attaques, dans cette section nous mettons en lumière l'impact de ces attaques sur le modèle basé sur le service cloud (IaaS, PaaS, SaaS)

8.2.1.1 Impact des attaques de la couche cloud

Le tableau III.3 résume les attaques du cloud et l'impact de chaque attaque sur le service cloud. Les attaques les plus dangereuses ce sont qui touchent plus d'un service parmi les services cloud (IaaS, PaaS, et SaaS).

Tableau III.3: L'impact des attaques de la couche de cloud sur le modèle basé sur les services cloud

	IaaS	PaaS	SaaS
Zombie attack	●		
Service injection attack		●	●
Attacks on virtualization	●	●	●
Man-in-the Middle	●		
Metadata spoofing		●	●
Phishing attack		●	●
Backdoor channel	●		

8.2.1.2 L'impact des attaques de la couche de transmission sur le modèle basé sur le service cloud

L'attaque qui concerne la couche de transmission est l'attaque de brouillage (jamming attack), et elle touche uniquement le service IaaS

Tableau III.4: L'impact des attaques de la couche cloud sur le modèle basé sur les services cloud

	IaaS	**PaaS**	**SaaS**
Jamming attack	●		

8.2.1.3 L'impact des attaques de la couche réseau sur le modèle basé sur les services cloud

Comme on peut le voir dans le tableau I, les attaques sont concentrées sur la couche réseau, le tableau IV résume l'impact de ces attaques sur les services cloud.

Le tableau IV révèle que le service le plus affecté est le IaaS, pour la raison que ce service contient la couche réseau (architecture VCN), et que cette couche est très ciblée par les attaques.

Tableau III.5: L'impact des attaques de la couche réseau sur le modèle basé sur les services

Les attaques	***IaaS***	***PaaS***	***SaaS***
Denial of Service attacks (DoS)	●		
Greedy behavior attack	●		
Blackhole attack	●		
Grayhole attack	●		
Sinkhole attack	●		
Wormhole attack	●		
Malware attack	●		●
Broadcast tampering attack	●	●	
Sybil attack		●	●
Node impersonation			
Tunnelling attack			
Key and/or Certificate Replication attack			
Eavesdropping attack			
Traffic analysis attack			
Masquerading attack	●		
Replay attack	●		
MessageTampering/ Suppression /Fabrication/ Alteration	●	●	●
Loss of events traceability			

8.2.1.4 Résumé et discussion

Dans ce contexte, nous sommes intéressés par l'impact des attaques sur le service cloud, ici les attaques sont classées par couches , et il est résumé dans le tableau III.6 , figure III.12, cette figure montre que les services les plus affectés par les attaques VCN sont IaaS (Infrastructure as a Service), car ce service inclut la couche réseau, la plus affectée par les attaques.

Tableau III.6: L'impact des attaques sur le modèle basé sur les services Cloud

	IaaS	**PaaS**	**SaaS**
Cloud Layer	7	3	4
Network layer	18	10	3
Transmission layer	1	1	0

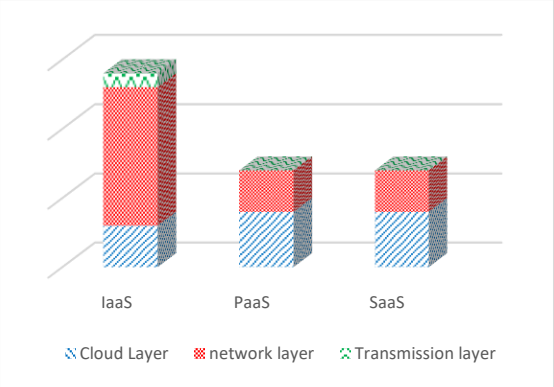

Figure III.13: L'impact des attaques sur le modèle basé sur les services Cloud

8.2.2 L'impact des attaques sur les exigences de sécurité :

8.2.2.1 Les attaques de la couche réseau

Le tableau ci-dessous montre l'effet des attaques de la couche réseau sur les exigences de sécurité du VCN

Tableau III.7: L'impact des attaques de la couche réseaux sur les exigences de sécurité

	Confidentiality	Authentication	Integrity	Availability	Privacy	Non-repudiation	Real-time	Audit	Traceability
Denial of Service attacks (DoS)				●					
Greedy behavior attack				●					
Blackhole attack				●					
Grayhole attack				●					
Sinkhole attack				●					
Wormhole attack				●					
Malware attack				●					
Broadcast tampering attack				●					
Sybil attack					●				
Node impersonation					●				
Tunnelling attack					●				
Key and/or Certificate Replication attack					●				
Eavesdropping attack	●								
Traffic analysis attack	●								
Masquerading attack	●		●						
Replay attack			●						
Message Tampering/Suppression /Fabrication/Alteration			●						
Loss of events traceability						●		●	●
Timming attack							●		
Brute force attack	●				●				

8.2.3 Attaques de la couche cloud

Le tableau III.8 montre l'impact des attaques de la couche de cloud attaque les exigences de sécurité du VCN

Tableau III.8: L'impact des attaques de la couche cloud sur les exigences de sécurité

	Confidentiality	*Authentication*	*Integrity*	*Availability*	*Privacy*	*Non-repudiation*	*Real-time constraints*	*Multi Tenancy*	*Data Leakage*
Zombie attack				●			●		●
Service injection attack			●					●	
Attacks on virtualization								●	●
Man-in-the Middle		●	●		●	●			
Metadata spoofing		●	●		●				
Phishing attack			●						
Backdoor channel		●	●						
Jamming attack	●						●		

8.2.4 Attaques sur la couche de transmission

Comme le montre le tableau III.9, les attaques de brouillage ont un impact sur la confidentialité, la disponibilité et les contraintes de temps réel.

Tableau III.9: L'impact des attaques de la couche de transmission sur les exigences de sécurité

	Confidentiality	Authentication	Integrity	Availability	Privacy	Non-repudiation	Real-time constraints	Multi Tenancy	Data Leakage
Jamming attack	●			●			●		

Le tableau IX résume l'impact des attaques sur les exigences de sécurité, comme il est détaillé dans les tableaux VI, VII et VIII. La figure (Fig.4) montre que les exigences de sécurité les plus affectées sont la confidentialité, l'intégrité, la disponibilité et la vie privée.

Les attaques de la couche réseau constituent la majorité des attaques contre la confidentialité, la disponibilité et la vie privée. Pour les autres exigences, ce sont les attaques de la couche cloud qui ont le plus d'impact.

Tableau III.1: Impact des attaques sur les exigences de sécurité (résumé)

	Confidentiality	Authentication	Integrity	Availability	Privacy	Non-repudiation	Real-time constraints	Audit	Traceability
Cloud Layer	1	3	5	1	2	1	2	2	2
Network layer	4	0	3	8	5	1	1	1	1
Transmission layer	1	0	0	0	0	0	0	0	0

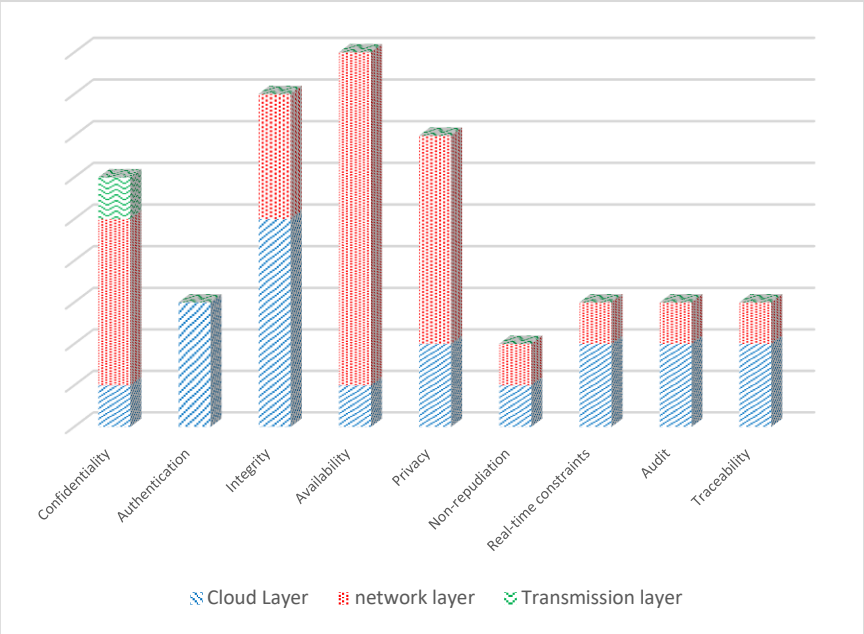

Figure III.10: Impact des attaques sur les exigences de sécurité

8.3 Solutions basées sur la cryptographie et les certificats pour le VCC

Comme le montre la Fig. 3, les exigences de sécurité les plus touchées dans le VCC sont la confidentialité, l'intégrité, la disponibilité et la vie privée. Notre proposition pour améliorer la sécurité dans les réseaux de VCC est d'utiliser les solutions basées sur les certificats (certificat numérique avec PKI, Pseudonymes).

Un certificat numérique (certificat de clé publique ou certificat d'identité) est un document électronique utilisé pour prouver la propriété d'une clé publique. Le certificat comprend des informations sur la clé, des informations sur l'identité de son propriétaire et la signature numérique d'une entité qui a vérifié que le contenu du certificat est correct. Si la signature est valide et que la personne qui examine le certificat fait confiance au signataire, elle sait qu'elle peut utiliser cette clé pour communiquer avec son propriétaire.

Le certificat numérique est utilisé dans le cadre d'un système global " infrastructure à clé publique (PKI) ", qui est un ensemble de rôles, de règles et de procédures nécessaires pour créer, gérer, distribuer, utiliser, stocker et annuler des certificats numériques et gérer le cryptage à clé publique.

Nous proposons l'utilisation des deux variantes de certificat (à long terme et à court terme) sous PKI pour améliorer la sécurité dans le CCV.

8.3.1 Certificat numérique et infrastructure à clé publique (PKI)

L'utilisation de la PKI et du certificat numérique en VCC renforce les exigences suivantes :

- *Confidentialité*

Une implémentation PKI assure la confidentialité des données transmises sur le réseau entre deux parties. Les données sont protégées par le cryptage des messages, de sorte que même dans les cas où les données sont interceptées, elles ne pourraient pas être interprétées. Des algorithmes de cryptage puissants assurent la confidentialité des données. Seules les personnes qui possèdent les clés seraient en mesure de décoder le message.

- *Authentification*

La PKI fournit également les moyens par lesquels l'expéditeur et le destinataire des messages de données peuvent authentifier l'identité de l'autre. Les certificats numériques qui contiennent des hachages cryptés sont utilisés pour l'authentification [25]

- *Intégrité*

L'intégrité des données est assurée lorsque les données ont été transmises sur le réseau et n'ont pas été manipulées ou modifiées n'importe quelle manière. Avec la PKI, toute modification apportée aux données d'origine peut être identifiée .

Parce que la plupart des attaques ont un impact sur IaaS comme un service cloud impact également sur la confidentialité, l'authentification, l'intégrité. Ainsi, l'utilisation de la PKI dans le VCC rend l'IaaS plus disponible et plus stable.

8.3.2 Certificat de pseudonyme

Le pseudonyme est un certificat temporaire, caractérisé par l'anonymat et une courte période de validité. Ce pseudonyme est utilisé à la place du certificat numérique pour assurer la vie privée

9 Opportunités et avenir pour le VCC

Le VCC joue un rôle majeur dans la vie des gens en raison de la gestion de la circulation et de fournir la sécurité, la sûreté, la confiance et le confort des passagers et des conducteurs, donc considéré comme un environnement très riche pour les chercheurs. Il considère la base pour l'amélioration et le développement de systèmes de transport intelligents[83].

Toutefois, le processus d'élaboration et d'amélioration reste limité par plusieurs facteurs tels que les défis et les problèmes pour le VCC. Plusieurs applications et services apparus dans les derniers temps résultent de l'exploitation des ressources par le cloud véhiculaire. L'avenir du

VCC dans les prochains jours bénéficie d'une ressource sous-utilisée et l'exploite au maximum en termes de rentabilité, de capacités de stockage et de calcul qui appartiennent aux véhicules modernes.

Dans [84], les auteurs présentent une nouvelle méthode, connue sous le nom de Virtual Cord Protocol (VCP), qui dépend de ce que peuvent offrir les véhicules en stationnement pour créer un cloud permettant de stocker des informations et pour établir une communication réseau entre le véhicule en mouvement et celui où les données demandées sont enregistrées.

Les techniques de routage inter-domaines utilisées pour activer les services dynamiques du cloud et pour assurer la communication entre les véhicules en mouvement et le cloud. Les auteurs de [85] ont proposé une nouvelle architecture pour les clouds de données véhiculaires basés sur IoT, en intégrant plusieurs dispositifs, le cloud computing et les IOT pour partager les ressources et échanger des informations entre les passagers, les véhicules et l'infrastructure routière [85]. Les auteurs de [85] étudient et font face à deux services de cloud de données véhiculaires : le premier est un service intelligent de cloud parking et le second est le service de données de maintenance des véhicules miniers. Bien qu'elle présente plusieurs défis, cette méthode offre d'énormes possibilités technologiques dans l'industrie automobile.

Les auteurs de [86] proposent une architecture contextuelle avec prise en charge des clouds mobiles et deux composants de service essentiels, les systèmes assister par le cloud (cloud-assisted) et Vehicular Cyer-physical systems (CVCs).

10 Défis dans le réseau cloud véhiculaire

Pour bénéficier de capteurs tels que la géolocalisation, le radar .. etc, les auteurs de [87] ont proposé une nouvelle méthode pour détecter les véhicules en cours de route ou stationnés sur le bord de la route afin de fournir le meilleur déplacement, la méthode la plus facile pour dépasser le véhicule stationné. En outre, aider les conducteurs à prendre la décision de choisir la voie la plus facile et la plus sûre pour éviter d'être gênés par d'autres véhicules.

Les accidents et les problèmes de circulation sont des défis majeurs pour le VCC, ils peuvent se produire lorsque les véhicules sont garés de manière inadéquate sur la route. Les auteurs de [88] ont donc présenté le nouveau système de surveillance de la circulation et de détection des flux de circulation afin d'éviter les accidents en utilisant les différences cumulatives de premier plan. Les résultats ont montré que la méthode est efficace et peut être considérée comme une composante du système intelligent de surveillance du trafic.

La nature du VCC a un moyen de communication ouvert, des changements rapides de topologie, et dynamique. Ainsi, l'un des principaux défis est l'échange d'informations en raison de la nature du VCC peut être falsifié et peut mener au partage de fausses informations entre conducteurs et passagers. Les auteurs de [89] ont présenté une nouvelle méthode en utilisant la cryptographie par courbe elliptique (ECC) pour assurer la sécurité des communications afin de garantir l'authentification, l'intégrité, la confidentialité et la confidentialité entre l'expéditeur et le destinataire[90].

Les auteurs de [91] ont présenté une nouvelle méthode, le système de calcul en cloud vérifiable par véhicule (Trust-Based Verifiable Vehicular Cloud Computing scheme -PTVC) basé sur la confiance et respectant la vie privée, pour améliorer la sécurité du trafic et offrir des services aux passagers et conducteurs [91]. Le mécanisme PTVC système fusionne entre les meilleurs avantages du VCC, les techniques de vérification, et les exigences de confidentialité, pour sélectionner le véhicule digne de confiance parmi les autres véhicules pour créer un véhicule en cloud. Le système PTVC prouve son efficacité, sa sécurité et sa robustesse contre plusieurs attaques.

11 Conclusion

Dans ce chapitre, nous avons présenté un aperçu sur les réseaux véhiculaire en cloud à travers une présentation globale du réseau, son architecture, les modèles de service pour le fonctionnement, et la taxonomie du réseau. Les applications du réseau véhiculaire en cloud sont caractérisées par la multitude et diversité, ce qui rend ce type de réseau très intéressant, alors il faut que l'utilisation du réseau soit en toute sécurité.

Pour donner un aperçu de la sécurité dans réseaux véhiculaire en cloud, nous avons fait un tour sur les exigences de sécurité, la classification des attaques et l'impact de ces attaques sur le modèle basé sur les services et les exigences de sécurité.

L'interprétation et l'analyse de l'impact des attaques nous donnent une idée des exigences les plus affectées, ce qui nous amène à proposer une solution pour renforcer la sécurité en VCN. A la lumière de cette analyse, nous avons déduit que les solutions basées sur la cryptographie vont renforcer les exigences les plus touché par les attaques (qui améliorent la confidentialité, l'intégrité, la disponibilité et la confidentialité)

Chapitre IV

La sécurisation du réseau véhiculaire en cloud

1 Introduction

La cryptographie est un moyen pour sécuriser les échanges entre deux entités, elle est basée sur un algorithme de cryptographie et une clé. Dans la cryptographie symétrique la clé doit être connue par les deux entités, ce type de cryptographie est caractérisé par un faible temps et de ressources de traitement, mais il est généralement cassable. L'autre type de cryptographie qui est la cryptographie asymétrique, consiste à crypter avec une clé et décrypter avec une autre, de ce fait chaque entité doit avoir une paire de clés. L'une des clés doit être rendu publique et une autre doit rester en secret. D'où la nécessiter d'une autorité de confiance ou toutes les entités doivent publier leurs clés publiques. Les clés publiques sont échangées entre entités sous le nom de certificats, où chaque certificat contient des informations identitaires et la clé publique.

La solution est standardisée et connue sous le nom « publique key infrastructure » PKI, la PKI a permet d'entreprendre des opérations cryptographiques telles que le chiffrement et la signature numérique. Ces opérations servent à garantir la confidentialité, l'authentification, l'intégrité et la non-répudiation lors des échanges sécurisé.

D'après l'analyse faite sur les attaques dans le chapitre précédent, la PKI et les certificats vont renforcer la sécurité dans les réseaux VCN.

Dans ce qui suit nous allons présenter quelques notions de base sur la cryptographie avant d'enchainer sur une proposition d'une solution complète basée sur la PKI dans les deux cas, centralisée (présence de la composante RSU pour accéder à l'autorité de certification), et décentralisé (en cas d'absence d'un accès à l'autorité de certification) en introduisant la technologie émergente blockchain. L'architecture du système proposé contient des autorités avec des niveaux différents pour garantir la sécurité, la vie privée et le service cloud.

2 Revue de la littérature

La cryptographie présente l'avantage de traiter et de résoudre plusieurs brèches de sécurité VANET à la fois [3]. Par exemple, le déploiement d'une autorité centrale de validation (VA) ou d'une PKI véhicule (VPKI)[92][93] pour l'authentification entre véhicules et la signature de messages d'avertissement résout des problèmes de sécurité comme les attaques sybil, replay et illusion. De plus, l'utilisation d'algorithmes de chiffrement fort et de génération de clés permet d'éviter plusieurs attaques telles que l'analyse du trafic, la force brute et l'écoute illicite.

Dans la présente synthèse documentaire, nous nous concentrons essentiellement sur les travaux existants relatifs aux solutions basées sur la cryptographie et la génération de clés pour les communications de groupe sécurisées dans les réseaux VANET.

Cette alternative peut résoudre simultanément plusieurs problèmes de sécurité et interdire par exemple à un intrus d'écouter ou de communiquer avec un groupe de véhicules[94][95]. L'absence de telles propositions techniques dans la littérature pour les réseaux VCC a été notre principale motivation pour proposer notre contribution détaillée plus loin. A notre connaissance, aucun travail antérieur n'a été consacré à l'utilisation de cryptographie asymétrique et le système à infrastructure PKI pour les VCCs.

Boyd présente dans [96] un exemple de l'approche distribuée qui utilise les concepts de la cryptographie asymétrique. Une clé de conférence de groupe doit être générée à partir des contributions de tous les membres. Cette clé de groupe est *f(C1 ; C2 ; :::: ; Cn)* où f est une fonction et Ci est la contribution du participant *i*. En dehors du chef de groupe, les membres du groupe envoient leurs contributions en clair à l'ensemble du groupe. Le responsable du groupe a crypté sa contribution avec la clé publique de chaque participant, et envoie les messages des composés à l'ensemble du groupe. Tous les membres du groupe peuvent alors déduire la clé de groupe.

Sur la base du système d'échange de clés Diffie-Hellman, Steiner et al. ont proposé une extension adaptée aux groupes d'utilisateurs[97]. Ce protocole, appelé GDH pour Generic ou Group DH a également fait l'objet de plusieurs versions, GDH-1, GDH-2 et GDH-3. Le plus courant est GDH-2 qui est la version originale du système CLIQUES[98]. Dans ce système, Steiner et al. décrivent des protocoles adaptés aux groupes dynamiques. En effet, ils présentent un protocole pour la génération initiale de clés appelé IKA (Initial Key Agreement) et des protocoles pour la régénération et la gestion des clés pour les groupes dynamiques appelés AKA (Auxiliary Key Agreement). CLIQUES a servi pour de nombreuses solutions récemment développées pour l'échange de clés collaboratives.

Pour faire face aux fameux problèmes de gestion des clés dans les VANET, tels que la connectivité limitée et la communication sensible avec une autorité centrale de certification, Busanelli et al[99] ont proposé une nouvelle approche de gestion des clés pour sécuriser les communications VANET.

En particulier, ils fournissent un environnement pour la multidiffusion des clés de groupe. Leur environnement est conçu en fonction d'un scénario de communication propre à VANET. En fait, ils ont proposé un schéma de génération d'une série de clés secrètes de courte durée, partagées par tous les abonnés d'un service spécifique. L'application cible les communications V2V et consiste à diffuser en toute sécurité des informations détenues par un petit nombre d'utilisateurs privilégiés à un plus grand nombre d'utilisateurs non privilégiés.

Nous avons déjà étudié dans le chapitre précédent les aspects et les défis de sécurité de VCC et l'impact des attaques sur les exigences de la sécurité pour apporter une contribution pratique à ce type de problèmes à l'aide d'outils cryptographiques.

3 Primitives et outils cryptographiques

Nous désignons par primitives cryptographiques, tous les services de sécurité que la cryptographie fournit. La cryptographie moderne offre plusieurs techniques de sécurité telles que la confidentialité, l'authentification, l'intégrité, la non-répudiation, le partage secret, etc [3].

Pour satisfaire ces services de sécurité, la cryptographie utilise des méthodes telles que les algorithmes de cryptage / décryptage, les protocoles de génération et d'échange de clés, les fonctions de hachage, la signature numérique et bien d'autres techniques. Dans ce qui suit, nous allons présenter les différentes primitives cryptographiques [93].

3.1 Cryptage/Décryptage

Le principe de cryptage et de décryptage d'un message, décrit schématiquement dans la figure, est le suivant :

- Un algorithme de cryptage / décryptage, qui est un ensemble d'opérations de traitement d'informations basées sur des fonctions mathématiques, reçoit en entrée un message clair et une clé de cryptage, puis émet un message crypté.

- L'algorithme de cryptage / décryptage reçoit en entrée un message crypté et une clé de décryptage, puis émet le message clair correspondant [3].

3.2 Cryptographie symétrique

Aussi appelée cryptographie à clé secrète. Pour cette technique, la clé de décryptage peut être facilement calculée à partir de la clé de cryptage, car ce type de cryptographie utilise la même clé de cryptage pour décrypter. La sécurité en cryptographie symétrique est basée sur la capacité à garder la clé en secret entre les parties en communication. Si la clé est révélée, le système est menacé.

La nécessité que les deux parties aient accès à la clé secrète est l'un des principaux inconvénients de la cryptographie symétrique par rapport à celle asymétrique [3].

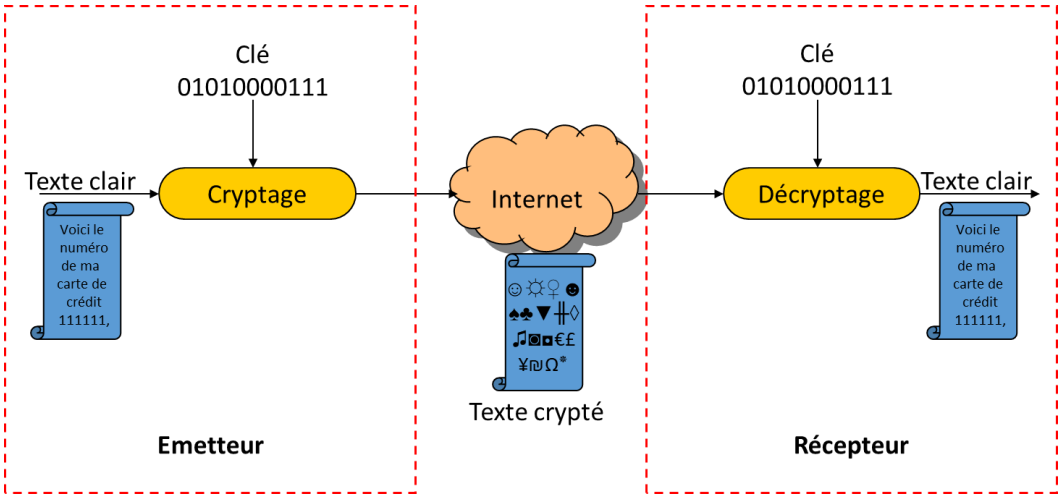

Figure IV.1: Cryptographie symétrique

3.3 Cryptographie asymétrique

Aussi connu sous le nom de cryptographie à clé publique. Le principe de fonctionnement est le suivant :

- Chaque utilisateur possède une paire de clés, une clé privée qu'il doit garder secrète et l'autre clé publique qu'il doit mettre à la disposition du public.

- Si nous cryptons avec la clé publique, seule la clé privée peut décrypter et vice versa.

- Il est pratiquement impossible (temps et ressources) de déterminer par exemple la clé privée connaissant la clé publique et vice versa.

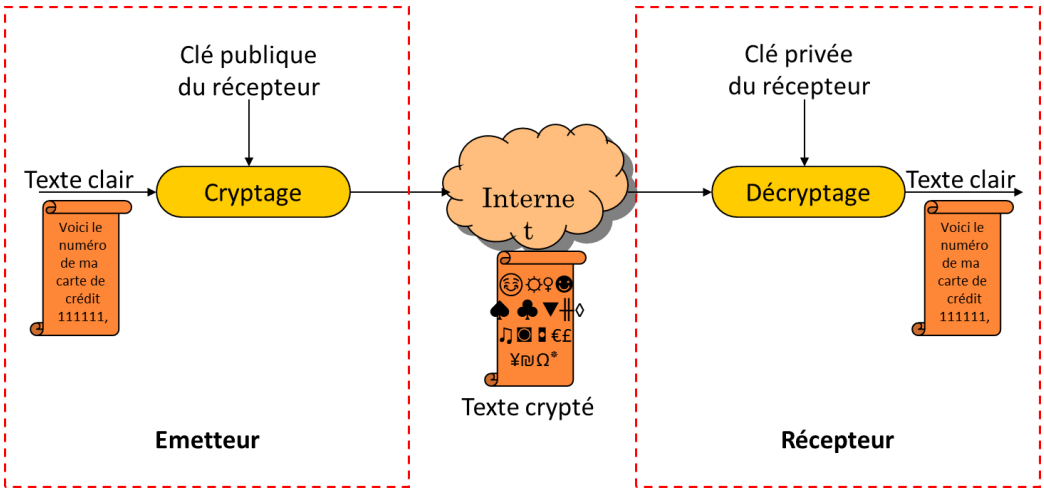

Figure IV.2: Cryptographie asymétrique

La cryptographie asymétrique peut également être utilisée dans le cryptage, mais par rapport aux algorithmes symétriques, elle est généralement plus lente. Il est principalement utilisé dans

les procédures d'échange de clés et dans l'outil d'authentification de signature numérique au moyen de certificats numériques. La cryptographie à clé publique résout plusieurs problèmes que la cryptographie à clé secrète ne réussit pas à résoudre [3].

3.4 PKI, certificats numériques et estampillage temporel

PKI, certificats numériques et estampillage temporel La gestion des clés privées et publiques pour un grand nombre d'utilisateurs nécessite la mise en place d'une PKI : Public Key Infrastructure, qui est un ensemble de composants logiciels, matériels et procédures.

3.4.1 Éléments de la PKI

3.4.1.1 Autorité de certification (Certification Authority - CA)

L'autorité de certification est un tiers de confiance qui authentifie les entités participant à une transaction électronique. Pour authentifier une entité, la CA délivre un certificat numérique. Ce certificat est un document numérique qui établit les références des entités participant à une transaction. Les certificats numériques émis par les CA contiennent des informations telles que le nom de l'abonné, la clé publique, ainsi que la clé publique de la CA délivrante. Cette information dépend de la politique de l'entreprise qui délivre les certificats.

Avant de délivrer un certificat numérique, la CA vérifie la demande de certificat auprès d'une autorité d'enregistrement (Registration Authority -RA). Pour valider les demandes de certificat, une CA utilise ses propres procédures. Ces procédures dépendent de la politique de l'organisation et de l'infrastructure disponible pour valider la demande. Si la demande est validée, la CA délivre le certificat [100].

Le rôle de CA est semblable à un notaire. La CA confirme l'identité des parties qui envoient et reçoivent des paiements électroniques ou d'autres communications. L'authentification est un élément nécessaire pour de nombreuses communications formelles entre les parties, y compris les opérations de paiement. Dans la plupart des transactions d'encaissement de chèques, un permis de conduire avec photo suffit pour l'authentification. Un numéro d'identification personnel (NIP) permet l'authentification électronique des transactions effectuées au guichet automatique bancaire (GAB) [101].

3.4.1.2 Autorité d'enregistrement (Registration Authority -RA)

Une RA est responsable de l'interaction entre les clients et les CAs. Souvent, en raison de la majorité des demandes de certificats, il n'est pas possible pour la CA d'accepter les demandes de certificats, valider les demandes et émettre les certificats. Dans ce genre de cas, la RA agit comme intermédiaire entre la CA et le client. Les tâches accomplies par la RA sont les suivantes:

- Recevoir les demandes des entités et les valider
- Envoyer les demandes à la CA.
- Recevoir le certificat traité de CA.
- Envoyer le certificat à l'entité concernée.

Les RA sont particulièrement utiles pour la mise à l'échelle des applications PKI sur différents sites géographiques. Par exemple, une CA peut déléguer ses responsabilités à différentes RA et attribuer une zone d'exploitation à chaque RA, comme une RA pour la région du Nord, la région du Sud et les régions de l'Est et de l'Ouest [100].

Une autorité d'enregistrement (RA) est une entité à laquelle la CA fait confiance pour enregistrer ou garantir l'identité des utilisateurs auprès d'une CA [101].

3.4.1.3 Les clients de la PKI

Les entités qui demandent aux CA ou aux RA de délivrer des certificats sont communément appelées clients de PKI. Pour obtenir un certificat numérique d'une CA, un client PKI doit effectuer les étapes suivantes :

1. Envoyer une demande pour générer une paire de clés public-privé. Une CA ou le client peut effectuer cette tâche. La paire de clés contient les détails du client.

2. Une fois la paire de clés générée, une demande est envoyée à la CA pour le certificat de la CA. Cette demande peut être acheminée par le biais d'une RA.

3. Une fois que le client a reçu le certificat de la CA, il peut l'utiliser pour s'identifier comme étant un détenteur de certificat authentifié.

Toutes les communications entre un client et la CA sont sécurisées. De plus, le client est responsable de la sécurité de sa clé privée. Si la clé privée est perdue, le message crypté ne peut pas être décrypté.

De plus, si la clé privée est piratée, toute personne non autorisée peut utiliser cette clé privée pour déchiffrer les messages. Dans de telles situations, la nécessité de sécuriser la clé privée devient plus évidente [100].

3.4.1.4 Certificats numériques

Il est important d'assurer la sécurité d'une clé publique pour éviter les brèches de sécurité liées à l'usurpation d'identité et à la modification de clé. Par conséquent, un mécanisme d'intégrité des données est nécessaire pour s'assurer qu'une clé publique modifiée ne passe pas inaperçue. Toutefois, les mécanismes d'intégrité des données ne suffisent pas à eux seuls à garantir que la clé publique appartient au propriétaire revendiqué. Il faut un mécanisme qui lie la clé publique à une partie de confiance globale qui peut assurer l'identité et l'authenticité de la clé publique. Le mécanisme souhaité devrait permettre d'atteindre les deux objectifs suivants :

- Établir l'intégrité de la clé publique
- Lier la clé publique et les informations associées au propriétaire d'une manière fiable.

Dans l'environnement PKI, les certificats numériques atteignent ces objectifs. Les certificats garantissent que seule la clé publique d'un certificat authentifié par une autorité de certification fonctionne avec la clé privée possédée par une entité. Cela élimine le risque d'usurpation d'identité.

- Un certificat comprend les éléments suivants :
- Numéro de série du certificat
- Signature numérique de la CA
- Clé publique de l'utilisateur auquel le certificat est délivré
- Date d'expiration
- Nom de la CA qui a délivré le certificat

Après l'obtention d'un certificat numérique, l'entité peut l'utiliser pour communiquer avec les destinataires de l'information de la manière suivante :

1. L'abonné signe numériquement le message avec sa clé privée pour assurer l'intégrité du message et sa propre authenticité et envoie le message au destinataire.
2. Le destinataire, après avoir reçu le message, vérifie la signature numérique avec la clé publique de l'abonné et interroge la base de données globale de l'annuaire pour vérifier la validité du certificat numérique de l'abonné.
3. La base de données de l'annuaire global renvoie l'état du certificat numérique des abonnés au destinataire. La transaction n'est effectuée que si le certificat est valide.

La CA signe les certificats numériques. Pour vérifier une signature, la clé publique de la CA est nécessaire. La clé publique fait partie du certificat numérique de la CA. Ces certificats sont généralement préinstallés dans les navigateurs Web.

Une fois qu'un certificat a été délivré, il doit être distribué aux utilisateurs et aux organisations. Ceci est fait par un système de distribution de certificats (CDS) ou un répertoire.

3.4.1.5 Système de distribution de certificats (CDS)

Le Système de distribution de certificats (CDS) distribue des certificats aux utilisateurs et aux organisations. Ces certificats peuvent être distribués de deux façons selon la mise en œuvre de la PKI dans l'organisation. Les certificats peuvent être distribués par les utilisateurs eux-mêmes ou par un serveur d'annuaire qui utilise LDAP pour interroger les informations stockées dans une base de données. La CDS distribue les certificats en collaboration avec un serveur d'annuaire. Le système de distribution est utilisé pour effectuer les tâches suivantes [100]:

- Générer et émettre des paires de clés
- Certifier la validité des clés publiques en signant la clé publique
- Révoquer les clés expirées ou perdues
- Publier les clés publiques dans le serveur de service d'annuaire

4 Les défis de sécurité de VANETs cloud et les solutions cryptographiques

Une pléthore de solutions cryptographiques ont été proposées dans la littérature pour éviter ou atténuer les attaques mentionnées ci-dessus.

Une solution proposée par[3] [102] consiste à déployer une validation de l'autorité centrale, qui valide les entités en temps réel. La validation peut être directe ou indirecte. En validation directe, l'entité a besoin d'accéder au réseau se connecte directement à l'autorité de validation. Dans la méthode indirecte, une entité déjà autorisée peut accepter une entité entrante. Pour limiter les inconvénients de cette fonctionnalité de délégation, l'autorité de validation peut utiliser ces certificats temporaires[103].

En cas de présence de liens authentiques et sécurisés avec des nœuds de confiance,[104] propose de réduire l'effet de l'attaque Sybil en validant les nœuds inconnus par la vérification de leur emplacement sécurisé.

L’auteur de [105] propose également une technique fondée sur la PKI pour atteindre cet objectif. Le changement du canal de transmission et l'utilisation de la technique du saut de

fréquence (FHSS : Frequency Hopping Spread Spectrum) ont également été proposés comme solution sécurisée. Il s'agit d'algorithmes cryptographiques pour générer des nombres pseudo-aléatoires. Cette proposition [106][107] exige une modification de la norme qui n'autorise actuellement que l'utilisation du OFDM.

Dans [108], un mécanisme d'authentification basé sur la signature numérique a été proposé pour réduire l'impact de certaines attaques du DoS. Une technique basée sur estampillage temporel a été proposée dans [109] pour appliquer des politiques d'authentification forte dans les VANETs.

L'utilisation de PKI pour garantir l'authentification entre pairs de communication et pour signer les messages échangés a été discutée dans [102]. Par exemple, l'établissement de communications de groupe[92] permettra l'échange sécurisé de clés cryptographiques gérées par un système de « Group Key Management (GKM) ». Ceci empêche un intrus de communiquer avec le groupe au moment de l'établissement de la clé de groupe. Les secrets pré-partagés peuvent également être utilisés pour écarter les attaquants pendant la phase de négociation. Cependant, cette technique est difficilement applicable dans les VANETs en raison des changements rapides dans la topologie du réseau.

Seuls quelques modèles de confiance ont été proposés pour assurer un partage fiable de l'information dans les réseaux de véhicules. Le modèle de confiance proposé par les auteurs de [110] et le modèle de gestion de la confiance à plusieurs volets proposé par Minhas et al[111] sont deux modèles typiques de confiance axés sur les entités.

Le modèle de confiance sociologique est proposé sur la base du principe de la confiance et du marquage de confiance. Raya et al[112] proposent que la confiance axée sur les données pourrait être plus appropriée dans le domaine des réseaux ad hoc éphémères tels que les VANETs. L'établissement d'un système de confiance centré sur les données permet d'évaluer la fiabilité des données communiquées par d'autres entités plutôt que la confiance des entités elles-mêmes.

5 La gestion de la confiance dans les réseaux VANET

En général, on suppose que chaque nœud d'un VANET est doté d'un système de confiance, qui permet de prendre des décisions de confiance (vérifier les déclarations, être conscient de la confiance, etc.). Il y a deux options de base pour l'établissement de la confiance : soit elle peut s'appuyer statiquement sur une infrastructure de sécurité, soit elle peut être construite de

manière dynamique et auto-organisée (voir figure IV.3). Le premier processus repose sur des paramètres système communs, globaux, fiables et bien connus (par exemple, autorité de confiance centrale TA), qui peut être utilisée pour authentifier les messages. Pour la deuxième méthode, processus manque de cette connaissance globale et de ce point de contrôle et il faut utiliser d'autres mécanismes de confiance[110].

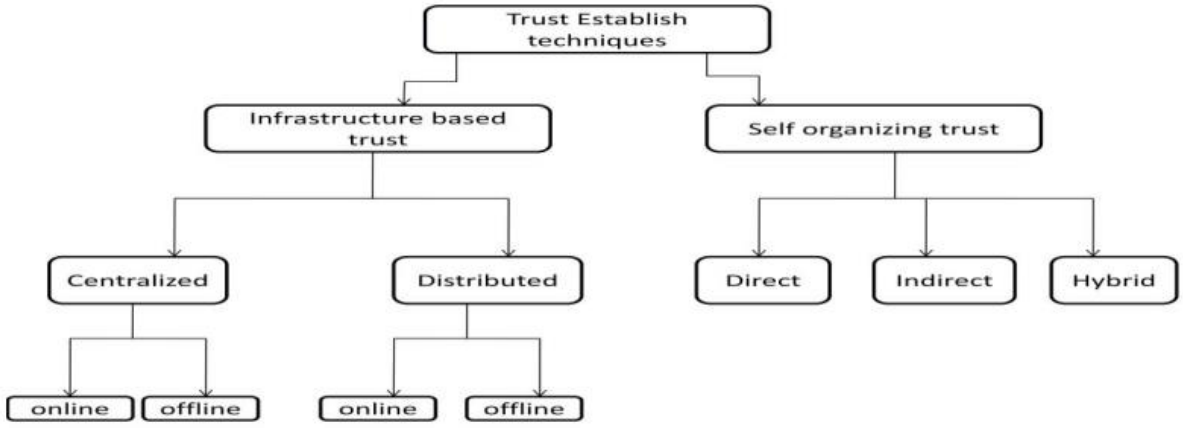

Figure IV.3: La gestion de la confiance dans les réseaux VANET [21]

1.1.1. Gestion de la confiance basée sur une infrastructures de sécurité

L'Autorité centrale certifiée (CA) fournit des certificats à tous les autres nœuds/véhicules qui fournissent l'authentification à des pairs/véhicules particuliers. La présence de RSU est nécessaire dans les modèles d'infrastructure de communication[111]. Parmi les systèmes de gestion de confiance basée sur une infrastructure on cite :

- ***Systèmes basés sur des certificats (Certificate-Based Systems CBS) :*** est un système dans lequel une autorité de certification utilise la cryptographie basée sur l'identification pour produire un certificat
- ***Kerberos :*** est un protocole d'authentification réseau qui repose sur un mécanisme de clés secrètes (chiffrement symétrique) et l'utilisation de tickets, et non de mots de passe en clair, évitant ainsi le risque d'interception frauduleuse des mots de passe des utilisateurs
- ***Les pseudonymes :*** Identifie un propriétaire, c'est-à-dire une ou plusieurs personnes le possédant mais qui ne divulguent pas leurs propres noms (leurs identités légales)
- ***Signature aveugle :*** la modification de la signature numérique, dans laquelle le contenu d'un message est masqué avant d'être signé

1.1.2. Modèles auto-organisés

Les environnements très dynamiques tels que les VANET ont besoin d'une forme adaptée pour établir un système de confiance. Les décisions relatives à la confiance envers d'autres nœuds doivent être prises de manière autonome car aucune connexion en ligne à une infrastructure de sécurité n'est possible et doivent être basées sur des informations partielles collectées à partir de nœuds inconnus pendant une courte période de temps [110].

-CONFIDANT: c'est un protocole qui offre la possibilité de détecter et d'isoler les nœuds non coopératifs d'un réseau VANET. Le protocole se concentre principalement sur les aspects le routage et le transfert. Il est destiné à être une extension d'un protocole de routage de source réactive comme le protocole DSR.

- Terminodes: ce système utilises une monnaie virtuelle appelée «nuglets» pour faire face aux nœuds égoïstes dans les réseaux VANET. Soit le routage d'un paquet doit être payé ou le paquet est abandonné. Les principaux objectifs sont d'une part d'encourager les nœuds à transférer des paquets et d'autre part de décourager les nœuds d'inonder le réseau avec trop de paquets[110].

6 Approche centralisée et décentralisée de la gestion de la sécurité

Lors de la mise en œuvre d'un système PKI, nous devons examiner si nous avons un accès à une autorité centrale qui gère les clés, sinon nous sommes dans une situation où nous devons implémenter un modèle décentralisé, dans lequel chaque utilisateur gère ses propres paires de clés.

Dans un modèle décentralisé, la distribution des clés, le processus de révocation et la garantie de l'identité et de l'intégrité des entités posent quelques difficultés.

Pour identifier ce qui convient, nous devons analyser le réseau Cloud Véhiculaire. Il contient deux domaines majeurs : VANET et le cloud computing. Le RSU est une composante importante de ce réseau, car il permet d'accéder à ces deux parties du réseau VC, et s'appuie également sur les réseaux VC avec d'autres réseaux (internet). Dans ce cas, il est possible de sécuriser le réseau avec une PKI centralisée (la présence du tiers de confiance).

Pour cela, la présence de la RSU dans le réseau est la clé pour faire le choix entre une approche centralisée ou décentralisée pour mettre en œuvre la PKI dans les réseaux VC.

Selon la taxonomie VC introduite dans la section III.5, nous notons que la RSU est présente dans deux types de VC, il s'agit du cas où les véhicules utilisent le cloud, et aussi dans le cloud inter véhiculaires.

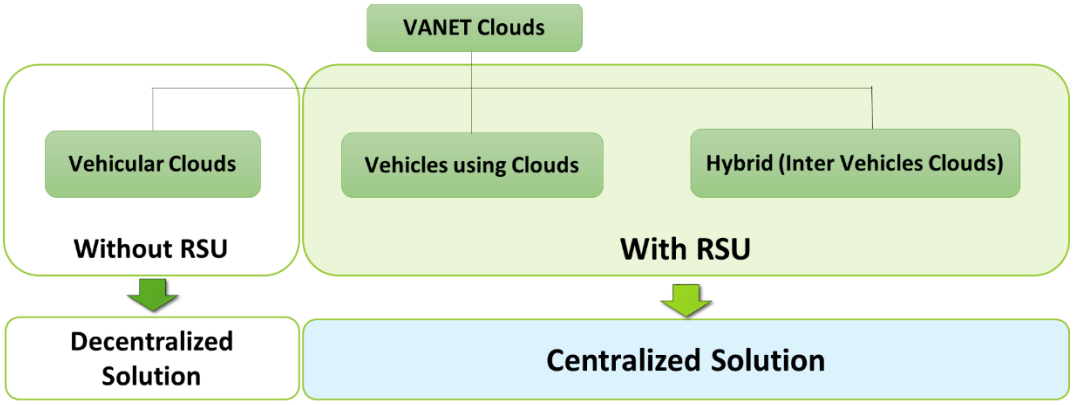

Figure IV.4: La gestion de confiance par rapport à RSU

Dans la suite nous allons présenter deux variantes de solutions basées sur le PKI, la première appelée VC-PKI (Vehicular Cloud-PKI) pour l'approche centralisée et la deuxième appelée BC-PKI (Blockchain-PKI)

7 Architecture proposée pour la sécurisation du Vehicular Cloud avec PKI (approche centralisée)

7.1 L'architecture du réseau (modèle proposé VC-PKI)

Les VCC sont composés de trois couches [113]

- La couche réseau (VANET)
- Couche d'infrastructure mobile
- Couche cloud computing

L'objectif de l'architecture de sécurisation VC est d'être en harmonie avec trois architectures principales (VANET, Cloud, PKI).

La figure IV.5 montre l'architecture du réseau et ses composants :

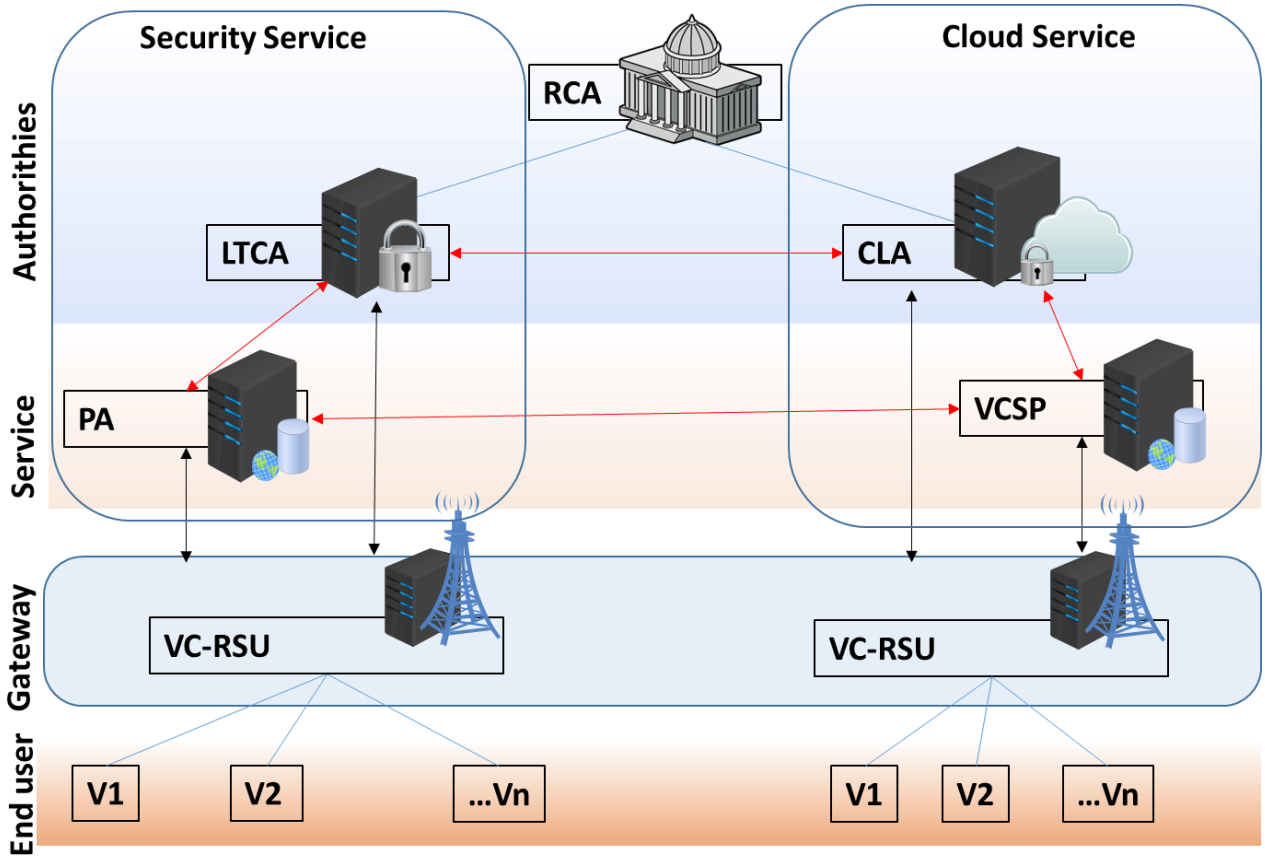

Figure IV.5: L'architecture VC-PKI

Nous expliquerons l'architecture en présentant les composants et avec une vue fonctionnelle et architecturale.

7.1.1 Composants :

- **RCA: Root CA**

La RCA est le point d'ancrage de la confiance dans le système où la confiance est supposée et non dérivée, son certificat est auto-signé. Son rôle principal est de délivrer et de signer des certificats uniquement pour les autorités subordonnées du système de sécurité VCPKI (LTCA, VCSP).

- **LTCA: Long-Term Certificate Authority**

LTCA délivre et signe un certificat à long terme pour les utilisateurs finaux du système (véhicules). Chaque entité doit envoyer sa demande directement à LTCA afin d'obtenir un certificat à long terme. De plus, la LTCA est responsable de l'émission des jetons pour les véhicules (ou autres entités), ces jetons sont utilisés pour demander des pseudonymes (certificat à court terme) à la PCA.

- **CLA: Cloud Authority**

La CLA est responsable de la gestion des comptes cloud des utilisateurs, ainsi que de l'émission de jetons pour les véhicules (ou autres entités), ces jetons sont utilisés pour demander un service cloud au VCSP.

- **VCSP: Vehicular Cloud Service Provider**

Il met le service cloud à la disposition des véhicules connectés. Pour cela, il recueille et gère les informations de l'infrastructure de calcul. Dans le cloud Véhiculaire, il existe deux types de ressources, les ressources véhicules (OBU) et les ressources informatiques (Datacenter).

- **PCA:Pseudonym Certificate Authority:**

L'utilisation de pseudonymes est importante pour protéger la vie privée des utilisateurs du réseau. Cette autorité a deux rôles principaux :

- *Délivrance de pseudonymes (certificat à court terme)*

Chaque véhicule envoie une demande au PCA le plus proche pour obtenir un ensemble de certificats pseudonymes. Ayant des identifiants pseudonymes, chaque véhicule peut communiquer avec d'autres nœuds de façon anonyme sans être surveillé, suivi ou identifié**.**

- *Résolution des pseudonymes*

La PCA est dotée d'une fonction de résolution de l'identité des pseudonymes. Cette opération est utilisée en cas de besoin, elle consiste à trouver le jeton associé à un pseudonyme spécifique, après quoi elle interroge LTCA pour identifier et révéler l'identité réelle de ce jeton. Si le pseudonyme est identifié comme étant malveillant, la PCA est en mesure de révoquer tout les pseudonymes associés.

- **VC-RSU: Local Vehicular Cloud Service Provider**

Il s'agit d'un RSU tel qu'utilisé dans VANET équipé de l'unité de calcul utilisée pour offrir plus de fonctionnalités et de services pour les véhicules.

Ainsi, le VC-RSU assure deux fonctions principales, la première consiste à gérer le réseau vanet et la seconde à gérer le cloud. La première fonction étant connue et déjà utilisée dans les réseaux VANET, la seconde consiste à offrir des services cloud locaux pour les véhicules, sans demander le service au VCSP.

7.1.2 Vue architecturale

L'architecture proposée peut être divisée en quatre couches :

- *The end users Layer:*
  Cette couche contient les véhicules connectés au VC-RSU le plus proche.
- *Gateway layer:*
  Cette couche peut être composée d'un ensemble de VC-RSU et autres équipements réseau (ex : routeurs) qui permettent l'accès direct aux autres composantes du système de sécurité (LTCA,CLA,VCSP,PCA).
- *Service Layer:*
  Dans cette couche, on trouve les composants qui permettent les services : la vie privée (PCA) et le Cloud Service (VCSP).
- *Authorities:*
  Trois éléments sont essentiels dans cette couche : La RCA (délivrer le certificat pour les composants de cette couche), la LTCA et la CLA

7.1.3 Vue fonctionnelle

Dans cette section, nous présentons des fonctions ou services, cette architecture offre deux services principaux : la sécurité et le cloud.

- *Service de sécurité :*

Ce service regroupe toutes les opérations de sécurité du réseau avec les entités de sécurité (LTCA, PCA). Ces opérations concernent essentiellement les certificats à long terme, les pseudonymes**.**

- *Service Cloud*

Ce service concerne les autorités de cloud computing (CLA, VCSP) et les opérations nécessaires pour obtenir un service cloud.

Ce service s'appuie directement sur le service de sécurité car nous voulons offrir un service cloud dans un contexte sécurisé.

7.2 Le fonctionnement du protocole VCPKI

7.2.1 Hypothèses:

- *La disponibilité des certificats des autorités*
  Les autorités (LTCA, CLA,PCA,VCSP) sont toujours en ligne, et leurs certificats sont disponibles au niveau des RSU pour les rendre accessibles aux véhicules pour effectuer différentes opérations.
- *Le module de sécurité matérielle HSM*

Chaque véhicule est équipé d'un HSM (Hardware Security Module) qui est un dispositif de calcul physique qui protège et gère les clés numériques pour une authentification forte et fournit un traitement de cryptage. Il doit être inviolable et disposer d'une API permettant l'échange d'informations avec les autres modules de l'architecture de sécurité qui fonctionne sur l'OBU[114] .

- *Identifiant du véhicule*

Chaque véhicule du réseau VC doit avoir un identifiant qui sert à identifier de manière unique les véhicules, cet identifiant peut être composé de deux parties, la première étant le VIN (numéro d'identification du véhicule), la seconde est l'identifiant de l'utilisateur sur le réseau.

Pourquoi utiliser ces deux parties, parce qu'un véhicule peut avoir plus d'un utilisateur dans une période de temps (exp : location de voiture), et si un véhicule est détecté comme malveillant, en réalité, le conducteur du véhicule est détecté comme malveillant.

- *Utilisation du service cloud*

Chaque véhicule qui veut faire une demande pour le service cloud doit avoir un LTC (Long Term Certificate) valide, qui est utilisé pour fournir un service cloud sécurisé et avec anonymat.

De plus, chaque utilisateur du service cloud doit avoir un compte cloud, où les exigences de l'utilisateur sont sauvegardées et le service est géré.

7.3 Service de sécurité :

7.3.1 Demande de certificat à long terme:

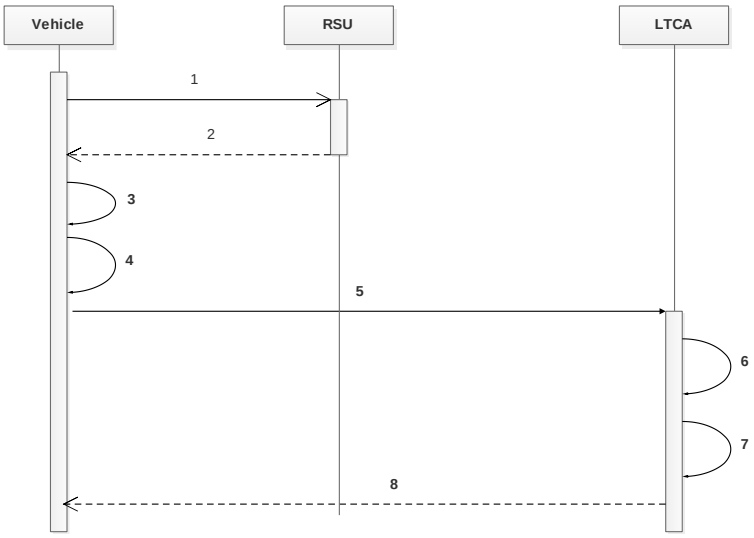

Figure IV.6: Demande de certificat à long terme

1. Le véhicule demande le certificat de l'autorité du RSU.
2. Le RSU envoie le certificat de l'autorité (LTCA) au véhicule.
3. Le véhicule génère une paire de clés (publique et privée) à courbe elliptique.
4. Le véhicule crée une demande de signature de certificat (CSR), cryptée par la clé publique de la LTCA.
5. Le véhicule l'envoie en ligne à LTCA.
6. LTCA établit un nouveaux LTC.
7. LTCA charge sa clé privée, signe LTC et crée un certificat.
8. LTCA le renvoie à l'abonné.

7.3.2 Demande d'un certificat de pseudonyme:

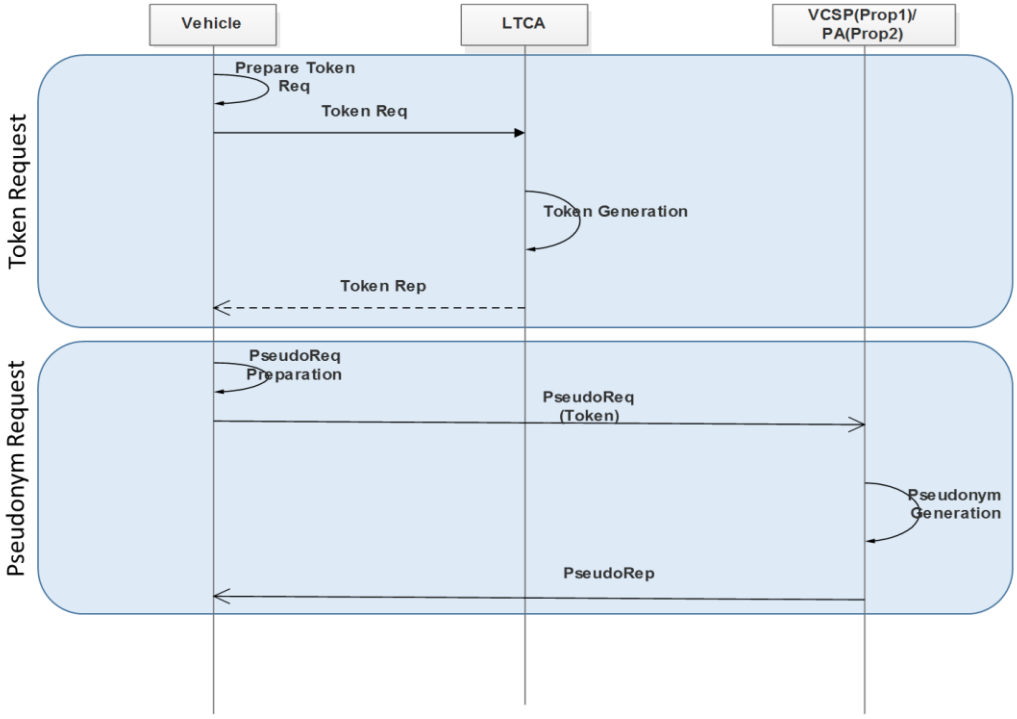

Figure IV.7: Demande d'un certificat de pseudonyme

a. Obtenir un jeton de sécurité:

1 : Préparer une demande de jeton

2 : Envoyer la demande de jeton à la LTCA

3 : Génération de jetons

4 : Retransmission du jeton

5 : Stocker le jeton dans HSM pour l'utiliser dans la phase suivante

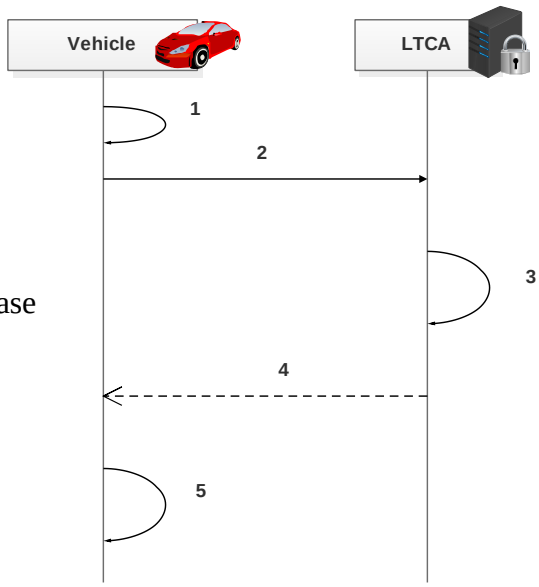

Figure IV.8 : Obtenir un jeton de sécurité

7.3.2.1 Obtenir un certificat de pseudonyme:

1 : Le véhicule prépare la demande de pseudonyme

2 : Le véhicule envoie la demande de pseudonyme au PCA, dans cette demande le jeton de sécurité est envoyé comme paramètre.

3 : Le PCA vérifie la requête et le jeton, et génère un ensemble de pseudonymes

4 : Le PCA envoie les pseudonymes générés au Véhicule

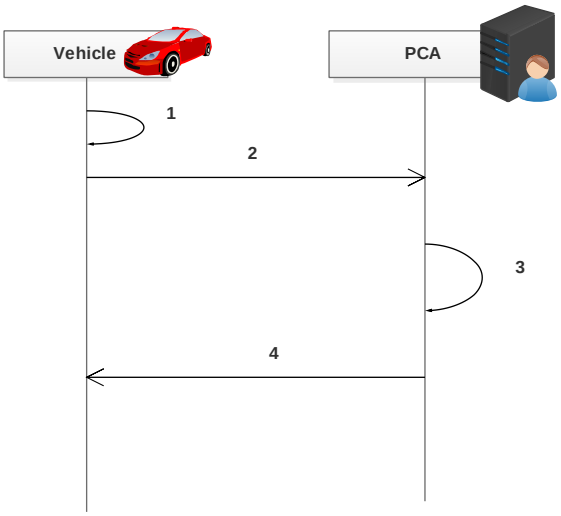

Figure IV. 9 : Obtenir un certificat de pseudonyme

7.3.2.2 Résolution des pseudonymes

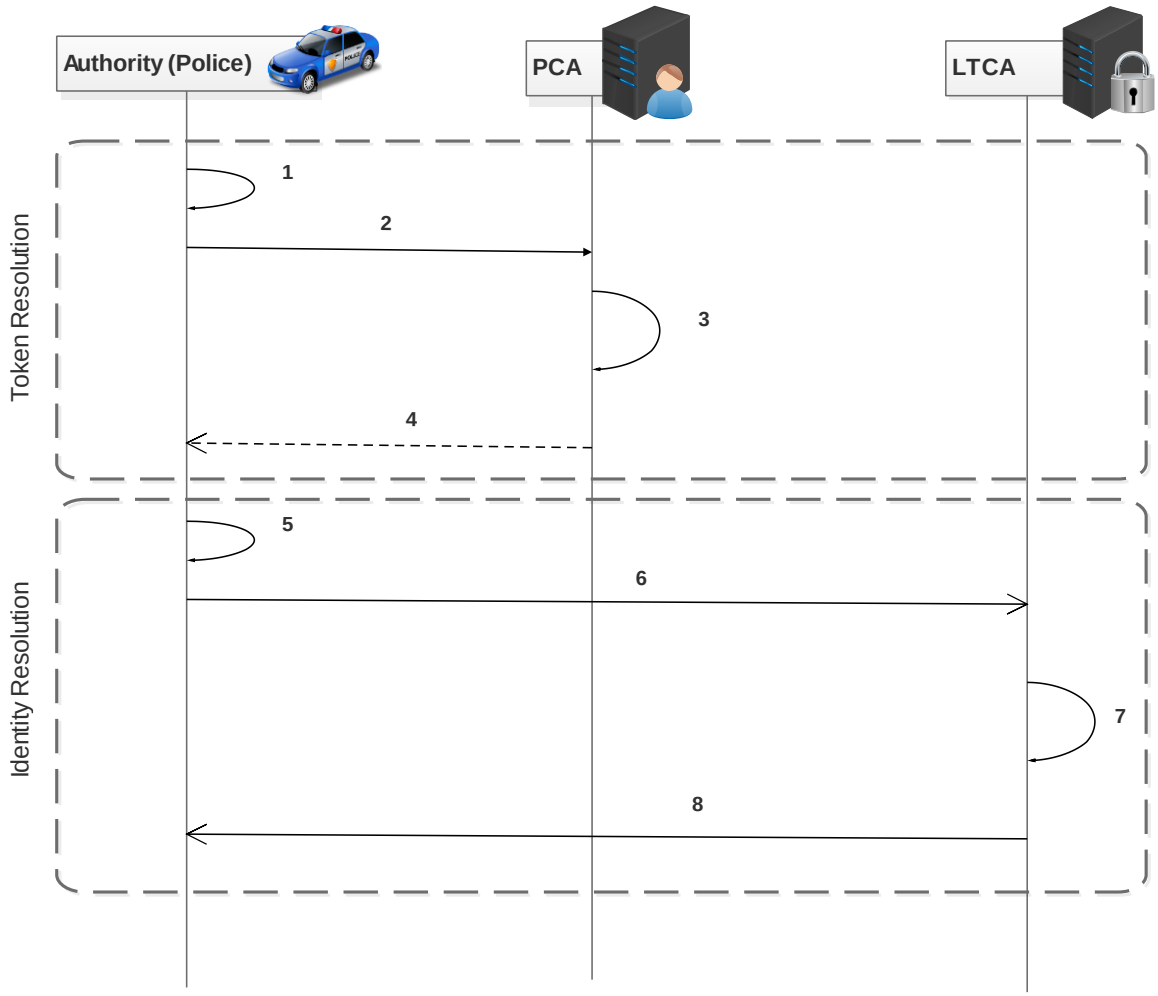

Figure IV.10: Résolution des pseudonymes

Étape 1 : Résolution du jeton

1: L'autorité (police) obtient le pseudonyme du nœud malveillant du réseau et prépare la requête de TokenResolutionRequest

2: L'autorité envoie TokenResolutionRequest au PCA, où le pseudonyme du nœud malveillant est envoyé comme paramètre

3: Le PCA trouve le jeton correspondant pour le pseudonyme

4: Le PCA envoie le jeton à l'autorité par le TokenResolutionReplay.

Étape 2 : Résolution de l'identité

5: L'autorité prépare la DemandeIdentitéRésolution.

6: L'autorité envoie une demande d'IdentitéRésolutionRequest à la LTCA.

7: Le LTCA trouve l'identité correspondante au jeton et prépare le message de réponse.

8: La LTCA envoie le IdentityResolutionReplay où le résultat de l'opération est envoyé.

7.4 Service Cloud sécurisé

7.4.1 Demander le service cloud

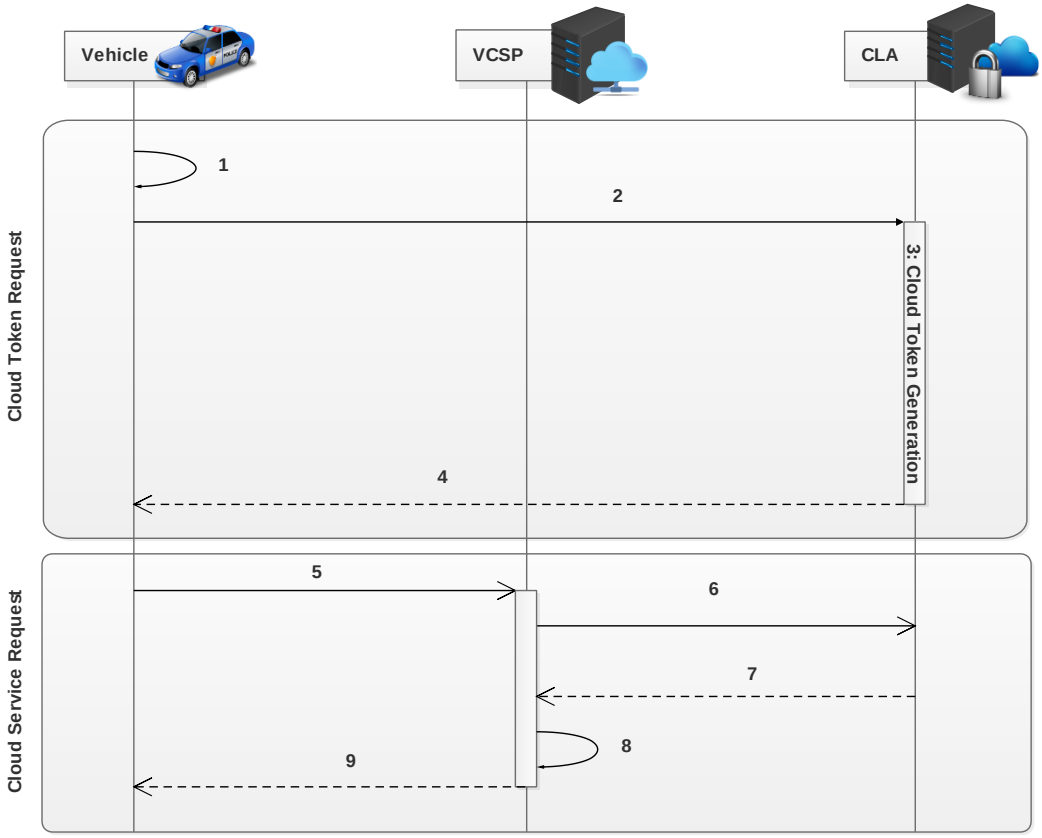

Figure IV.11: Demander le service cloud

Etape 1 : Demande de jeton cloud

1: Le véhicule prépare le jeton Cloud (demander un pseudonyme si ce n'était pas le cas auparavant)

2: Le véhicule envoie le CloudTokenRequest au CLA où l'ID du compte cloud et le pseudonyme sont envoyés comme paramètres.

3: L'Autorité de Cloud (CLA) vérifie l'ID du compte cloud et prépare un jeton pour le compte cloud de l'utilisateur.

4: L'Autorité du Cloud (CLA) renvoie le CloudTokenRepley qui contient le Cloud Token.

Etape 2 : Demande de service cloud

5: Le véhicule envoie une CloudServiceRequest au VCSP en utilisant le jeton cloud.

6: Le VCSP envoie un CloudAccountStatusReq à la CLA qui inclut le jeton.

7: La rediffusion CLA avec CloudAccountStatusRep contenant les informations sur le compte cloud.
8: Le VCSP stocke l'état du compte cloud avec le pseudonyme correspondant pour offrir le service cloud approprié.
9: Le VCSP envoie le CloudServiceReplay, si le service est accordé, le véhicule peut utiliser son pseudonyme pour utiliser son service cloud.

7.4.2 Renouvellement de la demande de service cloud

Comme il est présenté ci-dessus, le véhicule demande un Service Cloud en utilisant son pseudonyme, où les pseudonymes sont valides pour une période de temps et le véhicule peut utiliser un autre pseudonyme, pour chaque changement de pseudonyme, le véhicule envoi une requête de renouvellement du service cloud qui contient l'ancien et le nouveau pseudonyme

7.5 Analyse de la sécurité

Le protocole VCPKI vise à renforcer la sécurité pour les réseaux cloud véhiculaires, et surtout les exigences de sécurité les plus touchés par les attaques, notre analyse va se baser sur ces exigences.

7.5.1 Intégrité

Notre système est une solution basée sur PKI, les messages échangés doivent donc contenir une signature d'expéditeur valide, qui est facilement vérifiable par les autorités de certification (LTCA, PCA). Par conséquent, l'intégrité de notre système est une garantie.

7.5.2 Vie privée

Le pseudonyme est un certificat temporaire, caractérisé par l'anonymat et une courte période de validité. Ce pseudonyme est utilisé à la place du certificat numérique pour assurer la vie privée. Les pseudonymes garantissent la confidentialité dans l'utilisation du réseau, dans les réseaux VC, le défi est de garantir la vie privée dans l'utilisation du réseau et le service cloud. Pour cela, notre proposition est basée sur la séparation des autorités pour renforcer la vie privée dans le réseau et entre les autorités lors de l'utilisation du service cloud.

7.5.3 Non-répudiation

Dans le VCN et dans les situations d'urgence comme les accidents, les actions ou les changements doivent être associés à un véhicule unique (conducteur). De plus, les services dans les nuages sont offerts pour plusieurs clients, la non-répudiation est importante pour identifier

la participation du client dans toute transaction contestée. Dans le protocole VCPKI, des pseudonymes sont utilisés pour échanger des messages. L'expéditeur du message ne connaît que ce pseudonyme et, par conséquent, l'expéditeur ne peut pas répudier.

7.6 Analyse Des Performances

Pour évaluer l'impact de notre solution sur la performance du réseau, nous avons implémenté notre système VCPKI (Vehicular Cloud PKI) sur le simulateur OMNET ++ 5.0 [115] avec veins 4.4 [116] et simulateur SUMO-0.25.0[117].

Dans le tableau.1, nous présentons les paramètres de simulation

Tableau IV.1 : Les paramètres de simulation

Item	Value
Carte de tlemcen (Boujlida)	2,5km*2,5km
Temps de simulation	1000s
La Vitesse maximale	14m/s
La taille des paquets	1024 bytes
Débit	6 Mps
Le nbr de RSU	4
Portée de communication du véhicule	800m
Portée de communication RSU	800m

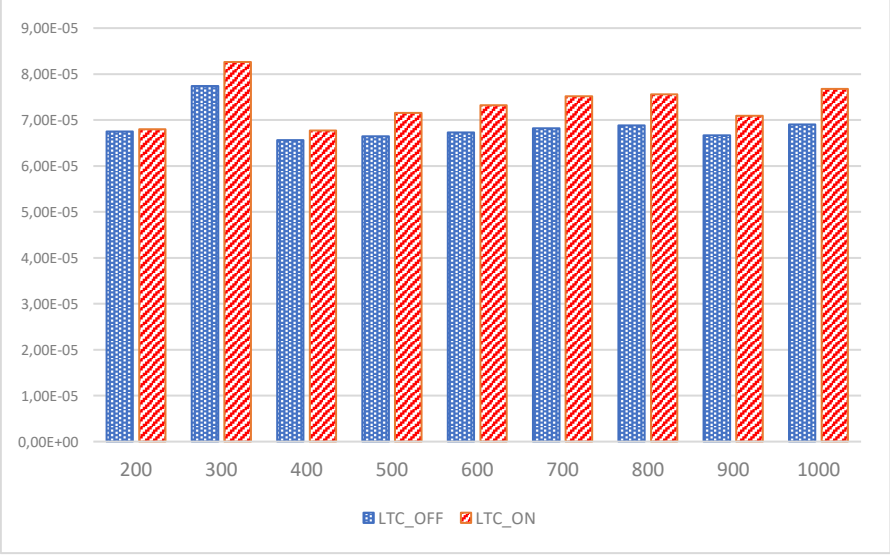

Figure IV.12. Le délai dans les réseaux VCC avec et sans VC-PKI

Dans cette simulation, nous avons mesuré le délai dans deux situations, la première sans utiliser le protocole VC-PKI, la seconde avec le réseau comme protocole de sécurité.

Dans la figure IV.12, l'axe des Xs représente le nombre de nœuds et l'axe des Ys représente le temps, comme le montre la figure IV.12, la différence est négligeable, elle se situe entre $2{,}1.10^{-5}$s et $7{,}73.10^{-5}$s.

Nous avons également mesuré le taux de distribution des paquets (PDR), comme le montre la figure IV.13 (les Xs : le nombre de neods, les Ys : le taux de perte), et il est le même pour les deux situations (avec, sans VCPKI).

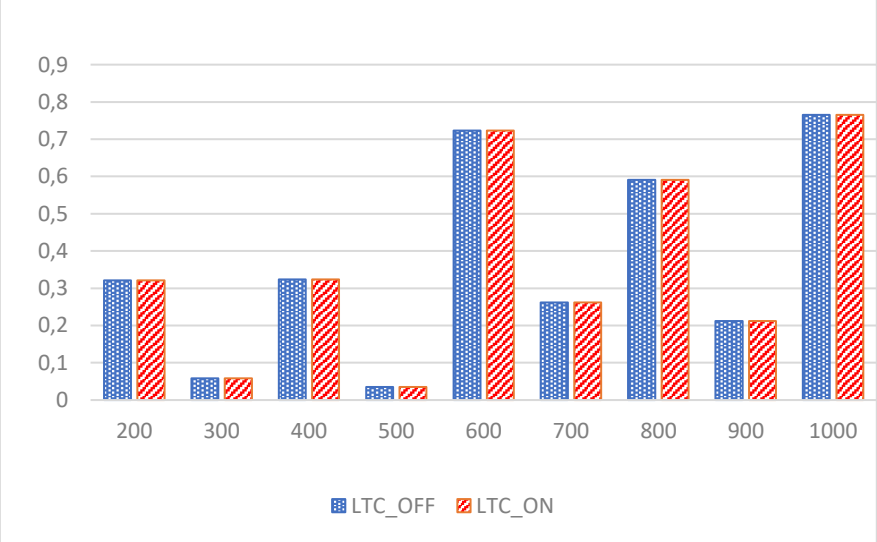

Figure IV.13 : L'impact du VC-PKI sur le PDR

Le protocole VCPKI n'a donc aucun impact sur le PDR dans le réseau.

8 BlockChain PKI (BC-PKI)

8.1 Préliminaires

8.1.1 Primitives cryptographiques

b. Fonctions de hachage cryptographique

Les fonctions de hachage cryptographique associent l'entrée d'un message de longueur arbitraire à une courte chaîne de sortie de longueur fixe. La sortie s'appelle le *hash* ou le *digest*. Les fonctions de hachage cryptographique sont formellement définies comme suit :

$$H : 0,1^* \rightarrow 0,1^{|H|}$$

Par définition, les fonctions de hachage posent les trois propriétés suivantes[118].

1. Résistance de pré-image : Il est difficile de trouver un message avec une valeur de hachage donnée.

2. Deuxième résistance de pré-image : Il est difficile de trouver deux messages avec la même valeur de hachage.

3. Résistance aux collisions : Étant donné un message, il est difficile de trouver un autre message avec les mêmes valeurs de hachage.

Les applications pratiques des fonctions de hachage sont l'authentification, les signatures numériques et le contrôle de l'intégrité des messages. Les fonctions de hachage les plus largement déployées sont MD-5, RIPEMD-160, SHA-1 et SHA-2 [118].

8.1.1.1 Arbres de Merkle

Les arbres de Merkle, aussi connus sous le nom d'arbres de hachage binaires ou arbres de hachage Merkle, ont été introduits en 1987 dans le contexte des signatures numériques [119]. Un arbre merkle (statique) est un arbre où chaque noeud de feuille est étiqueté avec le hachage d'un bloc de données et chaque noeud non feuille est étiqueté avec le hachage cryptographique des étiquettes de ses noeud fils.

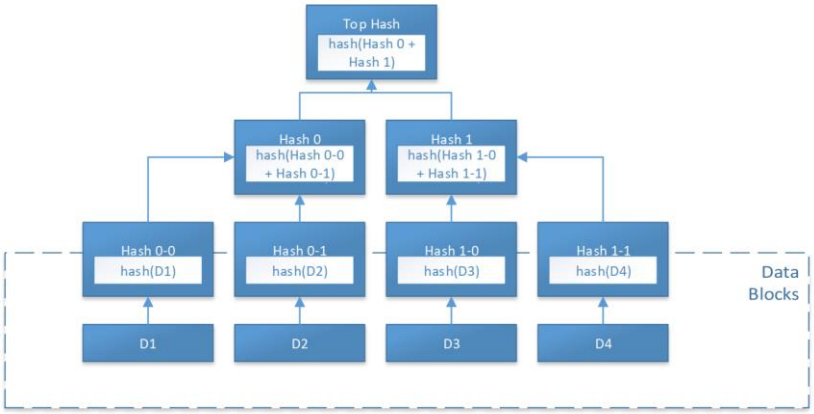

Figure IV.14 : Les arbres de merkle [127]

8.1.1.2 Tables de hachage distribuées

Une table de hachage distribuée (Distributed Hash Table - DHT) est un système distribué qui fournit un service comparable à une table de hachage, réparti sur un réseau distribué. La responsabilité de la gestion du mappage des clés aux valeurs est répartie entre tous les nœuds du réseau réparti. Les DHT sont souvent utilisées en combinaison avec des solutions de chaîne de blocs en raison de l'absence d'une partie centrale. En déployant des DHT, les nœuds sont en mesure de stocker des données sans avoir besoin d'une partie centrale.

8.2 Blockchain technology

8.2.1 Technologie de Blockchain

Un blockchain est un grand registre publique qui est répliqué parmi tous les nœuds connectés dans un réseau peer-to-peer. La technologie Blockchain a été conçue à l'origine pour stocker les transactions financières pour la crypto-monnaie Bitcoin. Présenté en 2009 par un pseudonyme nommé Satoshi Nakamoto [120], c'est le premier protocole qui a résolu le problème de la double dépense. Le problème de la double dépense est le problème d'empêcher les utilisateurs de votre système de dépenser un seul jeton numérique plus d'une fois. Là où les systèmes conventionnels ont toujours une autorité centrale de confiance qui garde la trace de ce qui a été dépensé, Blockchain doit mettre en place un système où les utilisateurs se mettent d'accord sur la validité des transactions lorsque l'état actuel du système est déterminé sur la base de schémas cryptographiques vérifiables, appelés modèles de consensus.

8.2.2 Définition

La technologie Blockchain est une forme de la Technologie du Registre Distribué [121], qui est une base de données partagée et synchronisée sur plusieurs nœuds. Chaque nœud réplique et sauvegarde une copie identique du registre. Cette technologie permet d'avoir des témoins publics pour une transaction.

La plus connue de la technologie de la chaîne de blocs est la cryptocurrencies, qui est une monnaie numérique qui utilise une forte cryptographie pour sécuriser les transactions. La chaîne de blocs est utilisée pour stocker les transcriptions de la monnaie.

8.2.3 Architecture

L'objectif principal du blockchain est de stocker les transactions. Les transactions se composent généralement d'une adresse de destinataire, d'une adresse d'expéditeur et d'une valeur. Les informations de ces transactions sont stockées dans une séquence de blocs, chaque bloc contient un pointeur vers le bloc précédent qui est en général sa valeur de hachage [121].

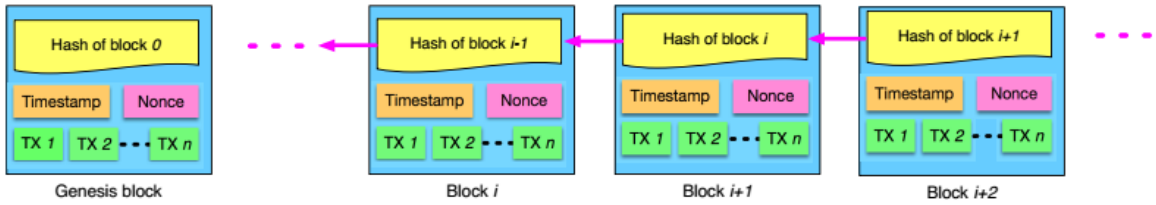

Figure IV.15 : La structures du blockchain[121]

Le premier bloc appelé « genesis block » ou bloc 0, ce bloc n'a pas de lien avec le bloc précédent.

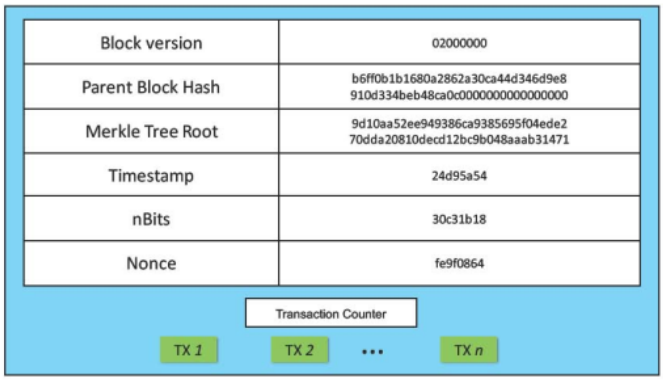

Figure IV. 16 : La structure d'un block

8.2.4 Caractéristiques

- ***Décentralisation***

Le blockchain est une technologie décentralisée, où la plate-forme n'est contrôlée par aucune autorité centralisée et où tous les nœuds du réseau peuvent ajouter, vérifier et valider des transactions en utilisant une copie du registre des transactions [121]

- ***Anonymité***

Chaque utilisateur de blockchain est identifié par une adresse publique et les transactions sont effectuées sans donner aucune information personnelle[121].

- ***Des enregistrements immuables***

La technologie de blockchain est basée sur le registre distribué, où chaque noeud a une copie du registre, ce mécanisme rend la transaction immuable.

- ***Enregistrements en temps réel***

Dans le blockchain, les transactions sont vérifiées et validées en temps réel, et les registres de blockchain sont mis à jour pour tous les participants du réseau.

8.2.5 Types de Blockchain

- ***Le blockchain publique***

Dans ce type de blockchain, tout le monde peut participer sans permission. N'importe qui peut créer, vérifier et valider des transactions. Ce type de blockchain est utilisé dans les cryptocurrencies (Bitcoin, etherieum . etc.) [122]

- ***Blockchain privé***

Dans ce type de chaîne de blocs, une autorité a le droit d'écriture, le droit de lecture peut être public ou restreint à des degrés divers. Les blockchains privés sont généralement utilisés dans la gestion des bases de données d'une entreprise [122]**.**

- ***Blockchain hybride***

Ce type de blockchain est également connu sous le nom de blockchain fédéré ou de consortium, il fonctionne sous le pilotage d'un groupe. L'utilisation de la chaîne de blocs hybride est essentielle dans le secteur bancaire [122].

8.3 Le PKI et la technonolgie blockchain (état de l'art)

La récente avancée de la technologie de blockchain a entraîné une augmentation de la recherche sur les infrastructures distribuées [123]. Dans le même temps, les récents incidents liés à la cybersécurité ont accru la recherche sur la façon d'améliorer les PKI. La PKI est actuellement largement utilisée pour établir des connexions SSL/TLS pour les sites Internet. A notre connaissance, il n'existe pas de spécification pour une infrastructure PKI complètement décentralisée avec validation fonctionnelle, récupération de clé et infrastructure de révocation de clé optimisée pour les périphériques avec un espace mémoire réduit et une faible puissance du calcul. Cette section traite des travaux existants sur les solutions PKI distribuées, en essayant de recenser toutes les recherches pertinentes qui ont été effectuées précédemment.

8.3.1 Solutions existantes basées sur le blockchain

Traditionnellement, PKI et DNS (Domain Name System) sont deux services séparés dans l'infrastructure Internet. Lorsque le DNS est utilisé pour mapper les noms de domaine aux adresses IP, une PKI est utilisée pour publier les clés associées aux identités. Dans les configurations centralisées, une PKI joue un rôle important et unique dans la vérification et la validation, garantissant qu'une clé est délivrée aux utilisateurs légitimes. Dans la recherche visant à développer des protocoles distribués, le rôle des infrastructures PKI et DNS sont souvent combinés. C'est pourquoi les sous-sections suivantes présentent souvent des protocoles qui sont développés pour une variété d'applications

c. Namecoin

Namecoin [124] a été l'une des premières modifications conçues de Bitcoin après son introduction. C'est une cryptocurrency qui est conçue pour agir comme un DNS décentralisé pour les adresses « .bit ». La cryptocurrency Bitcoin est étendue avec trois nouveaux types de transaction : name_new, name_firstupdate et name_update.

L'enregistrement d'un nom de domaine coûte 0,02 unité de Namecoin, pour les autres opérations, seuls des frais de transaction de 0,005NMC sont appliqués. Au 13 janvier 2018, ce chiffre serait d'environ 0,05 dollar. Bien que Namecoin soit initialement conçu comme un registre DNS décentralisé, il inclut la fonctionnalité d'enregistrement des certificats qui peuvent être utilisés pour authentifier l'identité associée. Namecoin a été l'une des premières solutions PKI basées sur la technologie Blockchain présentées. Il ne présente pas toutes les fonctionnalités, mais il est utilisé comme base par de nombreux protocoles. Les mécanismes de

vérification, d'authentification, de récupération de clé et de révocation de clé ne sont pas implémentés dans Namecoin. Namecoin ne serait pas non plus en mesure de gérer plus d'un milliard de nœuds avec une faible puissance de stockage et de calcul, puisque chaque nœud participant doit parcourir toute la chaîne de blocs pour rechercher des enregistrements.

8.3.1.1 Certcoin

En 2014, Certcoin[125] a été présenté. Certcoin est un système d'authentification décentralisé et accessible au public qui est basé sur Namecoin. L'enregistrement, la mise à jour et la révocation des certificats sont pris en charge. Dans ce système, chaque utilisateur doit générer une paire de clés en ligne et hors ligne (contenant une clé publique et une clé secrète).

L'utilisateur affiche ensuite ses clés publiques sur la chaîne de blocs, associées à des signatures prouvant qu'il est en possession de la clé secrète (vérifiable par chaque noeud). La clé secrète en ligne est utilisée par les utilisateurs dans le système pour authentifier les messages de et vers l'utilisateur, la clé secrète hors ligne doit être stockée en toute sécurité hors ligne. La clé secrète hors ligne fonctionne comme une sauvegarde et permet (1) de révoquer les anciennes clés et (2) de signer de nouvelles clés en cas de piratage de la clé.

Le protocole Certcoin est l'une des peu de solutions PKI distribuées qui fonctionne sur des réseaux extrêmement étendus (dans ce cas particulier, il supporte même plus d'un milliard de nœuds) et est donc considéré évolutif. En introduisant des accumulateurs cryptographiques, ce système permet aux utilisateurs de vérifier efficacement l'identité et les paires de clés sans avoir à traverser toute la chaîne de blocs.

8.3.1.2 Privacy-Aware Blockchain-Based PKI

PB-PKI [38] s'appuie sur le document-cadre Certcoin et met l'accent sur la protection de la vie privée. Tout comme dans Certcoin, un utilisateur génère une paire de clés en ligne et hors ligne. Contrairement à Certcoin, les utilisateurs de PB-PKI ne associent leur première clé en ligne qu'à leur identité, la paire de clés hors ligne est liée de manière indirecte à cette identité.

Les mises à jour, contenant de nouvelles clés publiques, ne contiennent pas d'identité. La nouvelle clé publique en ligne à chaque mise à jour est calculée en fonction de la clé publique en ligne précédente et de la clé secrète hors ligne (figure IV.17). Comme cette clé secrète hors ligne n'est connue que par l'utilisateur, un lien caché est créé entre les mises à jour et l'identité affichée initialement. Par conséquent, une fois qu'un ID d'identité est établi, les mises à jour des

clés sont anonymes. Un utilisateur ne peut pas rechercher quelle clé appartient à une identité (en supposant que cette clé a eu sa mise à jour initiale).

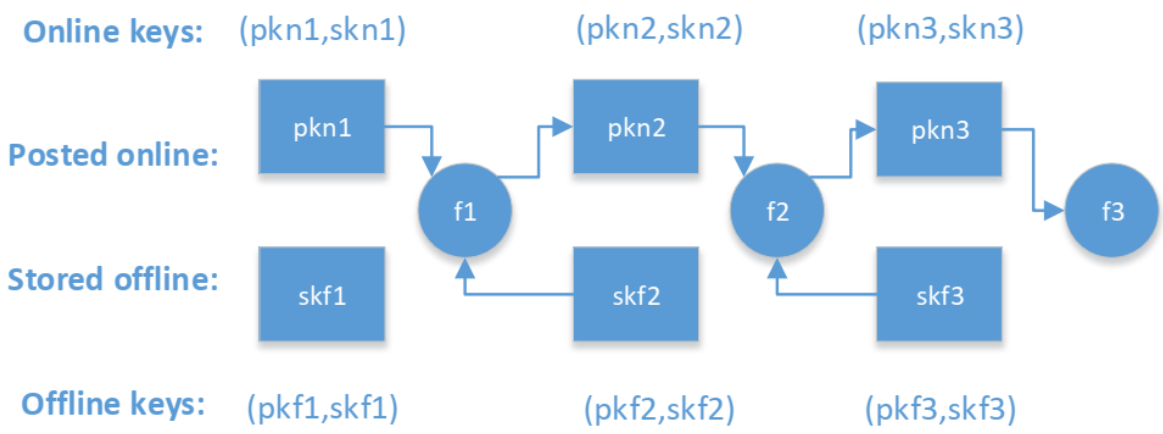

Figure IV.17 : Le protocole PB-PKI[39]

PB-PKI met en œuvre la divulgation contrôlées par l'utilisateur cela signifie que le propriétaire d'une identité enregistrée décide si le mappage d'une clé publique à son identité est affiché. Cette technique n'est donc pas utilisable dans le cas d'utilisation d'une PKI pour l'authentification des appareils IoT. Dans PB-PKI, les utilisateurs doivent enregistrer toutes les anciennes paires de clés hors ligne qu'ils ont générées dans le passé car ils doivent montrer toutes ces identités pour prouver le lien de leur identité avec une clé publique. En supposant que les clés soient renouvelées fréquemment, cela signifie que les identités devront stocker un grand nombre de clés avec le temps.

Les auteurs de PB-PKI estiment que les liens entre les identités et leurs clés publiques devraient être disponibles lorsque les services de police, par exemple, l'exigent. Pour mettre en œuvre cette fonctionnalité, ils ont décidé que, pour chaque mise à jour de clé dans leur système, chaque entité devrait partager sa clé secrète hors ligne entre une majorité du réseau utilisant un système de partage de secret. Bien que cela permette de localiser les entités qui se comportent mal, si nécessaire par connivence de la majorité du réseau, cela ajoute une couche supplémentaire de complexité et rend difficile le passage à un réseau étendu (plus d'un milliard de nœuds) sans modifications au système envisagé.

La révocation est mise en œuvre de multiples façons. En plus des deux paires de clés (en ligne et hors ligne) générées lors de la génération initiale des clés, chaque utilisateur génère également une paire de clés maître hors ligne lors de l'enregistrement initial. Cette paire de clés

maître est stockée hors ligne et n'est utilisée que pour la révocation. En cas de perte de clés, les opérations signées avec la paire de clés maître peuvent toujours annuler les opérations signées avec les autres paires de clés. Un utilisateur peut perdre sa paire de clés en ligne, sa paire de clés hors ligne et sa paire de clés maître hors ligne. Le papier décrit chaque scénario en détail, mais il est à noter que dans le pire des cas (lorsque toutes les clés sont volées), il n'existe aucun mécanisme permettant à un utilisateur de récupérer la propriété de sa clé publique. Comme mentionné précédemment, la PB-PKI n'est pas très évolutive lorsqu'on considère un réseau de plus d'un milliard de nœuds avec une faible puissance de calcul.

Chaque nœud doit garder la trace de chaque changement de clé et stocker ses clés hors ligne précédentes pour prouver le lien entre son identité et une clé publique.

Chaque mise à jour doit également être enregistrée par une majorité du réseau afin de faire le lien entre les identités et leurs clés publiques en cas de besoin par les services de police. PB-PKI ne fait pas non plus la preuve de techniques de vérification et d'authentification. Il s'agit toutefois d'un des peu de protocoles qui tient compte de la protection de la vie privée.

8.3.1.3 Blockstack

Introduit en 2016, Blockstack [128] est une conception plus récente d'un système présentant une PKI distribuée basée sur blockchain. Dans Blockstack, une architecture portable (également connue sous le nom de « blockchain agnostic ») est implémentée. Cela signifie qu'il est conçu pour être capable de lire et d'écrire à n'importe quelle blockchain et la logique d'exploitation du système de noms de domaine est dissociée de celle de blockchain sous-jacent [129].

L'architecture de Blockstack se compose de 4 couches. Une représentation graphique de ces quatre couches se trouve dans la figure IV.18 . Les couches 1 et 2 sont appelées le plan de contrôle, car leur tâche est de contrôler l'intégrité de toutes les réclamations faites dans le réseau Blockstack. La première couche de l'architecture Blockstack, la couche 1, est constituée d'une chaîne de blocs physique. Cette couche sert à deux objectifs : elle fournit le support de stockage pour les opérations et elle fournit un consensus sur l'ordre dans lequel les opérations ont été écrites[54]. La deuxième couche dans Blockstack est appelée la chaîne virtuelle. Cette couche définit de nouvelles opérations sans modifier la blockchain sous-jacente. Les nœuds de Blockchain voient les transactions brutes, mais la logique pour traiter les opérations de Blockstack n'existe qu'au niveau de la chaîne virtuelle[129]. La troisième et la quatrième couche dans Blockstack sont respectivement appelées la couche de routage et la couche de stockage, ces couches sont appelées le plan de données, puisque la tâche de ces couches est de mapper la

logique du plan de contrôle aux données. La couche de routage achemine les requêtes. Cette couche utilise des fichiers de zones pour stocker les informations de routage, ces fichiers de zones sont identiques aux fichiers de zones DNS dans leur format. Blockstack utilise un réseau basé sur DHT pour stocker les fichiers de zone. La couche de stockage héberge les valeurs de données réelles des paires nom-valeur. En stockant les valeurs de données en dehors du blockchain, il est possible de stocker des objets de taille arbitraire. Une variété de systèmes de stockage peuvent être utilisés. Le hachage des données, ou une signature de l'utilisateur, est stocké dans le plan de contrôle. Puisque les utilisateurs peuvent facilement vérifier l'intégrité des données en comparant un hachage des données avec la valeur de hachage stockée dans le plan de contrôle, les utilisateurs peuvent faire confiance aux données même si elles sont stockées dans un endroit non sécurisé. Cet plan de données peut utiliser des protocoles de stockage distribués ainsi que des protocoles de stockage non distribués (tels que Amazon S3 et Microsoft Azure). Il est à noter que Blockstack n'est pas seulement une solution PKI, mais une infrastructure pour des applications décentralisées. Il vise à adresser la centralisation à la couche applicative de l'Internet. Il a publié un navigateur open-source capable de communiquer avec le réseau Blockstack existant, ce qui permet de récupérer les identités et de stocker des informations dans son réseau.

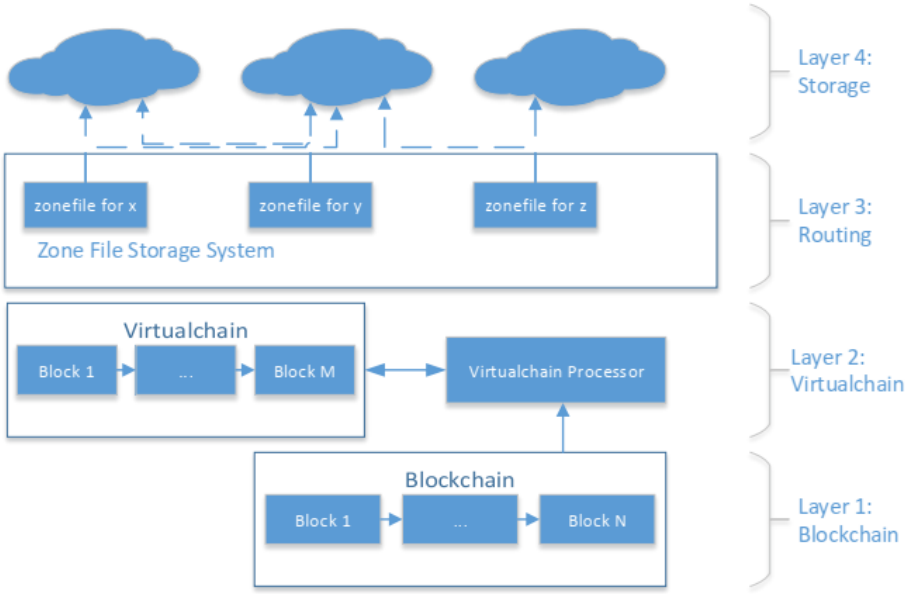

Figure IV.18 :L'architecture du Blackstack [127]

8.3.1.4 Smart Contract-based PKI and Identity System (SCPKI)

Dans Smart Contract-based PKI and Identity System (SCPKI) [130], une mise en œuvre d'une PKI décentralisée et transparente est introduite en utilisant un modèle WoT (Web of Trust). Il est construit à l'aide de contrats intelligents de la chaîne Ethereum. Tout comme dans Blockstack, ce système ne stocke pas toutes ses données sur le blockchain, il utilise une technique de stockage distribué appelée Inter Planetary File System (IPFS). La conception de SCPKI contient deux composantes principales : un contrat intelligent qui dicte le protocole système et fonctionne comme une interface connectée au blockchain pour la gestion des identités et des attributs. Le deuxième élément est un client. Le client interagit avec le contrat intelligent et d'autres systèmes tels que IPFS, pour permettre aux utilisateurs d'utiliser pleinement le système en leur permettant de rechercher et de filtrer les attributs. Le contrat intelligent SCPKI s'articule autour d'une entité représentée par une adresse Ethereum. Cette adresse Ethereum se compose d'une clé privée ou d'un contrat intelligent qu'une entité contrôle et publie un ensemble d'attributs, tels que des clés publiques ou des signatures. Comme ce système est basé sur le WoT, la confiance doit être échangée vers d'autres attributs des différentes entités du système afin de devenir fiable. Ceci peut être fait en publiant une preuve contraignante qui consiste en une signature cryptographique de l'adresse Ethereum de l'entité qui veut vérifier la confiance vers un attribut sur le réseau. Cette signature utilise la clé cryptographique représentée par l'attribut, prouvant que le propriétaire d'une clé privée est associé à une adresse Ethereum. Parce que les contrats intelligents pour le blockchain Ethereum sont utilisés, les utilisateurs doivent payer pour des opérations comme la signature et la révocation d'attributs ou la publication de contrats.

Ceci est défavorable car cela décourage les utilisateurs de soumettre des attributs inversés pour les entités qu'ils connaissent (car cela leur coûte de l'argent). Il s'agit là d'un sérieux inconvénient du protocole.

La mise en œuvre ne tient pas compte de la vie privée, elle ne convient que pour la publication des attributs que l'utilisateur souhaite rendre publics (tels que les diplômes). La vérification n'est pas prise en compte dans le système actuel, les utilisateurs peuvent soumettre la propriété d'une clé publique sans prouver qu'ils possèdent la clé secrète correspondante.

L'authentification d'autre part est implémentée à travers l'architecture WoT. Puisque l'article ne mentionne rien sur l'extensibilité, nous supposons que les nœuds doivent traverser tout le

blockchain d'Ethereum pour rechercher des valeurs. Le protocole n'est donc pas adapté aux réseaux de très grande taille avec, par exemple, plus d'un milliard de nœuds.

8.3.1.5 Authcoin

Authcoin[131] est lancé en 2016 et présente également une solution PKI distribuée avec les avantages d'un système de stockage basé sur blockchain. Authcoin utilise un système WoT où les utilisateurs doivent vérifier l'identité des utilisateurs. Authcoin implémente un schéma de validation et d'authentification basé sur la réponse aux défis. Contrairement à d'autres implémentations discutées précédemment, les étapes de validation et d'authentification doivent être franchies avant qu'un nœud puisse enregistrer la propriété d'une identité. Cette étape de validation est similaire au processus de validation déployé par "Let's Encrypt"[132].

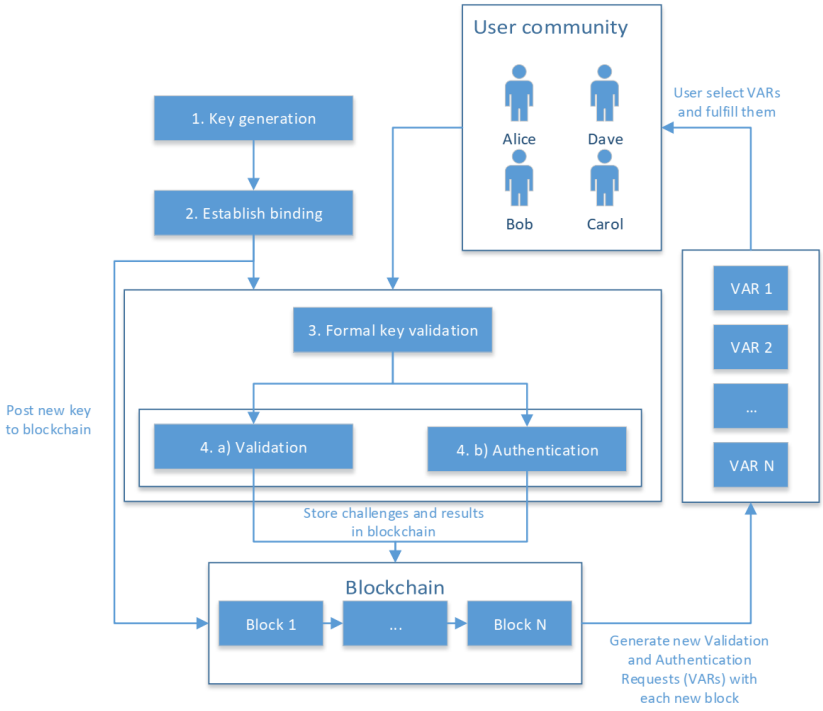

Figure IV.19 :Authcoin [39]

La figure IV.20 montre le flux de travail Authcoin. Un utilisateur ajoute la liaison qu'il souhaite au blockchain.

La validation se fait par, dans le cas d'un nom de domaine, un challenger demandant à l'utilisateur de fournir une certaine ressource sous une URI (Uniform Resource Identifier, identifiant d'une ressource sur un réseau informatique) spécifique et signant cette ressource avec

sa clé privée. Le challenger peut alors vérifier ce domaine en vérifiant simplement si la ressource signée correspond à la clé publique fournie.

Ceci ne vérifie que si une certaine entité avait effectivement accès au domaine au moment où le protocole Authcoin a été exécuté et que cette entité a également un accès aux deux clés correspondantes [43]. L'authentification fait également l'objet d'une remise en question. L'article n'introduit pas une technique standardisée mais donne quelques schémas possibles de réponse aux défis qui pourraient être exécutés.

8.4 Solution proposée (BC-PKI)

8.4.1 L'architecture du système

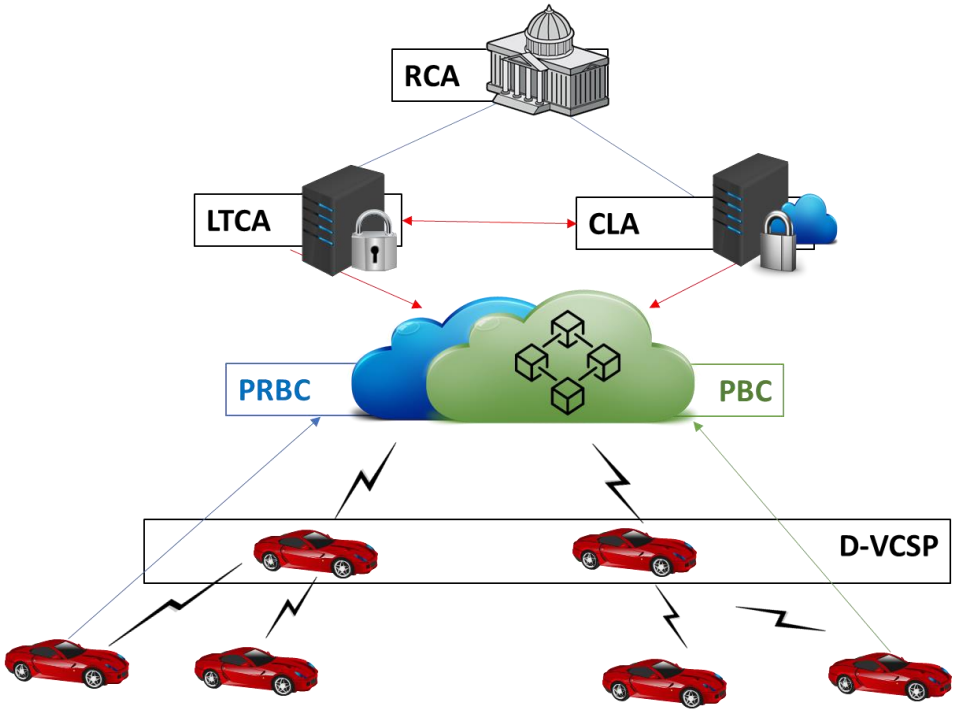

Figure IV.20: L'architecture BC-PKI

8.4.2 Les composantes du système

- ***RCA (Root Certificate Authority) :*** *Section 6.2*
- ***LTCA(Long-Term Certificate Authority) :*** *Section 6.2*
- ***CLA(Cloud Authority):*** *Section 6.2*
- ***D-VCSP(Distributed Vehicular Cloud Service Provider)***

Dans l'absence d'un accès vers le réseau internet , nous n'avons pas un accès vers les serveurs cloud, nous avons proposée une gestion distribué du cloud, et les ressources sont celles de l'ensemble des véhicule.

Pour une gestion pareil, l'ensemble des véhicules sont grouper sous-forme de cluster, et le cluster-head est une partie du serveur cloud distribué.

- ***PBC (Pseudonym BlockChain)***

C'est le blockchain où les pseudonymes sont stockés comme transaction, il agit comme un registre public pour tous les pseudonymes dans le réseau. la figure IV.21 montre la structure du PRBC

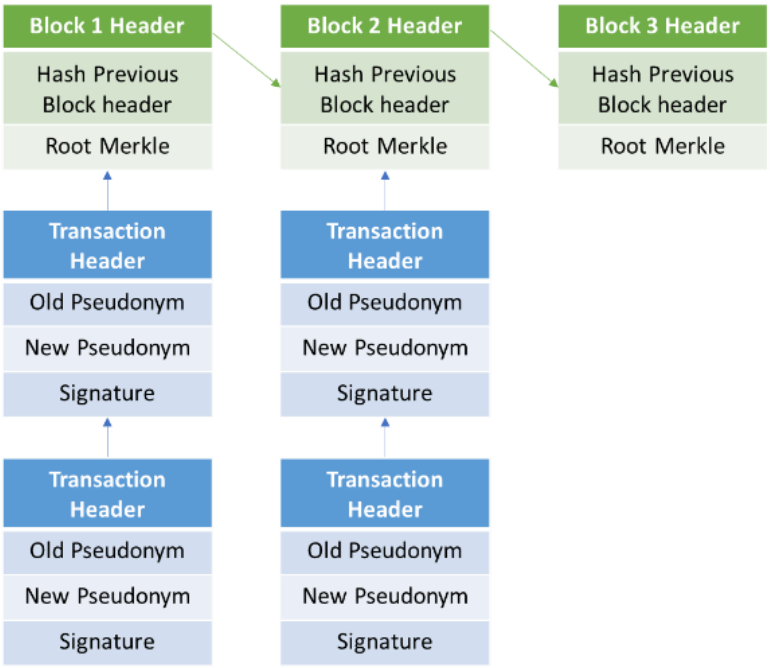

Figure IV.21: Pseudonym BlockChain

- ***PRBC (Pseudonym Revocation BlockChain)***

C'est le blockchain pour stocker la révocation de pseudonyme,la structure est détaillée dans la figure suivante :

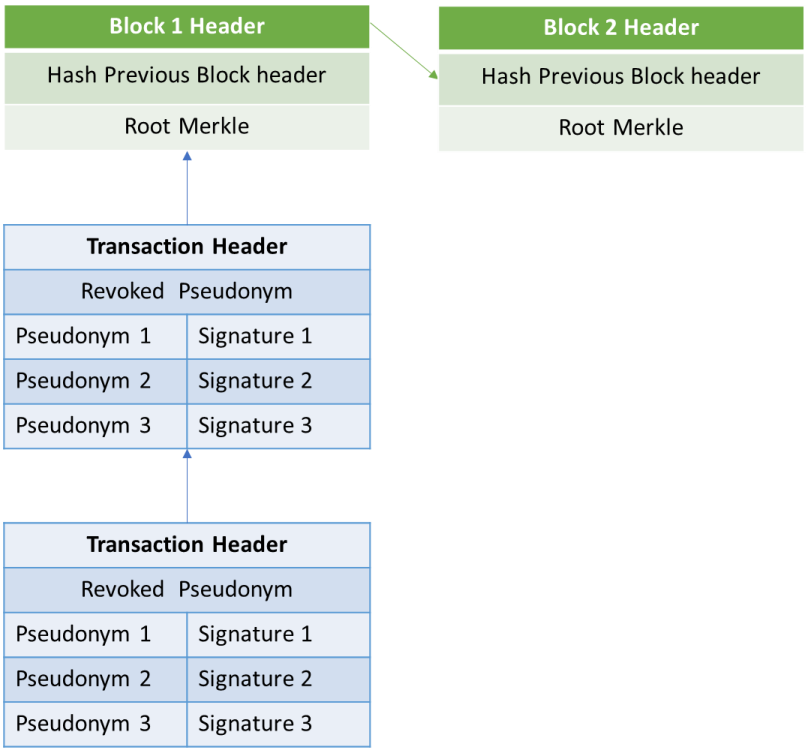

Figure IV.22: Pseudonym Revocation BlockChain

8.5 Fonctionnement du système

Dans cette section nous allons décrire l'ensemble des opérations et des échanges.

8.5.1 Demande de certificat à long terme:

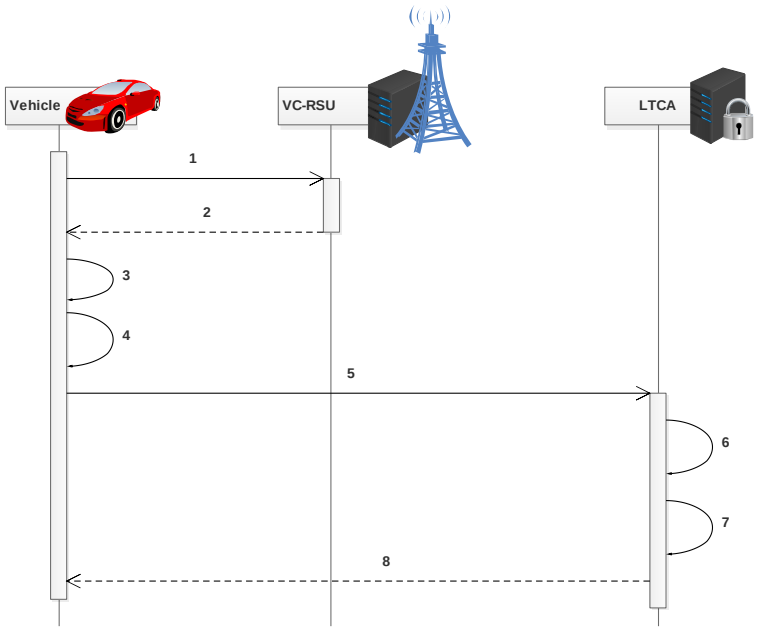

Figure IV.23 : Demande de certficat à long terme

1. Le véhicule demande le certificat de l'autorité du RSU.
2. Le RSU envoie le certificat de l'autorité (LTCA) au véhicule.
3. Le véhicule génère une paire de clés (publique et privée) à courbe elliptique.
4. Le véhicule crée une demande de signature de certificat (CSR), cryptée par la clé publique de la LTCA.
5. Le véhicule envoie une demande de certificat à LTCA.
6. LTCA charge sa clé privée, signe LTC et crée un certificat.
7. LTCA génère le pseudonyme initial (initial Short-Term Certificate -iSTC)
8. LTCA renvoie le LTC et l'iSTC à l'abonné.
9. LTCA stocke l'iSTC généré dans la Pseudonym Blockchain (PBC)

8.5.2 Créer un pseudonyme (certificat à court terme)

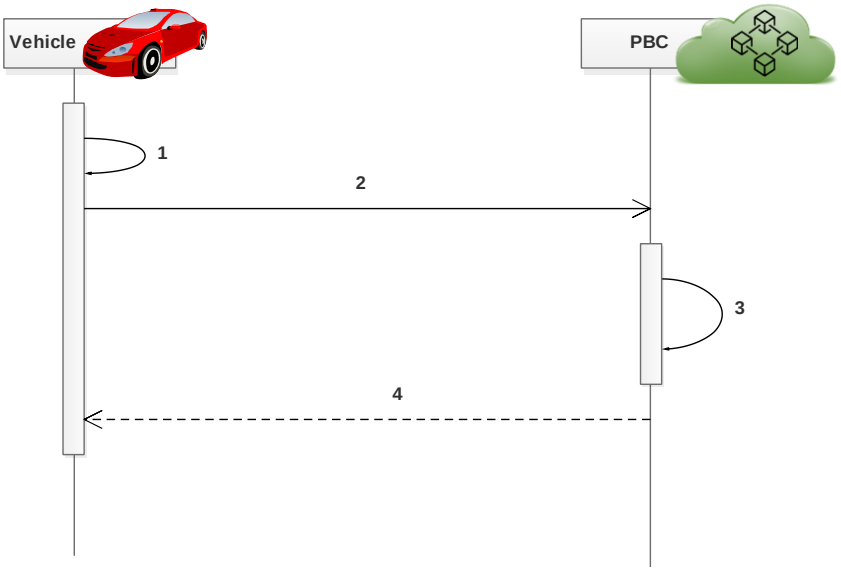

Figure IV.24 : la création d'un pseudonyme

1. Le véhicule crée un nouveau pseudonyme et définit sa durée de vie.
2. Le véhicule envoie l'ancien pseudonyme (pseudonyme initial pour la première utilisation - iSTC), le nouveau pseudonyme et la durée de vie comme une transaction dans la chaîne de blocs de pseudonymes (PBC).
3. Avant de valider la transaction, l'ancien pseudonyme doit vérifier deux conditions :
   - Enregistré dans la chaîne de pseudonymes (PBC)
   - N'est pas enregistré dans la chaîne de révocation de pseudonymes (PRBC)
4. Le véhicule reçoi la réponse de sa requête (accepter ou rejeter)

8.5.3 Processus de révocation des pseudonymes

a. Génaration de la révocation

1. Si un véhicule V détecte un nœud qui se comporte mal :
   - V crée un message d'expulsion de nœud (NEM), qui est un message multi-signe avec les voisins V comme signataires.
   - V envoie le NEM aux voisins
2. Si un véhicule Vn reçoit le NEM
   - Si Vn ∈ aux signataires du NEM
   - Si le nœud a un mauvais comportement (stocké dans une table locale)
     - Signez le NEM

- Si signatures ≥ ½ des signataires du NEM
  - Créer un message de transaction pour la révocation d'un nœud (NRTM)
  - Envoyer la transaction à Blockchain de révocation de pseudonyme (PRBC)
- Sinon, transférez le NEM

- Sinon, transmettre le NEM à d'autres signataires.

b. Validation de la transaction de révocation

Avant la validation de l'opération de révocation, les entités PRBC vérifient :

- Si numéro de signature ≥ ½
- Si une signature ∈ PRBC alors
  - Transaction rejetée
- Sinon, la transaction est validée.

8.5.4 La résolution d'identité

Dans le cas où l'identité doit être révélée par les autorités (police), le processus est le suivant :

1. L'autorité identifié le pseudonyme du nœud malveillant
2. L'autorité (la police) lance une requête de recherche du nœud malveillant avec son pseudonyme
3. PBC recherche du pseudonyme initial (généré par LTCA) dans Pseudonym Blockchain en faisant un retour en arrière dans le blockchain.
4. Une fois le pseudonyme trouvé, le PBC envoi le pseudonyme initial (généré par LTCA)
5. L'autorité (la police) génère une demande d'identité réelle (Real Identity Request-RIR)
6. Envoyer le RIR à LTCA.
7. LTCA fait la résolution de l'identité réelle
8. LTCA revoie le résultat à l'autorité (la police).

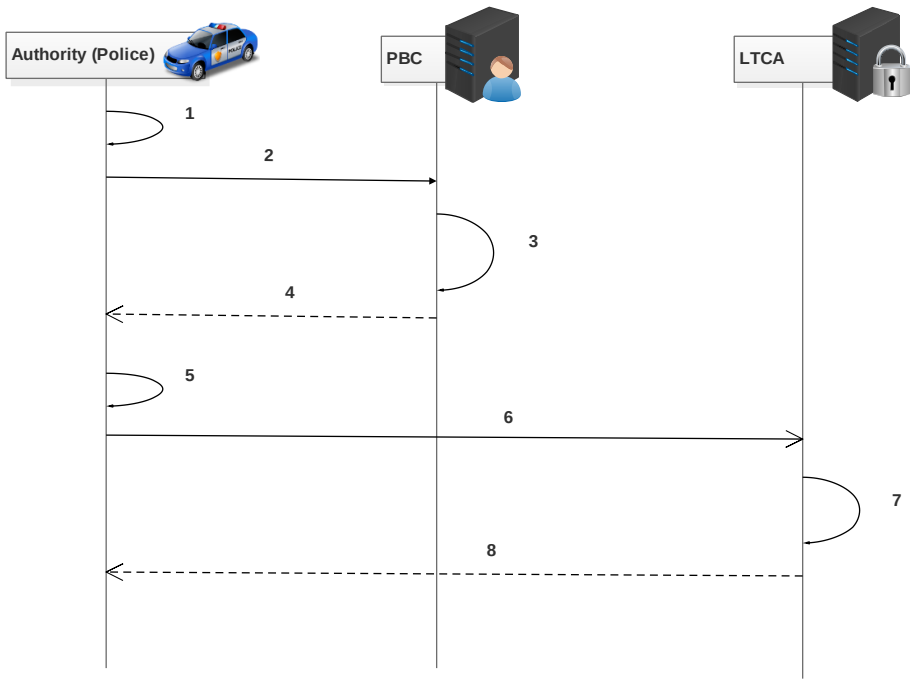

Figure IV.25 : La résolution d'identité

8.5.5 Le service cloud local

En absence d'un accès aux réseau internet, d'où l'absence d'accès aux serveurs cloud qui offrent des ressources important aux client cloud , le cloud local est une solution temporaire pour offrir un service cloud réduit aux ressources des véhicules connectés au réseau. Le service cloud local attribué comme suit (figure IV.27):

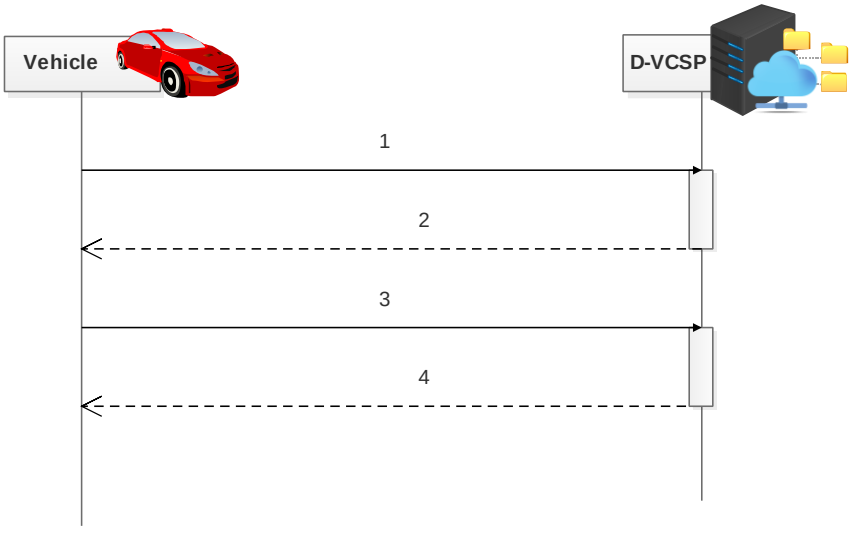

Figure IV.26 : Le service cloud local

1. Le véhicule envoi une requête d'inscription au service cloud local au D-VCSP (l'inscription se fait par le pseudonyme)
2. D-VCSP confirme l'inscription
3. Le véhicule envoi une requête de demande de service cloud local en spécifiant les ressources cloud requises.

4. En cas de disponibilité de ressource le D-VCSP envoi une repense favorable au véhicule avec un Cloud_ID
5. Si la réponse est favorable le véhicule peut utiliser le service en utilisant son Cloud_ID.

Puisque l'accès aux services cloud local se fait par un pseudonyme, en cas de changement de pseudonyme, le véhicule envoi une requête de renouvellement de service avec le nouveau pseudonyme, la requête doit contenir l'ancien pseudonyme, le nouveau pseudonyme et le Cloud_ID. La figure IV.28 détaille l'opération de changement de pseudonyme.

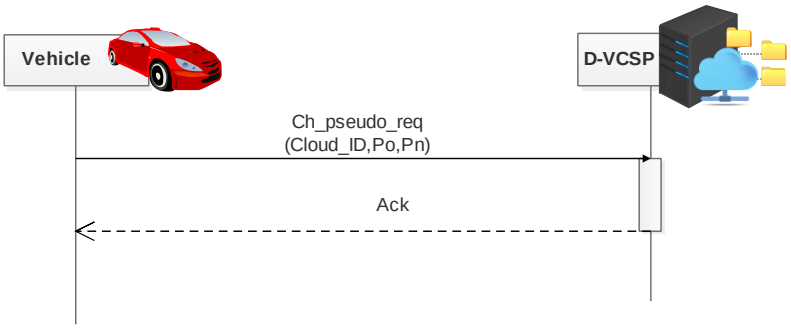

Figure IV.27 : changement de pseudonyme

8.6 Analyse de la sécurité

Le protocole BCPKI vise à renforcer la sécurité pour les réseaux cloud véhiculaires, dans un environnement isolé du réseau globale (ou internet). Notre analyse va se concentrer sur les exigences les plus touchés dans les réseaux véhiculaires en cloud.

8.6.1 Intégrité

Cette exigence est garantie par la cryptographie, puisque toute échange dans le système PKI est basé sur les certificats (à long terme, à court terme) et les clés publiques, toute échange est cryptée et les données sont protégé.

LTCA est l'autorités qui gères les certificats à long terme. Les certificats à court terme sont gérés par le blockchain PBC (Pseudonym Blockchain)

8.6.2 Vie privée

Pour protéger la vie privée des utilisateurs, le certificat temporaire ou le pseudonyme est un très bon outil.

Dans notre cas, nous avons proposé une gestion décentralisée des pseudonymes à l'aide de la technologie blockchain.

8.6.3 Non-répudiation

Le BC-PKI est basée sur les échanges sécurisés à l'aide de différentes utilisations de la cryptographie asymétrique, et la signature numérique le moyen pour garantir la non-répudiation, elle est utilisée soit par le certificats à long terme, ou par le certificat à court terme (pseudonym).

9 Conclusion

Nous avons proposé une solution sur la pki, cette solution a deux variantes VC-PKI et BC-PKI, une première qui s'adapte avec les réseaux cloud véhiculaires où il y a accès vers les autorités via le RSU. Après l'implémentation du protocole VC-PKI et ses différentes opérations sur le simulateur OMNET++ et les test sur l'impact du protocole sur les performances du réseaux, nous avons trouvé que ce protocole n'influe pas sur les performances réseaux. Après une analyse de sécurité, cette solution renforce d'une manière considérable la sécurité pour les réseaux VCC.

Pour la deuxième variante, la solution introduit la technologie blockchain pour une gestion décentralisée des pseudonymes (certificat à court terme) toute en supposant que chaque véhicule possède déjà le certificat globale (certificat à long terme) càd que véhicule est déjà reconnu par les autorités de sécurité. La technologie blockchain permet l'ensemble des véhicules de participer aux opérations de vérification et de contrôle des pseudonymes.

Pour les deux variantes, l'architecture du système est basée sur la séparation des entités offre un renforcement pour la protection de la vie privé.

Conclusion générale

Le travail présenté dans cette thèse porte sur la sécurisation du réseau véhiculaire en cloud, ce type de réseau est un résultat de l'évolution et la convergence de deux types de réseau, le cloud computing et les réseau véhiculaire (VANET), afin de prendre note du domaine, nous avons fait une étude de chaque réseau à part en focalisant sur l'aspect sécurité dans chaque réseau.

Nous avons consacré un chapitre pour les réseaux véhiculaires (VANET), où nous avons fait le tour sur les différents concepts de ce réseau pour former une vision globale du réseau. La sécurité est étudiée à travers les exigences de la sécurité, entités impliquées dans la sécurité, les types des véhicules malveillants, et les attaques sur les réseaux VANET.

Pour couvrir les concepts du deuxième type de réseau qui compose les réseaux véhiculaires en cloud qui est le cloud computing, nous avons consacré un chapitre pour cela. Le chapitre de cloud computing regroupe l'ensemble des notions sur le cloud computing tel que les technologies connexes, les caractéristiques et les différentes architectures de centre de données, aussi le mobile cloud computing est l'un des concepts importants car ce type de réseaux se rapproche du réseau véhiculaire en cloud. Dans ce chapitre nous avons consacré une partie pour parler de la sécurité, où nous avons fait un tour sur les exigences de la sécurité et les attaques les plus connues contre ce réseau.

Les réseaux véhiculaires en cloud ont des caractéristiques et des applications particulières, et possèdent des valeurs ajoutées par rapport aux réseaux vanet ou le cloud computing, pour aller plus loin dans l'étude de ces réseaux nous avons consacré un le chapitre sur les réseaux

véhiculaires en cloud où nous avons détallé l'architecture, les modèles de service. Notre contribution commence dans la section sécurité, dans cette partie nous avons définit l'ensemble des exigences de sécurité pour assurer un bon fonctionnement du réseau, suivi par une étude sur les attaques sur ce type de réseau et leurs impacts sur les services cloud et les exigences de la sécurité à fin de déterminer quelle sont les exigences les plus touché par les attaques, et à la lumière de cette analyse nous pouvons déduire les directives générale qui nous aide à proposer la solution la plus adéquate pour sécuriser les réseaux véhiculaires en cloud.

Après l'étude des attaques sur les réseaux véhiculaires en cloud nous avons déduit que les exigences de sécurité les plus touchés sont la confidentialité, l'intégrité, la disponibilité et la vie privée, et dans la littérature les solutions basées sur la cryptographie et les certificats sont les plus commodes pour renforcer la sécurité.

A la fin de l'étude de la sécurité dans les réseaux véhiculaire en cloud nous avons déduit que la solution doit être basé sur la cryptographie et les certificats, et le système pki et le plus puissant et le plus sure, pour cela nous avons décidé que la solution doit être basée sur le PKI, et puisque le réseau véhiculaire en cloud peut fonctionner en mode centralisé (liée au réseaux internet dans la plus part des cas), et en mode décentralisé (ou isolé dans des cas moins fréquents), nous avons proposé deux variantes de solutions basée sur le PKI. La première variante de la PKI est plus commode pour le réseau avec un accès au réseau internet où se trouve l'ensembles des autorités qui gèrent les différentes opérations de la sécurisation et du cloud computing. La deuxième variante est plus convenable pour les situations où le réseau internet est temporairement inaccessible, dans cette solution une partie des autorités est décentralisé comme la gestion des pseudonymes, et la gestion du cloud local à l'aide de la technologie blockchain. D'après les analyses de sécurité, la solution proposée basée sur le PKI renforce la sécurité dans les réseaux véhiculaires en cloud.

Comme perspective de ce travail nous pouvons proposer une généralisation de la technologie blockchain pour les réseaux véhiculaires en cloud. C'est une technologie prometteuse, qui permet de sécuriser les réseaux VCN. Il reste à évaluer l'impact de l'implémentation de bockchain sur le fonctionnement du réseau car elle engendre un échange d'information supplémentaire, et aussi l'impact au niveau des nœuds (véhicule) car une partie de la puissance de calcul et de stockage sont consommés pour gérer les blockchains. Généralement les tests des solutions commencent par la simulation, et nous estimant qu'une implémentation des blockchain pour le simulateur OMNET++ est très faisable, et peut aider à améliorer la technologie blockchain et l'adapter pour les réseaux véhiculaire en cloud.

Bibliographie

[1] A. Boukerche and R. E. De Grande, “Vehicular cloud computing: Architectures, applications, and mobility,” *Computer Networks*, vol. 135, pp. 171–189, 2018.

[2] J. Kakarla, S. Siva Sathya, B. Govinda Laxmi, and R. Babu B, “A Survey on Routing Protocols and its Issues in VANET,” *International Journal of Computer Applications*, vol. 28, no. 4, pp. 38–44, 2011.

[3] M. Nidhal, J. Ben-othman, and M. Hamdi, “Survey on VANET security challenges and possible cryptographic solutions,” *Vehicular Communications*, vol. 1, pp. 1–14, 2014.

[4] S. Al-Sultan, M. M. Al-Doori, A. H. Al-Bayatti, and H. Zedan, “A comprehensive survey on vehicular Ad Hoc network,” *Journal of Network and Computer Applications*, vol. 37, no. 1, pp. 380–392, 2014.

[5] K. Moghraoui, “Gestion de l’anonymat des communications dans les réseaux véhiculaires ad hoc sans fil (VANETs),” vol. 1, p. 48, 2015.

[6] “OBU Image.” [Online]. Available: https://fort-monitor.ru/en/fort_devices/new-fort-112m-on-board-unit-for-commercial-transport-is-already-on-sale/.

[7] “RSU image.” [Online]. Available: https://fort-monitor.ru/en/fort_devices/new-fort-112m-on-board-unit-for-commercial-transport-is-already-on-sale/.

[8] M. N. Mejri, J. Ben-Othman, and M. Hamdi, “Survey on VANET security challenges and possible cryptographic solutions,” *Vehicular Communications*, vol. 1, no. 2, pp. 53–66, 2014.

[9] F. Aadil, S. Rizwan, and A. Akram, “Vehicular Ad Hoc Networks (VANETs), Past Present and Future : A survey Vehicular Ad Hoc Networks (VANETs), Past Present and Future : A survey,” no. January, 2013.

[10] Y. J. Li, “An Overview of the DSRC / WAVE Technology,” *Eveleigh, NSW 2015, Australia*, pp. 544–545, 2015.

[11] V. Kumar, S. Mishra, and N. Chand, “Applications of VANETs: Present & Future,” *Communications and Network*, vol. 05, no. 01, pp. 12–15, 2013.

[12] S. Al-sultan, M. M. Al-doori, A. H. Al-bayatti, and H. Zedan, “Journal of Network and Computer Applications A comprehensive survey on vehicular Ad Hoc network,” *Journal of Network and Computer Applications*, vol. 37, pp. 380–392, 2014.

[13] Y. W. Lin, Y. S. Chen, and S. L. Lee, “Routing protocols in vehicular Ad Hoc networks: A survey and future perspectives,” *Journal of Information Science and Engineering*, 2010.

[14] P. K. Joshi, “A SURVEY OF VANET ROUTING PROTOCOLS,” *Journal of Analysis and Computation (JAC)*, vol. XI, no. I, pp. 1–6, 2019.

[15] S.-H. Cha, “A Survey of Greedy Routing Protocols for Vehicular Ad Hoc Networks,” *The Smart Computing Review*, vol. 2, no. 2, 2012.

[16] O. Senouci, “Survey : Routing Protocols in Vehicular Ad Hoc Networks,” in *AWICT ’17*, 2017.

[17] R. G. Engoulou, M. Bellaïche, S. Pierre, and A. Quintero, “VANET security surveys,” *Computer Communications*, vol. 44, pp. 1–13, 2014.

[18] G. Samara, W. A. H. Al-Salihy, and R. Sures, “Security Analysis of Vehicular Ad Hoc Nerworks (VANET),” *2010 Second International Conference on Network Applications, Protocols and Services*, pp. 55–60, 2010.

[19] Mohammed Saeed Al-kahtani, “Survey On Security Issue in Vehicular Ad Hoc Networks (VANET),” 2012.

[20] A. N. Upadhyaya, “Attacks on Vanet Security,” *International journal of Computer Engineering & Technology (IJCET)*, vol. 9, no. 1, pp. 8–19, 2018.

[21] D. B. Khadse and D. V. Jamthe, “Survey On Security Issue in Vehicular Ad Hoc Networks (VANET),” 2017.

[22] K. Dahbur, B. Mohammad, and A. B. Tarakji, “A survey of risks, threats and vulnerabilities in cloud computing,” *Proceedings of the 2011 International Conference on Intelligent Semantic Web-Services and Applications - ISWSA ’11*, pp. 1–6, 2011.

[23] P. Mell and T. Grance, “The NIST Definition of Cloud Computing Recommendations of the National Institute of Standards and Technology,” 2011.

[24] M. U. Bokhari and Q. M. and Y. K. Tamandani, “A survey on cloud computing architecture,” *Advances in Intelligent Systems and Computing*, vol. 3, no. August, pp. 1400–1405, 2012.

[25] L. B. and D. L. Fang Liu, Jin Tong, Jian Mao, Robert Bohn, John Messina, “NIST Cloud

Computing Reference Architecture: Recommendations of the National Institute of Standards and Technology," 2011.

[26] D. Kliazovich, P. Bouvry, and S. U. Khan, "GreenCloud: A packet-level simulator of energy-aware cloud computing data centers," *Journal of Supercomputing*, vol. 62, no. 3, pp. 1263–1283, 2012.

[27] A. Kertesz, "Chapter 1 : Characterizing Cloud Federation Approaches," in *Cloud Computing: Challenges, Limitations and R&D Solutions*, Springer International Publishing, 2014, pp. 1–26.

[28] R. Buyya, R. Ranjan, and R. N. Calheiros, "InterCloud : Utility-Oriented Federation of Cloud Computing Environments for Scaling of," in *in proc. 10th International Conference on Algorithms and Architectures for Parallel Processing (ICA3PP)*, 2010, pp. 13–31.

[29] A. Celesti, F. Tusa, M. Villari, and A. Puliafito, "How to enhance cloud architectures to enable cross-federation," in *Proceedings - 2010 IEEE 3rd International Conference on Cloud Computing, CLOUD 2010*, 2010, pp. 337–345.

[30] D. Bernstein, E. Ludvigson, K. Sankar, S. Diamond, and M. Morrow, "Blueprint for the intercloud - Protocols and formats for cloud computing interoperability," *Proceedings of the 2009 4th International Conference on Internet and Web Applications and Services, ICIW 2009*, pp. 328–336, 2009.

[31] A. C. Marosi, G. Kecskemeti, A. Kertész, and P. Kacsuk, "FCM : an Architecture for Integrating IaaS Cloud Systems," in *CLOUD COMPUTING 2011 The Second International Conference on Cloud Computing GRIDs and Virtualization*, 2011, no. c, pp. 7–12.

[32] H. T. Dinh, C. Lee, D. Niyato, and P. Wang, "A survey of mobile cloud computing: Architecture, applications, and approaches," *Wireless Communications and Mobile Computing*, 2013.

[33] "Mobile Cloud Computing Solution Brief: White Paper,AEPONA," 2010.

[34] J. H. Christensen, "Using RESTful web-services and cloud computing to create next generation mobile applications," 2009.

[35] L. Liu, R. Moulic, and D. Shea, "Cloud service portal for mobile device management," in *Proceedings - IEEE International Conference on E-Business Engineering, ICEBE 2010*, 2010.

[36] N. Fernando, S. W. Loke, and W. Rahayu, "Mobile cloud computing: A survey," *Future Generation Computer Systems*, vol. 29, no. 1, pp. 84–106, 2013.

[37] U. Varshney, "Pervasive healthcare and wireless health monitoring," *Mobile Networks and Applications*, 2007.

[38] D. Sinanc and S. Sagiroglu, "A review on cloud security," *Proceedings of the 6th*

International Conference on Security of Information and Networks - SIN '13, pp. 321–325, 2013.

[39] C. Modi, D. Patel, B. Borisaniya, A. Patel, and M. Rajarajan, "A survey on security issues and solutions at different layers of Cloud computing," *Journal of Supercomputing*, vol. 63, no. 2, pp. 561–592, 2013.

[40] "M. Eltoweissy, S. Olariu, M. Younis, Towards autonomous vehicular clouds, in Proceedings of AdHocNets'2010 (Victoria, BC, Canada, 2010)."

[41] "S. Olariu, M. Eltoweissy, M. Younis, Towards autonomous vehicular clouds. ICST Trans. Mob. Commun. Appl. 11(7–9), 1–11 (2011)."

[42] S. Olariu, I. Khalil, M. Abuelela, Taking VANET to the clouds. Int. J. Pervasive Comput. Commun. 7(1), 7–21 (2011).

[43] Florin, P. Ghazizadeh, A.G. Zadeh, S. Olariu, Enhancing dependability through redundancy in military vehicular clouds, in Proceedings of IEEE MILCOM'2015 (Tampa, Florida, 2015).

[44] K. Kai, W. Cong, and L. Tao, "Fog computing for vehicular Ad-hoc networks: Paradigms, scenarios, and issues," *Journal of China Universities of Posts and Telecommunications*, vol. 23, no. 2, pp. 56-65,96, 2016.

[45] R. Hussain, F. Abbas, J. Son, H. Oh, TIaaS: secure cloud-assisted traffic information dissemination in vehicular ad hoc networks, in 2013 13th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGrid) (2013), pp. 178–17.

[46] M. Whaiduzzaman, M. Sookhak, A. Gani, R. Buyya, A survey of vehicular cloud computing. J. Netw. Comput. Appl. 40, 325–344 (2014).

[47] S. Olariu, T. Hristov, G. Yan, "The next paradigm shift: from vehicular networks to vehicular clouds, in Mobile Ad Hoc Networking Cutting Edge Directions", ed. by S. Basagni, et al. (Wiley and Sons, New York, 2013), pp. 645–700.

[48] D. Lu, Z. Li, D. Huang, X. Lu, Y. Deng, A. Chowdhary, B. Li, Vc-bots: a vehicular cloud computing testbed with mobile robots, in Proceedings of First International Workshop on Internet of Vehicles and Vehicles of Internet (ACM, 2016), pp. 31–36.

[49] R. Florin, S. Abolghasemi, A.G. Zadeh, S. Olariu, Big Data in the parking lot, in Big Data Management and Procesing, chapter 21 ed. by K.-C. Li, H. Jiang, A. Zomaya (Taylor and Francis, Boca Raton, Florida, 2017), pp. 425–449.

[50] L. Gu, D. Zeng, S. Guo, Vehicular cloud computing: a survey, in Proceedings of IEEE Globecom Workshops (2013), pp. 403–407.

[51] S. Arif, S. Olariu, J. Wang, G. Yan, W. Yang, I. Khalil, Datacenter at the airport: Reasoning about time-dependent parking lot occupancy. IEEE Trans. Parallel Distrib. Syst. 23(11), 2067–2080 (2012).

[52] R. Roess, E. Prassas, W. McShane, Traffic Engineering, 4th edn. (Pearson, Boston,

2011).

[53] Texas Transportation Institute, 2012 urban mobility report (2013), http://mobility.tamu.edu/ ums/.

[54] R. Buyya, C. Vecchiola, S. Thamarai Selvi, Mastering Cloud Computing: Foundations and Applications Programming (Morgan Kaufman, Elsevier, 2013).

[55] J.L. Hennessy, D.A. Patterson, Computer Architecture a Quantitative Approach (Morgan Kaufman, Elsevier, 2012).

[56] D.C. Marinescu, Cloud Computing, Theory and Applications (Morgan Kaufman, Elsevier, 2013).

[57] B. Baron, M. Campista, P. Spathis, L.H. Costa, M. Dias de Amonim, O.C. Duarte, G. Pujolle, Y. Viniotis, Virtualizing vehicular node resources: feasibility study of virtual machine migration. Veh. Commun. 4, 39–46 (2016).

[58] D. Kapil, E.S. Pilli, R. Joshi, Live virtual machine migration techniques: Survey and research challenges, in Proceedings of 3rd International IEEE Advance Computing Conference (IACC) (Ghaziabad, India, 2013).

[59] P. Kaur, R.A. Virtual machine migration in cloud computing. Int. J. Grid Distrib. Comput. 8(5), 337–342 (2015).

[60] T.K. Refaat, B. Kantarci, H.T. Mouftah, Virtual machine migration and management for vehicular clouds. Veh. Commun. 4, 47–56 (2016).

[61] M. Whaiduzzaman, M. Sookhak, A. Gani, and R. Buyya, "A survey on vehicular cloud computing," *Journal of Network and Computer Applications*, vol. 40, no. 1, pp. 325–344, 2014.

[62] R. Hussain, J. Son, H. Eun, S. Kim, and H. Oh, "Rethinking Vehicular Communications: Merging VANET with cloud computing," *CloudCom 2012 - Proceedings: 2012 4th IEEE International Conference on Cloud Computing Technology and Science*, pp. 606–609, 2012.

[63] B. Ahmed, A. W. Malik, T. Hafeez, and N. Ahmed, "Services and simulation frameworks for vehicular cloud computing: a contemporary survey," *Eurasip Journal on Wireless Communications and Networking*, vol. 2019, no. 1, 2019.

[64] S. Arif, S. Olariu, J. Wang, G. Yan, W. Yang, I. Khalil, "Datacenter at the airport: Reasoning about time-dependent parking lot occupancy", IEEE Transactions on Parallel and Distributed Systems 23 (11) (2012) 2067– 2080.

[65] N. Mckelvey, K. Curran, B. Gordon, and E. Devlin, "Guide to Security Assurance for Cloud Computing," pp. 95–108, 2015.

[66] R. Yu, Y. Zhang, H. Wu, P. Chatzimisios, S. Xie, Virtual machine live migration for pervasive services in cloud-assisted vehicular networks, in: Proceedings of the 8th International ICST Conference on Communications and Networking in China, 2013, pp.

[67] T. Refaat, B. Kantarci, H. Mouftah, Dynamic virtual machine migration in a vehicular cloud, in: Proceedings of the IEEE Symposium on Computers and Communication, 2014, pp. 1–6.

[68] M. Gerla, "Vehicular cloud computing," *2012 the 11th Annual Mediterranean Ad Hoc Networking Workshop, Med-Hoc-Net 2012*, pp. 152–155, 2012.

[69] L. Gu, D. Zeng, and S. Guo, "Vehicular cloud computing: A survey," in *2013 IEEE Globecom Workshops, GC Wkshps 2013*, 2013, pp. 403–407.

[70] X. Yu, H. Zhao, L. Zhang, S. Wu, B. Krishnamachari, and V. O. Li, 'Cooperative sensing and compression in vehicular sensor networks for urban monitoring,' in 2010 IEEE International Conference on Communications (ICC). IEEE, 2010, pp. 1–5.

[71] D. Eckhoff, C. Sommer, R. German, and F. Dressler, 'Cooperative Awareness at Low Vehicle Densities: How Parked Cars Can Help See through Buildings,' in Proceedings of the 2011 Global Telecommunications Conference (GLOBECOM),. IEEE, 2011, pp. 1–6.

[72] M. Ma, Y. Huang, C.-H. Chu, and P. Wang, 'User-driven cloud transportation system for smart driving,' in Proceedings of the 4th International Conference on Cloud Computing Technology and Science (CloudCom). IEEE, 2012, pp. 658–665.

[73] D. Yang, G. Xue, X. Fang, and J. Tang, 'Crowdsourcing to Smartphones: Incentive Mechanism Design for Mobile Phone Sensing,' in Proceedings of the 18th annual International Conference on Mobile Computing and Networking (Mobicom). ACM, 2012, pp. 173–18.

[74] Nurmi D, Wolski R, Grzegorczyk C, Obertelli G, Soman S, Youseff L, et al. The eucalyptus open-source cloud-computing system. In: Proceedings of the 9th IEEE/ACM international symposium on cluster computing and the grid. Shanghai; 2009. p. 124–31.

[75] http://carfree.fr/parc-automobile-mondial-temps-reel.html.

[76] W. Kim and M. Gerla, "NAVOPT: Navigator Assisted Vehicular route OPTimizer," *Proceedings - 2011 5th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, IMIS 2011*, pp. 450–455, 2011.

[77] M. Eltoweissy, S. Olariu, and M. Younis, "Towards autonomous vehicular clouds: A position paper (Invited paper)," *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering*, vol. 49 LNICST, pp. 1–16, 2010.

[78] Alazawi Z, Altowaijri S, Mehmood R, Abdljabar MB. Intelligent disaster management system based on cloud-enabled vehicular networks. In: Proceedings of the 11th international conference on ITS telecommunications (ITST). St. Petersburg; 2011. p. 361–8.

[79] Panayappan R, Trivedi JM, Studer A, Perrig A. VANET-based approach for parking space availability. In: Proceedings of the 4th ACM international workshop on vehicular

ad hoc networks. Montreal, Quebec, Canada: ACM; 2007. p. 75–6.

[80] W. M. Kang, J. D. Lee, Y. S. Jeong, and J. H. Park, "VCC-SSF: Service-oriented security framework for vehicular cloud computing," *Sustainability (Switzerland)*, vol. 7, no. 2, pp. 2028–2044, 2015.

[81] V. H. La and A. Cavalli, "SECURITY ATTACKS AND SOLUTIONS IN VEHICULAR AD HOC NETWORKS : A SURVEY," *International Journal on AdHoc Networking Systems (IJANS)*, vol. 4, no. 2, pp. 1–20, 2014.

[82] D. Sinanc, "A Review on Cloud Security," pp. 321–325, 2013.

[83] Z. E. Ahmed, R. A. Saeed, and A. Mukherjee, "Challenges and Opportunities in Vehicular Cloud Computing," *Cloud Security*, no. January, pp. 2168–2185, 2019.

[84] Dressler, F., Handle, P., & Sommer, C. (2014, August). "Towards a vehicular cloud-using parked vehicles as a temporary network and storage infrastructure". In Proceedings of the 2014 ACM international workshop on Wireless and mobile technologies for smart

[85] He, W., Yan, G., & Da Xu, L. (2014). Developing vehicular data cloud services in the IoT environment. IEEE Transactions on Industrial Informatics, 10(2), 1587–1595. doi:10.1109/TII.2014.2299233.

[86] Wan, J., Zhang, D., Zhao, S., Yang, L., & Lloret, J. (2014). Context-aware vehicular cyber-physical systems with cloud support: Architecture, challenges, and solutions. IEEE Communications Magazine, 52(8), 106–113. doi:10.1109/MCOM.2014.6871677.

[87] Mei, X., Nagasaka, N., Okumura, B., & Prokhorov, D. (2015, June). Detection and motion planning for roadside parked vehicles at long distance. In Intelligent Vehicles Symposium (IV), 2015 IEEE (pp. 412- 418). IEEE. 10.1109/IVS.2015.7225720.

[88] Wahyono, W., & Jo, K. H. (2017). Cumulative Dual Foreground Differences For Illegally Parked Vehicles Detection.IEEE Transactions on Industrial Informatics,13(5), 2464–2473. doi:10.1109/TII.2017.2665584.

[89] M. K. Sharma, R. S. Bali, and A. Kaur, "Dyanimc key based authentication scheme for Vehicular Cloud Computing," *Proceedings of the 2015 International Conference on Green Computing and Internet of Things, ICGCIoT 2015*, pp. 1059–1064, 2016.

[90] M. K. Sharma and A. Kaur, "A survey on Vehicular Cloud Computing and its security," *Proceedings on 2015 1st International Conference on Next Generation Computing Technologies, NGCT 2015*, no. September, pp. 67–71, 2016.

[91] "Huang, C., Lu, R., Zhu, H., Hu, H., & Lin, X. (2016, December). PTVC: Achieving Privacy-Preserving Trust-Based Verifiable Vehicular Cloud Computing. In Global Communications Conference (GLOBECOM), 2016 IEEE (pp. 1-6). IEEE."

[92] Jeremy Blum and Azim Eskandarian. The threat of intelligent collisions. IT professional, 6(1):24-29, 2004.

[93] B. P. D. Singelee, "Location verification using secure distance bounding protocols," in

IEEE International Conference on Mobile Adhoc and Sensor, 2005.

[94] Sapna S Kaushik. Review of different approaches for privacy scheme in vanets. International Journal, 5, 2013.

[95] Josep Domingo-Ferrer and Qianhong Wu. Safety and privacy in vehicular communications. *In Privacy in Location-Based Applications*, pages 173{189. Springer, 2009.

[96] Colin Boyd. On key agreement and conference key agreement. In Information Security and Privacy, pages 294-302. Springer, 1997.

[97] Michael Steiner, Gene Tsudik, and Michael Waidner. *Diffie-hellman key distribution extended to group communication*. In Proceedings of the 3rd ACM conference on Computer and communications security, pages 31{37. ACM, 1996.

[98] Michael Steiner, Michael Waidner, and Gene Tsudik. Cliques: "A new approach to group key agreement". In 2013 IEEE 33rd International Conference on Distributed Computing Systems, pages 380-380. IEEE Computer Society, 1998.

[99] Stefano Busanelli, Gianluigi Ferrari, and Luca Veltri. "Short-lived key management for secure communications in vanets". In ITS Telecommunications (ITST), 2011 11th International Conference on, pages 613-618. IEEE, 2011.

[100] Y. Lee, J. Lee, and J. Song, “Design and implementation of wireless PKI technology suitable for mobile phone in mobile-commerce,” *Computer Communications*, vol. 30, no. 4, pp. 893–903, 2007.

[101] D. R. Kuhn, V. C. Hu, W. T. Polk, and C. Shu-Jen, “SP 800-32: Introduction to Public Key Technology and the Federal PKI Infrastructure,” *National Institute of Standards and Technology*, no. February, pp. 1–54, 2001.

[102] M. Raya, M. Raya, J. Hubaux, and J. Hubaux, “Securing vehicular ad hoc networks,” *Journal of Computer Security*, vol. 15, pp. 39–68, 2007.

[103] Mahmoud Al-Qutayri, Chan Yeun, and Faisal Al-Hawi. "Security and privacy of intelligent vanets". 2010.

[104] A. Bin Xiao, Bo Yu, “Detection and localization of sybil nodes in vanets,” in *workshop on Dependability issues in wireless ad hoc networks and sensor networks*, 2006.

[105] S RoselinMary, M Maheshwari, and M Thamaraiselvan. "Early detection of dos attacks in vanet using attacked packet detection algorithm (apda)". In Information Communication and Embedded Systems (ICICES), 2013 International Conference on, pages 237-240.”

[106] Li He and Wen Tao Zhu. "Mitigating dos attacks against signature-based authentication in vanets". In Computer Science and Automation Engineering (CSAE), 2012 IEEE International Conference on, volume 3, pages 261-265. IEEE, 2012.”

[107] Ajay Rawat, Santosh Sharma, and Rama Sushil. "Vanet: Security attacks and its possible

solutions". Journal of Information and Operations Management, 3(1):301- 304, 2012.

[108] Adil Mudasir Malla and Ravi Kant Sahu. "Security attacks with an effective solution for dos attacks in vanet". International Journal of Computer Applications, 66(22), 2013.

[109] and A. H. Sherali Zeadally, Ray Hunt, Yuh-Shyan Chen, Angela Irwin, "Vehicular ad hoc networks (vanets): status, results, and challenges," *Telecommunication Systems*, vol. 50, no. 4, 2017.

[110] P. Wex, J. Breuer, A. Held, and T. Leinm, "Trust Issues for Vehicular Ad Hoc Networks," in *IEEE Vehicular Technology Conference*, 2008, no. June.

[111] Matthias Gerlach. "Trust for vehicular applications". In Autonomous Decentralized Systems, 2007. ISADS'07. Eighth International Symposium on, pages 295-304. IEEE, 2007.

[112] Umar Farooq Minhas, Jie Zhang, Thomas Tran, and Robin Cohen. "Towards expanded trust management for agents in vehicular ad-hoc networks". International Journal of Computational Intelligence Theory and Practice (IJCITP), 5(1), 2010."

[113] P. Papadimitratos *et al.*, "Secure Vehicular Communication Systems : Design and Architecture," no. November, pp. 100–109, 2008.

[114] Objective Modular Network Testbed in C++ (OMNeT++). [Online]. Available: http://omnetpp.org.

[115] "Vehicles in Network Simulation (VEINS)." [Online]. Available: https://veins.car2x.org.

[116] "Simulation of Urban MObility (SUMO)." [Online]. Available:

https://sumo.dlr.de/userdoc/Downloads.html

[117] H. Delfs and H. Knebl, "Introduction to Cryptography - Principles and Applications, Third Edition, ser. Information Security and Cryptography". Springer, 2015. [Online]. Available: https://doi.org/10.1007/978-3-662-47974-2.

[118] N. P. Smart, "Cryptography Made Simple, ser. Information Security and Cryptography". Springer, 2016. [Online]. Available: https://doi.org/10.1007/978-3-319-21936-3.

[119] R. C. Merkle, 'A digital signature based on a conventional encryption function,' in Advances in Cryptology - CRYPTO '87, A Conference on the Theory and Applications of Cryptographic Techniques, Santa Barbara, California, USA, August 16-20, 1987, Proc.

[120] S. Nakamoto, 'Bitcoin: A peer-to-peer electronic cash system,http://bitcoin.org/bitcoin.pdf,' 2008.

[121] X. Chen, "Blockchain challenges and opportunities : a survey Zibin Zheng and Shaoan Xie Hong-Ning Dai Huaimin Wang," *Int. J. Web and Grid Services*, vol. 14, no. 4, pp. 352–375, 2018.

[122] I. C. Lin and T. C. Liao, “A survey of blockchain security issues and challenges,” *International Journal of Network Security*, vol. 19, no. 5, pp. 653–659, 2017.

[123] D. Tapscott and A. Tapscott, "Blockchain Revolution. Brilliance Audio", 2016.

[124] H. A. Kalodner, M. Carlsten, P. Ellenbogen, J. Bonneau, and A. Narayanan, ‘An empirical study of namecoin and lessons for decentralized namespace design,’ in 14th Annual Workshop on the Economics of Information Security, WEIS 2015, Delft, The Netherl.

[125] C. Fromknecht, D. Velicanu, and S. Yakoubov, ‘A decentralized public key infrastructure with identity retention,’ IACR Cryptology ePrint Archive, vol. 2014, p. 803, 2014. [Online]. Available: http://eprint.iacr.org/2014/803.

[126] L. Axon and M. Goldsmith, ‘PB-PKI: A privacy-aware blockchain-based PKI,’ in Proceedings of the 14th International Joint Conference on e-Business and Telecommunications (ICETE 2017) - Volume 4: SECRYPT, Madrid, Spain, July 24-26, 2017., 2017, pp. 311.

[127] M. H. Hoogland, “A Distributed Public Key Infras- tructure for the IoT,” Delft University of Technology, 2018.

[128] M. Ali, J. C. Nelson, R. Shea, and M. J. Freedman, ‘Blockstack: A global naming and storage system secured by blockchains,’ in 2016 USENIX Annual Technical Conference, USENIX ATC 2016, Denver, CO, USA, June 22-24, 2016., 2016, pp. 181–194.

[129] Blockstag.org, ‘Blockstack DNS vs. Namecoin,’ 2018. [Online]. Available: https: //blockstack.org/docs/blockstack-vs-namecoin.

[130] M. Al-Bassam, ‘Scpki: A smart contract-based pki and identity system,’ in Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts, ser. BCC ’17. New York, NY, USA: ACM, 2017, pp. 35–40.

[131] B. Leiding, C. H. Cap, T. Mundt, and S. Rashidibajgan, ‘Authcoin: Validation and authentication in decentralized networks,’ in 10th Mediterranean Conference on Information Systems, MCIS 2016, Paphos, Cyprus, 4-6 September 2016, 2016, p. 5.

[132] Letsencrypt.org, ‘Let’s Encrypt - How it works,’ 2018. [Online]. Available: https://letsencrypt.org/how-it-works/.