République Algérienne Démocratique et Populaire

Ministère de L'enseignement Supérieur et de la Recherche Scientifique

Université 20 AOUT 1955 SKIKDA

Faculté : Des Sciences

Département : Informatique

MEMOIRE DE FIN D'ETUDES

Pour l'obtention du diplôme de Master

THEME

La Sécurité des Véhicules Autonomes en Utilisant Blockchain et L'intelligence Artificielle

Filière : Informatique

Spécialité : Géni Logiciel Et Application Avancée

Présenté Par :

Halladj Ikram

Encadré Par :

Ali Guechi.F

Année Universitaire : 2023 / 2024

Remerciements

En tout premier lieu, je remercier le bon Dieu, tout puissant, qui ma a donné la force et la patience pour l'accomplissement de ce travail.

Je tiens à remercier vivement mon encadreur de mon travail Mme ALIGUECHI.F pour sa disponibilité, son encouragement, ses idées, ses conseils, son aide et sa gentillesse qui m'ont permis de mener à bien ce travail. Je remercie aussi les membres de jury. Bien entendu, je tiens surtout á remercié mes parents Pour leurs sacrifices et leur patience, tout au longue leurs vies.

TABLE DES MATIÈRES

Chapitre 2: La Sécurité des Véhicules Autonomes en Utilisant L'IA et Blockchain

Chapitre 3 : Une Approche pour la Sécurité des Véhicules Autonomes en Utilisant L'IA et Blockchain

Chapitre 4: L'implémentation

LISTE DES FIGURES

الملخص

يبشر وصول المركبات ذاتية القيادة بالعديد من الفوائد الكبيرة، بما في ذلك زيادة الأمان وتقليل استهلاك الطاقة والتلوث والازدحام. ومع ذلك، فإن هذه المحركات تطرح العديد من مشكلات الأمان والخصوصية التي يمكن أن تقوض الفوائد المتوقعة إذا لم يتم معالجتها. ستوفر المركبات الذاتية القيادة فرصًا جديدة للقراصنة لتنفيذ هجمات خبيثة، مما يشكل تهديدًا كبيرًا لمستقبل التنقل وحماية البيانات. تشير اتجاهات البحث في هذا المجال إلى أن الجمع بين تقنية البلوكشين والذكاء الاصطناعي يمكن أن يوفر حماية قوية للمركبات الذاتية القيادة ضد الهجمات الخبيثة. تتمتع تقنية البلوك تشين والذكاء الاصطناعي بنماذج عمل مختلفة، ولكن عند دمجهما، يمكنهما تعزيز بعضهما البعض وحل العديد من مشكلات الأمان والخصوصية للمركبات الذاتية القيادة. يمكن للذكاء الاصطناعي تحسين بناء البلوك تشين لجعله أكثر كفاءة وأمانًا وتوفيرًا للطاقة، بينما يوفر البلوك تشين ثبات البيانات وآلية الثقة لحلول الذكاء الاصطناعي، مما يجعلها أكثر شفافية وموثوقية وقابلة للتفسير. في هذه المذكرة سنقوم بتنفيذ نهج مقترح حديثا. يمثل هذا النهج بنية جديدة تدمج بين التقنيتين.

الكلمات المفتاحية: المركبات ذاتية القيادة ، الأمان ، البلوكشين ، الذكاء الاصطناعي.

RÉSUME

L'arrivée des véhicules autonomes (AV) promet de nombreux avantages considérables, notamment une sécurité accrue, une réduction de la consommation d'énergie, de la pollution et de la congestion. Cependant, ces moteurs présentent de nombreux problèmes de sécurité et de confidentialité qui pourraient compromettre les avantages escomptés s'ils ne sont pas traités. Les AV offriront de nouvelles opportunités aux pirates informatiques pour mener des attaques malveillantes, constituant ainsi une grande menace pour l'avenir de la mobilité et la protection des données. La tendance de la recherche dans ce domaine indique que la combinaison de la Blockchain et de l'IA pourrait offrir une protection solide aux AV contre les attaques malveillantes. La Blockchain et l'IA ont des paradigmes de fonctionnement différents, mais lorsqu'elles sont combinées, elles peuvent se renforcer mutuellement et résoudre de nombreux problèmes de sécurité et de confidentialité des AV. L'IA peut optimiser la construction de la Blockchain pour la rendre plus efficace, sécurisée et économe en énergie, tandis que la Blockchain offre l'immutabilité des données et un mécanisme de confiance pour les solutions basées sur l'IA, les rendant plus transparentes, fiables et explicables. Dans ce mémoire, on va réaliser une approche proposée récemment. Cette approche représente une nouvelle architecture intégrant les deux technologies.

Mots clés : Les véhicules autonomes, la sécurité, blockchain, l’intelligence artificielle.

ABSTRAIT

The arrival of autonomous vehicles (AVs) promises many great benefits, including increased safety and reduced energy consumption, pollution, and congestion. However, these engines have many security and privacy issues that could undermine the expected benefits if not addressed. AVs will provide new opportunities for hackers to carry out malicious attacks, posing a great threat to the future of mobility and data protection. The research trend in this field indicates that combining Blockchain and AI could bring strong protection for AVs against malicious attacks. Blockchain and AI have different working paradigms, but when merged, they can empower each other, and solve many security and privacy issues of AVs. AI can optimise the construction of the Blockchain to make it more efficient, secure and energy-saving, where Blockchain provides data immutability and trust mechanism for AI-based solutions and makes them more transparent, trustful, and explainable. In this thesis, we will implement a recently proposed approach. This approach represents a new architecture that integrates both technologies.

Key Words : Autonomous vehicles, Security, Blockchain, Artificial intelligence.

INTRODUCTION GÉNÉRALE

Les véhicules autonomes représentent une avancée technologique majeure qui promet de révolutionner le transport en offrant une conduite automatisée et sécurisée. Cependant, avec l'intégration croissante de l'Internet des objets (IoT) dans les véhicules autonomes, de nouvelles menaces de sécurité émergent. Les véhicules connectés offrent de multiples points d'interaction avec leur environnement, allant de la signalisation routière à la connectivité avec d'autres objets, ouvrant ainsi la voie à des attaques potentielles de cybercriminels.

En effet, les véhicules autonomes connectés sont exposés à de nouvelles menaces de sécurité comme le piratage, le vol de données personnelles ou la manipulation des systèmes de conduite. Les conséquences potentielles sont graves, allant de la perte de contrôle du véhicule à des accidents mortels. Assurer la sécurité des véhicules autonomes est donc un défi majeur à relever.

Pour contrer ces menaces, l'utilisation de technologies avancées telles que la blockchain et l'intelligence artificielle (IA) est cruciale. La blockchain peut sécuriser les communications entre les véhicules et les infrastructures, tandis que l'IA peut détecter les menaces en temps réel et renforcer la sécurité des véhicules autonomes. Ces technologies peuvent être mises en œuvre pour relever ce défi passionnant. On va concentrer surtout, sur une approche proposée récemment. Cette approche représente une nouvelle architecture intégrant les deux technologies : l'IA et blockchain.

Enfin, la problématique centrale dans ce mémoire est résidée dans l'élaboration d'un cadre de sécurité robuste pour les véhicules autonomes, en tenant compte des menaces émergentes, des dernières innovations technologiques comme l'IoT, la blockchain et l'IA, et des implications légales et éthiques. Dans ce mémoire explorera en profondeur comment garantir la sécurité des véhicules autonomes dans un environnement de plus en plus connecté et les défis associés à cette évolution

technologique majeure et comment ces technologies peuvent être mises en œuvre pour relever ce défi passionnant.

Les chapitres de ce mémoire sont présentés comme suit :

Chapitre 1 : Présente les généralités sur les véhicules autonomes et sur l'internet des objets et comment l'Internet des objets est impliqué dans les véhicules autonomes, les principales menaces de la sécurité.

Le chapitre 2 : Se concentre sur à l'exploration des technologie Intégrées de Sécurité pour les Véhicules Autonomes.

Le chapitre 3 : Présente une approche pour la sécurité des véhicules autonomes en utilisant l'IA et blockchain.

Le chapitre 4 : Implémentation de l'approche.

CHAPITRE 1

Généralités Sur Les Véhicules Autonomes

Les véhicules autonomes (AV) représentent une avancée majeure dans le domaine du transport, offrant la promesse de déplacements plus sûrs, plus efficaces et plus confortables. Ces véhicules, capables de naviguer et de prendre des décisions sans intervention humaine, reposent sur une combinaison de technologies avancées, telles que les capteurs, l'intelligence artificielle (IA) et les systèmes de navigation. Une composante essentielle qui renforce les capacités des véhicules autonomes est l'Internet des objets (IoT).

L'objet de ce chapitre consiste à faire une présentation de l'Internet des objets et des véhicules autonomes (AV) ainsi que les principales menaces de sécurité auxquelles ils sont exposés.

1. L'internet des Objets

1.1 Définition

L'internet des objets (IoT) décrit le réseau de terminaux physiques, les « objets », qui intègrent des capteurs, des softwares et d'autres technologies en vue de se connecter à d'autres terminaux et systèmes sur Internet et d'échanger des données avec eux. Ces terminaux peuvent aussi bien être de simples appareils domestiques que des outils industriels d'une grande complexité, l'IoT inclut également le gigantesque réseau qui connecte les appareils, les personnes et même les animaux via le cloud [1]. L'Internet des Objets est une combinaison d'innovations technologiques récentes et de solutions déjà existantes, où les choses deviennent partie intégrante de l'Internet dont il faut cependant définir sa nature, ses fonctionnalités où tous les objets sont identifiés de manière unique et accessibles à travers le réseau, où leurs positions et statuts sont connus. Ils sont munis d'une

identification électronique unique capable de lire et de transmettre via un protocole dans le réseau Internet [2].

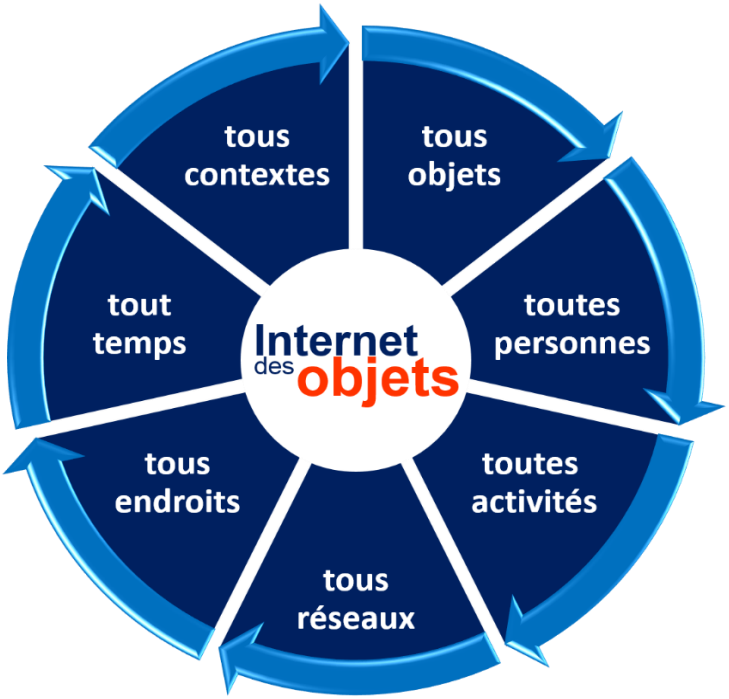


FIGURE 1: INTERNET DES OBJETS [3].

1.2 Les Composants de Internet des Objets

L'internet des objets permet la connectivité des différents objets via un réseau pour fonctionner efficacement et à distance, pour faire cette connectivité on a besoin de [1] :

- **Objet physique :** c'est un objet permet de transcender des nouveaux services en lui fournissant des capteurs.
- **Capteurs :** ils sont installés sur l'objets connecté pour capter toutes les informations nécessaires sur cet objet. Les capteurs connus sont : Capteurs de température et thermostats, Capteurs de pression, Humidité / niveau d'humidité, Détecteurs d'intensité lumineuse.
- **Plateforme :** elle est considérée comme un type d'inter-logiciel utilisé pour connecter les composants IoT (objets, personnes, services, etc.) à l'environnement l'IoT. Elle fournit de nombreuses fonctions : Accès aux appareils, Assurer une installation / un comportement correct de l'appareil, Analyse des donnée et Connexion interopérable avec le réseau local, le cloud ou d'autres périphériques.
- **Réseaux :** les composants IoT relie entre eux et avec le serveur par un réseau.

- **Prestations de service :** peuvent être utilisés pour traiter les Big Data et les transformer en informations précieuses, construire et exécuter des applications innovantes et optimiser les processus métier en intégrant les données de l'appareil.

1.3 Les Avantages de L'internet des Objets

L'Internet des objets (IoT) offre plusieurs avantages significatifs qui ont révolutionné notre façon de vivre et de travailler. Voici quelques-uns des principaux avantages [4] :

- Améliorer les services traditionnels généraux comme le transport et les parkings.
- La surveillance et maintenance des lieux publics.
- Suivi le taux de la validité des instructions pour le travail.
- Réduire le temps perdu dans les transactions administratives dans la ville.
- Economiser du temps.
- Renforcer la sécurité routière.
- L'organisation et l'amélioration de la qualité d'Airlines.
- Economiser la consommation de l'énergie dans la ville.
- L'éclairage intelligent.

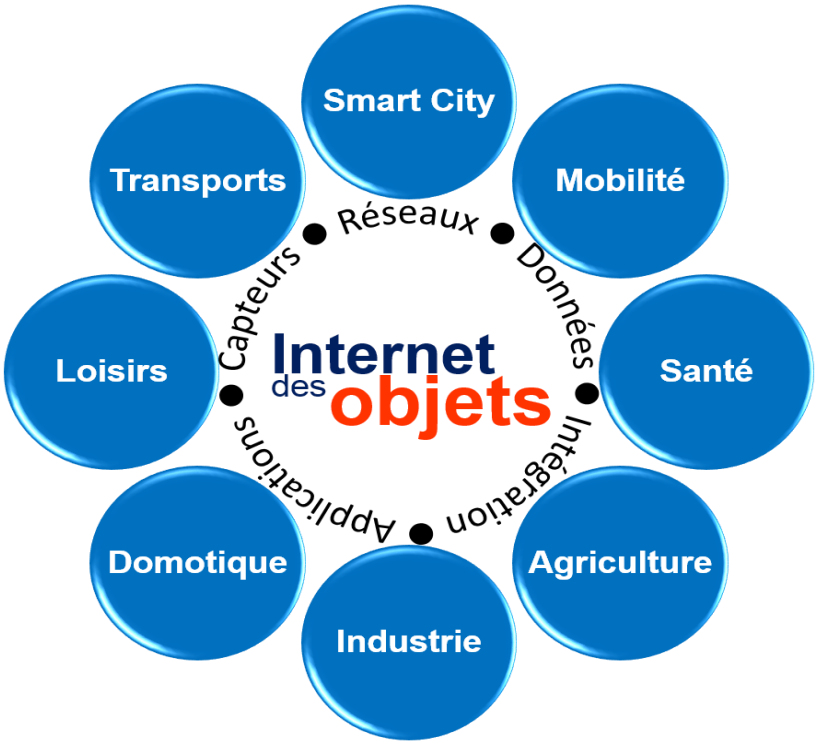


FIGURE 2: DOMAINES D'APPLICATION L'IOT [3].

1.4 Domaine d'Applications de l'Internet des objets

L'IoT couvrira un large éventail d'applications et touchera quasiment à tous les domaines que nous affrontons au quotidien, ceci permettra l'émergence d'espaces intelligents. Parmi ces espaces intelligents, on peut citer :

1.4.1 Santé intelligente

Les patients porteront des capteurs médicaux qui surveillent les constantes biologiques, telles que la température corporelle, la pression artérielle et l'activité respiratoire [5].

D'autres capteurs portables (accéléromètres, gyroscopes, etc.), ou fixes, seront utilisées pour recueillir les données permettant de surveiller les activités des patients dans leur milieu de vie. Ces données seront agrégées localement et transmises aux centres médicaux distants, qui pourront effectuer une surveillance à distance et seront capables de prendre des mesures rapides en cas de besoin [6].

1.4.2 Les Villes Intelligentes

Les villes intelligentes sont des villes qui utilisent l'Internet des Objets (IoT) pour surveiller et contrôler les systèmes de transport, de gestion des déchets, de sécurité et de gestion des ressources [7].

FIGURE 3: SCHEMA DE VILLE INTELLIGENTE [8].

Les villes intelligentes peuvent également être utilisées pour surveiller les conditions météorologiques et de circulation, ce qui permet aux autorités locales de mieux gérer leurs villes [7].

1.4.3 La Domotique

La domotique est l'ensemble des techniques permettant de centraliser le contrôle des différents systèmes d'une habitation. Le principe de la domotique est de faire en sorte qu'une maison devienne intelligente, indépendante et qu'elle réfléchisse par elle-même. Tous ces principes sont possibles grâce à l'IoT qui permet de connecter les dispositifs de la maison à un réseau et de les piloter à distance. La domotique a pour but d'améliorer le confort quotidien en automatisant ou en gérant à distance les tâches récurrentes [5].

1.4.4 Systèmes de Transport Intelligents

Les capteurs, les dispositifs IoT et les réseaux sans fil sont utilisés de manière efficace dans l'échange de données sur les systèmes de transport intelligents dans les villes intelligentes [9]. Les véhicules sont équipés de capteurs pour collecter des données sur place. Les informations dynamiques concernant la localisation, la navigation et la vitesse des véhicules sont fournies aux conducteurs par des services de type messages courts [9]. Le déplacement des véhicules sur la route vers les destinations requises se fait sans intervention humaine. Les smartphones connectés aux réseaux de véhicules fournissent des informations en temps réel. Les capteurs en bord de route sont installés à une distance uniforme pour recueillir des données sur le mouvement des véhicules dans cette région [10]. Les dispositifs IoT peuvent développer une interconnectivité avec les dispositifs environnants automatiquement [9].

2. Internet des Véhicules (IoV)

L'Internet des Véhicules (IoV) est un sous-ensemble de l'Internet des Objets (IoT), un réseau mondial qui interconnecte et permet une communication transparente entre des objets intelligents. Il étend ces capacités spécifiquement aux véhicules, lançant l'ère du transport intelligent. Le concept de l'IoV remonte à la fin du 20e siècle, lorsqu'il est devenu évident que de nombreux accidents étaient causés par des erreurs humaines au volant [11]. Pour remédier à ce problème, l'idée de déployer des

véhicules autonomes interconnectés a pris de l'ampleur. Ce changement de paradigme a conduit à l'émergence de nouveaux concepts, tels que les véhicules autonomes (autonomous vehicle AV) interconnectés et les systèmes de communication véhiculaire. Ces innovations facilitent la coopération et le partage d'informations entre les divers nœuds qui composent l'infrastructure routière moderne, comme illustré dans la figure 4.

FIGURE 4: REPRESENTATION DE L'INTERNET DES VEHICULES (IOV) [11].

3. Les Véhicules Autonomes

3.1 Définition

Les véhicules autonomes, également appelés véhicules automatisés ou véhicules sans conducteur, sont une catégorie d'automobiles dans lesquels une partie ou la totalité des choix de conduite sont effectués sans intervention humaine [12]. Un véhicule est dit « autonome » s'il est capable d'utiliser des capteurs pour se faire une idée de son environnement et de prendre des décisions de conduite sur la base de ces données sans l'intervention d'un opérateur humain [12].

3.2 Niveaux d'autonomie

Les véhicules disposent de six niveaux pour les systèmes avancés d'assistance à la conduite (ADAS) pour les véhicules automatisés sont classifiés en six niveaux par la Society of Automotive Engineers (SAE). Ces niveaux vont de 0 à 5 et décrivent le degré d'automatisation des véhicules, comme montré dans la Figure 5, sont [13] :

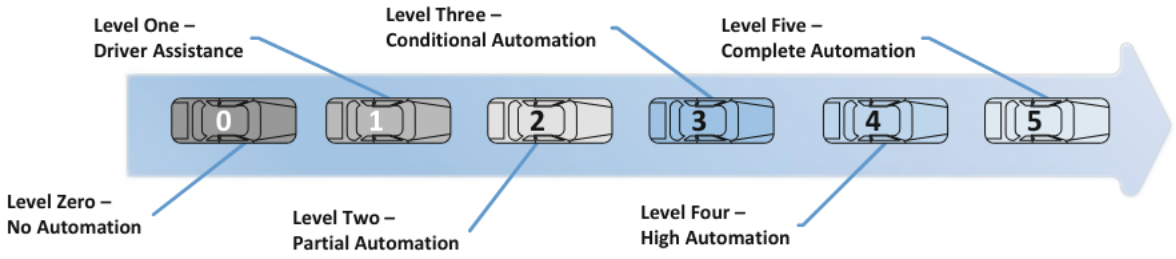


FIGURE 5: LE PARCOURS DE L'AUTOMATISATION VERS LE VEHICULE ENTIEREMENT AUTONOME [13].

- Niveau 0 : aucune automatisation, et l'humain exécute toutes les tâches de conduite dynamique comme l'accélération ou le ralentissement, la direction, le freinage, etc.
- Niveau 1 : assistance au conducteur par un système d'accélération/décélération ou de direction en utilisant des informations sur les conditions de conduite.
- Niveau 2 : automatisation partielle du véhicule qui combine des fonctions automatisées d'accélération/décélération et de direction.
- Niveau 3 : automatisation conditionnelle du mode de conduite avec une performance précise par un système de conduite automatisée lorsque le conducteur répond à une demande.
- Niveau 4 : haute automatisation, le véhicule est capable d'effectuer toutes les fonctions de conduite dans certaines conditions, même si un conducteur humain ne répond pas à une demande.
- Niveau 5 : automatisation complète, le véhicule est capable d'effectuer toutes les tâches/fonctions de conduite dans toutes les conditions.

3.3 Technologies Clé

3.3.1 Capteurs et Systèmes de Détection

Les véhicules autonomes s'appuient sur des capteurs pour surveiller leur environnement et collecter des données pour une conduite en toute sécurité. Les trois principaux capteurs AV sont [14] :

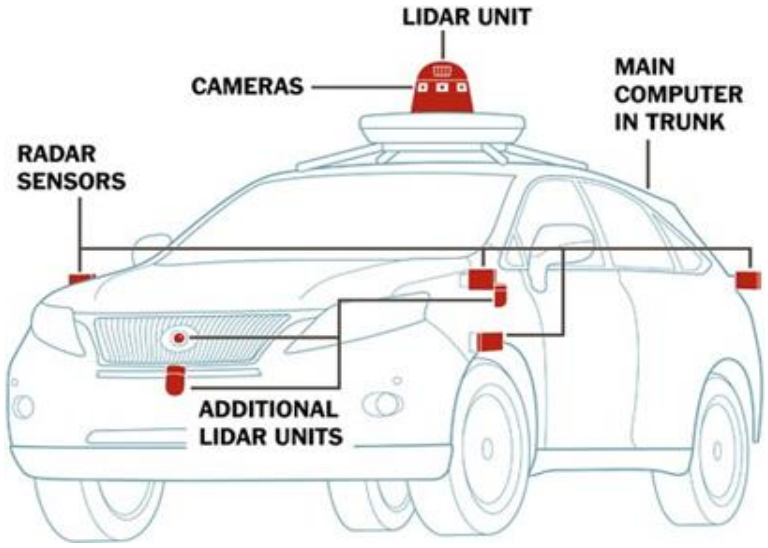


FIGURE 6: LES COMPOSANTS DE AV [14].

- **Les caméras :** Les caméras vidéo lisent les feux de circulation, les panneaux de signalisation et surveillent les piétons et les obstacles.
- **Le LiDAR :** Le LiDAR (Light Imaging detection and ranging) utilise un laser à longueur d'onde plus courte pour une meilleure précision des mesures.
- **Le RADAR :** Le RADAR utilise des ondes radio pour détecter des objets dans une certaine plage.

D'autres capteurs, tels que l'odométrie et l'unité de mesure inertielle (IMU), déterminent les positions relatives et absolues du véhicule.

3.3.2 Système de communication V2X

V2X (Vehicle-to-Everything), est une technologie qui permet la communication entre un véhicule et divers éléments de son environnement [15], Cela inclut [15] :

- **Vehicle-to-Network (V2N) :** La communication V2N implique l'échange de données entre les véhicules et un réseau central ou une plateforme basée sur le cloud. Cela peut inclure des mises à jour sur les conditions de circulation, les informations météorologiques, les fermetures de routes et d'autres données

pertinentes pour aider à optimiser le routage, la gestion du trafic et l'efficacité globale des transports.

- **V2V (Vehicle-to-Vehicle) :** Dans la communication V2V, les véhicules échangent des informations avec d'autres véhicules à proximité. Cela peut inclure des données telles que la vitesse du véhicule, sa position, sa direction, son accélération et d'autres informations pertinentes pour améliorer la sécurité et permettre la conduite coopérative.
- **V2I (Vehicle-to-Infrastructure) :** La communication V2I implique l'échange d'informations entre les véhicules et les infrastructures, telles que les feux de signalisation, les panneaux de signalisation et les péages. Cela peut fournir des informations en temps réel sur les conditions de circulation, les dangers sur la route et d'autres données pertinentes pour aider les véhicules à prendre des décisions éclairées.
- **V2P (Vehicle-to-Pedestrians) :** La communication V2P permet aux véhicules de communiquer avec les piétons, généralement en utilisant des dispositifs portables ou des smartphones. Cela peut fournir des avertissements aux piétons concernant les véhicules approchants, en particulier dans les environnements urbains où la sécurité des piétons est une préoccupation.

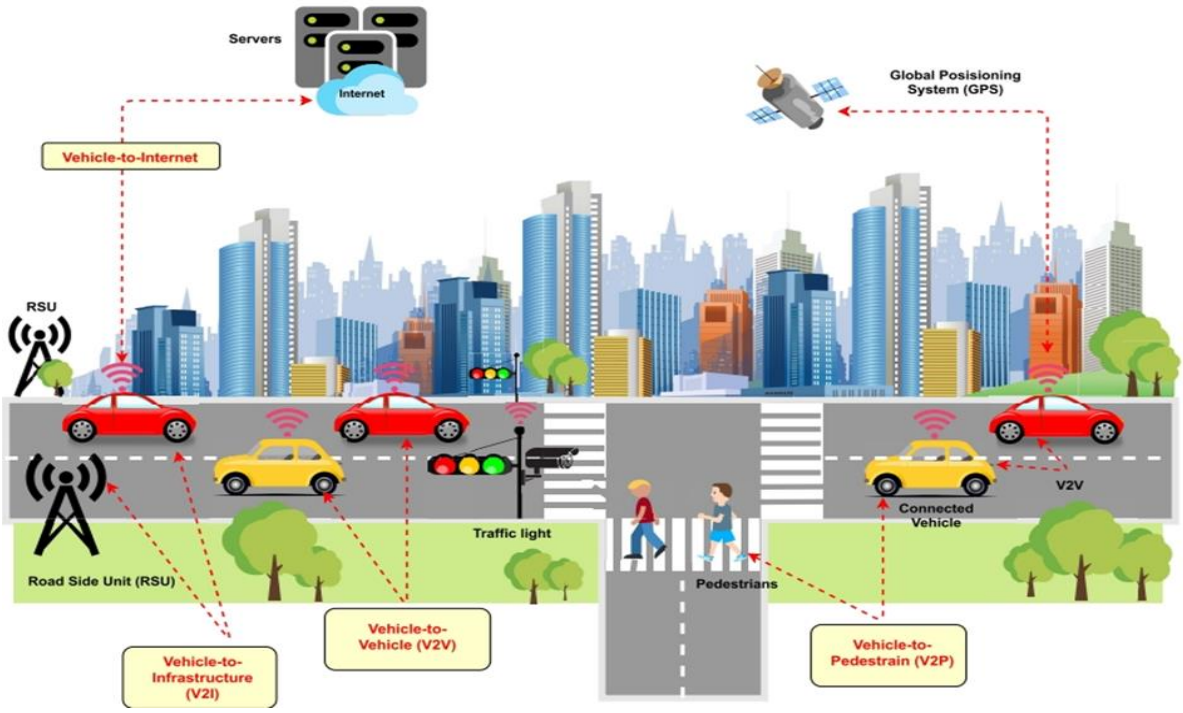


FIGURE 7: LA COMMUNICATION V2X [14].

3.3.3 Réseaux Ad-Hoc Véhiculaires (VANETs)

Les VANETs sont une sous-classe émergente des réseaux ad-hoc mobiles capables de créer spontanément un réseau de dispositifs/véhicules mobiles [16]. Les VANETs peuvent être utilisés pour la communication véhicule-à-véhicule (V2V) et véhicule-à-infrastructure (V2I) [17,18]. L'objectif principal de cette technologie est d'assurer la sécurité sur les routes. Les principaux composants de la technologie VANET sont [22]:

- **Unité Embarquée (OBU) :** Il s'agit d'un dispositif de suivi basé sur GPS intégré dans chaque véhicule pour communiquer entre eux et avec l'unité en bord de route (RSU) [18,19]. Pour récupérer les informations vitales, l'OBU est équipé de nombreux composants électroniques tels que le processeur de commande des ressources (RCP), des dispositifs de capteur et des interfaces utilisateur [22]. Son objectif principal est de communiquer entre différentes RSU et OBU via une liaison sans fil [17].
- **Unité en Bord de Route (RSU) :** La RSU est une unité informatique fixée à des emplacements spécifiques sur les routes, les parkings et les intersections [20]. Son objectif principal est de fournir une connectivité entre les véhicules autonomes et l'infrastructure et d'assister également dans la localisation des véhicules [17,20]. Elle peut également être utilisée pour connecter les véhicules avec d'autres RSU en utilisant différentes topologies de réseau [17]. Elles sont également alimentées par des sources d'énergie ambiante telles que l'énergie solaire [21].

3.4 Les Avantages des Véhicules Autonomes

Les véhicules autonomes offrent plusieurs avantages, notamment [22] :

- **Victimes :** Les véhicules autonomes peuvent réduire considérablement le nombre d'accidents.
- **Moins de dépenses :** La conduite autonome précise peut réduire la consommation de carburant et augmenter la durabilité des autres pièces.
- **Productivité :** Le trajet peut être productif en permettant de réaliser d'autres activités que la conduite.
- **Confort :** Les intérieurs des véhicules autonomes peuvent être confortables et spacieux.

4. Principales Menaces à la Sécurité et à la Vie Privée pour les Véhicules Autonomes

Les véhicules autonomes, avec leurs nombreux capteurs, systèmes de communication et logiciels complexes, présentent une surface d'attaque importante pour les cybercriminels [14]. La compromission de la sécurité de ces véhicules peut avoir de graves conséquences, allant du vol de données privées au détournement potentiel du contrôle du véhicule. Les principales menaces à la cybersécurité et à la vie privée sont classées dans les catégories principales suivantes [14] : Attaques basées sur la manipulation, Attaques basées sur l'identité, Attaques basées sur les services, Attaques basées sur des logiciels, Confidentialité des données.

4.1 Attaques Basées sur la Manipulation

Le but de cette catégorie d'attaques est d'obtenir un accès non autorisé à un véhicule nucléaire afin de compromettre la sécurité des données et de détruire la vie privée des utilisateurs [14]. De nombreuses attaques ont été signalées, la plus importante étant celle de l'homme du milieu [14]. Ces attaques impliquent des pirates malveillants qui tentent de supprimer les communications entre les antivirus et les appareils tiers, généralement via les protocoles Wi-Fi, Bluetooth, ZigBee et mobiles [23]. Ils peuvent contrôler l'AV, l'OBU ou le RSU, ce qui leur permet de modifier les messages lorsque les deux équipes pensent être en contact direct [24], [25].

4.2 Attaques basées sur l'identité

Chaque véhicule autonome est identifié par un identifiant unique qui peut aider à reconnaître le véhicule autonome et les messages échangés [26]. Les attaques basées sur l'identité sont l'une des menaces les plus sérieuses pour les véhicules autonomes connectés, car elles falsifient des identités pour se faire passer pour des entités autorisées afin d'obtenir un accès aux composants du véhicule autonome et de les manipuler [26] ,[25], [27], [28], ou pour envoyer des informations falsifiées via les canaux de communication V2V et V2I afin de perturber le fonctionnement des véhicules autonomes et le flux de trafic [26] ,[29]. Ces attaques ciblent principalement des composants dépourvus de méthodes d'authentification solides, tels que les réseaux CAN et les signaux des capteurs [26], [30]. Les cyberattaques les plus critiques dans cette catégorie sont les attaques Sybil [14]. Le but de ces attaques est qu'un grand nombre d'identités sont falsifiées ou créées simultanément dans le but de

mener plusieurs opérations malveillantes [26],[31], telles que la propagation d'informations falsifiées via les communications V2V et V2I pour perturber le fonctionnement des véhicules autonomes et le flux de trafic [29].

4.3 Attaques basées sur les services

L'objectif principal des attaques basées sur les services est d'interrompre les opérations audiovisuelles ou de perturber le flux de trafic dans une zone étendue. Cette catégorie comprend plusieurs attaques [14]. Par exemple Attaque par déni de service (DoS) et déni de service distribué (DDoS) sont parmi les menaces les plus dangereuses auxquelles les véhicules autonomes peuvent être confrontés [14]. En effet, plusieurs études ont prouvé que les attaques DoS/DDoS peuvent être utilisées pour arrêter les composants clés du véhicule, tels que la caméra, le LiDAR, le radar, le bus CAN et les unités de contrôle électronique (ECU), par une surcharge de processus [26], [32]. Par exemple, des études [33], [34] ont montré par des expériences que le protocole CAN ne dispose d'aucune mesure de sécurité contre les attaques DoS et ont démontré la facilité de ce type d'attaque.

4.4 Attaques basées sur des logiciels

En plus de toutes les attaques mentionnées ci-dessus, il existe de nombreux vecteurs d'attaque logiciels qui présentent des risques indéniables en matière de sécurité et de confidentialité et auxquels il faut remédier [14]. Cela inclut les logiciels malveillants, les attaques de ransomwares, les attaques d’applications mobiles [31] et les attaques contre le système d’apprentissage automatique [29]. Par exemple Attaques de logiciels malveillants, Constituent de graves menaces pour les systèmes des véhicules, en utilisant des vulnérabilités telles que Bluetooth et WiFi [35],[36]. Ces attaques peuvent infecter les véhicules par diverses méthodes, permettant aux pirates informatiques d'accéder aux ordinateurs du véhicule et d'exécuter du code malveillant [37]. Les recherches montrent que les logiciels malveillants peuvent se propager via différents canaux de communication, créant ainsi un réseau de zombies [34].

4.5 Confidentialité des données

Les véhicules autonomes génèrent et stockent de vastes quantités de données, identifiant les propriétaires, les passagers et leurs activités [38]. Ces données sont précieuses pour les hackers, les annonceurs et les compagnies d'assurance, ce qui suscite des préoccupations en matière de sécurité et de confidentialité. La propriété

de ces données et leurs éventuelles transmissions restent floues [39]. Des recherches ont étudié les menaces spécifiques à la vie privée dans les véhicules autonomes [14]. Par exemple les attaques par analyse de trafic collectent passivement des données précieuses sur la victime cible [26],[40]. Ces données peuvent être utilisées pour d'autres attaques telles que le brouillage, l'écoute clandestine, le suivi de localisation et les attaques de type Sybil [41], [40]. Ces attaques représentent une menace de haut niveau pour la confidentialité des utilisateurs et la confidentialité des données dans les communications véhiculaires (V2V), visant à briser l'anonymat des communications entre les véhicules et avec les unités de bordure de route (V2I) [41], [28].

5. Conclusion

Ce chapitre a passé en revue le concept de l'Internet des objets (IoT), ses composants, ainsi que certains domaines d'applications IoT et leurs avantages. Après, il a également été présenté les véhicules autonomes et leurs technologies, enfin a été identifié certaines principales menaces à la sécurité et à la vie privée pour les véhicules autonomes.

La Sécurité Des Véhicules Autonomes En Utilisant L'IA Et Blockchain

La révolution technologique actuelle se caractérise par l'émergence de technologies de pointe telles que la blockchain et l'intelligence artificielle (IA). Ces innovations transforment profondément divers secteurs, notamment celui des transports, où la sécurité des véhicules autonomes devient une priorité majeure. Ce chapitre explore en profondeur ces concepts, en examinant les types de blockchain et d'IA, leurs avantages respectifs, et comment leur intégration peut transformer la sécurité des véhicules autonomes. L'objectif est de démontrer comment ces technologies, en combinant sécurité, transparence et intelligence, peuvent contribuer à un avenir plus sûr et plus efficace pour les transports autonomes.

1. Blockchain

La technologie de la blockchain possède de nombreuses caractéristiques, telles que le fait d'être décentralisée, immuable et sans défaillance [42]. La blockchain peut fonctionner dans un environnement décentralisé, où chaque membre de la chaîne possède une copie intégrale du registre, ce qui signifie que les données sont stockées dans un environnement pair à pair [43]. Cette redondance d'informations garantit la non-répudiation des données, ce qui rend difficile toute perturbation majeure [43]. La blockchain est conçue pour être immuable ; une fois qu'un bloc est ajouté à la chaîne, toute modification à l'intérieur du bloc sera extrêmement difficile [43].

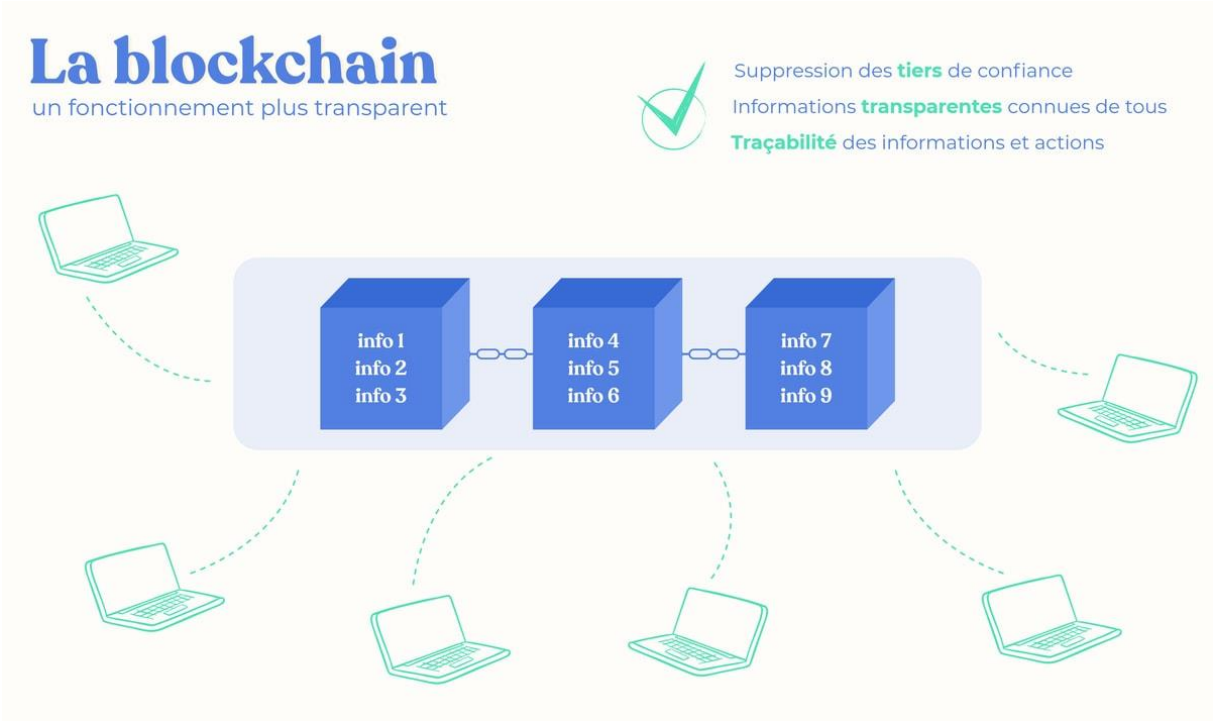


FIGURE 8: SCHEMA DE BLOCKCHAIN [44].

1.1 Les Types de Blockchains

Il existe trois différents types de blockchains [45] :

1.1.1 La Blockchain Publique

C'est la blockchain la plus répandue dans le monde et la plus connue. Elle utilise un réseau pair à pair, c'est à dire sans organe de contrôle, où tout le monde peut effectuer des transactions et les vérifier (libre accès). Les transactions ne sont pas anonymes, mais utilisent un pseudonyme et une adresse publique. Par exemple, c'est cette blockchain que le Bitcoin utilise.

1.1.2 La Blockchain Privée

Complètement centralisée, elle est dirigée par un organe central (une sorte d'administrateur) appelé gérant. C'est lui qui va ajouter les blocs à la chaîne et il peut la modifier à sa guise. Il n'y a pas de lien entre les différents acteurs. Il faut l'autorisation du gérant pour participer à la blockchain et les autres participants peuvent refuser cet accès suivant les mécanismes de contrôle misent en place. Utilisée principalement par des entreprises voulant garder leurs transactions privées et avoir une confidentialité élevée, comme par exemple les banques.

1.1.3 La Blockchain De Consortium

Elle regroupe des acteurs qui veulent travailler ensemble. Seul certains acteurs (les plus importants) pourront prendre les décisions. C'est un système décentralisé avec des droits d'écritures modifiables. Ce sont ces décisionnaires qui choisissent quelles informations seront rendues publiques (quels blocs sont privés ou publics).

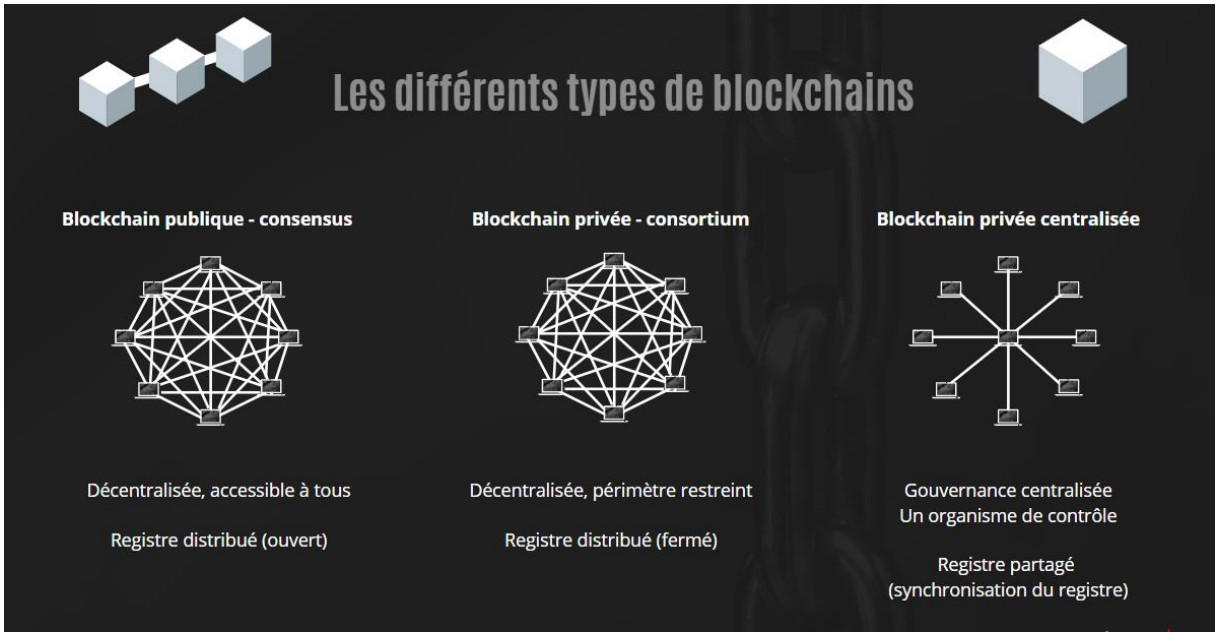


FIGURE 9: LES DIFFERENTS TYPES DE BLOCKCHAINS [46].

1.2 Consensus de la Blockchain

Les algorithmes de consensus sont un sujet de recherche actif depuis plusieurs années [47], et ce, bien avant la création de la blockchain elle-même [48]. L'objectif des algorithmes de consensus est de maintenir en toute sécurité des informations partagées et répliquées. Dans la blockchain, les protocoles de consensus sont l'élément clé du modèle de fonctionnement de la blockchain [48]. Un consensus de blockchain décide de la manière dont l'accord doit être atteint parmi les mineurs pour ajouter un nouveau bloc à la chaîne [48]. Les auteurs de [49] définissent le consensus de la blockchain comme un algorithme qui aide le réseau distribué à prendre des décisions. De même, les auteurs de [50] décrivent l'algorithme de consensus comme le mécanisme qui permet à tous les mineurs de prendre une décision concernant la même transaction, soit pour l'ajouter à la chaîne, soit pour la rejeter. Ci-après, nous présentons certains types d'algorithmes de consensus de la blockchain existants [48]:

- **Proof of Work (PoW) :** Le premier consensus créé est la Preuve de Travail (PoW), utilisée par Bitcoin et de nombreuses autres cryptomonnaies. Le consensus PoW implique une puissance de calcul importante et un processus d'authentification long. Pour atteindre un consensus PoW, chaque mineur tente de résoudre une énigme mathématique en estimant la valeur de hachage secrète. La complexité de l'énigme dépend du nombre de mineurs actifs et de la charge du réseau ; cela s'appelle la difficulté du PoW. Une fois qu'un mineur a résolu l'énigme, il ajoute le nouveau bloc à sa chaîne et le diffuse sur le réseau. Cela permet à tous les mineurs de la blockchain de vérifier le bloc publié et donc de l'ajouter à leurs copies de la chaîne.
- **Proof of Stake (PoS) :** Le consensus de Preuve d'Enjeu (PoS) vise à réduire la consommation d'énergie croissante du consensus PoW en utilisant les parts économiques des pairs. Dans ce cas, les termes "mineurs" sont remplacés par "validateurs" et seul un validateur sélectionné est choisi pour forger un nouveau bloc. Le processus de sélection se fait de manière aléatoire en proportion de la quantité de participation du validateur. Par conséquent, les algorithmes classiques de PoS sont sujets à plusieurs attaques, telles que l'attaque des 51 %, où un validateur de la blockchain détient 51 % de la cryptomonnaie ou de la puissance de calcul et utilise cette majorité pour contrôler/modifier la blockchain.
- **Proof of Activity (PoA) :** Le consensus de Preuve d'Activité (PoA) surmonte les faiblesses des systèmes PoS en combinant les avantages du PoW et du PoS. Le PoA est proposé pour encourager à la fois la propriété et l'activité dans la blockchain [51]. Dans ce consensus, les mineurs sont récompensés par le travail qu'ils ont accompli pour trouver le nonce. Pour ajouter un nouveau bloc à la chaîne, celui-ci doit être signé par plusieurs mineurs pour être approuvé. Cette règle élimine le risque d'une attaque des 51 %. Bien qu'un mineur puisse posséder 51 % du réseau, il ne peut pas contrôler la création du bloc et a besoin de l'approbation du reste du réseau.
- **Tolérance aux Pannes Byzantines Pratique (Practical Byzantine Fault Tolerance, PBFT) :** Le consensus PBFT est un algorithme qui résout le problème général byzantin, c'est-à-dire décider d'une stratégie pour éviter une défaillance complète [52]. Dans le PBFT, les mineurs sont classés en deux catégories : mineurs primaires (c'est-à-dire, les leaders) et mineurs secondaires (c'est-à-dire, les suppléants). L'objectif de cette classification est que seuls les mineurs honnêtes

coopèrent pour parvenir à un accord sur l'état du système en utilisant la règle de la majorité. Un nouveau bloc est ajouté à la chaîne en trois phases : phase de pré-préparation, phase de préparation et phase de commit. Un primaire est responsable de maintenir l'ordre des transactions. Pour passer d'une phase à l'autre, le mineur doit recevoir plus de 2/3 des votes de la totalité des mineurs. Le PBFT établit un consensus distribué tout en économisant de l'énergie et n'implique pas de calculs mathématiques complexes comme le PoW. Cependant, le PBFT est vulnérable aux attaques de type Sybil, en particulier à grande échelle, où une minorité de mineurs contrôle la majorité.

Les algorithmes de consensus sont essentiels pour préserver l'intégrité du réseau de la blockchain [48]. En effet, un consensus de blockchain aide les membres distribués de la chaîne à parvenir à un accord sur la version de la blockchain à conserver [48]. Bien que la technologie de la blockchain dispose de différents types de consensus, chacun n'est adapté qu'à quelques scénarios [48]. Par conséquent, le choix entre ces types de consensus doit respecter les exigences du système [48].

1.3 Applications de Blockchain

1.3.1 Bitcoin

Le bitcoin est la première crypto-monnaie décentralisée créée. Aucune autorité centrale ne contrôle le bitcoin. Il utilise la technologie blockchain pour créer des transactions numériques sécurisées. Au lieu de faire confiance à une banque pour s’assurer que les fonds d’un compte sont disponibles pour un transfert, le bitcoin rend publiques les informations sur le compte et l’historique des transactions. Cela permet aux utilisateurs de confirmer la disponibilité des fonds avant d’effectuer une transaction [53].

1.3.2 Ethereum

Ethereum est une plateforme blockchain lancée en 2015 qui permet de créer et d'exécuter des applications décentralisées (dApps) grâce à ses "smart contracts". Sa cryptomonnaie native est l'Ether (ETH) [54].

1.3.3 Hyperledger

Hyperledger, un projet open-source de la Fondation Linux, est destinée à développer des technologies de blockchain pour les entreprises. Launché en décembre 2015, il a connu une croissance rapide et intègre plusieurs frameworks pour proposer des

blockchains privées ou publiques personnalisables. Hyperledger Fabric, une plateforme particulièrement modulable et requirent une autorisation, est créé pour répondre aux besoins des entreprises et à une méthode de consensus sur mesure [55].

1.3.4 Smart contract

Les contrats intelligents sur la blockchain sont des programmes auto-exécutables stockés sur une blockchain qui s'exécutent lorsque des conditions prédéterminées sont remplies [48]. Ces contrats, codés en utilisant Solidity, sont mis en œuvre de manière permanente dans la blockchain pour gérer des systèmes ou établir un contrôle d'accès [48]. Les contrats se composent de quatre phases : création, déploiement, exécution et achèvement. La caractéristique d'immutabilité de la blockchain empêche les modifications, et les transactions effectuées lors de l'exécution sont stockées dans la blockchain [48].

1.4 Les Avantages de Blockchain

La structure si particulière de la blockchain lui confère des avantages indéniables [56] :

- **La traçabilité :** au sein de la chaîne, aucune information ne peut être supprimée. Chaque nœud du réseau dispose d'une copie intégrale du registre de la blockchain. Il s'agit donc d'un système stable assurant la traçabilité des données, au sein duquel il s'avère compliqué, voire impossible, de dissimuler la moindre action. Une transaction financière frauduleuse serait, de fait, immédiatement détectée.
- **La sécurité :** bien qu'il soit, comme indiqué précédemment, complètement transparent, le système de blockchain reste inviolable. La cybersécurité étant un enjeu majeur, cette caractéristique constitue l'un des principaux avantages de la blockchain.
- **L'efficacité :** la blockchain étant gérée par les utilisateurs eux-mêmes, elle peut fonctionner 24h sur 24h. Sans intermédiaire, les délais de transaction sont largement réduits par rapport aux instances traditionnelles (banques, gouvernement…). La validation d'un bloc, dans la plupart des cas, est instantanée. Autre point non-négligeable : l'absence d'intermédiaire permet également de réduire les coûts (frais financiers, frais de contrôle) et les erreurs éventuelles, comme les doublons.

2. L’intelligence Artificielle

L’intelligence artificielle est un procédé logique et automatisé reposant généralement sur un algorithme et en mesure de réaliser des tâches bien définies [57]. Pour le Parlement européen, constitue une intelligence artificielle tout outil utilisé par une machine afin de « reproduire des comportements liés aux humains, tels que le raisonnement, la planification et la créativité ». Plus précisément, la Commission européenne considère que l’IA regroupe [57] :

- Les approches d’apprentissage automatique .
- Les approches fondées sur la logique et les connaissances.
- Les approches statistiques, l’estimation bayésienne, et les méthodes de recherche et d’optimisation.

2.1 Les Techniques d’intelligence Artificielle

Dans l’ère moderne, de nombreux termes liés à l’intelligence artificielle, l’apprentissage automatique et l’apprentissage profond sont largement utilisés dans de nombreux domaines [58]. Dans ces domaines, la prédiction et l’analyse exactes des données sont cruciales, quelle que soit la taille des données [58]. Ainsi, le rôle de l’intelligence artificielle commence à analyser les mégadonnées à partir de techniques scientifiques [59].

2.1.1 L’apprentissage Automatique (Machine Learning)

L'apprentissage automatique est une technique de l'intelligence artificielle et utilise des algorithmes pour identifier schémas et tendances à partir de vastes ensembles de données. Les avancées méthodes explorer des données diverses, telles que structurées, non-structurées, textes et images, souvent de grande dimension et appelées "Big Data" [60]. Ils utilisent algorithmes sophistiques capables de détecter complexes et non-linéaires associations. L'apprentissage par renforcement est une technique d'apprentissage automatique où un agent apprend par interaction avec un environnement, recevant récompenses ou penalties en fonction de ses actions. Il est particulièrement efficace pour modéliser systèmes où les actions d'un agent influencent directement son environnement, tels que la gestion des smart contracts dans blockchain [61].

2.1.2 Les Réseaux de Neurones

Formels se proposaient à l'origine de construire une intelligence artificielle s'inspirant des systèmes nerveux biologiques. Soixante ans après leur création, ces algorithmes inspirés du vivant occupent une position prépondérante parmi les techniques utilisées, tant dans les systèmes téléphoniques que dans les équipements industriels [58].

2.1.3 L'apprentissage Profond (Deep Learning)

L'apprentissage profond permet des modèles informatiques composés de multiples couches de traitement pour apprendre des représentations de données à plusieurs niveaux d'abstraction [58]. Ces méthodes ont considérablement amélioré l'état de l'art dans la reconnaissance vocale, la reconnaissance visuelle des objets, la détection des objets et de nombreux autres domaines tels que la découverte de médicaments et la génomique [58]. L'apprentissage profond découvre une structure complexe dans de grands ensembles de données en utilisant l'algorithme pour indiquer comment une machine devrait modifier ses paramètres internes qui sont utilisés pour calculer la représentation dans chaque couche à partir de la représentation dans la couche précédente [58]. Les réseaux convolutionnels profonds ont permis des percées dans le traitement des images, de la vidéo, de la parole et de l'audio, tandis que les réseaux récurrents ont mis en lumière des données séquentielles comme le texte et la parole [62].

2.1.4 Le Traitement des Langues Naturelles (TLN)

TLN est un sous-domaine de l'intelligence artificielle dédié à la compréhension et à la génération du langage [58]. Les avancées récentes dans les technologies de TALN permettent une analyse rapide de grandes quantités de texte, ouvrant ainsi de nouvelles possibilités de recherche dans le domaine de la santé et de prise de décisions éclairées par des données probantes [58]. L'analyse et l'extraction de données à partir de la documentation scientifique, des rapports techniques, des dossiers de santé, des médias sociaux, des enquêtes, des registres et d'autres documents peuvent appuyer les fonctions essentielles de la santé publique [63].

2.1.5 Les Algorithmes Génétiques

Les algorithmes génétiques (AG) ont été inventés par John Holland dans les années 1960 et ont été développés par ses étudiants et collègues de l'Université du Michigan dans les années 1960 et 1970. Le but initial de Holland n'était pas de concevoir des

algorithmes des problèmes spécifiques, mais plutôt étudier formellement le phénomène d'adaptation tel qu'il se produit dans la nature des moyens d'importer les mécanismes d'adaptation naturelle dans les systèmes informatiques. L'AG est une méthode pour passer d'une population de "chromosomes" à une nouvelle population en utilisant une sorte de "sélection naturelle" [64].

2.1.6 Le system-expert

SE désignent des systèmes informatiques qui imite la capacité de décision d'un expert humaine, qui vise à résoudre des problèmes complexes par la connaissance du raisonnement. En 1959, Newell, Shaw et Simon développé le Général Problème Solutionne (GPS) qui est un résumé de l'activité de réflexion pour les gens résoudre des problèmes. Maintenant, toutes sortes de SE s'épanouissent, la demande de system-expert est encore renforcée, et les gens sont désireux d'utiliser un SE pour résoudre des problèmes plus complexes [65].

2.2 Les Types d'Intelligence Artificielle

L'IA est divisée selon ses capacités en trois sections de sorte que chaque section a une fonction et des caractéristiques qui peuvent être définies comme suit [58] :

2.2.1 L'intelligence Artificielle Etroite (ANI)

L'ANI surpasse déjà l'Homme dans certains domaines, elle ne nous surpasse que dans une tâche spécifique. Par exemple, le logiciel AlphaGo de Google DeepMind, a battu les champions du monde au jeu de go en 2016 (DeepMind). Cela est considéré comme une avancée technologique, car au contraire du jeu d'échec où il y a un nombre fini de possibilité que l'ordinateur peut simuler avant de jouer, les règles du jeu inscrites dans son système et n'a fait que jouer contre soi-même. Il n'a donc eu aucune donnée humaine pour l'entraîner. Mais demandez au même logiciel s'il y a un chat sur une photo, il en sera tout simplement incapable. Il n'est expert que dans une tâche très précise et reste donc encore loin des capacités humaines [66].

2.2.2 L'intelligence Artificielle Générale (AGI)

Le système AGI se compose de nombres de systèmes ANI qui fonctionnent et interagissent les uns avec les autres pour imiter la pensée humaine. Ses caractéristiques, il peut effectuer qui peut effectuer des tâches cognitives au niveau humain dans une variété de domaines, tels que la pensée computationnelle, le traitement de l'image, le traitement du langage et ainsi de suite [67], Pour la plupart

des spécialistes, l'AGI fait référence à la capacité de la machine autonome à effectuer toute tâche intellectuelle pouvant être réalisée par un humain. Dans le sens où ils fonctionnent uniquement dans les limites des scénarios pour lesquels ils sont programmés. Cela passe notamment par la généralisation et l'abstraction de l'apprentissage sur un ensemble de fonctions cognitives [68].

2.2.3 Super Intelligence Artificielle (ASI)

Enfin, malgré le fait qu'ils approchent du territoire de la science-fiction, ASI est vu comme la prochaine étape évidente suivant AGI. Dans tous les sens, une technologie ASI serait en mesure de surpasser les humains. Cela impliquerait des choses comme créer de meilleurs arts et de former des relations émotionnelles, ainsi que les systèmes d'IA seront en mesure d'améliorer rapidement leurs talents et s'étendre dans des mondes qu'ils n'auraient jamais pu envisager une fois AGI atteint [67].

2.3 Les Avantages de L'intelligence Artificielle (IA)

Les avantages de l'intelligence artificielle (IA) dans différents secteurs, en se basant sur les sources fournies :

- **Gains de temps et d'efficacité**

  L'IA permet d'automatiser des tâches répétitives et chronophages, faisant gagner du temps et augmentant la productivité [69].

  Elle peut traiter de grands volumes de données plus rapidement que les humains [69].
- **Réduction des erreurs**

  Les systèmes d'IA sont capables d'effectuer des tâches avec une grande précision, réduisant ainsi les erreurs humaines [69].
- **Amélioration des processus métier**

  L'IA peut optimiser et améliorer les processus d'entreprise en identifiant des tendances et en prenant des décisions éclairées à partir des données [69].
- **Personnalisation et expérience utilisateur améliorée**

  Grâce à l'apprentissage automatique, l'IA peut personnaliser les services et produits en fonction des préférences et comportements des utilisateurs [69].
- **Aide à la prise de décision**

  L'analyse de données complexes par l'IA permet de fournir des informations et des recommandations pour faciliter la prise de décision [69].

- **Sécurité et transparence dans les télécommunications**

L'IA offre des avantages en matière de sécurité, de sûreté et de transparence dans les réseaux de télécommunications [70].

3. La Sécurité des Véhicules Autonomes

3.1 La Sécurité Véhicule Autonome Basé Sur Blockchain

Les principales caractéristiques de la BC, y compris l'intégrité, l'immutabilité des données, la décentralisation, l'irréversibilité, la persistance, la transparence et l'anonymat [71], [72], en font la solution la plus adaptée dans tous les domaines nécessitant un partage sécurisé des données entre plusieurs parties. La conduite autonome est certainement l'un des domaines d'application importants de la BC, où elle a été considérée par la communauté de recherche comme une solution potentielle pour améliorer la sécurité, l'intégrité et la transparence des données [73], [74], [72], [75]. En particulier, la communauté des chercheurs a appliqué les technologies de BC et de registre distribué aux aspects suivants de la sécurité et de la confidentialité des véhicules autonomes.

3.1.1 Stockage Transparent et Sécurisé des Données

Stockage de données transparent et sécurisé : Les analystes prévoient que les véhicules autonomes (VA) généreront bientôt beaucoup plus de données que les humains, avec plus de 4000 Go de données par jour [76]. La blockchain (BC), avec ses fonctionnalités de partage d'informations distribuées et de résistance à la falsification, peut fournir un stockage transparent et sécurisé des données sensibles générées par les systèmes VA [77], [78], [79]. Dans ce contexte, de nombreuses études ont examiné l'utilisation de la BC pour le stockage distribué et sécurisé des données dans les réseaux de véhicules. Par exemple :

- Dans [71], les données à distribuer sur le réseau BC ont été classées en cinq catégories principales : les données surveillées par les RSU (par exemple, la vitesse, les habitudes de conduite) et les données sensorielles à l'intérieur du véhicule (par exemple, l'électronique, la pression barométrique). température), les données d'assurance du véhicule, les données d'info divertissement (telles que l'audio et la vidéo) et les données de transactions financières du véhicule (telles que le ravitaillement, la recharge, le lavage). Ainsi, cinq centres de communication

différents ont été conçus en fonction de différentes applications dans les réseaux de véhicules. Les communications de données pour différents types de centres d'affaires sont indépendantes.

- Dans [80], les auteurs ont proposé une architecture de stockage basée sur BC pour le stockage décentralisé et sécurisé des données générées par AV dans la couche cloud à l'aide de la table de hachage distribuée (DHT). Cette architecture est implémentée à l'aide de la plateforme Ethereum, où les nœuds maîtres sont des AV et des RSU. Les nœuds RSU sont utilisés pour l'exploration de données, la création de blocs, l'authentification et la vérification des données.

3.1.2 Sécuriser les Canaux de Communication

La blockchain (BC) en tant que technique de sécurité collaborative et décentralisée peut également rendre les canaux de communication des véhicules autonomes (VA) (qu'il s'agisse de canaux de communication inter ou intra) plus fiables, sécurisés, fiables et à l'épreuve des falsifications [71], [74], [81], [79]. Ainsi, un certain nombre d'études ont exploité les principes de la BC afin de sécuriser la transmission des données dans divers canaux. Par exemple :

- Dans [82], la BC est utilisée pour prévenir les attaques à 51% et garantir que les VA malveillants ne peuvent pas manipuler, modifier ou supprimer les messages d'événements critiques dans un réseau de véhicules ad hoc (VANET).
- Les problèmes de sécurité et de confidentialité liés aux capteurs IoT des VA ont été abordés dans [83] en proposant une solution basée sur la BC, où chaque capteur/actionneur de VA est enregistré dans le réseau BC avant d'acquérir l'un des services. Pour des raisons de performance, les auteurs ont proposé que seules les informations pertinentes liées au capteur IoT soient stockées dans la BC. Par conséquent, même si un ou plusieurs capteurs intelligents sont compromis, les VA connectés au réseau BC sont conscients des informations enregistrées sous ce capteur compromis.

3.1.3 Intégrité des Données et Confidentialité

Les caractéristiques d'immutabilité et de décentralisation de la blockchain (BC) en font une solution de sécurité puissante pour résoudre les problèmes d'intégrité et de confidentialité des données [79]. À cet effet, de nombreuses études ont proposé

l'utilisation de la technologie BC pour améliorer l'intégrité et la confidentialité des données dans l'écosystème des véhicules autonomes (VA). Par exemple :

- Dans [84], une solution basée sur la blockchain est proposée pour la collecte sécurisée et résiliente des données à l'intérieur des véhicules. Les capteurs IoT et les contrôleurs participant au réseau de la blockchain nécessiteront des modules de gestion d'entité internes pour garantir l'intégrité et la validité des données lors de la collecte. De plus, un environnement d'exécution de confiance est utilisé pour une exécution sécurisée afin d'intégrer des données essentielles et prendre des décisions en temps réel.
- Dans [77] ont proposé une architecture basée sur la blockchain pour améliorer l'intégrité des informations au sein des VA, où chaque unité de commande électronique (ECU) peut agir comme un matériel nu et partager ses informations avec d'autres ECUs. Les ECUs agissant en tant que mineurs ont une copie de la blockchain et le bus CAN est utilisé pour diffuser toutes les transactions et les blocs.

3.1.4 Applications en Matière d'investigation

La technologie Blockchain a été exploitée à des fins médico-légales, où les données des véhicules autonomes sont enregistrées dans un registre externe partagé accessible par des tiers autorisés, dans le but d'empêcher toute altération malveillante et de permettre une vérification précise. De nombreuses solutions ont été proposées, notamment :

- Dans [85], il a proposé un système d'enregistrement d'événements basé sur une blockchain pour les enquêtes sur les accidents. Dans ce travail, les auteurs conçoivent un nouveau schéma de consensus dynamique, appelé Event Proof, pour l'enregistrement et la diffusion d'événements. De plus, le pointage de crédit est utilisé pour mesurer la confiance dans la voiture autonome. Cela inclut le fait d'être témoin ou d'être témoin d'un accident.
- Un système basé sur la blockchain pour l'analyse médico-légale des accidents de la route a été proposé dans [86]. Le cadre blockchain connecte les véhicules autonomes aux prestataires de services de maintenance, aux constructeurs automobiles, aux forces de l’ordre et aux compagnies d’assurance. Les preuves et autres données pertinentes sont collectées et stockées dans une blockchain autorisée qui utilise des protocoles de consensus byzantins.

3.1.5 Gestion de la Réputation et de la Confiance

Afin de résoudre les limitations des modèles de confiance centralisés, de nombreuses études sur les modèles de confiance véhiculaires ont appliqué la technologie de la blockchain pour stocker les informations de réputation des véhicules autonomes afin d'assurer des communications fiables et d'atténuer les attaques adverses. Par exemple :

- Un consortium blockchain a été utilisé dans [87] pour stocker les mises à jour transactionnelles via un score de réputation. Les nœuds avec un score d'enregistrement supérieur à un seuil sont autorisés à communiquer des messages dans le réseau V2X.
- Dans [88], une blockchain légère est utilisée dans le réseau embarqué pour stocker des informations de trafic local créées pour une journée et détruites le jour suivant, tandis que les informations de réputation du véhicule autonome sont enregistrées et gérées à travers une blockchain mondiale où la RSU est un nœud complet.

3.2 La Sécurité véhicule Autonome basé sur L'intelligence Artificielle

3.2.1 Détection et Prévention des Intrusions

De nombreuses tentatives ont été faites pour concevoir de nouvelles techniques de détection d'intrusion basées sur l'apprentissage automatique (ML) et l'apprentissage profond (DL) pour sécuriser les réseaux CAN et VANET. Les techniques de classification telles que les k-voisins les plus proches (K-NN), les machines à vecteurs de support (SVM), les réseaux de neurones artificiels (ANN), le modèle de Markov caché (HMM) et les systèmes de support monocouche (OCSVM) ont retenu l'attention de nombreux chercheurs dans ce domaine, telles que :

- Dans [89], un système de sécurité a été proposé pour protéger les réseaux ad hoc de véhicules. Ce système a utilisé l'algorithme K-NN pour identifier les composés nocifs des communications externes dans les véhicules autonomes et semi-autonomes.
- Dans [90] a été proposé une nouvelle méthode de détection d'intrusion basée sur un SVM modifié à classe unique dans le trafic CAN en déployant trois attaques (c'est-à-dire attaques par déni de service, brouillage et usurpation d'identité).

L'apprentissage profond (DL), l'une des techniques puissantes d'apprentissage automatique, a également été appliqué par de nombreux chercheurs pour concevoir des IDS/IPS pour la cybersécurité des véhicules [91], [92], [93]. Les réseaux de neurones profonds (DNN), la mémoire à court terme (LSTM), les réseaux de neurones récurrents (RNN) et les réseaux de neurones convolutifs (CNN) font partie des modèles DL les plus utilisés dans ce domaine.

- Dans [92], LSTM a été utilisé pour proposer un IDS permettant de détecter diverses attaques sur le réseau de bus CAN, telles que le DDoS, le brouillage et l'usurpation d'identité. LSTM a également été utilisé avec RNN dans [94] pour identifier les attaques d'usurpation d'identité sur le bus CAN. Un réseau hybride combinant les modèles CNN et LSTM a été appliqué dans [95] pour identifier quatre types d'attaques sur le bus CAN, à savoir les attaques par inondation, brouillage, usurpation d'identité et rejeu.
- Dans [96], les auteurs se sont concentrés sur la détection des attaques DDoS, de l'injection de commandes et des logiciels malveillants ciblant le réseau embarqué en appliquant l'apprentissage profond récurrent (RDL) et le LSTM.

3.2.2 Analyse et Classification des Logiciels Malveillants

Dans la lutte sans fin contre les logiciels malveillants, de nombreux chercheurs dans le domaine de la sécurité des AV ont appliqué des techniques d'apprentissage automatique (ML/DL) pour la détection de nouveaux logiciels malveillants en raison de leur capacité à automatiser le processus d'analyse et de détection des logiciels malveillants [97]. Par exemple :

- Dans le domaine des AV, les auteurs de [35] ont proposé un classificateur de logiciels malveillants basé sur le ML, entraîné sur des caractéristiques multiples à l'aide de dix méthodes d'apprentissage différentes, y compris K-NN, ainsi que des fonctionnalités d'Opcode N-gram et Pixel. La méthode proposée a pu classifier les logiciels malveillants dans leur famille avec une précision de 99,99 %.
- Dans [98], les auteurs ont proposé un cadre basé sur le ML pour détecter de nouveaux logiciels malveillants de type bot zero-day spécifiques au contexte des véhicules, en particulier, le protocole de message court WAVE (WSMP)-Flood et GeoWSMP Flood. La solution proposée a été testée avec les algorithmes de ML Naive Bayes (NB), SVM, k-NN, arbres de décision (DT), forêt aléatoire (RF), réseau

neuronal (NN) et perceptron multicouche (MLP). Les résultats expérimentaux ont montré que cette solution surpassait les solutions existantes avec un taux de détection supérieur à 97 %.

3.2.3 Gestion de la Réputation et de la Confiance

De nombreuses études ont proposé des modèles de réputation et de confiance dynamiques pour sécuriser la communication des AV en utilisant différentes techniques de ML . Par exemple :

- Les études [99], [100], [101] et [102] ont appliqué l'apprentissage par renforcement profond (DRL) pour concevoir des modèles de confiance dynamiques pour sécuriser la communication des AV. Le DRL est un sous-ensemble novateur de ML qui combine des algorithmes DL avec des méthodes RL (par exemple, Q-learning, SARSA) afin d'aider les agents logiciels à apprendre à atteindre leurs objectifs [90].
- Dans [99], les auteurs ont proposé une méthode basée sur la confiance pour limiter les faux retours d'information des véhicules malveillants. Dans ce travail, les retours d'information des AV sont combinés dans des serveurs de calcul de bord véhiculaires et les résultats sont utilisés pour prédire le nombre moyen de vrais messages. Le serveur de bord utilise ensuite une méthode DRL qui combine la méthode Q-Learning avec DNN pour déterminer la politique de mise à jour de réputation optimale pour inciter les véhicules à envoyer de vrais retours d'information. Les auteurs ont affirmé que leur méthode de confiance obtenait de meilleurs résultats en termes de nombre moyen de vrais retours d'information par rapport aux méthodes basées sur la réputation existante. Alors que, dans [100], un contrôleur de réseau défini par logiciel (SDN) est utilisé comme agent pour apprendre le chemin de routage le plus fiable par DNN dans les VANETs, où le modèle de confiance est conçu pour évaluer le comportement des voisins de transfert d'informations de routage.

3.2.4 Confidentialité et Intégrité des Données

Récemment, il y a eu une recherche intensive sur l'utilisation de l'approche de l'Apprentissage Fédéré (FL) pour soutenir la confidentialité et l'intégrité des données, en dissociant les données générées par les AV et l'agrégation des modèles ML [103], [104], [105], [106]. FL est simplement la forme décentralisée de ML, où l'algorithme d'apprentissage est formé sur plusieurs dispositifs ou serveurs décentralisés

contenant des échantillons de données locaux. Cette approche d'apprentissage collaboratif résout de nombreux problèmes critiques liés à la confidentialité et à l'intégrité des données, aux droits d'accès aux données et à l'accès aux données hétérogènes [103]. Dans les méthodes ML traditionnelles, s'il existe plusieurs ensembles de données dans un serveur, ils pourraient être liés et entraîner une violation de la confidentialité, même si un ensemble de données a été "anonymisé". Au contraire, dans le cadre de FL, les données transmises consisteraient en "des mises à jour minimales" de sorte que la précision d'un modèle d'apprentissage soit améliorée. Les mises à jour elles-mêmes pourraient être temporaires et ne contiendraient pas plus d'informations que les données brutes utilisées pour l'entraînement [104]. Par exemple :

- Dans un travail plus récent [107], les auteurs ont introduit FL dans la conduite autonome pour préserver la confidentialité des véhicules en conservant les données d'origine dans un véhicule local et en partageant uniquement le paramètre du modèle d'entraînement avec l'aide d'un serveur de calcul de bord multi-accès (MEC). Le problème des serveurs MEC malveillants et des véhicules malveillants a été abordé en utilisant un système de réputation auxiliaire basé sur la blockchain.
- Dans un travail plus récent [108], un système de détection de comportement malveillant est proposé en utilisant FL pour l'entraînement local du modèle à l'aide de données de message de service de base (BSM) générées sur les véhicules. Les BSM peuvent inclure des informations critiques et privées telles que la vitesse actuelle, l'emplacement, etc. Différents algorithmes ML et DL ont été utilisés comme algorithmes d'entraînement, notamment SVM, KNN, LSTM et ANN.

3.3 La Sécurité Véhicule Autonome basé sur Intégration L'intelligence Artificielle et Blockchain

La blockchain et les technologies d'IA ont des paradigmes de fonctionnement différents, comme illustré dans le Tableau IV [109], mais lorsqu'elles sont fusionnées, elles peuvent se renforcer mutuellement et résoudre les problèmes de sécurité et de confidentialité dans divers secteurs [109]. Dans ce contexte, certaines grandes entreprises commencent à investir dans la combinaison de projets BC et IA afin d'améliorer la sécurité et la confidentialité des données dans différents domaines. Dans le contexte des véhicules autonomes, de nombreuses études récentes ont

montré que l'intégration de la blockchain et de l'IA est puissante et est destinée à améliorer la confidentialité des AV et la protection contre les cybers attaques.

3.3.1 Canaux de communication sécurisés

Les techniques d'IA peuvent optimiser la construction de la BC pour la rendre plus efficace, sécurisée et économe en énergie [74], [104], [109]. Alors que, les principales caractéristiques de la BC, y compris la sécurité, la transparence, la décentralisation et l'immutabilité, permettent aux solutions basées sur l'IA appliquées à la sécurité des AV de devenir plus transparentes, dignes de confiance et explicables [109]. Dans ce contexte, la plateforme CUB [110], qui est un projet récent, a intégré à la fois la BC et l'IA avec des AV pour protéger le réseau embarqué et les communications V2X. Dans ce projet, une solution BC hybride est déployée en combinant une BC publique avec leur propre BC privée afin de fournir un traitement, une transmission et une réception des données plus rapides et plus dignes de confiance. Dans ce travail, la méthode d'apprentissage en profondeur descente de gradient stochastique (SGD) est appliquée pour améliorer la vitesse de traitement de la BC. De plus, les modèles d'apprentissage profond et d'apprentissage par renforcement ont été utilisés pour fournir à la BC CUBE une intelligence puissante pour le traitement des données et l'identification des attaques malveillantes sur les AV. De plus, une solution de cryptographie de hachage quantique est utilisée pour améliorer la sécurité du réseau BC. De même, les auteurs de [111] ont déployé à la fois un réseau de neurones profonds (DNN) et une BC pour répondre aux défis de sécurité dans les réseaux véhiculaires intelligents. Dans ce travail, une BC publique est utilisée pour assurer une communication sécurisée entre les composants authentifiés (par exemple, les AV, les RSU, etc.) dans les réseaux véhiculaires, tandis que le DNN est adopté pour détecter les composants anormaux qui sont victimes d'attaques, puis mettre à jour leur statut en invalide dans la BC. Cela permet aux autres composants de prendre conscience des composants invalides et les empêche d'être associés aux appareils compromis. Dans [112], les auteurs ont intégré l'IA et la BC dans un réseau pour résoudre efficacement les problèmes de sécurité routière et de sécurité des données dans les réseaux véhiculaires. Dans ce contexte, le modèle de mémoire à court et long terme (LSTM) est utilisé pour assurer une conduite autonome sûre en utilisant des données véhiculaires en série temporelle pour extraire des informations utiles. Chaque cluster de RSU approuvés déploie un réseau BC de consortium qui utilise le protocole de consensus Tolérance aux fautes

byzantines-Délégation de preuve d'enjeu (BFT-DPoS) afin d'assurer un excellent débit de transaction nécessaire pour prendre en charge les opérations en temps réel dans le réseau véhiculaire. Les auteurs ont confirmé que leur approche maintenait une haute précision de prédiction de 92,5 % à 93,8 %, comparée aux approches centralisées traditionnelles.

3.3.2 Confidentialité et Intégrité des Données

L'intersection de la BC et de l'IA offrira également la possibilité de protéger les données générées par les AV contre les cyberattaques ainsi que d'accéder aux données de manière décentralisée [113], [114]. Dans ce contexte, les auteurs de [113] ont utilisé l'IA et la BC pour renforcer la sécurité et résister à toute modification indésirable des données dans les réseaux véhiculaires. Dans ce travail, les données générées par les différents composants et capteurs des AV sont envoyées au RSU le plus proche pour le stockage et le traitement. Pour stocker les données de manière sécurisée et préserver l'anonymat des AV les générant, une BC de consortium (architecture BC 2.0) est déployée comme réseau sous-jacent pour chaque grappe de RSU, formée par des RSU voisins. La Blockchain 2.0, qui est une extension de la Blockchain 1.0, utilise des algorithmes de consensus efficaces, tels que la tolérance aux fautes byzantines d'Istanbul (IBFT) [115], l'Endossement Sélectif (SE) [116], et les mécanismes de consensus basés sur Raft [116], qui peuvent traiter un grand nombre de transactions à des taux de vitesse plus élevés avec moins de consommation d'énergie. En raison des capacités de stockage médiocres des RSU, les données nouvellement reçues sont transmises au cloud pour une analyse plus poussée, où un modèle RL est utilisé pour reconnaître les nouveaux motifs de données et les catégoriser selon les différentes conditions. Dans une autre étude pertinente [114], la BC et l'IA ont été fusionnées pour préserver la confidentialité des données échangées entre les AV et les RSU. Dans ce travail, la BC est utilisée pour créer des canaux de partage d'informations transparents et fiables entre les AV et les RSU, tandis que des algorithmes d'IA sont utilisés pour percevoir les besoins des AV sous-jacents et prédire les exigences de contenu pertinentes pour les RSU ou les AV qui choisissent d'être des fournisseurs de contenu.

3.3.3 Apprentissage Collaboratif

De nombreuses études récentes ont exploité la BC pour traiter les données d'apprentissage de l'IA de manière distribuée, sans être limitées à un ensemble de

données unique [104], [117], [118], [119], [120]. Il s'agit d'un aspect très important de l'intégration de la BC et de l'IA car cela permet d'avoir un contrôle total sur l'utilisation des données et des modèles d'apprentissage et donc, de résoudre les préoccupations croissantes en matière de confidentialité concernant le partage des données brutes des AV [121], [122], [123]. Dans ce contexte, les auteurs de [124] ont combiné la BC avec un algorithme hiérarchique de FL pour garantir la sécurité et la confidentialité des connaissances pendant le processus de partage. Les AV apprennent les données environnementales grâce à des méthodes d'apprentissage automatique et partagent les connaissances acquises avec les autres via le réseau BC. De plus, le cadre basé sur la BC est conçu pour traiter efficacement certaines attaques malveillantes. Les auteurs ont confirmé que le modèle BC basé sur l'IA proposé réduisait efficacement la consommation de calcul par rapport aux systèmes BC conventionnels et améliorait la précision de l'apprentissage d'environ 10 % pour le réseau MLP et de 3 % pour le réseau CNN. Dans une approche similaire [119], une solution d'apprentissage collectif basée sur la BC est proposée, où chaque AV peut partager le modèle local appris en tant que connaissances pour améliorer l'efficacité et la précision de l'IA. Le système BC, qui remplace le serveur central, est utilisé pour rendre le processus d'apprentissage collectif sécurisé, automatique et transparent. Dans la même direction, les études [117], [125], [126] ont proposé une conception d'apprentissage fédéré basée sur la BC (BFL) pour une communication véhiculaire efficiente et respectueuse de la confidentialité, où les mises à jour locales du modèle ML sur véhicule (oVML) sont échangées et vérifiées de manière distribuée.

3.3.4 Détection d'intrusions Collaborative

FL et BC ont également été utilisés pour concevoir des systèmes de détection d'intrusions basés sur l'IA collaboratifs et distribués pour les AV. FL à la capacité d'éviter de partager directement des données sensibles en entraînant des modèles localement sur chaque véhicule. En revanche, la BC peut résoudre le problème de l'entraînement de données centralisées traditionnelles qui dépend fortement de la robustesse et de la fiabilité d'un serveur central. Les auteurs de [121] ont proposé un mécanisme de détection d'intrusions basé sur l'apprentissage profond distribué qui décharge le modèle d'entraînement sur des dispositifs de bord distribués (par exemple, les véhicules connectés et les unités de bord de route (RSUs)), en utilisant FL et BC. Dans ce travail, la BC Ethereum est utilisée pour stocker et partager de manière

sécurisée les modèles d'entraînement. Alors que, le modèle FL est implémenté en utilisant des DNN et la bibliothèque "Syft". Dans une approche similaire [122], les auteurs ont introduit un IDS basé sur le DL pour détecter les cyberattaques dans les réseaux de véhicules. Le système proposé est intégré dans un cadre d'intelligence de bord géré par BC où les nœuds de bord (AV, RSUs) participent de manière collaborative et fiable à l'entraînement fédéré du schéma de détection d'intrusion.

4. Conclusion

Ce chapitre a exploré en profondeur les concepts de la blockchain et de l'intelligence artificielle (IA), en mettant en lumière la sécurité dans AV basée sur la blockchain et celle basée sur l'IA. Il a également examiné l'intégration de ces deux technologies pour sécuriser les véhicules autonomes.

CHAPITRE 3

Une Approche Pour La Sécurité Des Véhicules Autonomes En Utilisant L'IA Et Blockchain

Initialement, les applications de L'Internet des Véhicules (IoV) sont complexes dans le sens où elles nécessitent des techniques avancées pour être exécutées en raison du comportement imprévisible et aléatoire des véhicules. En conséquence, les chercheurs ont adopté l'IA pour assister dans le processus décisionnel accablant depuis lors (comme discuté précédemment) [113]. Malgré ces efforts et contributions, l'IA augmente encore la charge de calcul sur l'infrastructure de l'IoV et nécessite un environnement incubateur et exempt de malveillance pour fonctionner comme prévu. Sinon, l'IA peut perdre sa fiabilité et menacer la sécurité routière en raison de sa vulnérabilité aux cyberattaques. De telles attaques peuvent manipuler ces algorithmes et perturber leur comportement, avec des modifications minimes, entraînant des décisions inexactes pouvant mettre en danger la vie des gens. Cela est principalement dû au manque d'explicabilité des décisions prises par ces algorithmes. Dans ce contexte, l'intégration de l'IA avec la Blockchain présente des avantages pour les applications et la gestion de l'infrastructure, permettant un IoV décentralisé, intelligent et sécurisé [113]. Cependant, essayer de surmonter les limitations ci-dessus en intégrant la Blockchain entraîne une charge de calcul plus élevée sur l'infrastructure de l'IoV, ce qui peut nuire à ses performances. Ainsi, il est nécessaire de disposer d'une architecture qui combine à la fois l'IA et la Blockchain, et bénéficie du Vehicular Edge Computing (VEC) pour utiliser et soutenir efficacement l'infrastructure de l'IoV afin de répondre aux exigences des deux technologies [113].

1. Définitions

1.1 Cloud Computing

Le cloud computing ou informatique en nuage est une infrastructure dans laquelle la puissance de calcul et le stockage sont gérés par des serveurs distants auxquels les usagers se connectent via une liaison Internet sécurisée. L'ordinateur de bureau ou portable, le téléphone mobile, la tablette tactile et autres objets connectés deviennent des points d'accès pour exécuter des applications ou consulter des données qui sont hébergées sur les serveurs. Le cloud se caractérise également par sa souplesse qui permet aux fournisseurs d'adapter automatiquement la capacité de stockage et la puissance de calcul aux besoins des utilisateurs [127].

Pour le grand public, le cloud computing se matérialise notamment par les services de stockage et de partage de données numériques type Box, Dropbox, Microsoft OneDrive ou Apple iCloud sur lesquels les utilisateurs peuvent stocker des contenus personnels (photos, vidéos, musique, documents...) et y accéder n'importe où dans le monde depuis n'importe quel terminal connecté [127].

1.2 Fog Computing

La décentralisation et la flexibilité sont les principales différences entre le Fog computing et le cloud computing. Le Fog computing, également appelé Fog networking ou Fogging, décrit une structure informatique décentralisée située entre le cloud et les appareils qui produisent des données. Cette structure flexible permet aux utilisateurs de placer des ressources, y compris des applications et les données qu'elles produisent, dans des emplacements logiques pour améliorer les performances [128].

L'objectif de cette structure est de localiser les services d'analyse de base à la périphérie du réseau, plus près de l'endroit où ils sont nécessaires. Cela réduit la distance à travers le réseau que les utilisateurs doivent transmettre des données, améliorant ainsi les performances et l'efficacité globale du réseau [128].

Les problèmes de sécurité liés au Fog computing offrent également des avantages aux utilisateurs. Le paradigme du Fog computing peut segmenter le trafic de bande passante, permettant aux utilisateurs d'améliorer la sécurité avec des pare-feux supplémentaires dans le réseau [128].

Le Fog computing conserve certaines des caractéristiques du cloud computing, dont il est issu. Les utilisateurs peuvent toujours stocker des applications et des données hors site, et payer non seulement pour le stockage hors site, mais aussi pour les mises à niveau et la maintenance du cloud pour leurs données tout en utilisant un modèle de Fog computing. Leurs équipes pourront toujours accéder aux données à distance, par exemple [128].

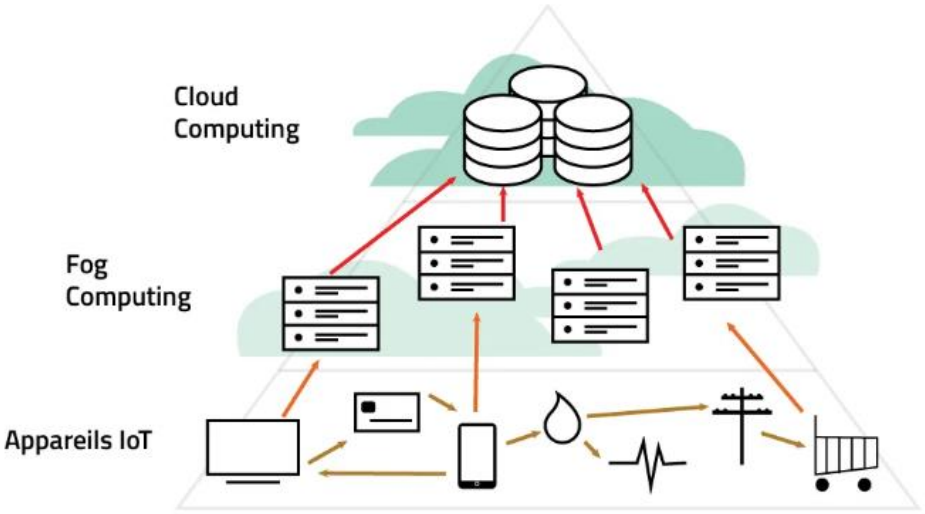


FIGURE 10: L'ARCHITECTURE DE FOG COMPUTING [129].

2. Architecture de L'approche

Dans cette section, Dans [111] les auteurs ont présenté une vue d'ensemble de leurs architecture proposée qui intègre des modèles d'IA avec un réseau Blockchain évolutif sur une infrastructure VEC multi-couches. La Figure 11 illustre comment les trois technologies peuvent utiliser les composants de l'IoV dans trois couches hiérarchiques :Génération de données IoV, Bord Véhiculaire et Cloud/Fog. Présenté leur architecture de bas en haut, ils ont commencé par les différents composants de l'IoV qui génèrent des données véhiculaires, exécutent des modèles d'IA et réalisent diverses tâches. Au niveau du Bord, la fiabilité des données est assurée par plusieurs Blockchains hybrides déployées sur des clusters de RSU. Après approbation de la Blockchain, les données véhiculaires sont gérées et stockées dans des centres de données. Ensuite, ils ont utilisé des puissants serveurs Fog connectés à ces Blockchains, assistés par des serveurs cloud, pour former une base de calcul solide pour soutenir l'IoV. Les serveurs Cloud/Fog exécutent des tâches de calcul déchargées par les véhicules. Ils sont également responsables de la mise à jour des modèles d'IA véhiculaires en apprenant

des nouvelles données stockées dans les centres de données. Pour préciser davantage, ils ont donnée ci-dessous quelques détails sur les fonctionnalités essentielles de chaque couche [113].

2.1 Couche de Génération de Données IoV

Initialement, ils ont supposé que les véhicules sont toujours connectés au Bord Véhiculaire, soit directement, soit par un nœud maître. Un véhicule (ou tout autre dispositif Iov, par exemple une caméra routière) génère des données routières via les capteurs qu'il est équipé, puis les envoie à la RSU la plus proche. De plus, cette couche génère des tâches de calcul à décharger vers l'infrastructure VEC.

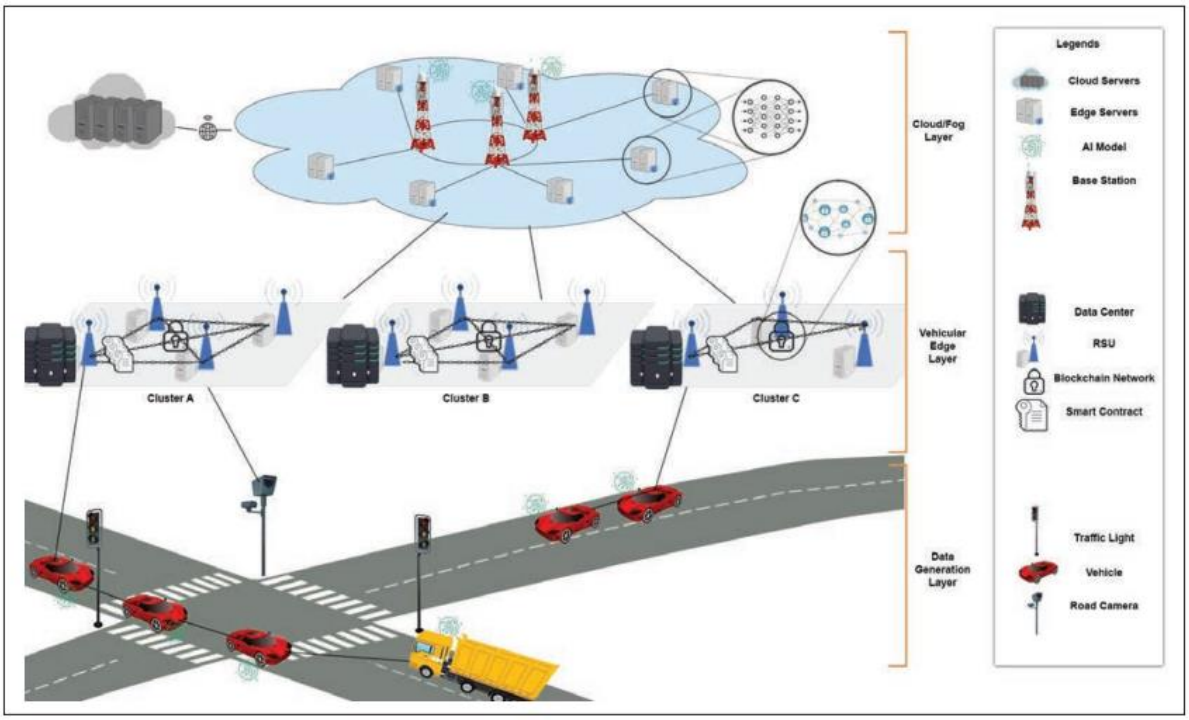


FIGURE 11: ARCHITECTURE VEC BASEE SUR LA BLOCKCHAIN SOUTENANT L'IA DANS L'IOV [113].

2.2 Couche de Bord Véhiculaire

Les données générées doivent être stockées, filtrées, puis transférées de manière sécurisée, sans être altérées, vers des serveurs riches en capacités de traitement pour traitement. Les nœuds de bord, dans notre cas les RSU, sont responsables de ces tâches, en plus d'éviter la congestion du réseau sur les couches supérieures en raison de la quantité massive de données. Comme le montre la Figure 11, les RSU voisins forment un cluster pour servir efficacement les véhicules. En raison des faibles capacités de stockage des RSU, ils ont assisté le cluster en déployant un centre de données à portée. Les nouvelles données reçues par la RSU sont transmises au

centre de données. La RSU réceptrice n'utilise que des métadonnées faisant référence aux nouvelles données pour le traitement. Pour stocker les données en toute sécurité et maintenir l'anonymat des véhicules les générant, ils proposée d'utiliser une architecture Blockchain 2.0 de consortium comme réseau sous-jacent pour chaque cluster de RSU. Dans une telle Blockchain, la méthode de consensus utilisée diffère du Proof-of-Work (PoW) typique, qui consomme beaucoup d'énergie et de temps. En général, elle utilise un algorithme de consensus efficace, tel que Istanbul Byzantine Fault Tolerance, Selective Endorsement, et des mécanismes de consensus basés sur Raft, qui peuvent traiter un grand nombre de transactions à des vitesses plus élevées avec moins d'énergie consommée. De plus, elle permet un accès hybride afin que les entités internes et externes aient un accès complet ou limité, selon leur rôle, pour gérer la Blockchain et faire des demandes. Dans ce contexte, le Bord est responsable d'un certain ensemble d'actions intégrées dans trois contrats intelligents distincts comme indiqué ci-dessous :

- **Authentification des Participants** : Pour qu'un véhicule interagisse avec l'infrastructure, le contrat d'authentification reconnaît d'abord la connexion avec ce véhicule. Ensuite, il crée un profil et stocke des informations de base à son sujet qui resteront actives tant qu'il reste sous la couverture du même cluster de Bord.
- **Stockage des Données** : Ce contrat peut différencier plusieurs types de données captées. Il intègre un mécanisme qui catégorise et étiquette les données à transférer vers le centre de données. Cette phase facilite le processus de transfert des données collectées vers les différents types d'applications qui les demandent.
- **Gestion des Modèles d'IA Véhiculaire** : Supposons que les véhicules sont en communication récurrente avec le Bord. Une fois que le véhicule est authentifié, ce contrat se déclenche fréquemment pour gérer la mise à jour des modèles d'application IoV (comme le modèle d'IA de conduite autonome) intégrés dans les véhicules chaque fois qu'une nouvelle version est reçue de la couche Cloud/Fog. Le modèle mis à jour est transféré aux véhicules exécutant l'application d'IA concernée.

2.3 Couche Cloud / Fog

Comme les défis l'impliquent, il est nécessaire d'avoir un environnement sécurisé et riche en capacités de calcul pour effectuer des traitements lourds. En général, affiner

un modèle d'IA à jour nécessite des traitements lourds, ce que peuvent offrir les serveurs Fog fournis par des fournisseurs de confiance. Les modèles mis à jour s'appuient sur de nouvelles données routières récupérées de la couche Bord Véhiculaire pour les mettre à jour et augmenter leur précision en raison de la dynamique de l'Iov. En cas de surcharge des serveurs Fog, ils dépendent du déchargement de certaines tâches vers les Clouds. Les modèles d'application d'IA sont transmis au véhicule lui-même via le Bord pour lui permettre de générer des décisions instantanées. Le modèle de gestion des ressources peut être déployé sur les BS pour gérer de manière optimale les ressources des serveurs Fog afin de garantir une QoS satisfaisante.

3. Conclusion

Ce chapitre définit d'abord le Cloud computing et le Fog computing. J'ai ensuite choisi une approche parmi les approches qui proposent des solutions autour de la combinaison Blockchain et IA. Dans cette les auteurs, ils ont proposé une nouvelle architecture VEC hybride multicouche basée sur la blockchain, visant à prendre en charge l'intégration de l'intelligence artificielle au sein de l'IOV pour surmonter les menaces ciblant les véhicules autonomes.

L'implémentation

Ce chapitre présente la mise en œuvre de l'architecture dont nous avons parlé dans le chapitre précédent qui combine blockchain et intelligence artificielle dans VEC.

1. Exploration des Environnements de Développement

1.1 Eclipse IDE

Eclipse IDE est un environnement de développement intégré (IDE) libre, extensible, universel et polyvalent, permettant de créer des projets de développement dans de nombreux langages de programmation [130] .

1.2 Remix IDE

Remix est un environnement de développement intégré (IDE) open-source basé sur le web pour le développement de contrats intelligents en utilisant le langage de programmation Solidity. Il offre une interface conviviale pour écrire, tester, déboguer et déployer des contrats intelligents sur divers réseaux blockchain tels qu'Ethereum, Binance Smart Chain, et plus encore. Remix dispose d'un compilateur et d'un débogueur intégrés, ce qui facilite la rédaction de contrats intelligents efficaces et sécurisés pour les développeurs [131].

2. Langages de Programmation et bibliothèques utilisé

2.1 Java avec web3j

Web3j est une bibliothèque Java qui fournit une enveloppe pour l'API JSON-RPC d'Ethereum et vous permet d'interagir facilement avec la blockchain Ethereum. Web3j est décrite comme une bibliothèque Java et Android hautement modulaire, réactive et sûre en termes de types, pour travailler avec les contrats intelligents et s'intégrer aux clients (nœuds) du réseau Ethereum. Cela vous permet de travailler avec la blockchain Ethereum sans avoir à écrire votre propre code d'intégration pour la plateforme [132].

2.2 Solidity

Solidity est le langage principal utilisé pour écrire des smart contracts sur la blockchain Ethereum. Un smart contract est un contrat auto-exécutable composé de règles et protocoles que deux parties conviennent de suivre. Une fois déployé sur la blockchain, un smart contract est immuable [133].

3. Plateforme utilisée

3.1 Ganache

Ganache est une blockchain personnelle pour le développement rapide d'applications distribuées Ethereum. Il permet de développer, déployer et tester vos dApps dans un environnement sûr et déterministe. Ganache offre une console pour exécuter du code Solidity, la possibilité de forker le réseau principal ou de test Ethereum, et de nombreuses autres fonctionnalités utiles pour le développement [134].

3.2 MétaMask

MetaMask est un portefeuille Ethereum qui fait le lien entre les interfaces utilisateur pour Ethereum (comme les navigateurs Mist et les DApps) et le web standard (comme Chrome, Firefox, les sites web). Il injecte une bibliothèque JavaScript appelée web3.js dans l'espace de noms de chaque page chargée par votre navigateur. MetaMask est principalement utilisé comme un plugin dans Chrome [133].

4. Déploiement des Contrats Intelligents pour l'Architecture IoV

Dans cette section, nous avons déployé l'architecture proposée pour intégrer modèle d'IA avec un réseau Blockchain évolutif sur une infrastructure VEC (Vehicular Edge Computing) multi-couches. Nous détaillerons également le rôle des contrats intelligents dans cette architecture et leur implémentation en utilisant Remix, Metamask, Ganache.

Une fois les contrats intelligents compilés, vous pouvez les déployer sur la blockchain Ganache en utilisant MetaMask pour signer les transactions.

4.1 Authentification des Participants

Le contrat AuthenticationContract gère l'authentification des véhicules et la création de leurs profils. Il crée un profil pour chaque véhicule et stocke des informations de base.

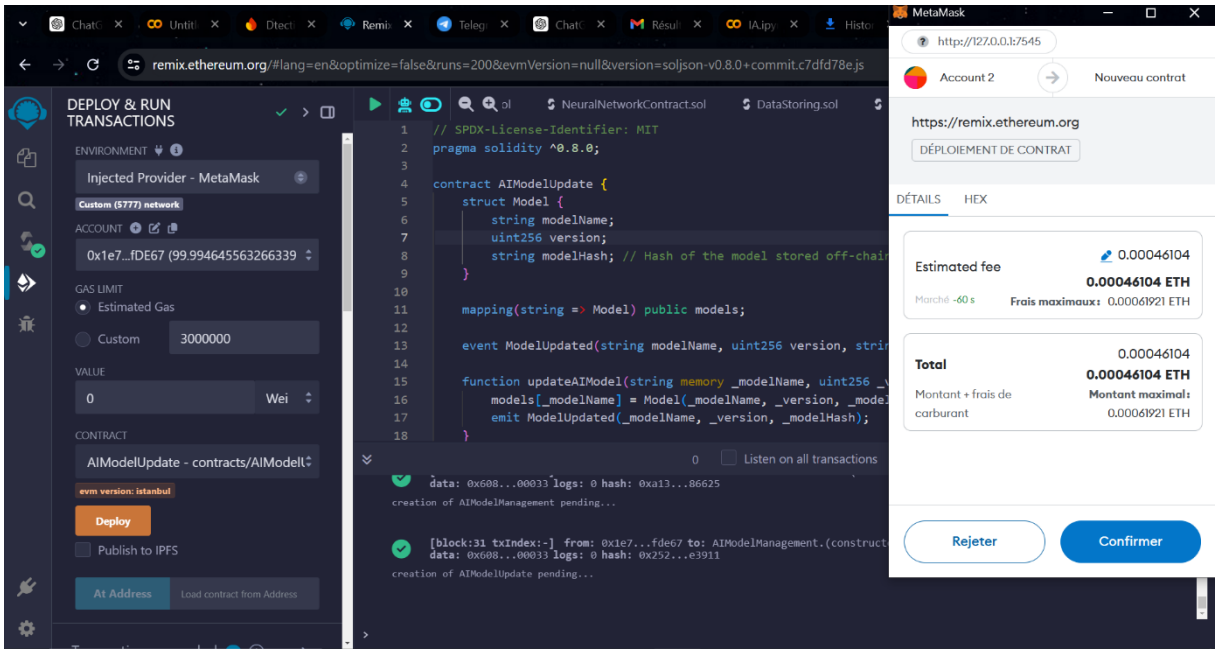


FIGURE 12: DEPLOIEMENT LE CONTACT D'AUTHENTIFICATION AVEC META MASK.

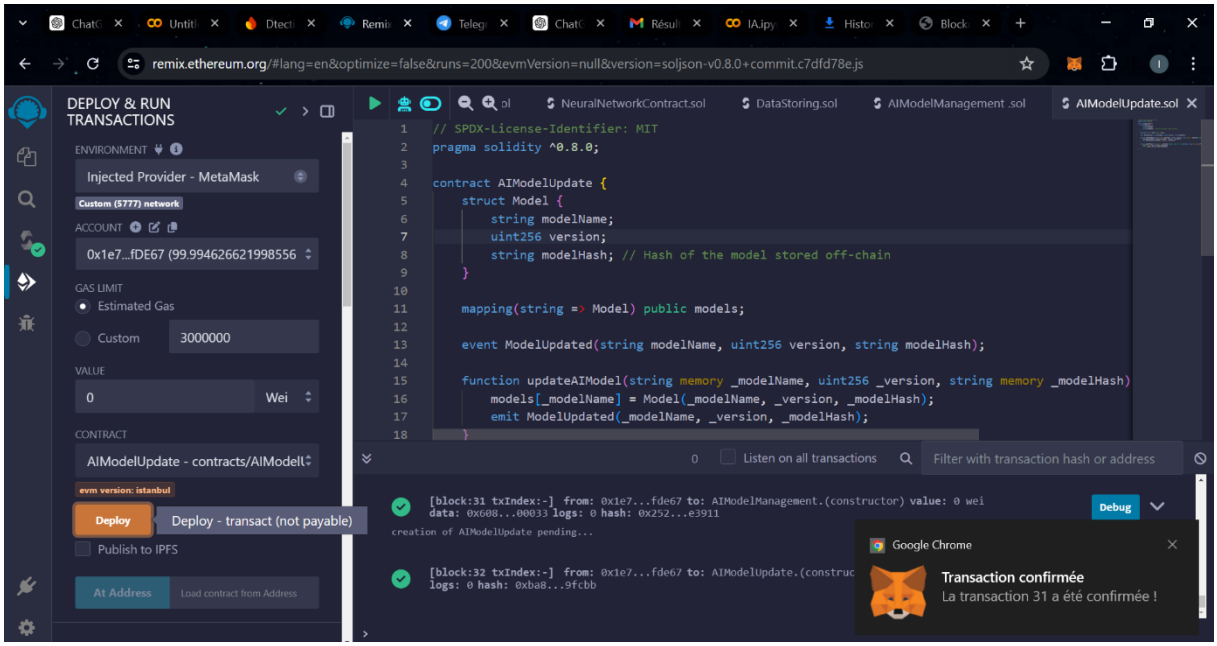


FIGURE 13: LA TRANSACTION CONFIRMÉE AVEC META MASK.

4.2 Stockage des Données

Le contrat DataStorageContract gère le stockage des données, leur catégorisation et leur labellisation. Il permet de différencier plusieurs types de données et facilite leur transfert vers les applications concernées.

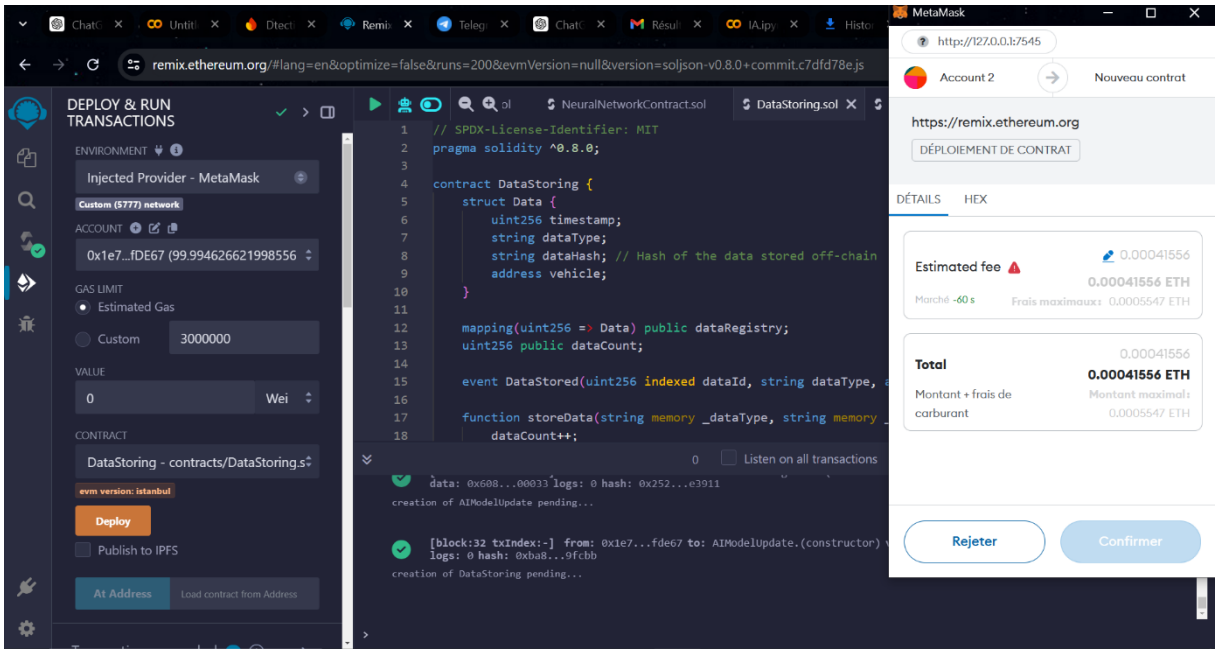


FIGURE 14: DEPLOIYEMENT LE CONTRACT STOCKAGE DES DONNEES.

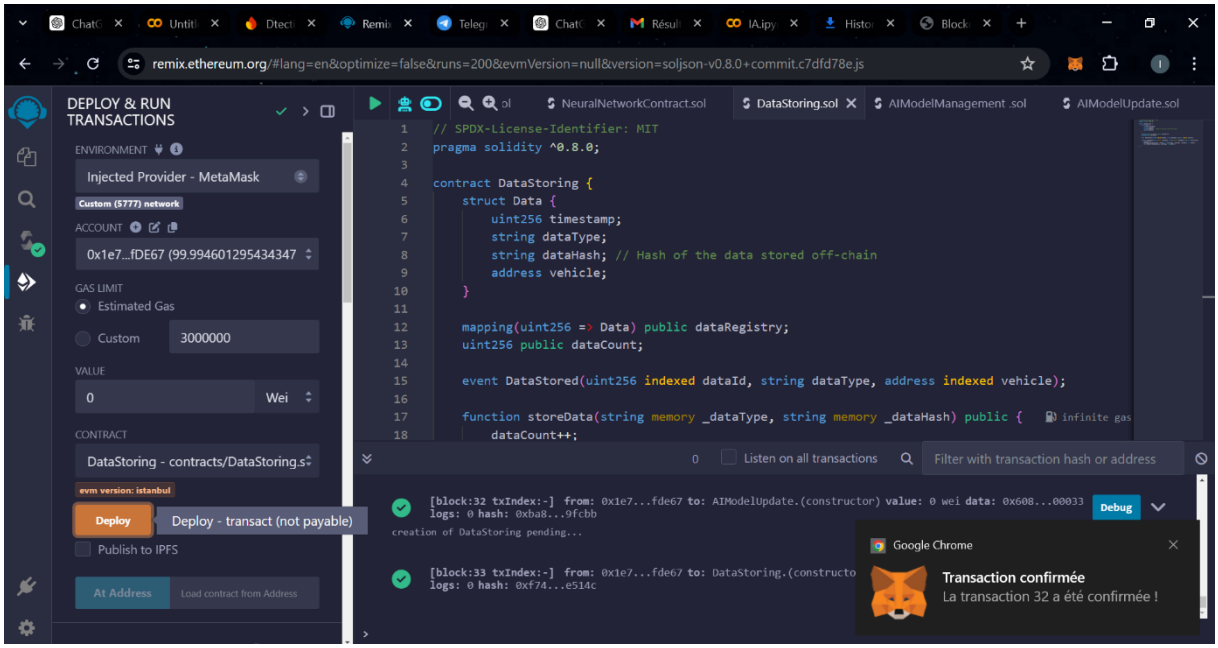


FIGURE 15: TRANSACTION CONFERMÉE AVEC META MASK.

4.3 Gestion des Modèles d'IA

Le contrat AIModelManagementContract gère la mise à jour des modèles d'IA pour les véhicules. Il permet de mettre à jour les modèles d'application IoV intégrés aux véhicules.

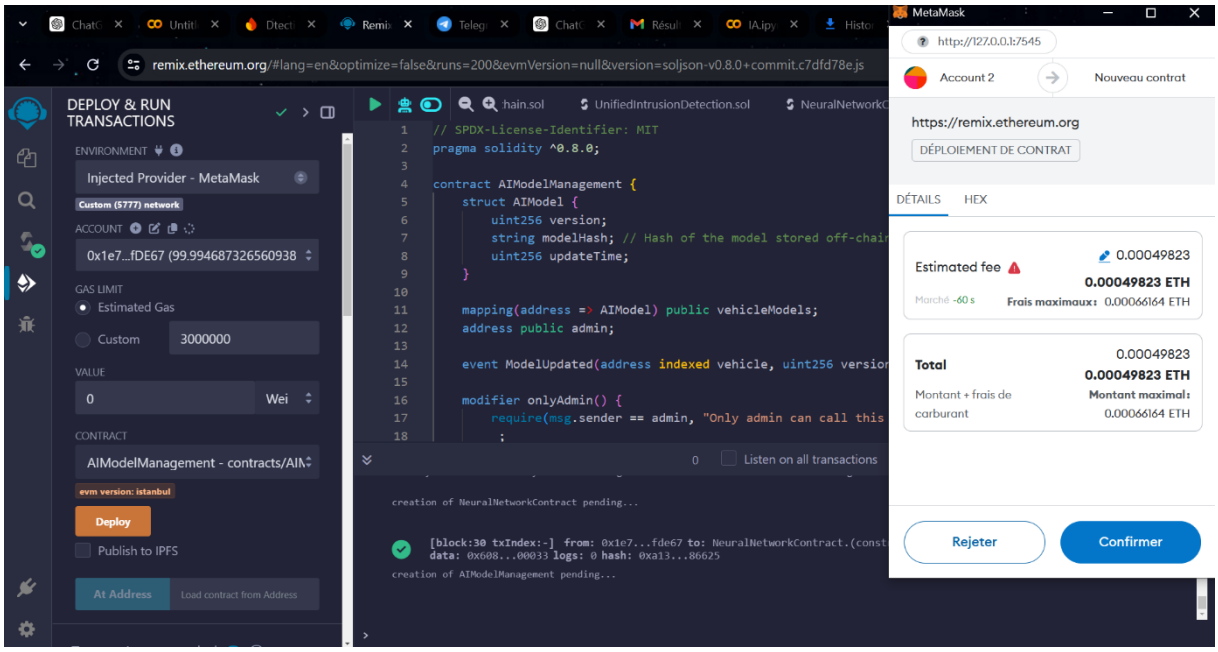


FIGURE 16: DEPLOIYEMENT LE CONTRACT GESTION DES MODELES D'IA AVEC METAMASK.

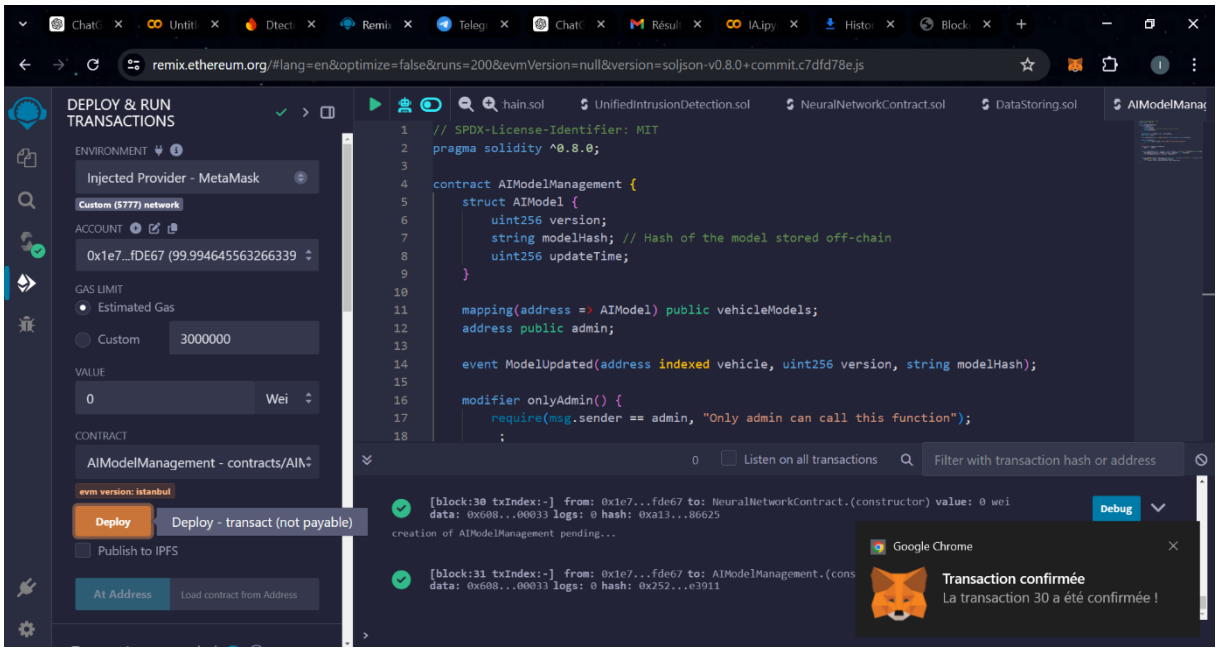


FIGURE 17: LA TRANSACTION CONFERMÉE AVEC META MASK.

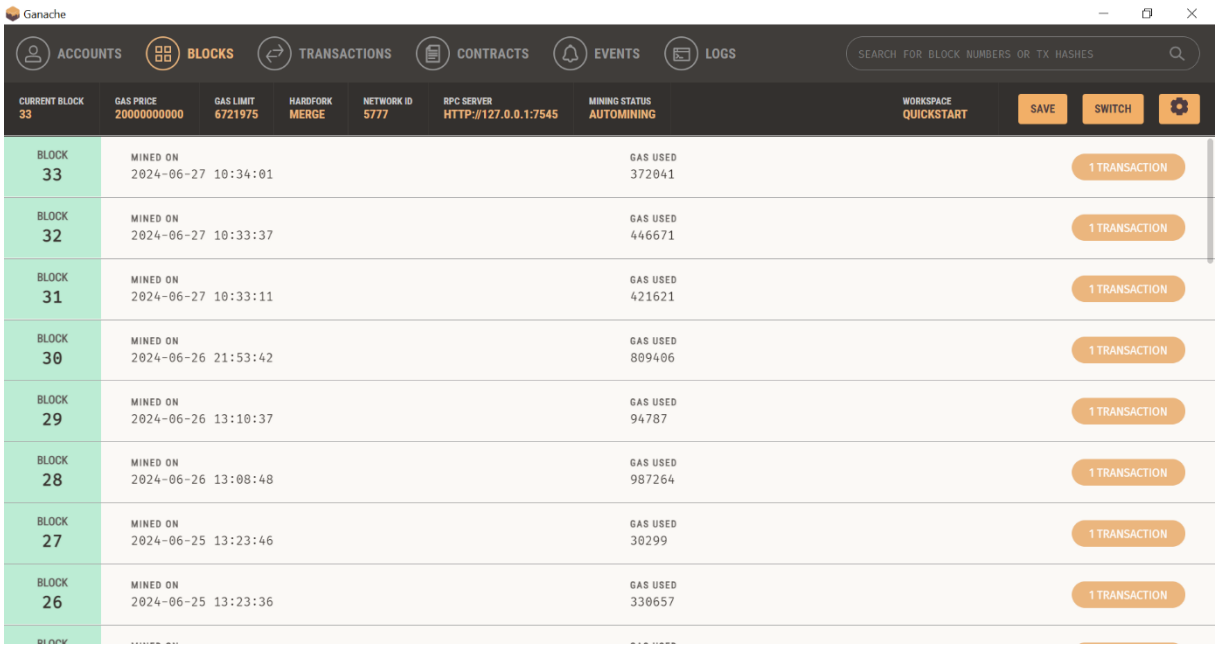


FIGURE 18: LES TRANSACTION DANS GANACHE.

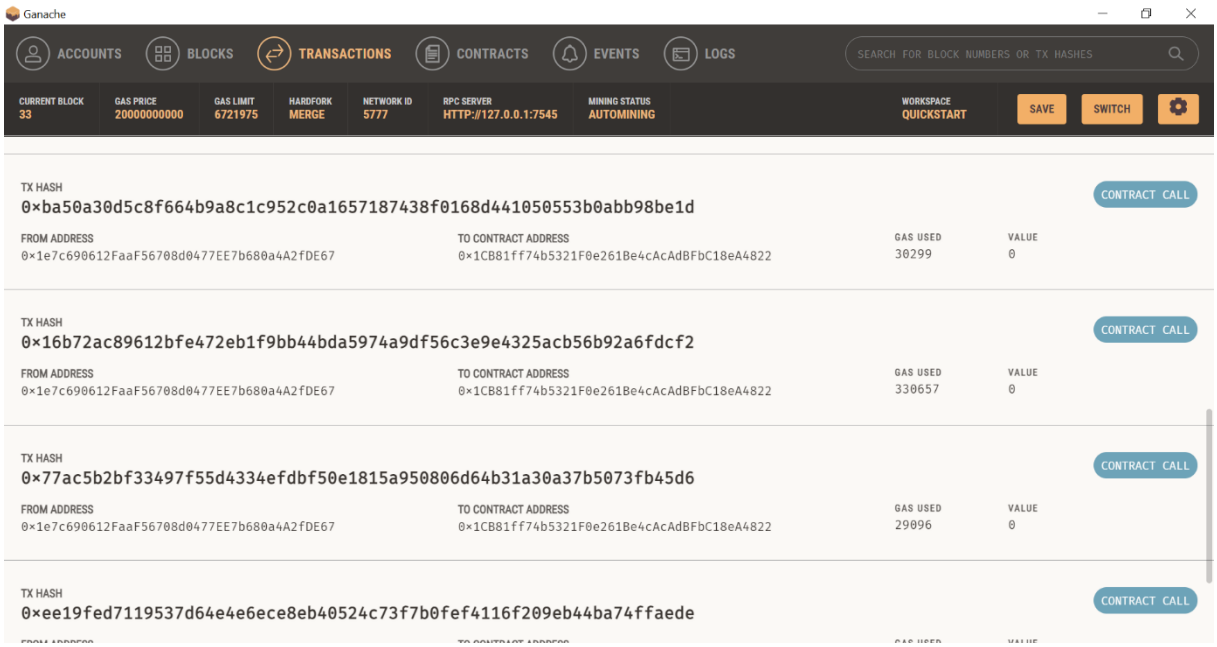


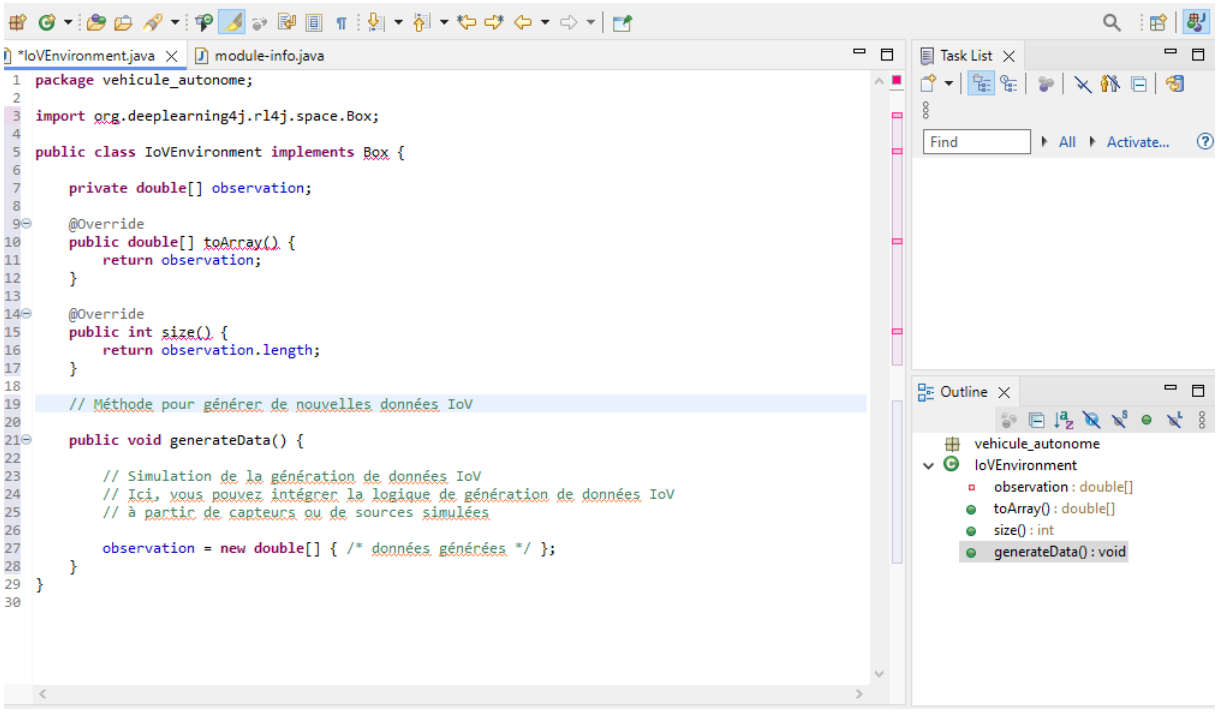
FIGURE 19: LES 3 CONTRAT DANS GANACHE.

5. Développement un modèle L'IA de l'approche

Nous allons utiliser Deeplearning4j pour l'IA RL et Web3j pour l'interaction avec Ethereum. Le modèle d'apprentissage par renforcement (RL) sera simplifié pour illustrer les concepts de base.

5.1 Environnement RL pour la Génération de Données IoV

Définissons d'abord l'environnement RL qui simule la génération de données IoV :

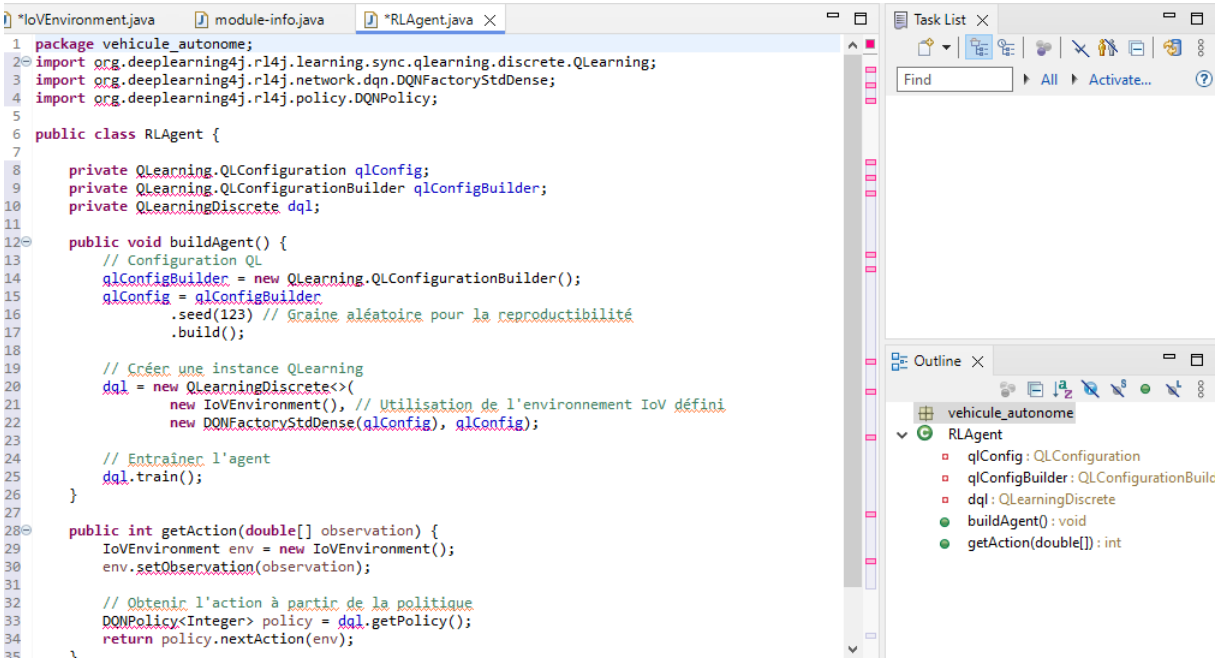



```java
package vehicule_autonome;

import org.deeplearning4j.rl4j.space.Box;

public class IoVEnvironment implements Box {

    private double[] observation;

    @Override
    public double[] toArray() {
        return observation;
    }

    @Override
    public int size() {
        return observation.length;
    }

    // Méthode pour générer de nouvelles données IoV

    public void generateData() {

        // Simulation de la génération de données IoV
        // Ici, vous pouvez intégrer la logique de génération de données IoV
        // à partir de capteurs ou de sources simulées

        observation = new double[] { /* données générées */ };
    }
}
```

FIGURE 20: LA CLASSE DE L'ENVIRONNEMENT RL QUI SIMULE LA GENERATION DE DONNEES IOV.

5.2 Agent d'Apprentissage par Renforcement

Ensuite, créons un agent RL qui interagit avec cet environnement pour apprendre à prendre des décisions :




```java
package vehicule_autonome;
import org.deeplearning4j.rl4j.learning.sync.qlearning.discrete.QLearning;
import org.deeplearning4j.rl4j.network.dqn.DQNFactoryStdDense;
import org.deeplearning4j.rl4j.policy.DQNPolicy;

public class RLAgent {

    private QLearning.QLConfiguration qlConfig;
    private QLearning.QLConfigurationBuilder qlConfigBuilder;
    private QLearningDiscrete dql;

    public void buildAgent() {
        // Configuration QL
        qlConfigBuilder = new QLearning.QLConfigurationBuilder();
        qlConfig = qlConfigBuilder
                .seed(123) // Graine aléatoire pour la reproductibilité
                .build();

        // Créer une instance QLearning
        dql = new QLearningDiscrete<>(
                new IoVEnvironment(), // Utilisation de l'environnement IoV défini
                new DQNFactoryStdDense(qlConfig), qlConfig);

        // Entraîner l'agent
        dql.train();
    }

    public int getAction(double[] observation) {
        IoVEnvironment env = new IoVEnvironment();
        env.setObservation(observation);

        // Obtenir l'action à partir de la politique
        DQNPolicy<Integer> policy = dql.getPolicy();
        return policy.nextAction(env);
    }
```

FIGURE 21: LA CLASSE CREONS UN AGENT RL QUI INTERAGIT AVEC L'ENVIRONNEMENT RL.

5.Conclusion

En conclusion, dans ce chapitre décrit la manière dont les contrats intelligents sont utilisés pour sécuriser et gérer les données générées par les véhicules dans une architecture IoV complexe. En utilisant Remix, MetaMask et Ganache pour développer, déployer et tester ces contrats, nous avons pu démontrer la faisabilité et l'efficacité de cette approche.

CONCLUSION GENERALE

La sécurité des véhicules autonomes est un enjeu crucial dans le domaine de la mobilité automatisée. Ce mémoire a exploré en profondeur les défis et les solutions liés à ce sujet, en se concentrant sur l'intégration de technologies émergentes telles que la blockchain et l'intelligence artificielle (IA) pour renforcer la protection des AV contre les cybers risques.

Dans un premier temps, nous avons examiné la réalité des véhicules autonomes et leur intégration croissante avec l'Internet des Objets (IoT). Cette généralité nous a permis de comprendre l'importance cruciale des capteurs IoT dans le fonctionnement autonome des véhicules et leur capacité à interagir avec leur environnement.

Ensuite, nous avons plongé dans les technologies avancées de sécurité, en mettant l'accent sur la blockchain et l'IA. La blockchain offre une solution robuste pour sécuriser les échanges de données et assurer la traçabilité des transactions, tandis que l'IA renforce la détection et la prévention des menaces, améliorant ainsi la résilience des systèmes autonomes.

Une approche novatrice d'architecture basée sur l'informatique en périphérie a été choisi et présenté dans le chapitre 3 pour intégrer l'IA et la blockchain dans l'Internet des Véhicules (IoV), offrant des avantages significatifs en termes de sécurité et d'efficacité des ressources informatiques.

Enfin, une mise en œuvre concrète a été réalisée avec le développement d'une application utilisant la blockchain et l'IA pour sécuriser les véhicules autonomes. Cette application représente l’implémentation de l’approche présentée dans le chapitre 3.

En conclusion, ce mémoire a contribué à approfondir une compréhension des défis et des solutions en matière de sécurité des véhicules autonomes. L’intégration des technologies innovantes ouvre la voie à des systèmes autonomes plus sûrs et plus fiables

BIBLIOGRAPHIE

[1] ILTEN, A & HADDOUCHE, C. (2022). Internet des objets appliqué à la domotique, Mémoire de Master. Université de A/Mira Bejaia, Algérienne Démocratique et Populaire.

[2] https://internetdesobjetsdomotiquedotcom.wordpress.com/2015/11/22/questque-linternet-des-objets/

[3] https://www.naxoo.ch/linternet-des-objets-internet-of-things-iot/

[4] Souhayla, F. (2021). *l'internet des objets révolutionne notre vie quotidienne: application pour une maison intelligent* (Doctoral dissertation, Universite laarbi tebessi tebessa).

[5] DJEFFAL,L.(2019).Gestion dynamique du spectre pour l'Internet des objets (IoT).Mémoire de Master.Université Mohamed Khider – BISKRA.

[6] Atoumi Yanis et Bensadi Sonia, Approche évolutionnaire pour la composition de services sensible à la QoS dans l'Internet des Objets à large échelle, Mémoire de Master Recherche, Université Abderahmane Mira de Béjaia, pp 3-6, 2018.

[7] https://web-app-art.fr/fr/a-propos/domaines-iot

[8] https://cyberjustice.blog/2019/11/27/les-smart-cities-un-danger-pour-les-donnees-personnelles/

[9] Fantin Irudaya Raj, E., & Appadurai, M. (2022). Internet of things-based smart transportation system for smart cities. In Intelligent Systems for Social Good: Theory and Practice (pp. 39-50). Singapore: Springer Nature Singapore

[10] Miller, J. : Vehicle-to-vehicle-to-infrastructure (V2V2I) intelligent transportation system architecture. In: 2008 IEEE intelligent vehicles symposium, pp. 715–720. IEEE (2008)

[11] Benelmir, R. (2024). Navigation coopérative de véhicules autonomes basée sur la communication V2X dans un réseau de 5ème génération (Doctoral dissertation, Université Mohamed Khider (Biskra-Algérie)).

[12] https://www.redhat.com/fr/topics/edge-computing/what-is-an-autonomous-vehicle

[13] Khayyam, H., Javadi, B., Jalili, M., & Jazar, R. N. (2020). Artificial intelligence and internet of things for autonomous vehicles. *Nonlinear approaches in engineering applications: Automotive Applications of engineering problems*, 39-68.

[14] Bendiab, G., Hameurlaine, A., Germanos, G., Kolokotronis, N., & Shiaeles, S. (2023). Autonomous vehicles security: Challenges and solutions using blockchain and artificial intelligence. IEEE Transactions on Intelligent Transportation Systems, 24(4), 3614-3637.

[15] Tigadi, A., & Chandra, M. (2023). Literature Review on the Future of V2X Communication in Connected and Autonomous Vehicles. International Journal of Research and Analytical Reviews, 10, 5.

[16] Hartenstein, H.; Laberteaux, L.P. A tutorial survey on vehicular ad hoc networks. IEEE Commun. Mag. 2008, 46, 164–171. [CrossRef].

[17] Sheikh, M.S.; Liang, J. A Comprehensive Survey on VANET Security Services in Traffic Management System. Wirel. Commun. Mob. Comput. 2019, 2019, 2423915. [CrossRef]

[18] Toor, Y.; Muhlethaler, P.; Laouiti, A.; La Fortelle, A.D. Vehicle Ad Hoc networks: Applications and related technical issues. IEEE Commun. Surv. Tutor. 2008, 10, 74–88. [CrossRef]

[19] Harri, J.; Filali, F.; Bonnet, C. Mobility models for vehicular ad hoc networks: A survey and taxonomy. IEEE Commun. Surv. Tutor. 2009, 11, 19–41. [CrossRef]

[20] Zhang, R.; Yan, F.; Xia, W.; Xing, S.; Wu, Y.; Shen, L. An Optimal Roadside Unit Placement Method for VANET Localization. In Proceedings of the Global Communications Conference (GLOBECOM), Singapore, 4–8 December 2017; pp. 1–6.

[21] Zaidi, S.A.R.; Afzal, A.; Hafeez, M.; Ghogho, M.; Mclernon, D.C.; Swami, A. Solar energy empowered 5G cognitive metro-cellular networks. IEEE Commun. Mag. 2015, 53, 70–77. [CrossRef]

[22] Ahangar, M. N., Ahmed, Q. Z., Khan, F. A., & Hafeez, M. (2021). A survey of autonomous vehicles: Enabling communication technologies and challenges. Sensors, 21(3), 706.

[23] M. C. Chow, M. Ma, and Z. Pan, “Attack models and countermeasures for autonomous vehicles,” in Intelligent Technologies for Internet of Vehicles. Cham, Switzerland: Springer, 2021, pp. 375–401.

[24] X. Sun, F. R. Yu, and P. Zhang, “A survey on cyber-security of connected and autonomous vehicles (CAVs),” IEEE Trans. Intell. Transp. Syst., vol. 23, no. 7, pp. 6240–6259, Jul. 2022.

[25] A. Chowdhury, G. Karmakar, J. Kamruzzaman, A. Jolfaei, and R. Das, “Attacks on self-driving cars and their countermeasures: A survey,” IEEE Access, vol. 8, pp. 207308–207342, 2020.

[26] M. Pham and K. Xiong, “A survey on security attacks and defense techniques for connected and autonomous vehicles,” Comput. Secur., vol. 109, Oct. 2021, Art. no. 102269

[27] M. El-Said, X. Wang, S. Mansour, and A. Kalafut, “Building an impersonation attack and defense testbed for vehicle to vehicle systems,” in Proc. 22st Annu. Conf. Inf. Technol. Educ., Oct. 2021, pp. 65–66.

[28] M. Dibaei et al., “Attacks and defences on intelligent connected vehicles: A survey,” Digit. Commun. Netw., vol. 6, no. 4, pp. 399–421, Nov. 2020.

[29] X. Sun, F. R. Yu, and P. Zhang, “A survey on cyber-security of connected and autonomous vehicles (CAVs),” IEEE Trans. Intell. Transp. Syst., vol. 23, no. 7, pp. 6240–6259, Jul. 2022.

[30] H. S. Sanchez, D. Rotondo, V. Puig, T. Escobet, and J. Quevedo, “Detection of replay attacks in autonomous vehicles using a bank of QPV observers,” in Proc. 29th Medit. Conf. Control Autom. (MED), Jun. 2021, pp. 1149–1154.

[31] K. Kim, J. S. Kim, S. Jeong, J.-H. Park, and H. K. Kim, “Cybersecurity for autonomous vehicles: Review of attacks and defense,” Comput. Secur., vol. 103, Apr. 2021, Art. no. 102150.

[32] S. Kim, “Blockchain for a trust network among intelligent vehicles,” in Advances in Computers, vol. 111. Amsterdam, The Netherlands: Elsevier, 2018, pp. 43–68.

[33] M. Bozdal, M. Samie, S. Aslam, and I. Jennions, “Evaluation of CAN bus security challenges,” Sensors, vol. 20, no. 8, p. 2364, Apr. 2020.

[34] A. Palanca, E. Evenchick, F. Maggi, and S. Zanero, “A stealth, selective, link-layer denial-of-service attack against automotive networks,” in Proc. Int. Conf. Detection Intrusions Malware, Vulnerability Assessment. Cham, Switzerland: Springer, 2017, pp. 185–206.

[35] X. Han, F. Jin, R. Wang, S. Wang, and Y. Yuan, “Classification of malware for self-driving systems,” Neurocomputing, vol. 428, pp. 352–360, Mar. 2021.

[36] A. Al-Sabaawi, K. Al-Dulaimi, E. Foo, and M. Alazab, “Addressing malware attacks on connected and autonomous vehicles: Recent techniques and challenges,” in Malware Analysis Using Artificial Intelligence and Deep Learning. Cham, Switzerland: Springer, 2021, pp. 97–119.

[37] S. Ornes. (2022). How to Hack a Self-Driving Car. Accessed: Jan. 1, 2022. [Online]. Available: https://physicsworld.com/a/how-tohack-a-self-driving-car/

[38] L. Collingwood, “Privacy implications and liability issues of autonomous vehicles,” Inf. Commun. Technol. Law, vol. 26, no. 1, pp. 32–45, Jan. 2017.

[39] H. Lim and A. Taeihagh, “Autonomous vehicles for smart and sustainable cities: An in-depth exploration of privacy and cybersecurity implications,” Energies, vol. 11, no. 5, p. 1062, Apr. 2018.

[40] M. Obaidat, M. Khodjaeva, J. Holst, and M. B. Zid, “Security and privacy challenges in vehicular ad hoc networks,” in Connected Vehicles Internet Things. Cham, Switzerland: Springer, 2020, pp. 223–251.

[41] J. Cui, L. S. Liew, G. Sabaliauskaite, and F. Zhou, “A review on safety failures, security attacks, and available countermeasures for autonomous vehicles,” Ad Hoc Netw., vol. 90, Jul. 2019, Art. no. 101823.

[42] Abou El Houda, Z., Hafid, A., & Khoukhi, L. (2019, December). Co-IoT: A collaborative DDoS mitigation scheme in IoT environment based on blockchain using SDN. In 2019 IEEE Global Communications Conference (GLOBECOM) (pp. 1-6). IEEE.

[43] Moudoud, H. (2022). Intégration de la Blockchain à l'Internet des Objets (Doctoral dissertation, Troyes).

[44] https://lebondigital.com/blockchain-technologie-ethique/

[45] GUYOMAR, R., BOURGEAUX, M., & KACIMI, S. TPE: Programmation d'une Blockchain à l'aide de la plateforme Hyperledger.

[46]https://www.axiocode.com/application blockchain/?utm_source=pinterest&utm_medium=epingle&utm_campaign=promotion-blog&utm_content=blockchain-app

[47] J. Turek and D. Shasha. The many faces of consensus in distributed systems. Computer, 25(6) :8–17, June 1992.

[48] Moudoud, H. (2022). Intégration de la Blockchain à l'Internet des Objets (Doctoral dissertation, Troyes).

[49] Lakshmi Siva Sankar, M. Sindhu, and M. Sethumadhavan. Survey of consensus protocols on blockchain applications. In 2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS), pages 1–5, Coimbatore, India, January 2017

[50] Iuon-Chang Lin and Tzu-Chun Liao. A Survey of Blockchain Security Issues and Challenges. International Journal of Network Security, 19(5) :653–659, September 2017.

[51] John Adler, Ryan Berryhill, Andreas Veneris, Zissis Poulos, Neil Veira, and Anastasia Kastania. Astraea : A Decentralized Blockchain Oracle. arXiv :1808.00528 [cs], August 2018.

[52] Y. Malahov Z. Hess and J. Pettersson. æternity - a blockchain for scalable, secure and decentralized æpps, 2017.

[53] https://www.techopedia.com/fr/dictionnaire/bitcoin

[54]https://www.journaldunet.fr/patrimoine/guide-des-finances-personnelles/1195520-blockchain-definition-bitcoin-tout-ce-qu-il-faut-savoir/

[55] https://journalducoin.com/lexique/hyperledger/

[56] https://www.talend.com/fr/resources/blockchain/

[57] https://www.cnil.fr/fr/definition/intelligence-artificielle

[58] Mezati, M., & Otmani, R. S. *Réalisation d'une application intelligente pour l'ambulance (Smart Ambulance* (Doctoral dissertation, UNIVERSITY OF KASDI MERBAH OUARGLA).

[59] Karan Aggarwal, Maad M Mijwil, Abdel-Hameed Al-Mistarehi, Safwan Alomari, Murat Gök, Anas M Zein Alaabdin, Safaa H Abdulrhman, et al. Has the future started ? the current growth of artificial intelligence, machine learning, and deep learning. Iraqi Journal for Computer Science and Mathematics, 3(1) :115–123, 2022.

[60] R Sun, M Lerousseau, T Henry, A Carré, A Leroy, T Estienne, S Niyoteka, S Bockel, A Rouyar, É Alvarez Andres, et al. Intelligence artificielle en radiothérapie : radiomique, pathomique, et prédiction de la survie et de la réponse aux traitements. Cancer/Radiothérapie, 25(6-7) :630–637, 2021.

[61] https://larevueia.fr/apprentissage-par-renforcement/

[62] Yann LeCun, Yoshua Bengio, and Geoffrey Hinton. Deep learning. nature, 521(7553) :436–444, 2015.

[63] Oliver Baclic, Matthew Tunis, Kelsey Young, Coraline Doan, Howard Swerdfeger, and Justin Schonfeld. Le traitement du langage naturel (tln), une sous-zone d'intelligence artificielle. 2020.

[64] Melanie Mitchell. An introduction to genetic algorithms. MIT press, 1998.

[65] Haocheng Tan. A brief history and technical review of the expert system research. In IOP Conference Series : Materials Science and Engineering, volume 242, page 012111. IOP Publishing, 2017.

[66] Julie Soriano. Les enjeux de l'intégration de solutions d'intelligence artificielle au sein d'OBNL. PhD thesis, 2018.

[67] Rashmi Priyadarshini, RM Mehra, Amit Sehgal, and Prabhu Jyot Singh. Artificial Intelligence : Applications and Innovations. CRC Press, 2022.

[68] Nicolas Miailhe and Cyrus Hodes. La troisième ère de l'intelligence artificielle.

[69]https://www.josh-digital.com/6-avantages-de-intelligence-artificielle-ia-pour-les-entreprises/

[70]https://www.ericsson.com/fr/blog/2024/1/four-benefits-of-ai-for-security-safety-and-transparency-in-telecom

[71] R. Gupta et al., "VAHAK: A blockchain-based outdoor delivery scheme using UAV for healthcare 4.0 services," in Proc. IEEE INFOCOM Conf. Comput. Commun. Workshops (INFOCOM WKSHPS), Jul. 2020, pp. 255–260.

[72] M. B. Mollah, J. Zhao, D. Niyato, Y. L. Guan, and L. H. Koh, "Blockchain for the Internet of Vehicles towards intelligent transportation systems: A survey," IEEE Internet Things J., vol. 8, no. 6, pp. 4157–4185, Mar. 2021.

[73] R. Gupta, S. Tanwar, N. Kumar, and S. Tyagi, "Blockchain-based security attack resilience schemes for autonomous vehicles in industry 4.0: A systematic review," Comput. Electr. Eng., vol. 86, Sep. 2020, Art. no. 106717.

[74] M. Dibaei et al., "Investigating the prospect of leveraging blockchain and machine learning to secure vehicular networks: A survey," IEEE Trans. Intell. Transp. Syst., vol. 23, no. 2, pp. 683–700, Feb. 2022.

[75] T. Dargahi, H. Ahmadvand, M. Alraja, and C. Yu, "Integration of blockchain with connected and autonomous vehicles: Vision," Technology, vol. 26, no. 28, pp. 33–50, 2021.

[76] B. Krzanich. (2021). Data is the New Oil in the Future of Automated Driving. [Online]. Available: https://newsroom.intel.com/editorials/ krzanich-the-future-of-automated-driving/#gs.htm2ps .

[77] L. Davi, D. Hatebur, M. Heisel, and R. Wirtz, "Combining safety and security in autonomous cars using blockchain technologies," in Proc. Int. Conf. Comput. Saf., Rel., Secur. Cham, Switzerland: Springer, 2019, pp. 223–234.

[78] P. K. Sharma, N. Kumar, and J. H. Park, “Blockchain-based distributed framework for automotive industry in a smart city,” IEEE Trans. Ind. Informat., vol. 15, no. 7, pp. 4197–4205, Jul. 2019.

[79] N. Kamble, R. Gala, R. Vijayaraghavan, E. Shukla, and D. Patel, “Using blockchain in autonomous vehicles,” in Artificial Intelligence and Blockchain for Future Cybersecurity Applications. Cham, Switzerland: Springer, 2021, pp. 285–305

[80] S. K. Singh, J. H. Park, P. K. Sharma, and Y. Pan, “BIIoVT: Blockchain-based secure storage architecture for intelligent Internet of vehicular things,” IEEE Consum. Electron. Mag., vol. 11, no. 6, pp. 75–82, Nov. 2022.

[81] C. Oham, R. A. Michelin, R. Jurdak, S. S. Kanhere, and S. Jha, “B-FERL: Blockchain based framework for securing smart vehicles,” Inf. Process. Manage., vol. 58, no. 1, Jan. 2021, Art. no. 102426.

[82] R. Shrestha and S. Y. Nam, “Regional blockchain for vehicular networks to prevent 51% attacks,” IEEE Access, vol. 7, pp. 95033–95045, 2019.

[83] G. Rathee, A. Sharma, R. Iqbal, M. Aloqaily, N. Jaglan, and R. Kumar, “A blockchain framework for securing connected and autonomous vehicles,” Sensors, vol. 19, no. 14, p. 3165, Jul. 2019.

[84] S. Mitra, S. Bose, S. S. Gupta, and A. Chattopadhyay, “Secure and tamper-resilient distributed ledger for data aggregation in autonomous vehicles,” in Proc. IEEE Asia Pacific Conf. Circuits Syst. (APCCAS), Oct. 2018, pp. 548–551.

[85] H. Guo, E. Meamari, and C.-C. Shen, “Blockchain-inspired event recording system for autonomous vehicles,” in Proc. 1st IEEE Int. Conf. Hot Inf.-Centric Netw. (HotICN), Aug. 2018, pp. 218–222.

[86] M. Cebe, E. Erdin, K. Akkaya, H. Aksu, and S. Uluagac, “Block4Forensic: An integrated lightweight blockchain framework for forensics applications of connected vehicles,” IEEE Commun. Mag., vol. 56, no. 10, pp. 50–57, Oct. 2018.

[87] P. Bhattacharya, A. Shukla, S. Tanwar, N. Kumar, and R. Sharma, “6Blocks: 6G-enabled trust management scheme for decentralized autonomous vehicles,” Comput. Commun., vol. 191, pp. 53–68, Jul. 2022

[88] C. Pu, “A novel blockchain-based trust management scheme for vehicular networks,” in Proc. Wireless Telecommun. Symp. (WTS), Apr. 2021, pp. 1–6.

[89] K. M. A. Alheeti and K. McDonald-Maier, “An intelligent security system for autonomous cars based on infrared sensors,” in Proc. 23rd Int. Conf. Autom. Comput. (ICAC), Sep. 2017, pp. 1–5.

[90] O. Avatefipour et al., “An intelligent secured framework for cyberattack detection in electric vehicles’ CAN bus using machine learning,” IEEE Access, vol. 7, pp. 127580–127592, 2019.

[91] C. Yan, W. Xu, and J. Liu, “Can you trust autonomous vehicles: Contactless attacks against sensors of self-driving vehicle,” DEF CON, vol. 24, p. 109, Aug. 2016.

[92] M. D. Hossain, H. Inoue, H. Ochiai, D. Fall, and Y. Kadobayashi, “LSTM-based intrusion detection system for in-vehicle can bus communications,” IEEE Access, vol. 8, pp. 185489–185502, 2020.

[93] M.-J. Kang and J.-W. Kang, “Intrusion detection system using deep neural network for in-vehicle network security,” PLoS ONE, vol. 11, no. 6, Jun. 2016, Art. no. e0155781.

[94] Y. Yang, Z. Duan, and M. Tehranipoor, “Identify a spoofing attack on an in-vehicle CAN bus based on the deep features of an ECU fingerprint signal,” Smart Cities, vol. 3, no. 1, pp. 17–30, Jan. 2020.

[95] T. H. Aldhyani and H. Alkahtani, “Attacks to automatous vehicles: A deep learning algorithm for cybersecurity,” Sensors, vol. 22, no. 1, p. 360, 2022.

[96] G. Loukas, T. Vuong, R. Heartfield, G. Sakellari, Y. Yoon, and D. Gan, “Cloud-based cyber-physical intrusion detection for vehicles using deep learning,” IEEE Access, vol. 6, pp. 3491–3508, 2018.

[97] C. Catal, H. Gunduz, and A. Ozcan, “Malware detection based on graph attention networks for intelligent transportation systems,” Electronics, vol. 10, no. 20, p. 2534, Oct. 2021.

[98] R. Rahal, A. A. Korba, N. Ghoualmi-Zine, Y. Challal, and M. Y. Ghamri-Doudane, “AntibotV: A multilevel behaviour-based framework for botnets detection in vehicular networks,” J. Netw. Syst. Manage., vol. 30, no. 1, pp. 1–40, Jan. 2022.

[99] S. Gyawali, Y. Qian, and R. Hu, “Deep reinforcement learning based dynamic reputation policy in 5G based vehicular communication networks,” IEEE Trans. Veh. Technol., vol. 70, no. 6, pp. 6136–6146, Jun. 2021.

[100] D. Zhang, F. R. Yu, R. Yang, and H. Tang, “A deep reinforcement learning-based trust management scheme for software-defined vehicular networks,” in Proc. 8th ACM Symp. Design Anal. Intell. Veh. Netw. Appl., Oct. 2018, pp. 1–7.

[101] G. Karmakar, A. Chowdhury, R. Das, J. Kamruzzaman, and S. Islam, “Assessing trust level of a driverless car using deep learning,” IEEE Trans. Intell. Transp. Syst., vol. 22, no. 7, pp. 4457–4466, Jul. 2021.

[102] D. Zhang, F. R. Yu, R. Yang, and L. Zhu, “Software-defined vehicular networks with trust management: A deep reinforcement learning approach,” IEEE Trans. Intell. Transp. Syst., vol. 23, no. 2, pp. 1400–1414, Feb. 2022.

[103] T. Zeng, O. Semiari, M. Chen, W. Saad, and M. Bennis, “Federated learning on the road: Autonomous controller design for connected and autonomous vehicles,” 2021, arXiv:2102.03401.

[104] S. R. Pokhrel and J. Choi, “Federated learning with blockchain for autonomous vehicles: Analysis and design challenges,” IEEE Trans. Commun., vol. 68, no. 8, pp. 4734–4746, Aug. 2020.

[105] A. M. Elbir, B. Soner, S. Coleri, D. Gunduz, and M. Bennis, “Federated learning in vehicular networks,” 2020, arXiv:2006.01412.

[106] U. Majeed, L. U. Khan, A. Yousafzai, Z. Han, B. J. Park, and C. S. Hong, “ST-BFL: A structured transparency empowered cross-silo federated learning on the blockchain framework,” IEEE Access, vol. 9, pp. 155634–155650, 2021.

[107] Y. Li, X. Tao, X. Zhang, J. Liu, and J. Xu, “Privacy-preserved federated learning for autonomous driving,” IEEE Trans. Intell. Transp. Syst., vol. 23, no. 7, pp. 8423–8434, Jul. 2022.

[108] A. Uprety, D. B. Rawat, and J. Li, “Privacy preserving misbehavior detection in IoV using federated machine learning,” in Proc. IEEE 18th Annu. Consum. Commun. Netw. Conf. (CCNC), Jan. 2021, pp. 1–6.

[109] S. Singh, P. K. Sharma, B. Yoon, M. Shojafar, G. H. Cho, and I.-H. Ra, “Convergence of blockchain and artificial intelligence in IoT network for the sustainable smart city,” Sustain. Cities Soc., vol. 63, Dec. 2020, Art. no. 102364.

[110] CUBE. Cube Autonomous Car Network Security Platform Based on Blockchain. Accessed: Dec. 5, 2021. [Online]. Available: https://cubeint.io/.

[111] E. Rabieinejad, A. Yazdinejad, A. Dehghantanha, R. M. Parizi, and G. Srivastava, “Secure AI and blockchain-enabled framework in smart vehicular networks,” in Proc. IEEE Globecom Workshops (GC Wkshps), Dec. 2021, pp. 1–6.

[112] L. Xia, Y. Sun, R. Swash, L. Mohjazi, L. Zhang, and M. A. Imran, “Smart and secure CAV networks empowered by AI-enabled blockchain: The next frontier for intelligent safe driving assessment,” 2021, arXiv:2104.04572.

[113] A. Hammoud, H. Sami, A. Mourad, H. Otrok, R. Mizouni, and J. Bentahar, “AI, blockchain, and vehicular edge computing for smart and secure IoV: Challenges and directions,” IEEE Internet Things Mag., vol. 3, no. 2, pp. 68–73, Jun. 2020.

[114] Y. Qian, Y. Jiang, L. Hu, M. S. Hossain, M. Alrashoud, and M. Al-Hammadi, “Blockchain-based privacy-aware content caching in cognitive Internet of Vehicles,” IEEE Netw., vol. 34, no. 2, pp. 46–51, Mar. 2020.

[115] H. Moniz, “The Istanbul BFT consensus algorithm,” 2020, arXiv:2002.03613.

[116] J. Khamar and H. Patel, “An extensive survey on consensus mechanisms for blockchain technology,” in Data Science and Intelligent Applications. Cham, Switzerland: Springer, 2021, pp. 363–374.

[117] S. R. Pokhrel and J. Choi, “A decentralized federated learning approach for connected autonomous vehicles,” in Proc. IEEE Wireless Commun. Netw. Conf. Workshops (WCNCW), Apr. 2020, pp. 1–6.

[118] S. K. Lo et al., “Towards trustworthy AI: Blockchain-based architecture design for accountability and fairness of federated learning systems,” IEEE Internet Things J., early access, Jan. 19, 2022, doi: 10.1109/JIOT.2022.3144450.

[119] Y. Fu, F. R. Yu, C. Li, T. H. Luan, and Y. Zhang, “Vehicular blockchainbased collective learning for connected and autonomous vehicles,” IEEE Wireless Commun., vol. 27, no. 2, pp. 197–203, Apr. 2020.

[120] Y. Lu, X. Huang, K. Zhang, S. Maharjan, and Y. Zhang, “Blockchain empowered asynchronous federated learning for secure data sharing in Internet of Vehicles,” IEEE Trans. Veh. Technol., vol. 69, no. 4, pp. 4298–4311, Apr. 2020.

[121] H. Liu et al., “Blockchain and federated learning for collaborative intrusion detection in vehicular edge computing,” IEEE Trans. Veh. Technol., vol. 70, no. 6, pp. 6073–6084, Jun. 2021.

[122] M. Abdel-Basset, N. Moustafa, H. Hawash, I. Razzak, K. M. Sallam, and O. M. Elkomy, “Federated intrusion detection in blockchain-based smart transportation systems,” IEEE Trans. Intell. Transp. Syst., vol. 23, no. 3, pp. 2523–2537, Mar. 2022.

[123] I. Aliyu, M. C. Feliciano, S. van Engelenburg, D. O. Kim, and C. G. Lim, “A blockchain-based federated forest for SDN-enabled invehicle network intrusion detection system,” IEEE Access, vol. 9, pp. 102593–102608, 2021

[124] H. Chai, S. Leng, Y. Chen, and K. Zhang, “A hierarchical blockchainenabled federated learning algorithm for knowledge sharing in internet of vehicles,” IEEE Trans. Intell. Transp. Syst., vol. 22, no. 7, pp. 3975–3986, Jul. 2021.

[125] L. Barbieri, S. Savazzi, M. Brambilla, and M. Nicoli, “Decentralized federated learning for extended sensing in 6G connected vehicles,” Veh. Commun., vol. 33, Jan. 2022, Art. no. 100396.

[126] P. K. Sharma, D. Vohra, and S. Rathore, “Security and privacy in V2X communications: How can collaborative learning improve cybersecurity?” IEEE Netw., vol. 36, no. 3, pp. 32–39, May 2022.

[127] https://www.futura-sciences.com/tech/definitions/informatique-cloud-computing-11573/

[128] https://www.heavy.ai/technical-glossary/fog-computing

[129] https://iotindustriel.com/glossaire-iiot/fog-computing/

[130] https://www.techno-science.net/glossaire-definition/Eclipse-logiciel.html

[131] https://shardeum.org/blog/remix-ide/#What_is_the_Remix_IDE_Layout

[132] https://web3developer.io/introduction-to-web3j/

[133]https://www.geeksforgeeks.org/how-to-use-metamask-to-deploy-a-smart-contract-in-solidity-blockchain/

[134] https://archive.trufflesuite.com/docs/ganache/