

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

**Ministère de l'Enseignement Supérieur et de la Recherche
Scientifique**

Université Mouloud MAMMERI Tizi-Ouzou

Faculté Génie électrique et Informatique



MEMOIRE

Présenté pour l'obtention du **diplôme de MASTER**

En : Informatique

Spécialité : Réseaux Mobilité et Systèmes embarqués

Par :

Mr. AMIROU Zakaria Rahim

Mlle. MAHNI Djouher

MONITORING SYSTEM D'UN DATACENTER

Soutenu publiquement, le 16 / 07 /2019, devant le jury composé de :

Mr. Daoui .M : Président du jury.

Mme . Belkadi .M : Examinatrice.

Mme . Hadaoui.R : Promotrice

Mr. Ait Mameur Omar : Co promoteur .

REMERCIEMENTS

On remercie **ALLAH**, le tout puissant, qui nous a donné la force, la volonté et surtout le courage pour accomplir ce modeste mémoire.

Au terme de ce travail, on tient à remercier particulièrement Madame **Hadaoui**, notre encadreur, enseignante à l'université **Mouloud Mammeri de Tizi-Ouzou** pour son encadrement, Sa disponibilité, ses critiques et ses remarques pertinentes. Elle nous a conseillé et guidé du début du projet à sa fin.

On exprime notre profonde reconnaissance et nos sincères remerciements également à Mr. **Ait Mameur Omar** , notre encadreur à **MOBILIS** , de nous avoir aidés et pour son soutien permanent , sa patience et sa sympathie .

On voudrait aussi adresser nos sincères remerciements à **tous les enseignants** qui ont assuré notre formation durant notre parcours universitaire, pour l'ensemble des connaissances qui ont a consenti à leurs égards.

Et finalement on tient à remercier chaleureusement et respectivement tous ceux qui ont contribués de près ou de loin à la réalisation de ce modeste travail .

DÉDICACES

.....A tous ceux qui nous ont quitté

.....A nos parents

.....A nos familles

.....A nos amis

.....Et à tous ceux qui nous sont chers

En particulier à **Nelya**

T ABLE DES MATIERES

SOMMAIRE

INTRODUCTION GENERALE	1
<i>I.1. QU'EST-CE QUE L'INTERNET DES OBJETS ?.....</i>	<i>5</i>
<i>I.2. HISTOIRE DE L'INTERNET DES OBJETS.....</i>	<i>7</i>
<i>I.3. ARCHITECTURE DE L'INTERNET DES OBJETS.....</i>	<i>10</i>
<i>I.4. Les composants d'internet des objets.....</i>	<i>11</i>
<i>I.5. Les normes et les standards de l'iot.....</i>	<i>13</i>
<i>I.6. protocoles et communication dans l'iot.....</i>	<i>16</i>
<i>I.6.1. Les protocoles.....</i>	<i>16</i>
<i>I.6.2. La communication.....</i>	<i>19</i>
<i>I.7. Domaines d'application de l'iot.....</i>	<i>20</i>
<i>I.8. Les problèmes rencontrés dans l'iot.....</i>	<i>22</i>
<i>I.9. la sécurité dans l'iot.....</i>	<i>23</i>
CONCLUSION.....	25
<i>II.1. DEFINITION.....</i>	<i>27</i>
<i>II.2. LES COMPOSANTS D'un data center.....</i>	<i>29</i>
<i>II.3. Infrastructure adéquate pour un data center</i>	<i>29</i>
<i>II.4. les différents tiers de centres de données.....</i>	<i>29</i>
<i>II.5. ARCHITECTURE et design d'un datacenter.....</i>	<i>30</i>
<i>II.6. La sécurité et la sûreté d'un data center</i>	<i>31</i>
<i>II.6.1. la sécurité.....</i>	<i>32</i>
<i>II.6.2. la sûreté.....</i>	<i>32</i>

<i>conclusion</i>	33
<i>III.10.Le cloud computing et le datacenter</i>	34
<i>III.11.La relation entre l'IOT et le cloud computing</i>	34
<i>III.1.Définition</i>	36
<i>III.2.Les cinq caractéristiques essentielles du Cloud computing</i>	37
<i>III.3.modèles de services du cloud computing</i>	37
III.3.1.L'IaaS (Infrastructure as a Service).....	38
III.3.2.Le PaaS (Platform as a Service).....	39
III.3.3.Le SaaS (Software as a service).....	39
<i>III.4.modèles de déploiement d'un cloud</i>	40
<i>III.5.Les caractéristiques communes des clouds</i>	41
<i>III.6.Cloud computing et sécurité</i>	41
<i>III.7.les composants sécurité d'un système cloud computing</i>	41
<i>III.8.Les avantages du cloud computing</i>	42
<i>III.9.Les obstacles et les désavantages du cloud computing</i>	42
<i>III.10.Le cloud computing et le datacenter</i>	43
<i>III.11.La relation entre l'IOT et le cloud computing</i>	43
<i>conclusion</i>	45
<i>IV.1.INTELLIGENCE ARTIFICIELLE</i>	48
IV.1.1.Définition.....	48
IV.1.2.histoire.....	48
iv.1.3.DOMAINES D'APPLICATION DE L'IA.....	48
<i>iv.2.MACHINE LEARNING</i>	50
iv.2.1.Définition.....	50
iv.2.2.Les différents types de machine learning.....	50
iv.2.3.APPLICATIONS DE L'APPRENTISSAGE AUTOMATIQUE.....	54
<i>iv.3.LE DEEP LEARNING</i>	54
iv.3.1.Définition.....	54
iv.3.2.fONCTIONNEMENT DU DEEP LEARNING.....	54
iv.3.3.Domaines d'application de deep learning.....	55
iv.4.La différence entre le machine learning traditionnel et le deep learning.....	56
<i>Conclusion</i>	57
<i>V.1.QU'Est-ce que la reconnaissance faciale</i>	60
<i>V.2.histoire de la reconnaissance faciale</i>	60

V.3.Avantages.....	61
V.4.inconvenients.....	61
V.5. etapes de la reconnaissance faciale.....	62
V.6.Les principales difficultés de la reconnaissance faciale.....	64
Conclusion.....	65
I.1.Présentation de l'entreprise.....	68
I.2.présentation du centre de tizi-ouzou.....	68
I.3.sa situation geographique.....	69
I.4.son importance et sa classification.....	69
Problematique.....	70
ii.1.LA CARTE RASPBERRY.....	74
II.1.1.PRESENTATION DE LA CARTE RASPBERRY.....	74
ii.1.2.les modeles raspberry pi.....	74
II.1.3.Raspberry pi b+.....	76
ii.2.LA RASPBERRY CAMERA MODULE.....	77
II.2.1.Présentation.....	77
ii.2.2.CARACTERISTIQUES.....	78
ii.2.3.Details de la camera.....	78
ii.3.CONVERTISSEUR ANALOGIQUE ADC ADS1115.....	79
ii.3.1.presentation.....	79
II.3.2.utilisation.....	80
ii.3.3.spécifications techniques.....	80
ii.4.LES CAPTEURS UTILISES.....	81
II.4.1.Le detecteur de gaz et de fume : MQ-2.....	81
II.4.1.1.presentation.....	81
ii.4.1.2.specificationS.....	81
ii.4.1.3.CABLAGE.....	82
ii.4.2.DETECTEUR DE LA QUALITE DE L'AIR MQ-135.....	82
II.4.2.1.PRESENTATION.....	82
II.4.2.2.Specifications.....	83
II.4.2.3.cABLAGE.....	83
II.4.3.capteur d'humidité et de température DHT-11.....	84
II.4.3.1.Presentation.....	84
II.4.3.2.sPECIFICATIONS.....	84
II.4.3.3.Cablage.....	85
II.5.PUBNUB.....	85
II.6.EON.....	86

II.7.OPENCV.....	86
II.7.1.pRESENTATION.....	86
II.7.2.Applications OpenCV.....	87
II.7.3.Fonctionnalité OpenCV.....	88
II.8.FRITZING.....	88
II.9.GOOGLE DOC.....	89
II.10.APPLICATION WEB.....	89
II.10.1.Flask python.....	89
II.10.2.google drive.....	90
II.10.3.Sqlite.....	90
iii.1.partie embarquée :.....	93
iii.2.partie logicielle.....	93
CONCLUSION GENERALE.....	99
ANNEXE	103

T ABLE DES Figures

Figure 1 : Figure expliquant le concept de l'IoT	6
Figure 2 : Collision entre Moore et Metcalfe	8
Figure 3 : M2M VS IOT	9
Figure 4 : La lampe DAL	10
Figure 5 : Lapin Nabaztag	10
Figure 6 : Architecture de l'IoT	11
Figure 7 : Composants de l'IoT	13
Figure 8 : Standards de l'IoT	15
Figure 9 : Normes pour l'IoT	16
Figure 10 : Les protocoles dans l'IoT	19
Figure 11 : Domaines d'applications de l'IoT	22
Figure 12 : Fonctionnement d'un Datacenter	28
Figure 13 : Les différents tiers du Datacenter	30
Figure 14 : les différents contrôles dans un datacenter	32
Figure 15 : Image qui représente le Cloud	36
Figure 16 : Modèles de services du Cloud Computing	38
Figure 17 : Domaines d'application de l'IA	49
Figure 18 : Image qui représente l'apprentissage supervisé	51
Figure 19: Image qui représente l'apprentissage non supervisé	52
Figure 20 : Image qui représente l'apprentissage par renforcement	53
Figure 21 : Image qui résume le machine learning	53
Figure 22 : Exemple de Deep Learning	55
Figure 23 : Différence entre le Machine Learning traditionnel et le Deep Learning	56
Figure 24 : IA, Machine Learning, Deep Learning	57
Figure 25 : Histoire de la reconnaissance faciale	60
Figure 26 : Schéma qui résume le fonctionnement de la reconnaissance faciale	64
Figure 27 : Algérie Télécom	68
Figure 28 : Les directions régionales de Mobilis	69
Figure 29 : Logo Mobilis	70
Figure 30 : Modèle A+	75
Figure 31 : Modèle A	75
Figure 32 : Types du modèle B	76
Figure 33 : Le modèle zéro	76

Figure 34 : Raspberry Pi B+	77
Figure 35 : GPIOs de la Raspberry Pi	77
Figure 36 : Camera rev 1.3	78
Figure 37 : caméra rev 1.3	79
Figure 38 : ADC ADS1015	80
Figure 39 : Câblage de MQ-2	83
Figure 40 : MQ-135	83
Figure 41 : Câblage MQ-135	84
Figure 42 : Câblage DH-11	86
Figure 43 : Logo PubNub	87
Figure 44 : Logo EON	87
Figure 45 : Logo OpenCV	88
Figure 46 : Logo FRITZING	89
Figure 47 : Logo Google Doc	90
Figure 48 : Logo Flask	90
Figure 49: Logo Google Drive	91
Figure 50 : Logo SQLite	91
Figure 51 : Schéma qui représente le câblage de notre système embarqué	93
Figure 52 : Interface PubNub	94
Figure 53:l'interface principale de l'application web	95
Figure 54: la table SQLite.	95
Figure 55 : diagramme de cas d'utilisation.	96
Figure 56: Transformation des valeurs de la température et de l'humidité en un graphe	97
Figure 57 : Reconnaissance faciale avec caméra rev 1.3	97
Figure 58 : Enregistrement du nom de la personne reconnue	98
Figure 59: Représentation fonctionnelle d'un capteur	103
Figure 60 : éléments constitutifs d'un capteur	104
Figure 61: classification des capteurs	105

Liste Des Tables

Tableau 1: numéro des broches	94
Tableau 2 : Les taches des cas d'utilisation	97
Tableau 3 : Liste des capteurs les plus fréquents.	106

INTRODUCTION GÉNÉRALE

D'après l'étude menée par le cabinet **Synergy Research**, les investissements mondiaux dans les datacenters ont augmenté de 17% pour atteindre le record de 150 milliards de dollars investis en 2018. Ce Boom est principalement dû à l'accroissement exponentielle du trafic des données et la demande de puissance de calcul. Sans le savoir nous sommes tous dépendant des datacenters, qui jouent alors un rôle crucial dans la sphère de notre société numérique. Smartphones, ordinateurs, objets, frigo, pacemaker... On constate aujourd'hui, que tout est connecté à un data center.

Ils sont devenus les organes vitaux de notre société numérique, un cœur qui ne doit jamais s'arrêter de battre, car sans eux c'est toute l'économie numérique qui s'arrêterait de tourner.

Ce qui nous mène à poser quelques questions pertinentes :

- Comment fonctionne un datacenter ?
- Comment sécuriser un datacenter ?
- Comment monitorer et contrôler un data center ?

Un datacenter est un bâtiment, ou partie de bâtiment, intégrant des équipements informatiques. Le matériel installé, des serveurs, des baies de stockage, des systèmes de réseaux et de télécommunications permettent d'échanger, de traiter et de stocker des données. En effet, un datacenter héberge des données stratégiques indispensables au fonctionnement des entreprises à qui elles appartiennent. Les protéger, ainsi que les équipements qui les centralisent, contre toute intrusion ou événement interne/externe est donc une nécessité absolue.

Notre travail consiste à concevoir et implémenter des solutions sécurisées dans un datacenter, au sein de l'entreprise MOBILIS.

Pour cela, nous proposons quelques solutions de sécurité. Parmi elles :

- L'autorisation d'accès au datacenter avec la reconnaissance faciale.
- Le contrôle de la température et de l'humidité.
- Le contrôle de gaz et de fumé.
- Le contrôle de la qualité de l'air.



Avant de passer à l'implémentation de notre application, il est évident de définir quelques concepts de base, pour cela nous avons opté pour le plan suivant :

1. Partie 1 : Etat de l'art :

Dans cette partie nous abordons les concepts théoriques dont on aura besoin tout au long de ce travail, cette partie est structurée comme suit :

- **Chapitre 1** : intitulé : « INTERNET DES OBJETS ».
- **Chapitre 2** : intitulé « DATA CENTER ».
- **Chapitre 3** : intitulé : « CLOUD COMPUTING ».
- **Chapitre 4** : intitulé : « L'IA, LE MACHINE LEARNING ET LE DEEP LEARNING ».
- **Chapitre 5** : intitulé « LA RECONNAISSANCE FACIALE ».

2. Partie 2 : Contribution :

Dans cette partie nous décrivons notre projet, l'organisme d'accueil et nous proposons ainsi une solution à la problématique. Cette partie est structurée comme suit :

- **Chapitre 1** : intitulé : « PRESENTATION DE L'ORGANISME D'ACCUEIL ».
- **Chapitre 2** : intitulé : « Outils et Technologies utilisés ».
- **Chapitre 3** : intitulé : « REALISATION ».

PARTIE 1. ETAT DE L'ART

I NTERNET DES OBJETS

I

SOMMAIRE

I.1. QU'EST-CE QUE L'INTERNET DES OBJETS ?	5
I.2. HISTOIRE DE L'INTERNET DES OBJETS	7
I.3. ARCHITECTURE DE L'INTERNET DES OBJETS	10
I.4. LES COMPOSANTS D'INTERNET DES OBJETS	11
I.5. LES NORMES ET LES STANDARDS DE L'IOT	13
I.6. PROTOCOLES ET COMMUNICATION DANS L'IOT	16
I.6.1. LES PROTOCOLES	16
I.6.2. LA COMMUNICATION	19
I.7. DOMAINES D'APPLICATION DE L'IOT	20
I.8. LES PROBLÈMES RENCONTRÉS DANS L'IOT	22
I.9. LA SÉCURITÉ DANS L'IOT	24
CONCLUSION	25

Depuis la fin des années 1980, Internet a évolué de manière spectaculaire. La dernière étape est l'utilisation de ce réseau mondial pour la communication avec des objets ou entre objets, évolution nommée Internet des Objets (IoT pour Internet of Things).

L'évolution de l'IoT est rapide : depuis 2014, le nombre d'objets connectés est supérieur au nombre d'humains connectés et il est prévu que 50 milliards d'objets seront connectés en 2020.

L'Internet des Objets (l'IoT) repose sur l'idée que tous les objets peuvent être connectés à Internet et sont donc capable d'émettre de l'information et éventuellement de recevoir des commandes, il n'existe pas de définition standard, unifiée et partagée de l'internet des objets. Certaines techniques de l'IoT, tandis que l'autres se concentrent plutôt sur les usages et les fonctionnalités. Il faut réussir à exprimer ce que représente l'internet des objets tout en restant accessible aux non experts, et suffisamment concert pour représenter son impact dans la vie quotidienne. L'IoT désigne une information qui se fond dans notre quotidien pour nous simplifier la vie.

Dans ce premier chapitre, nous abordons en détails le monde d'Internet des objets, son architecture ainsi que ses différents composants. Enfin nous traitons la notion de la sécurité et ses enjeux dans le monde d'Internet des objets.

I.1. QU'EST-CE QUE L'INTERNET DES OBJETS ?

Définition 1 :

Une des inventions les plus significatives du monde moderne, l'internet, est une réalité qui est disponible pour l'utilisation publique depuis 25 ans. Un de ses aspects les plus importants est ses nombreuses perspectives d'utilisations (Coetzee & Ekstee, 2011). En effet, de nouvelles applications et technologies dépendantes de l'internet se développent tous les jours. A ses débuts, internet était principalement un protocole utilisé pour transmettre des messages d'un point à l'autre au moyen d'ordinateurs. Aujourd'hui, on est passé d'un internet connectant les gens et les ordinateurs vers un internet connectant les « choses » et les « objets ». Ce phénomène est appelé « Internet des objets », pour lequel nous utiliserons dans la suite de ce mémoire son abréviation anglaise, la plus répandue : IoT (Internet of Things).

Définition 2 :

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

Définition 3 :

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

Définition 4 :

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

Définition 5 :

Une autre définition plus simple est la présente : internet des objets = des objets + de l'intelligence (un "minuscule" ordinateur pouvant exécuter un "logiciel"= un microcontrôleur) + une connexion réseau vers internet par exemple :



Figure 1 : Figure expliquant le concept de l'IoT

Définition 6 :

L'Internet des objets a deux composants : Internet et les objets.

Internet : désigne la grande catégorie d'applications et de protocoles au sein du réseau.

Objet : désigne toute chose capable de se connecter à Internet, y compris les appareils intelligents, les capteurs et toute autre entité capable de communiquer avec d'autres objets connectés. Cela inclut les personnes qui utilisent les appareils et utilisent les applications.

I.2.HISTOIRE DE L'INTERNET DES OBJETS

Deux lois ont marqué l'histoire de l'informatique : la loi de Moore, relative à la puissance des ordinateurs et la loi de Metcalfe, relative à la valeur des réseaux. Alors quel est le rapport entre ces deux lois et notre thème qui est l'internet des objets ?

Moore a prédit dès 1965 que le nombre de transistors pouvant être intégrés à un circuit imprimé doublerait tous les 18 à 24 mois. Force est de constater que d'un point de vue empirique ce qui était initialement qu'une conjecture s'est transformée en loi. Dès lors, la conception de calculateurs toujours plus puissants permet d'y intégrer une intelligence toujours plus poussée. Un corollaire est que les PC et systèmes de contrôles deviennent de plus en plus intelligents mais aussi de plus en plus petits.

Sur un autre registre, Metcalfe a quant à lui énoncé que la valeur d'un réseau est directement liée au nombre d'objets interconnectés, donc au nombre de liaisons potentielles (à savoir le carré du nombre d'utilisateurs divisé par deux). Et nous pouvons aisément confirmer de manière empirique cette proposition au regard de la récente explosion de l'internet mondiale !

La convergence des lois facteur d'innovation Il n'y a encore pas si longtemps, qui aurait pu prédire que l'une et l'autre loi allait interagir et créer une accélération incroyable d'innovation au niveau global et être à l'origine de l'IoT ? Quoi qu'il en soit Moore et Metcalfe avaient toutes les deux raisons.

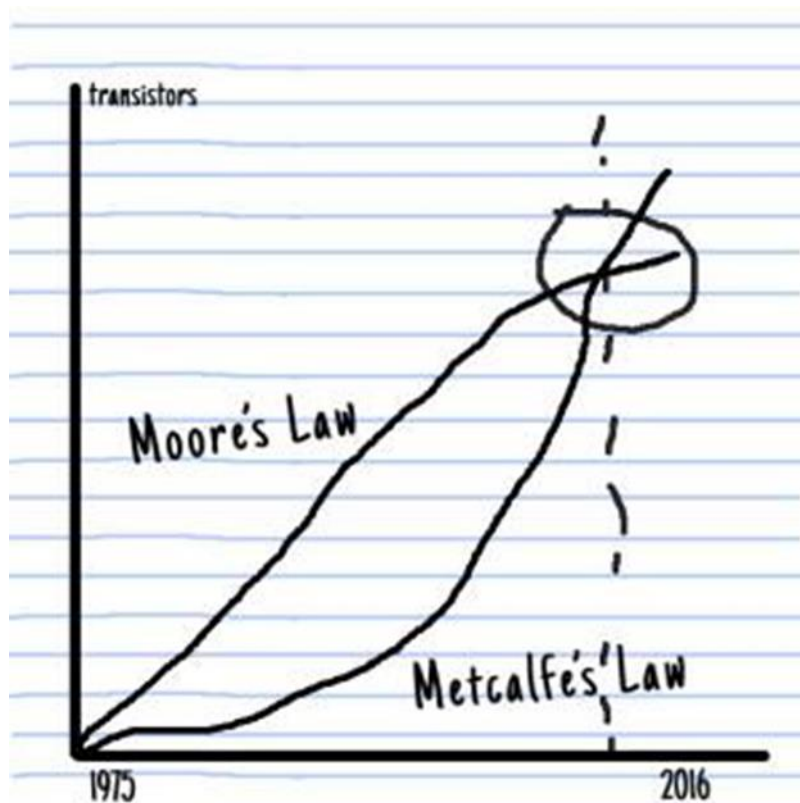


Figure 2 : Collision entre Moore et Metcalfe

Nous vivons actuellement dans un monde où les technologies évoluent si rapidement que même les industries les plus frileuses se font littéralement happer par cette dynamique. Soit par le fait d'ajouter de nouvelles capacités dont elles rêvaient depuis des années, soit par le fait de rendre plus accessible des capacités existantes, en les rendant plus simples, plus petites, moins énergivores et surtout moins coûteuses que ce qu'elles étaient traditionnellement.

On a parlé sur les lois qui ont prédit l'évolution exponentielle de l'informatique et de l'internet jusqu'à ce qu'on arrive à l'IoT, alors parlons un peu sur l'histoire de l'internet des objets en particulier.

Le terme Internet of Things, ou IoT, a été inventé et utilisé pour la première fois en 1999 lors d'une présentation faite par le pionnier britannique des technologies, Kevin Ashton, sur la gestion de la chaîne d'approvisionnement au MIT

Les premières formes de communication avec un IoT impliquaient souvent une machine du même type, appelée communication machine à machine ou communication M2M. Par exemple, les périphériques utilisés dans les systèmes de gestion de la chaîne

logistique pour suivre les stocks où toutes les communications étaient établies localement au sein du même système.

Aujourd'hui, l'Internet des objets s'étend au-delà de la machine à la machine et des systèmes fermés entre machines du même type. Désormais, les appareils et capteurs de tous types peuvent communiquer les uns avec les autres de partout dans le monde. Ceux-ci peuvent inclure des applications industrielles à plus grande échelle, telles que des systèmes SCADA (système de contrôle et d'acquisition de données), des produits commerciaux tels que des smartphones ou des réseaux locaux de capteurs pour collecter et transférer des données telles que des systèmes de surveillance du trafic ...

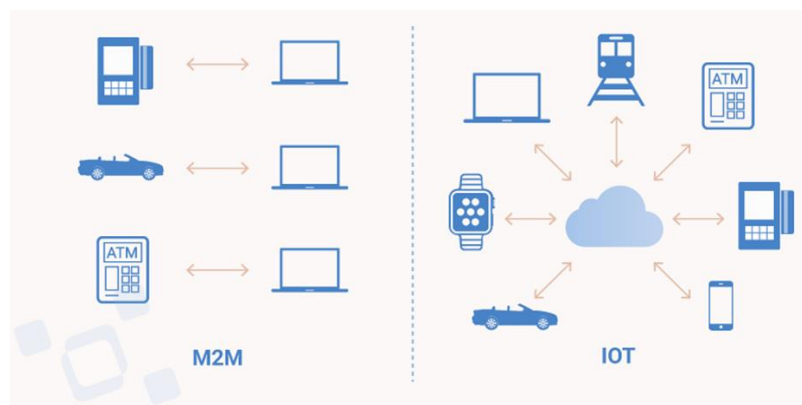


Figure 3 : M2M VS IOT

Le premier objet connecté est commercialisé en 2003 par la firme Violet. C'est la lampe DAL, équipée de 9 leds qui s'allument en fonction des événements. Deux ans plus tard, en 2005, Violet lance le célèbre lapin Nabaztag. Racheté par Mindscape puis Aldebaran Robotics en 2013, il disparaîtra en 2015.



Figure 4 : La lampe DAL



Figure 5 : Lapin Nabaztag

I.3.ARCHITECTURE DE L'INTERNET DES OBJETS I.3

L'architecture d'un système IoT est composée de plusieurs niveaux qui communiquent entre eux pour relier le monde tangible des objets au monde virtuel des réseaux et du cloud. Tous les projets n'adoptent pas une architecture formellement identique, néanmoins il est possible de schématiser le parcours de la donnée.

Un capteur commence par relever une mesure qui peut être, par exemple, la température, la pression, le taux de CO₂, la géolocalisation...

Le rôle de la passerelle est de traduire les protocoles pour établir une communication entre les objets et le réseau (public ou privé, souvent le cloud). Parfois, une intelligence embarquée dans la passerelle permet le traitement et le stockage de la donnée, ainsi que des fonctions de pilotage de l'objet. Pour les protocoles courte portée (Zigbee, Z-Wave, WiFi, BLE...), la passerelle est locale et se connecte souvent à la box du fournisseur d'accès à internet. Pour les protocoles longue portée (Sigfox, LoRa, LTEM, NBIoT, 3G/4G, ...), la passerelle se trouve sur le réseau de l'opérateur télécom.

La plateforme collecte les données, surveille, et contrôle les objets connectés. La plateforme logicielle IoT embarque une intelligence qui offre de multiples possibilités. Les mesures peuvent être stockées dans l'objectif de créer une historisation permettant la prédiction. La plateforme IoT communique avec différentes plateformes de services qui délivrent un service digital à l'utilisateur final restituant les données collectées des objets, permettant des actions de pilotage et apportant une couche d'intelligence (alertes, conseils, ...).

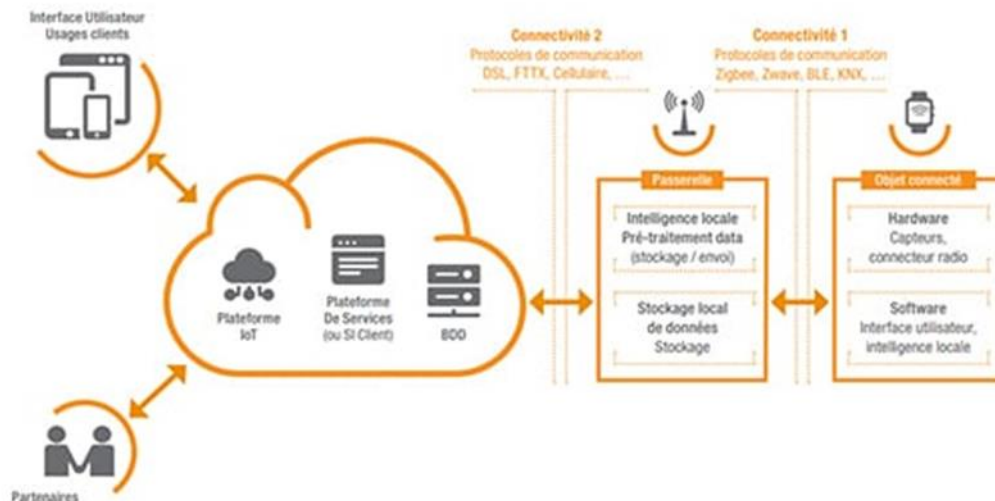


Figure 6 : Architecture de l'IoT

L'utilisateur bénéficie, dans la plupart des cas, d'une interface dédiée sur son terminal mobile, type smartphone. Il peut alors piloter son objet, accéder à l'historique des mesures relevées, et utiliser les différentes fonctionnalités prévues par la solution IoT. De part cette interface, l'entreprise peut communiquer avec l'utilisateur de façon directe et personnalisée.

Il faut noter que la stratégie de sécurité doit être intégrée entièrement dans l'architecture pour éviter les failles matérielles et logicielles à tous les niveaux du système.

L'IoT crée une rupture permettant de faire coopérer de nombreux acteurs en mutualisant l'information et en encourageant les initiatives collaboratives. C'est dans cette perspective qu'une architecture IoT doit être considérée

I.4.LES COMPOSANTS D'INTERNET DES OBJETS

Les deux composants principaux de l'IdO sont : hardware et software. Ces composants communiquent en utilisant une grande variété de protocoles.

Hardware : fait référence aux périphériques physiques utilisés pour collecter les données des objets. Par exemple, des capteurs, des actionneurs ou présentent les données collectées, telles que les interfaces homme-machine. Quelques exemples de capteurs matériels sont les capteurs de température, les capteurs de proximité, les capteurs de pression et d'humidité. Le matériel

comprend également les périphériques standard. Tout appareil connecté, y compris les périphériques réseau standard, tels que les routeurs et les commutateurs. Les périphériques utilisés dans la couche d'application ou les applications dorsales, tels que les périphériques utilisés dans le traitement des données, le trafic intelligent, les appareils médicaux personnels, sont également inclus dans la section matérielle. Les appareils IoT sont capables de convertir de manière analogique-numérique, de collecter et de générer des données, une connexion à distance, ce qui signifie la possibilité d'être contrôlée sur Internet, une surveillance en temps réel des systèmes de surveillance en ligne, la sécurité des appareils pour la sécurité des données.

Software : Le software (logiciel) IoT est un programme qui permet le stockage de données, le traitement de données, le transfert de données, l'analyse de données et la connexion des composants matériels de l'IoT aux services principaux. Le logiciel IoT aide à fournir les protocoles suivants : collecte de données, intégration de données, analyse en temps réel, optimisation et protocoles de communication. Lors de la collecte de données, le logiciel gère la détection, les mesures, le filtrage des données et la sécurité des données à l'aide de certains protocoles permettant de connecter les périphériques physiques à des réseaux en temps réel. Le logiciel permet de connecter les périphériques qui collectent les données aux applications de l'utilisateur final. Pour transférer la tâche de la couche d'application aux périphériques. Cela peut donc fonctionner dans les deux sens. Le logiciel d'intégration de périphérique prend en charge l'intégration de tous les périphériques du système pour créer la structure du système IoT. Et pour vous aider à gérer les divers applications, protocoles et limitations de chaque périphérique afin de permettre la communication. Les logiciels fournissent également des résultats en temps réel dans certains secteurs, comme le nucléaire, par exemple. L'analyse en temps réel est essentielle. Ces applications prennent des données ou des entrées provenant de divers appareils et les convertissent en actions utiles basées sur l'analyse des informations en fonction des différents algorithmes pour chaque application spécifique. Et en fonction de divers paramètres et exigences de conception. Les logiciels d'optimisation sont également courants dans les secteurs industriel et manufacturier. Au fur et à mesure que le logiciel optimise la sortie en fonction des données collectées à partir des périphériques du système IoT. Le logiciel IoT inclut également les différents protocoles de communication utilisés pour compléter le système IoT. Certains exemples de logiciels IoT utilisés dans les systèmes d'exploitation sont Microsoft Windows, Apple Mac OS.

Un autre exemple pour le logiciel de gestion de données, Microsoft SQL Server et Oracle. Parmi les exemples de logiciels IoT utilisés dans les systèmes immotiques, on peut citer l'IHM, l'interface homme-machine, le SCADA, le contrôle de supervision et l'acquisition de données. D'autres exemples sont les logiciels utilisateur quotidiens tels que Bluetooth, GPS, applications mobiles ou même Internet.



Figure 7 : Composants de l'IoT

I.5.LES NORMES ET LES STANDARDS DE L'IOT

La normalisation est une coopération volontaire entre l'industrie, les clients, les autorités publiques et d'autres parties intéressées en vue de l'élaboration d'une spécification technique reposant sur un consensus afin de convenir de méthodes d'essai. Et d'une exigence de performances en matière de sécurité, de santé et d'environnement. Différentes organisations de normalisation régionales et internationales travaillent à la production des normes de l'IdO.

IEEE, Institution de génie électrique et électronique, en est un exemple ; CEI, Commission électrotechnique internationale ; ISO, Organisation internationale de normalisation ; ISA, Société internationale d'automatisation ; IETF, le groupe de travail sur l'ingénierie Internet. Pour les normes au sein de l'IoT, il en existe des spécifiques pour chaque domaine. Par exemple, la gestion de l'énergie, les technologies de l'information, la communication et les réseaux, la santé et l'éducation.

Chacun des secteurs ci-dessus a une norme distincte concernant l'IdO en fonction de l'application Internet des objets de sa région. Un des exemples de normes IoT est celui utilisé pour IEEE. En IEEE, il existe environ 350 normes IEEE. Il a plus de 140 normes existantes liées à l'Internet des objets. Prenons donc un exemple de l'une des normes IEEE relatives à l'IoT.

Le document standard donne un aperçu complet des règles et des spécifications pour cette norme spécifique. Les fonctions principales du document standard IEEE-SA P2413 sont la définition d'un cadre architectural IoT. Décrire les différents domaines IoT, définir les obstacles et fournir des modèles de référence. Cette norme couvre également d'autres spécifications et détails, mais il s'agit généralement d'une vue d'ensemble de haut niveau. Vous pouvez en savoir plus sur cette norme sur le site IEEE.

Un autre exemple est celui des normes ISO, Organisation internationale de normalisation. Les normes ISO liées à l'IoT sont généralement développées par un groupe de normalisation international qui fonctionne comme une collaboration très productive entre l'ISO et la CEI. ISO / IEC JTC 1 / SWG est un exemple de ce nom.

Le nom signifie ISO, Organisation internationale de normalisation ; CEI, Commission électrotechnique internationale ; JTC 1, comité technique mixte ; et SWG, groupe de travail spécial. Le comité travaille donc à l'élaboration des normes IoT. ISO / IEC 30141 en est un exemple.

L'Architecture de référence de l'Internet of Things ou IoT RA. La norme couvre les éléments suivants : définition du domaine IoT, des caractéristiques du système IoT, du modèle de référence IoT et de l'identification de l'entité IoT et de l'interopérabilité. La standardisation au sein de l'IdO présente certains défis. Certains des défis, sans toutefois s'y limiter, consiste à proposer une définition commune de l'IdO facilitant l'identification de ses composants.

L'autre est une portée et une coordination mondiales. C'est une étape très importante car elle permet de gagner du temps et d'économiser des efforts au sein des différentes organisations qui travaillent à l'élaboration des normes.

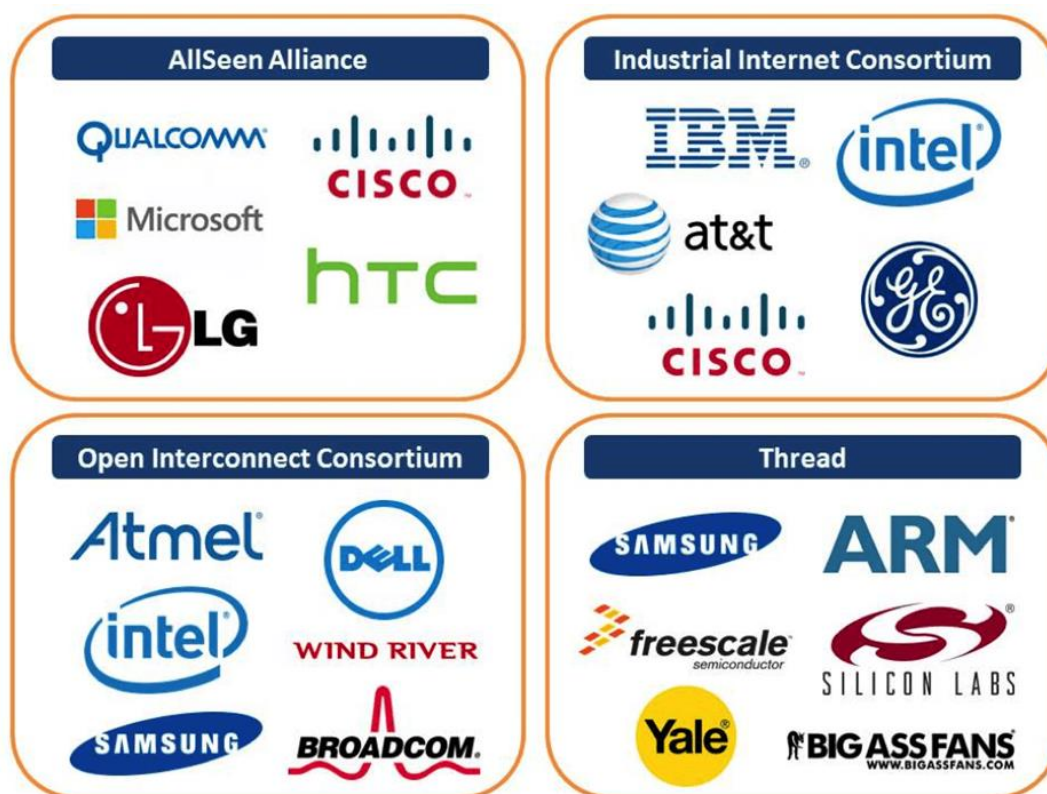


Figure 8 : Standards de l'IoT

Normes pour l'IoT – Paysage

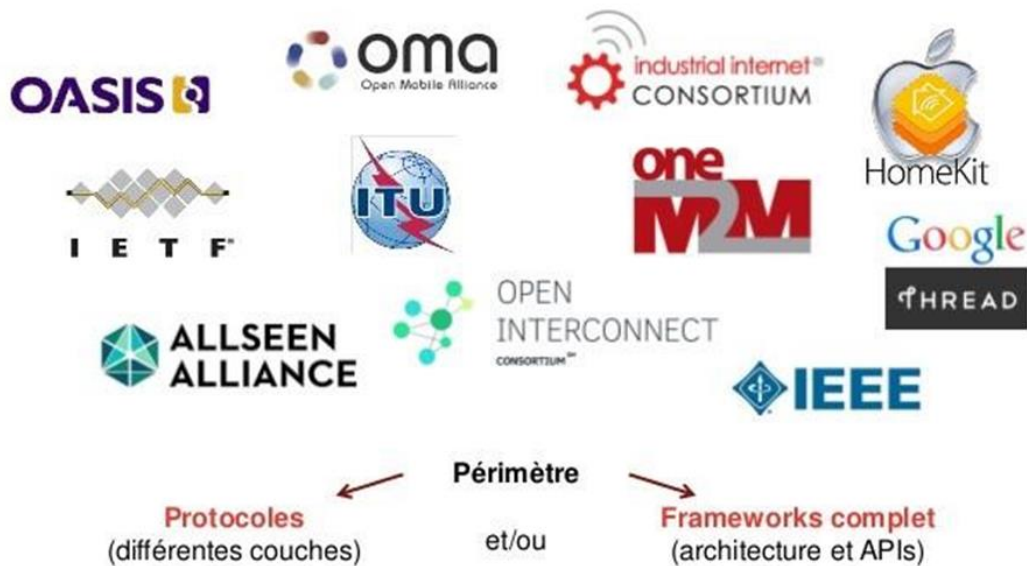


Figure 9 : Normes pour l'IoT

I.6.PROTOCOLES ET COMMUNICATION DANS L'IOT

I.6.1.LES PROTOCOLES

Une suite de protocoles est un groupe de protocoles interdépendants qui permettent d'assurer l'interopérabilité entre les périphériques réseau. L'une des suites de protocoles réseau les plus courantes est la suite Internet. Protocole de transmission, protocole Internet, ou TCP / IP. Le modèle TCP / IP à quatre couches comprend les couches suivantes :

- **La couche application** : qui initie la communication sur le réseau.
- **La couche de transport** : transporte des données.
- **La couche Internet** : responsable de l'adressage et du routage.
- **La couche d'accès au réseau** : déplace les données sur le réseau.

En général, au fil du temps, la plupart des protocoles n'ont pas beaucoup changé. Cependant, le protocole Internet a dû être modifié, principalement en raison du manque d'espace d'adresse. Bien que nous considérions généralement le protocole Internet et IPv6 comme un élément essentiel pour l'IoT, tous les appareils n'ont pas besoin d'une adresse IP. Le fait est que ces petits appareils ne conviennent pas aux communications nécessitant un contrôle et une hiérarchisation personnalisés. Les appareils IoT qui assurent le contrôle industriel et la domotique reposent sur une topologie maillée généralement synonyme de faible MTU et de faible taux de transmission. Les appareils sont petits, dotés d'un microprocesseur de 8, 16 ou 32 bits et d'une mémoire flash limitée. De plus, ils ne communiquent pas toujours, car ils peuvent être en mode veille lorsqu'ils ne communiquent pas activement. TCP / IP joue un rôle essentiel dans le transfert de données sur les réseaux, mais nous avons également besoin d'autres protocoles pour transférer les données au sein des réseaux de capteurs. Les développeurs ont rapidement estimé que les appareils IoT de faible puissance, dotés de capacités de traitement limitées, devaient pouvoir communiquer sur l'IoT. Pour les objets sur l'IoT, plusieurs protocoles existent. Les exemples incluent 802.15.4. C'est le protocole qui définit la couche physique et le contrôle d'accès au support pour les réseaux personnels sans fil à faible débit. Il constitue la base de ZigBee. Les développeurs peuvent utiliser 802.15.4 avec 6LoWPAN et les protocoles Internet standard. 6LoWPAN est une abréviation pour IPv6 et réseau personnel sans fil de faible puissance. Cela permet même aux plus petits appareils à traitement limité de transmettre des informations sans fil à l'aide d'un protocole Internet. ZigBee appartient et est contrôlé par un consortium et repose sur la norme IEEE 802.15.4. Les développeurs utilisent ZigBee dans des réseaux personnels ou domestiques, ou dans un maillage sans fil pour des réseaux à longue portée. Bluetooth est un protocole couramment utilisé pour échanger des données entre des périphériques proches, tels qu'un casque compatible Bluetooth et un téléphone. Et la communication en champ proche est une norme lorsqu'on échange des articles à proximité, généralement à quelques centimètres près ; par exemple, un téléphone portable et un lecteur.

MQTT : (Depuis le livre : MQTT Essentials - A Lightweight IoT Protocol) MQTT signifie MQ Telemetry Transport. Il s'agit d'un protocole de messagerie de publication / abonnement extrêmement simple et léger, conçu pour les périphériques limités et les réseaux à faible bande passante, à latence élevée ou peu fiables. Les principes de conception consistent à réduire au minimum les besoins en bande passante réseau et en ressources de l'appareil, tout

en veillant à assurer la fiabilité et une certaine assurance de livraison. Ces principes ont également pour effet de faire du protocole idéal le monde émergent des appareils connectés «M2M » ou « Internet des objets », ainsi que pour les applications mobiles où la bande passante et la puissance de la batterie sont primordiales.

MQTT a été inventé par le Dr Andy Stanford-Clark d'IBM et Arlen Nipper d'Arcom (maintenant Eurotech) en 1999.

HTTP : (Depuis le livre : HTTP Précis et concis) : HyperText Transfer Protocol est le protocole qui se cache derrière la toile mondiale, http est utilisé pour chaque transaction web, il se cache derrière chaque demande d'un document ou graphique web, et est le protocole le plus utilisé. HTTPS (avec un S pour sécuriser) est la variante du HTTP sécurisée par l'usage de certains protocoles de sécurité.

Il s'agit d'un protocole client-serveur (requête/réponse) : Un client demande l'accès à une ressource (ça peut être aussi l'exécution d'un programme) en indiquant entre autres un URL. Le serveur répond en renvoyant la ressource demandée (ou les résultats de l'exécution du programme). Parmi les clients les plus connus : les navigateurs Web et les robots d'indexation de pages Web. Parmi les serveurs les plus connus : Apache (C), Tomcat (Java) IIS (C# & ASP.Net) et serveurs écrits avec Node.js (JavaScript).

Websockets : (Depuis le livre : Lightweight Client-Server Communications) WebSocket est un protocole qui permet d'ouvrir un canal de communication interactif (bi-directionnel) permanent entre un navigateur (côté client) et un serveur, afin de résoudre certains problèmes posés par le caractère unidirectionnel et déconnecté du protocole HTTP. Avec cette API vous pouvez envoyer des messages à un serveur et recevoir ses réponses de manière événementielle sans avoir à aller consulter le serveur pour obtenir une réponse. La spécification permettant d'utiliser les WebSockets est développée par le W3C, tandis que le protocole de communication est standardisé par l'IETF.

COAP : (Depuis le livre : Encapsulation of Real-time IoT CoAP Traffic) : CoAP (Constrained Application Protocol) est un protocole de transfert Web optimisé pour les périphériques et réseaux contraints utilisés dans les réseaux de capteurs sans fil pour former l'Internet des objets., Le protocole COAP est principalement destiné aux équipements et aux

machines qui n'ont parfois qu'un microcontrôleur 8 bits pour tout processeur, très peu de mémoire et qui, en prime, sont connectés par des liens radio lents et peu fiables (les « LowPAN » ou les LPWAN), allant parfois à seulement quelques dizaines de kb/s, Le protocole d'application contraint (COAP) a joué un rôle déterminant dans le déploiement de capteurs et d'actionneurs sans fil dans les réseaux à faible débit et faible consommation de l'Internet des objets.

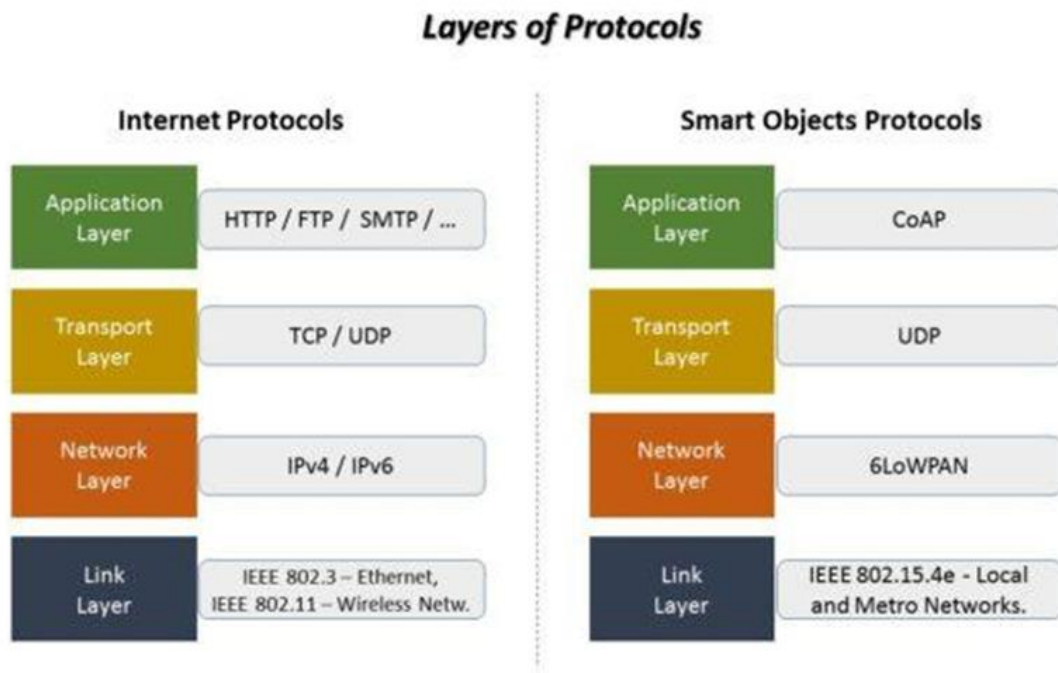


Figure 10 : Les protocoles dans l'IoT

I.6.2.LA COMMUNICATION

3G/4G : Respectivement, la troisième et quatrième génération du réseau de téléphonie mobile qui introduit du très haut débit pouvant aller, en théorie, jusqu'à 150 Mbit/s.

Wifi : Le terme « Wi-Fi » (contraction de l'anglais « Wireless Fidelity ») désigne un protocole de communication sans fil dont le standard technique a été normalisé par le groupe IEEE 802.11. Fonctionnant avec des ondes radio dans une bande de fréquence de 2,4 ou 5 GHz, il permet de relier des équipements informatiques et de téléphonie mobile dans un réseau sans fil haut débit. Les objets connectés ont des exigences de connectivité variées en termes de

portée, de débit de données, d'efficacité énergétique et de coût des périphériques, Le Wi-Fi est souvent un choix évident, car la couverture Wi-Fi dans le bâtiment est presque omniprésente.

Ethernet : Ethernet est la technologie traditionnelle pour la connexion de réseaux locaux câblés, permettant aux périphériques de communiquer entre eux via un protocole - un ensemble de règles ou un langage réseau commun. En tant que protocole de couche de liaison de données dans la pile TCP / IP, Ethernet décrit comment les périphériques réseau peuvent formater et transmettre des paquets de données afin que les autres périphériques situés sur le même segment de réseau local ou de campus puissent les reconnaître, les recevoir et les traiter. Un câble Ethernet est le câblage physique encapsulé sur lequel les données transitent. Dans un système IOT, Ethernet peut être utilisé pour connecter des périphériques IOT fixes.

Zigbee : (Depuis le livre : ZigBee Network Protocols and Applications) : ZigBee est un standard pour la communication de données entre des périphériques basse consommation normalement associés aux tâches de lecture de capteurs dans divers scénarios, notamment la domotique, les maisons intelligentes et les appareils industriels, et même la surveillance de la santé humaine.

Bluetooth : Le Bluetooth est une technologie sans fil qui permet à des appareils électroniques d'échanger des données à courte distance. Appliquée à la téléphonie mobile, le Bluetooth a eu des répercussions pratiques importantes. Du fait de sa disponibilité généralisée dans les smartphones, le Bluetooth a joué un rôle central dans la révolution de l'IoT - en particulier pour la communication sans fil à courte portée dans les appareils dans lesquels la vie de la batterie est essentielle.

I.7.DOMAINES D'APPLICATION DE L'IOT

Les objets connectés sont appliqués dans les différents domaines tel que :

La domotique : Cette technologie permet de gérer à distance de nombreuses fonctionnalités de la maison : ouverture, fermeture des volets, mise en marche du système de chauffage, d'appareils électriques, de la lumière, etc. La domotique. Cette technologie permet de gérer à distance de nombreuses fonctionnalités de la maison : ouverture, fermeture des volets, mise en marche du système de chauffage, d'appareils électriques, de la lumière, etc.

L'énergie : grâce à l'internet des objets, les appareils du réseau énergétique peuvent partager des informations en temps réel pour distribuer et mieux gérer l'énergie.

Les usines intelligentes : la technologie de l'IoT permet aujourd'hui aux usines de maximiser l'efficacité opérationnelle, d'optimiser la production, et d'augmenter la sécurité des travailleurs.

La voiture autonome : La voiture autonome est une voiture qui peut se déplacer sans l'intervention d'un conducteur. Les premiers à l'avoir lancée sont Google, en 2010. De nombreux freins empêchent encore sa démocratisation, tel le coût, la lenteur actuelle des véhicules et les problèmes liés à la sécurité.

La santé : grâce aux accessoires cliniques comme les tablettes ou aux équipements chirurgicaux sophistiqués, l'internet des objets est en train de transformer la santé.

Transports intelligents : l'IoT peut sauver des vies, réduire le trafic et minimiser l'impact du véhicule sur l'environnement, non seulement en connectant des voitures qui se conduisent toutes seules, mais aussi en rendant le transport intelligent ainsi que les systèmes de logistique. Les vélos connectés vous diront également quand ils ont été volés où ils sont avec une carte pour que vous puissiez aller les chercher.

Agriculture : vos plantes installées avec une puce électronique dans la terre pourront communiquer et poster sur twitter par exemple. La plante pourra se plaindre si elle n'a pas assez d'eau et enverra des informations toute la journée et tous les jours de la semaine. Par exemple, la plante au bureau communiquera avec vous quand vous êtes absent. Elle vous donnera la température au bureau, la condition de la lumière (par exemple si vous avez oublié d'éteindre la lumière). Vous n'aurez plus d'excuse si votre plante meurt, car elle vous aura prévenu de sa condition.

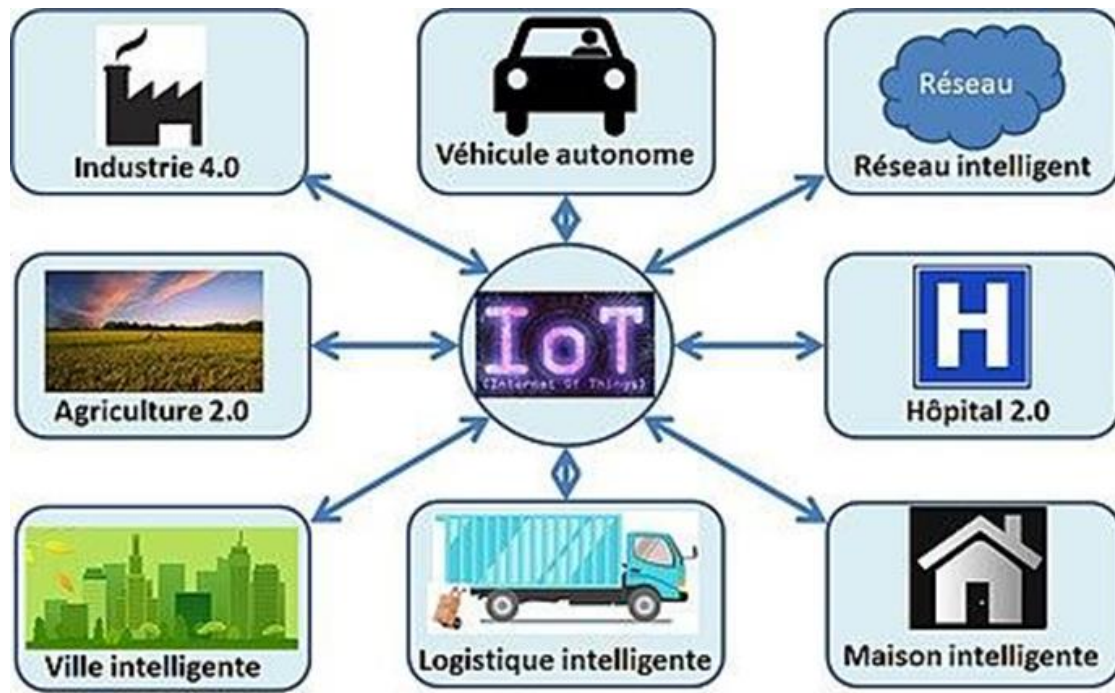


Figure 11 : Domaines d'applications de l'IoT

I.8.LES PROBLÈMES RENCONTRÉS DANS L'IOT

a) La consommation électrique

Les objets connectés consomment beaucoup d'énergie. Comment pourra-t-on faire face aux besoins énergétiques des 20 milliards d'objets connectés en circulation d'ici à 2050 ? Si des solutions existent, telle que l'utilisation de piles rechargeables à l'énergie solaire ou l'adoption de technologies utilisant moins d'énergie que d'autres, cela reste un enjeu majeur.

b) La gestion des capteurs

Aujourd'hui, nous ne possédons que peu d'objets connectés. Mais lorsque chacun d'entre nous possèdera 10 ou 20 objets connectés, la gestion des capteurs nécessaires à leur fonctionnement deviendra problématique. Il sera indispensable de développer un système de supervision aussi automatisé que possible et de repenser l'architecture et l'infrastructure de l'IoT.

c) L'uniformisation des standards techniques

L'IoT est un marché très fragmenté qui ne désigne pas une seule technologie mais des dizaines de standards fonctionnant différemment. En termes d'expérience utilisateur, c'est très complexe. Or, il ne peut y avoir d'adoption de masse d'une technologie trop complexe à maîtriser. Il faut donc effacer cette complexité, soit par l'uniformisation des pratiques, soit en équipant les box internet de plusieurs technologies prenant en charge tous les objets connectés de la maison.

d) La gestion des données

À l'avenir, l'IoT va créer un océan de data gérable uniquement grâce à l'IA. À titre d'exemple, sur un avion de ligne, il y a 20 000 capteurs et une simple turbine d'A380 fournit 10G de données à chaque vol ! Comment les gérer et donner du sens à ces milliards de données ? Il faudra donc compter sur l'intelligence artificielle et notamment le machine Learning pour y parvenir.

e) La sécurité et la vie privée

❖ Vulnérabilité :

Les technologies modernes de sécurité (chiffrement, authentification, échange de clé, signature, etc.) sont inadéquates aux environnements de l'IdO ceci rend les objets vulnérables aux attaques informatiques cela, représente un danger pour les biens et les personnes.

❖ Surveillance de masse :

La simple présence d'un individu dans l'environnement entraîne implicitement la collecte d'informations. De manière générale, il n'est plus possible de savoir où, quand, pourquoi et par qui les données sont collectées. En effet, même en l'absence d'intentions malveillantes de la part des propriétaires d'objets, l'utilisation massive des réseaux sans fil facilite les écoutes clandestines. Enfin, l'identification unique des objets, rend possible la construction des profils possible. Ces profils uniques peuvent ensuite être utilisés pour suivre les individus en temps réel et à très grande échelle, en se basant sur la détection des objets et sur les différents capteurs placés dans l'environnement.

I.9.LA SÉCURITÉ DANS L'IOT

Authentification : L'authentification peut être définie comme le processus de prouver une identité revendiquée. Lorsqu'il existe une seule preuve de l'identité (mot de passe) on parle d'authentification simple lorsque cette dernière nécessite plusieurs facteurs on parle alors d'authentification forte.

Confidentialité : La confidentialité est le fait de s'assurer que l'information n'est accessible qu'à ceux dont l'accès est autorisé, permet de garder la communication des données privée entre un émetteur et un destinataire. Le chiffrement des données est la seule solution pour assurer la confidentialité des données

Ceux dont l'accès est autorisé, permet de garder la communication des données privée entre un émetteur et un destinataire. Le chiffrement des données est la seule solution pour assurer la confidentialité des données.

Intégrité : L'intégrité permet de garantir que les données sont bien celles que l'on croit être, donc permet de garantir la protection des données contre les modifications et les altérations non autorisées.

Disponibilité : La disponibilité est un service réseau qui permet de donner une assurance aux entités autorisées d'accéder aux ressources réseaux. L'objectif est d'éviter les attaques de type Denial of Service.

Non-répudiation : Non-répudiation permet de garantir qu'une transaction ne peut être niée et qu'un message a bien été envoyé par un émetteur et reçu par un destinataire aucun des deux ne pourra nier l'envoi ou la réception du message.

CONCLUSION

L'Internet des objets n'est donc pas une technologie récente mais elle est aujourd'hui associée à d'autres technologies en plein développement telles que l'intelligence artificielle, la big data ou la VR. C'est cette synergie qui révolutionnera nos usages. Ainsi, dans un avenir proche nous vivrons dans un monde où nous pourrons non seulement interagir avec tous nos appareils à distance et en temps réel, mais nos appareils pourront également interagir entre eux, s'échanger des données et les analyser pour nous proposer toujours plus de services et de fonctionnalités parfaitement adaptés à nos besoins.

On ne peut améliorer que ce qu'on peut mesurer. Or, l'IoT peut tout mesurer à distance, de manière instantanée et automatisée. C'est en cela que c'est une technologie révolutionnaire.

DATACENTER

II

SOMMAIRE

II.1.DEFINITION.....	27
II.2.LES COMPOSANTS D’UN DATA CENTER	29
II.3.INFRASTRUCTURE ADEQUATE POUR UN DATA CENTER	29
II.4.LES DIFFERENTS TIERS DE CENTRES DE DONNEES	30
II.5.ARCHITECTURE ET DESIGN D’UN DATA CENTER	31
II.6.LA SECURITE ET LA SURETE D’UN DATA CENTER	31
II.6.1.LA SECURITE	32
II.6.2.LA SURETE	32
CONCLUSION.....	33

Cette année, l'humanité aura créé 1 200 milliards Go de données, soit l'équivalent de 75 milliards d'iPod de 16 Go. Un volume considérable de données stockées au sein de datacenters qui ont, certes, gagné en puissance de calcul, mais qui doivent surtout être d'une fiabilité à toute épreuve.

Sans le savoir, nous sommes tous dépendants des datacenters. Quand un internaute envoie une requête à un moteur de recherche, quand vous faites un achat en ligne ou que vous dialoguez avec vos contacts Facebook, ce sont des datacenters qui opèrent derrière et relayent les informations. Il faut en effet savoir que les informations échangées chaque heure sur Internet permettraient de remplir 7 millions de DVD.

Dans ce chapitre nous abordons le concept du Data center, où on va le voir de différents angles tels ses composants, son infrastructure, son architecture, la sécurité dans les data centers ...

II.1.DEFINITION

Définition 1 :

Un data center est un réseau de ressources de calcul et de stockage permettant la mise à disposition d'applications logicielles et de données partagées. Dans le monde de l'informatique d'entreprise, le datacenter prend en charge les applications de l'entreprise. Cela va de la simple messagerie et du partage de fichiers, aux systèmes de gestion de la relation client (CRM) et de planification des ressources de l'entreprise (ERP), en passant par le Big Data, les communications et les services de collaboration.

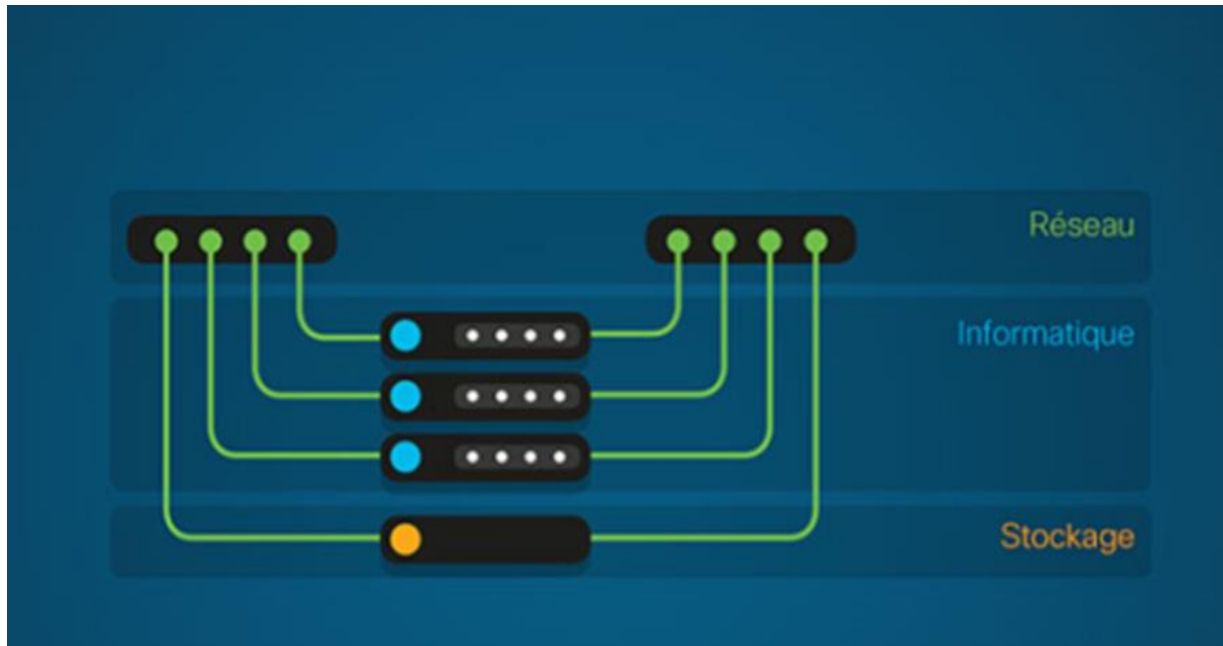


Figure 12 : Fonctionnement d'un Datacenter

Définition 2 :

Un data center (centre de données en français) est un endroit physique où sont rassemblées de nombreuses machines (bien souvent des serveurs) contenant des données informatiques.

Définition 3 :

Un data center ou centre de données, est une infrastructure composée d'un réseau d'ordinateurs et d'espaces de stockage. Cette infrastructure peut être utilisée par les entreprises pour organiser, traiter, stocker et entreposer de grandes quantités de données. En règle générale, une entreprise repose fortement sur les applications, les services et les données contenues dans un centre de données. Il s'agit donc d'une part essentielle de l'entreprise au quotidien.

II.2.LES COMPOSANTS D'UN DATA CENTER

Un centre de données basique regroupe des :

- Des serveurs
- Des sous-systèmes de stockage
- Des commutateurs de réseau
- Des routeurs
- Des firewalls
- Des câbles et des racks physiques permettant d'organiser et d'interconnecter tout cet équipement informatique.

II.3.INFRASRUTRUCTURE ADEQUATE POUR UN DATA CENTER

Pour garantir un bon fonctionnement du data center on doit lui assurer une infrastructure adéquate, comme suit :

- Un système distribution d'énergie.
- Un commutateur électrique.
- Des réserves d'énergie.
- Des générateurs dédiés au backup.
- Un système de ventilation et de refroidissement.
- Une puissante connexion Internet.

NB : une telle infrastructure nécessite un espace physique suffisamment grand et sécurisé.

II.4.LES DIFFERENTS TIERS DE CENTRES DE DONNEES

Les data centers ne sont pas déterminés par leur taille physique. Les petites entreprises peuvent utiliser une petite salle où sont juxtaposés plusieurs serveurs et espaces de stockage interconnectés. Les entreprises informatiques de grande envergure, comme Facebook, Amazon ou Google, peuvent quant à elles remplir un immense entrepôt. Il est également possible de mettre en place des installations mobiles, telles que des containers, aussi appelés « **data centers in a box** », pouvant être déplacés et déployés au besoin.

Il est en revanche possible de définir un datacenter selon :

- Son niveau de fiabilité.
- Son niveau de résilience.

On classe ainsi les centres de données par tiers. En 2005, l'ANSI et la TIA ont publié le standard ANSI/TIA-942, Télécommunications Infrastructure Standard for Data Centers. Ce standard définit quatre tiers de designs de Data center, (voire la figure suivante).



Figure 13 : Les différents tiers du Datacenter

II.5.ARCHITECTURE ET DESIGN D'UN DATACENTER

Théoriquement, n'importe quel espace suffisamment vaste peut servir de datacenter. Cependant, le design et l'implémentation d'un Datacenter nécessite de prendre plusieurs précautions. Par-delà les problèmes basiques du coût et des taxes, les sites sont sélectionnés sur de nombreux critères, comme :

- La localisation géographique.
- La stabilité météorologique.
- L'accès aux routes et aux aéroports.
- La disponibilité énergétique.
- Les télécommunications ou encore l'environnement politique.

Une fois qu'un site est sécurisé, l'architecture d'un Datacenter peut être conçue en portant attention à l'infrastructure électrique et mécanique, et aussi à la composition et à disposition de l'équipement informatique. Tous ces critères dépendent du tiers de Datacenter visé.

II.6.LA SECURITE ET LA SURETE D'UN DATA CENTER

Les administrateurs de datacenters font face à d'importants challenges. Ils doivent sécuriser les nouveaux environnements de datacenter sans en compromettre les performances ni le fonctionnement.



Figure 14 : les différents contrôles dans un datacenter

II.6.1.LA SECURITE

Pour protéger le data center des événements non intentionnels, fortuits, accidentels, pouvant affecter sa continuité de service ou son bon fonctionnement il faut mettre en place un système de :

- Détection d'incendie et d'extinction d'incendie
- Détection de températures excessives : urbanisation, confinement, refroidissement.
- Détection de fuites et dégâts des eaux.
- Détection de Fuite de gaz.
- Etc...

II.6.2.LA SÛRETE

Pour protéger le datacenter des actes et des événements intentionnels et malveillants, il faut mettre en œuvre des solutions telles :

- Gestion et contrôle des accès au datacenter
- Protection périmétrique, passive ou active
- Télésurveillance et vidéo
- Mesures pour assurer la cybersécurité des équipements
- Etc...

CONCLUSION

La surveillance des centres de données est souvent axée sur les ordinateurs.

Surveiller les performances du système, suivre les charges de travail virtuelles et réagir aux inévitables avertissements et alertes qui posent problème aux serveurs, au réseau ou au stockage de l'architecture. Cependant, les centres de données modernes ont besoin d'une stratégie de surveillance plus globale prenant en compte des facteurs environnementaux tels que la température et l'humidité - non seulement dans la pièce - mais à un niveau granulaire dans les racks et les serveurs.

CLOUD COMPUTING

III

SOMMAIRE

III.1.DEFINITION	36
III.2.LES CINQ CARACTERISTIQUE ESSENTIELLES DU CLOUD COMPUTING	38
III.3.MODELES DE SERVICES DU CLOUD COMPUTING	39
III.3.1.IaaS	39
III.3.2.PaaS.....	40
III.3.3.SaaS.....	40
III.4.MODELES DE DEPLOIEMENT D'UN CLOUD	41
III.5.LES CARACTERISTIQUES COMMUNES DES CLOUDS	42
III.6.LES COMPOSANTS SECURITE D'UN SYSTEME CLOUD COMPUTING	42
III.7.LES OBSTACLES ET LES DESAVANTAGES DU CLOUD COMPUTING	43
III.8.LE CLOUD COMPUTING ET LE DATA CENTER	43
III.9. LA RELATION ENTRE L'IOT ET LE CLOUD COMPUTING.....	44
III.10.LE CLOUD COMPUTING ET LE DATACENTER	44
III.11.LA RELATION ENTRE L'IOT ET LE CLOUD COMPUTING.....	45
CONCLUSION.....	45

Longtemps avant que l'expression "Cloud computing" ne naisse, les architectes de réseaux (ceux qui conçoivent les réseaux intra et inter-entreprise) schématisent internet par un nuage dans leurs croquis. En anglais, on parlait alors de "the cloud", ce qui signifiait à peu de choses près l'internet que nous connaissons. Ce nuage évoquait alors une connexion vers une quantité indéfinie d'utilisateurs et non pas des services tel que nous l'entendons maintenant.

Le premier nuage était construit autour du réseau (abstraction TCP/IP). Le deuxième nuage était celui des documents (abstraction du World Wide Web). Le nuage actuel, Cloud computing, est une abstraction de l'infrastructure informatique qui masque la complexité des serveurs, des applications, des données et des plates-formes hétérogènes.

L'Internet actuel fournit un contenu sous les formes des vidéos, e-mails et les informations servis dans les pages web. Avec le Cloud computing, la prochaine génération d'internet va nous permettre d'acheter des services informatiques à partir d'un portail web. Nous serions en mesure de louer à partir d'une vitrine virtuelle la base nécessaire pour construire un centre des données virtuel, tels que le processeur, la mémoire et le stockage, et ajouter au-dessus le middleware nécessaire tels que les serveurs d'applications Web, bases de données et bus serveur d'entreprise, etc.

Dans ce chapitre nous allons voir de près ce qu'est le cloud computing, ses caractéristiques, ses modèles ainsi que ses services...

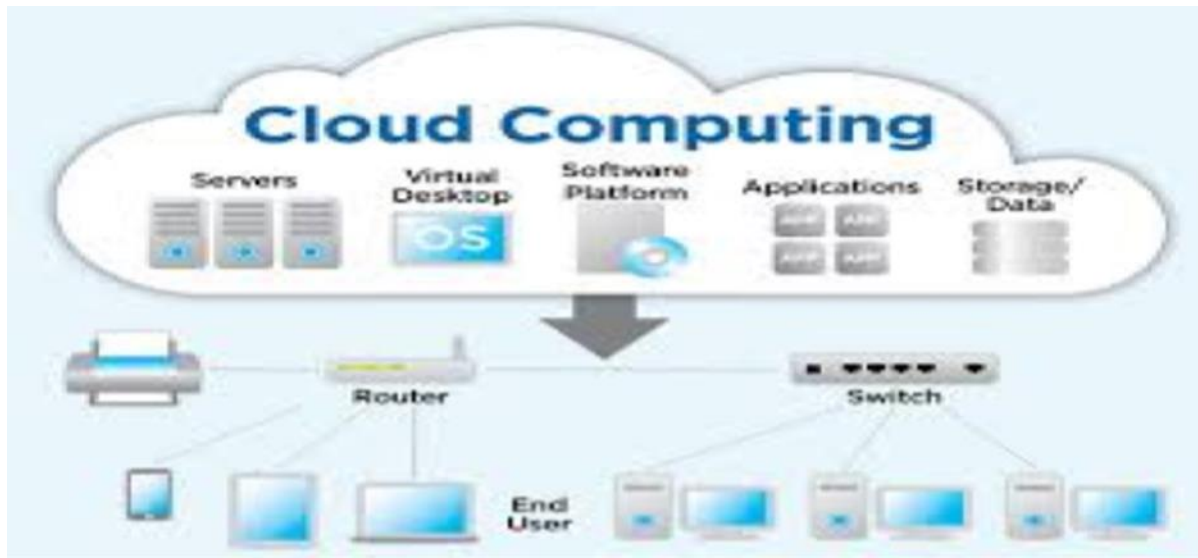


Figure 15 : Image qui représente le Cloud

III.1.DEFINITION

Définition 1 :

Le Cloud Computing est un concept qui consiste à accéder à des données et des services sur un serveur distant. Traditionnellement, une entreprise utilisait sa propre infrastructure pour héberger ses services. Elle achetait donc ses propres serveurs, et assurait le développement et la maintenance des systèmes nécessaires à son fonctionnement. Par opposition, le Cloud Computing se repose sur une architecture distante, Le fournisseur donc assure la continuité du service et de la maintenance. Les services de Cloud Computing sont accessibles via un navigateur web. Le terme Cloud Computing étant anglais, on retrouve comme synonymes les termes suivants : informatique virtuelle, informatique dans les Cloud et informatiques en Cloud ou encore informatique dématérialisée. L'emplacement des données dans le Cloud n'est pas connu des clients, ceux-ci ont simplement l'accès à la partie applicative, sans se soucier du reste.

Définition 2 :

Le Cloud Computing, ou « informatique dans les nuages », est un « nouveau » modèle informatique qui consiste à proposer des services informatiques sous forme de services à la demande, accessibles de n'importe où, n'importe quand et par n'importe qui.

Cette approche n'est pas tout à fait nouvelle (modèle ASP). La réelle nouveauté réside dans son approche systématique.

III.2.LES CINQ CARACTERISTIQUES ESSENTIELLES DU CLOUD COMPUTING

Le modèle Cloud Computing se différencie par les cinq caractéristiques essentielles suivantes :

➤ **Accès aux services par l'utilisateur à la demande :**

Ces centres de traitement sont généralement raccordés directement sur le backbone Internet pour bénéficier d'une excellente connectivité. Les grands fournisseurs répartissent les centres de traitement sur la planète pour fournir un accès aux systèmes en moins de 50 ms de n'importe quel endroit.

➤ **Réservoir de ressources (non localisées) :**

La plupart de ces centres comportent des dizaines de milliers de serveurs et de moyens de stockage pour permettre des montées en charge rapides. Il est souvent possible de choisir une zone géographique pour mettre les données "près" des utilisateurs.

➤ **Redimensionnement rapide (élasticité) :**

La mise en ligne d'une nouvelle instance d'un serveur est réalisée en quelques minutes, l'arrêt et le redémarrage en quelques secondes. Toutes ces opérations peuvent s'effectuer automatiquement par des scripts. Ces mécanismes de gestion permettent de bénéficier pleinement de la facturation à l'usage en adaptant la puissance de calcul au trafic instantané.

➤ **Facturation à l'usage :**

Il n'y a généralement pas de coût de mise en service (c'est l'utilisateur qui réalise les opérations). La facturation est calculée en fonction de la durée et de la quantité de ressources utilisées. Une unité de traitement stoppée n'est pas facturée.

III.3.MODELES DE SERVICES DU CLOUD COMPUTING

Trois modèles de services peuvent être offerts sur le Cloud : « **Software as a Service (SaaS)** », « **Platform as a Service (PaaS)** », « **Infrastructure as a Service (IaaS)** ».

Ces trois modèles de service doivent être déployés sur des Infrastructures qui possèdent les cinq caractéristiques essentielles citées plus haut pour être considérées comme du Cloud Computing.

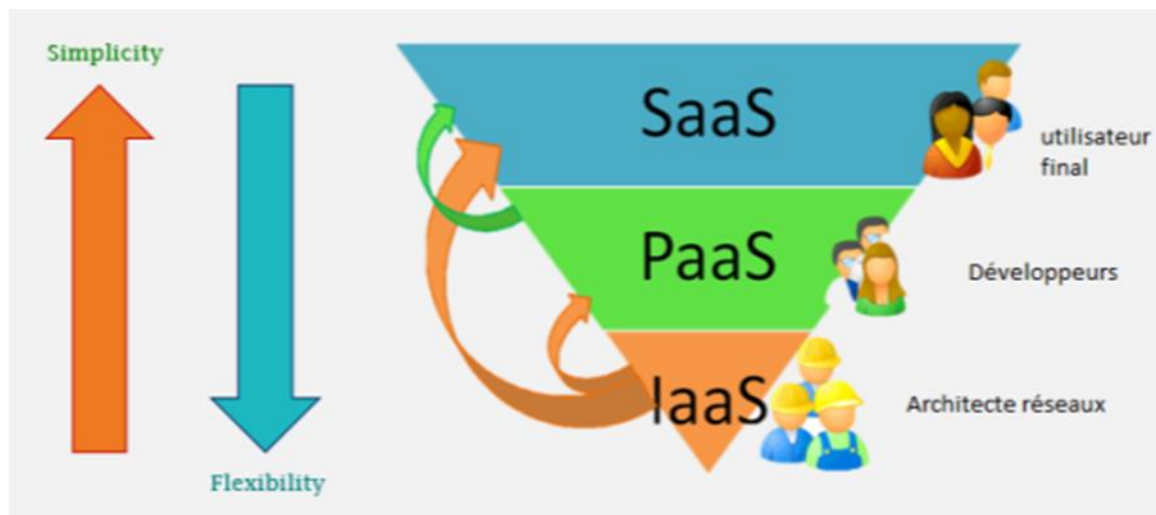


Figure 16 : Modèles de services du Cloud Computing

III.3.1.L'IAAS (INFRASTRUCTURE AS A SERVICE)

Ou infrastructure sous forme de service est une offre de cloud computing dans laquelle un fournisseur offre aux utilisateurs l'accès à des ressources informatiques comme des serveurs du stockage et de l'équipement de réseau. Les entreprises utilisent leurs propres plateformes et applications dans l'infrastructure du fournisseur.

Principales caractéristiques :

- Au lieu d'acheter le matériel, les utilisateurs paient pour l'IaaS à la demande.
- L'infrastructure est évolutive en fonction des besoins de traitement et de stockage.

- Les entreprises économisent les coûts d'achat et de maintenance de leur propre matériel.
- Comme les données sont dans le cloud, une défaillance ne peut pas entraîner l'indisponibilité.
- Permet la virtualisation des tâches d'administration, ce qui libère du temps pour d'autres activités à plus forte valeur ajoutée.

III.3.2.LE PAAS (PLATFORM AS A SERVICE)

Ou plateforme sous forme de service est une offre de cloud computing qui fournit aux utilisateurs un environnement cloud dans lequel ils peuvent développer, gérer et mettre à disposition des applications. Outre le stockage et les autres ressources informatiques, les utilisateurs peuvent utiliser une suite d'outils disponibles pour développer, personnaliser et tester leurs applications.

Principales caractéristiques :

- Le PaaS offre une plateforme avec des outils pour tester, développer et héberger les applications dans le même environnement.
- Permet aux entreprises de se concentrer sur le développement sans avoir à se soucier de l'infrastructure sous-jacente.
- Les fournisseurs gèrent la sécurité, les systèmes d'exploitation, les logiciels de serveur et les sauvegardes.
- Facilite le travail collaboratif même lorsque les équipes travaillent à distance.

III.3.3.LE SAAS (SOFTWARE AS A SERVICE)

Ou logiciel sous forme de service est une offre de cloud computing qui donne aux utilisateurs l'accès aux logiciels en cloud d'un fournisseur. Les utilisateurs n'installent pas les applications sur leur terminal. Elles résident sur un réseau cloud distant auquel ils accèdent par le web ou par une API. Avec les applications, les utilisateurs peuvent stocker et analyser des données et collaborer sur des projets.

Principales caractéristiques :

- Les logiciels et applications sont proposés aux utilisateurs par les fournisseurs de SaaS selon un modèle par abonnement.

- Les utilisateurs n'ont pas à gérer, installer ou mettre à niveau les logiciels ; ce sont les fournisseurs qui s'en chargent.
- Les données sont sécurisées dans le cloud ; une panne d'un équipement n'entraîne pas de perte de données.
- L'utilisation des ressources peut être dimensionnée en fonction des besoins de l'entreprise.
- Les applications sont accessibles depuis presque n'importe quel terminal connecté à Internet et depuis virtuellement n'importe où dans le monde.

III.4.MODELES DE DEPLOIEMENT D'UN CLOUD

Il existe quatre modèles de déploiement d'un cloud représentés comme suit :

➤ **Cloud privé :**

L'infrastructure Cloud est utilisée par une seule organisation. Elle peut être gérée par l'organisation ou par une tierce partie. L'infrastructure peut être placée dans les locaux de l'organisation ou à l'extérieur.

➤ **Cloud communautaire :**

L'infrastructure Cloud est partagée par plusieurs organisations pour les besoins d'une communauté qui souhaite mettre en commun des moyens (sécurité, conformité, etc..). Elle peut être gérée par les organisations ou par une tierce partie et peut être placée dans les locaux ou à l'extérieur.

➤ **Cloud public :**

L'infrastructure cloud est ouverte au public ou à de grands groupes industriels. Cette infrastructure est possédée par une organisation qui vend des services Cloud. C'est le cas le plus courant. C'est celui de la plate-forme Amazon Web Services déjà citée.

➤ **Cloud hybride :**

L'infrastructure Cloud est composée d'un ou plusieurs modèles ci-dessus qui restent des entités séparées. Ces infrastructures sont liées entre elles par la même technologie qui autorise la portabilité des applications et des données. C'est une excellente solution pour répartir ses moyens en fonction des avantages recherchés.

III.5.LES CARACTERISTIQUES COMMUNES DES CLOUDS

- Des infrastructures gigantesques.
- Une grande homogénéité des moyens.
- Virtualisation.
- Elasticité [Resilient computing].
- Coûts de logiciels très réduits.
- Distribution géographique.
- Orientation Service.
- Fonctions de sécurité avancées.

III.6.CLOUD COMPUTING ET SECURITE

Toutes les enquêtes montrent que la sécurité est la préoccupation majeure des organisations dans le processus d'adoption des technologies Cloud. Les questions sont nombreuses comme par exemple :

- Quelle confiance peut-on avoir dans le stockage des données à l'extérieur de l'entreprise ?
- Quels sont les risques associés à l'utilisation de services partagés ?
- Comment démontrer la conformité des systèmes à des normes d'exploitation ?

Les infrastructures Cloud sont de gigantesques systèmes complexes. Ils peuvent cependant être réduits à un petit nombre de primitives simples qui sont instanciées des

milliers de fois et à quelques fonctions communes. La sécurité du Cloud est donc un problème gouvernable moins complexe qu'il n'y paraît.

III.7.LES COMPOSANTS SECURITE D'UN SYSTEME CLOUD COMPUTING

Les différents composants qui participent à la sécurité d'un système de Cloud computing présentent les caractéristiques suivantes :

- Service de console de gestion (Provisioning).
- Service de stockage des données.
- Infrastructures de calcul.
- Services de support.
- Sécurité périmétrique du réseau Cloud.

III.8.LES AVANTAGES DU CLOUD COMPUTING

Le Cloud Computing offre de nombreux avantages que plusieurs travaux ont listés. Parmi ces avantages on trouve :

- Réduction des coûts d'infrastructure.
- Réduction des coûts de développement.
- Réduction des coûts des logiciels.
- Des ressources et services plus rapide à allouer et plus simple à utiliser.
- Accès aux ressources plus flexible.
- Meilleure utilisation, plus efficace, des ressources.
- Augmentation de la puissance de calcul.
- Grande capacité de stockage (quasi illimitée).
- Moins de problèmes d'entretien.

- Gestion des mises à jour plus simple et rapide.
- Pas de perte de données.
- Tout est considéré comme un service défini par un SLA.
- Infrastructure allouée et disponible juste à temps.
- Réduction du temps de mise sur le marché.

III.9.LES OBSTACLES ET LES DESAVANTAGES DU CLOUD COMPUTING

Le Cloud Computing n'a pas que des avantages, il possède quelques obstacles et désavantages, parmi ces obstacles il y a :

- Données Lock-in.
- Confidentialité des données.
- Chiffrement des données.
- Nécessité d'un accès réseau constant.
- Mauvais fonctionnement avec les connexions à basse vitesse.
- Faible niveau de la qualité de service dans le réseau.
- Risque d'engorgements lors des transferts de données.
- Problème d'interopérabilité.
- Problème de portabilité.
- Faible contrôlabilité.
- Manque de fonctionnalités d'audit.
- Des contrats de service SLAs non normalisés.

III.10.LE CLOUD COMPUTING ET LE DATACENTER

Le cloud computing fonctionne grâce aux data centers. Un data center héberge des systèmes informatiques et les composants associés. Il peut occuper une pièce, un ou plusieurs

étages, voire un bâtiment entier. La construction et l'entretien des data centers sont en général très coûteux. C'est pour cela que les grandes entreprises utilisent des data centers privés pour stocker leurs données et fournir des services aux utilisateurs. Les entreprises de plus petite taille qui n'ont pas le budget suffisant pour gérer leur propre data center privé peuvent réduire le coût total de possession (TCO) en louant des services de serveur et de stockage à un data center de plus grande envergure hébergé dans le cloud.

Le cloud computing est souvent fourni en tant que service par les datacenters. Les fournisseurs de services cloud utilisent les datacenters pour héberger leurs services et leurs ressources basés dans le cloud. Pour garantir la disponibilité des services et des ressources de données, ils veillent souvent à disposer d'espace dans plusieurs datacenters.

III.11.LA RELATION ENTRE L'IOT ET LE CLOUD COMPUTING

L'Internet des objets a développé le nouveau concept de réseau Internet. Ceci permet la communication entre plusieurs objets comprenant :

- Appareils intelligents
- Appareils mobiles
- Capteurs et autres.

L'architecture de l'Internet des objets assure une communication efficace entre tous les éléments de l'architecture. Les éléments pourraient être

- Objets.
- Portes.
- Infrastructure de réseau.
- Infrastructure cloud.

L'utilisation simultanée de l'IdO et du cloud computing présente de nombreux avantages :

Dans une infrastructure en nuage, vous pouvez déployer des applications pour traiter et analyser rapidement des données et prendre des décisions le plus rapidement possible. (dans +notre projet on a utilisé PUBNUB).

On estime que près de 4,4 milliards de Go de données vont être générés d'ici 2020. Il ne fait aucun doute que cela exercera une énorme pression sur ses infrastructures. Il est donc nécessaire de minimiser cette énorme pression et de trouver une solution pour transférer les données. Le cloud computing, quant à lui, offre des performances et une évolutivité adéquate pour stocker et exploiter un volume de données aussi important

L'IdO et l'informatique en nuage ont une relation complémentaire. Alors que l'IoT génère de grandes quantités de données, de nombreux fournisseurs de cloud permettent le transfert de données via Internet, ce qui facilite la navigation dans les données.

Le cloud computing permet de collaborer au développement IoT. En utilisant la plate-forme Cloud, les développeurs IoT peuvent stocker les données à distance et accéder facilement.

Le cloud computing aide à faire progresser l'analyse et la surveillance des périphériques IoT.

Les appareils IoT qui utilisent des API communes et une infrastructure dorsale peuvent recevoir instantanément d'importantes mises à jour de sécurité via le Cloud dès qu'une faille de sécurité se produit dans l'infrastructure. Cette fonctionnalité combinée de l'Internet des objets et du cloud est un paramètre essentiel pour la sécurité et la confidentialité des utilisateurs.

CONCLUSION

L'IdO et l'informatique en nuage peuvent facilement simplifier les tâches que nous effectuons quotidiennement, que ce soit au travail, à la maison ou en conduisant pour le travail ou la maison. Une relation solide existe entre les deux.

L'IA, LE MACHINE LEARNING ET LE DEEP LEARNING IV

SOMMAIRE

. SOMMAIRE

IV.1 INTELIGENCE ARTIFICIELLE	48
IV.1.1.DEFINITION	48
IV.1.2.HISTOIRE	48
IV.1.3. DOMAINE D'APPLICATION DE L'IA.....	48
IV.2MACHINE LEARNING	50
IV.2.1. DEFINITION	50
IV.2.2. LES DIFFERENTS TYPES DE MACHINE	
LEARNING.....	50
IV.2.3. APPLICATION DE L'APPRENTISSAGE AUTOMATIQUE	54
IV.3.DEEP LEARNING	54
IV.3.1.DEFINITION	54
IV.3.2.FONCTIONNEMENT DU DEEP LEARNING.....	54
IV.3.3. DOMAINE D'APPLICATION DU DEEP LEARNING	55
IV.4. DIFFERENCE ENTRE LE ML TRADITIONNEL ET LE DEEP	
LEARNING.....	56

CONCLUSION.....	57
-----------------	----

Si certaines promesses semblent directement sorties d'un film de science-fiction, l'IA est déjà bien présente dans la plupart des secteurs d'activité : santé, transports, énergie, finance, commerce, administration... Dans ce chapitre on parlera de l'intelligence artificielle, du machine learning et du deep learning. On abordera ces concepts plus en détails.

Dans ce chapitre, nous abordons l'intelligence artificielle, le machine learning ainsi que le deep learning. Nous expliquerons en détails chacun de ces concepts.

IV.1.INTELIGENCE ARTIFICIELLE

IV.1.1.DEFINITION

L'intelligence artificielle (IA, ou AI en anglais pour Artificial Intelligence) consiste à mettre en œuvre un certain nombre de techniques visant à permettre aux machines d'imiter une forme d'intelligence réelle. L'IA se retrouve implémentée dans un nombre grandissant de domaines d'application.

IV.1.2.HISTOIRE

La première notion d'intelligence artificielle a été abordée en 1950 par le mathématicien Alan Turing. Ce dernier crée alors un test visant à déterminer si une machine peut être considérée comme « consciente ». Le test de Turing est toujours utilisé par les scientifiques de nos jours, mais sa pertinence est régulièrement remise en cause.

Il faudra attendre 1956 pour obtenir une définition de l'IA proposée par Marvin Lee Minsky : « La construction de programmes informatiques qui s'adonnent à des tâches qui sont, pour l'instant, accomplies de façon plus satisfaisante par des êtres humains car elles demandent des processus mentaux de haut niveau tels que : l'apprentissage perceptuel, l'organisation de la mémoire et le raisonnement critique. »

De Google à Microsoft en passant par Apple, IBM ou Facebook, toutes les grandes entreprises dans le monde de l'informatique planchent aujourd'hui sur les problématiques de l'intelligence artificielle en tentant de l'appliquer à quelques domaines précis. Chacun a ainsi mis en place des réseaux de neurones artificiels constitués de serveurs et permettant de traiter de lourds calculs au sein de gigantesques bases de données.

IV.1.3.DOMAINES D'APPLICATION DE L'IA

- Reconnaissance vocale.
- Reconnaissance faciale.

- La voiture autonome.
- Le transport.
- La santé.
- Les banques.
- L'assistante personnelle.
- La défense.
- Etc...

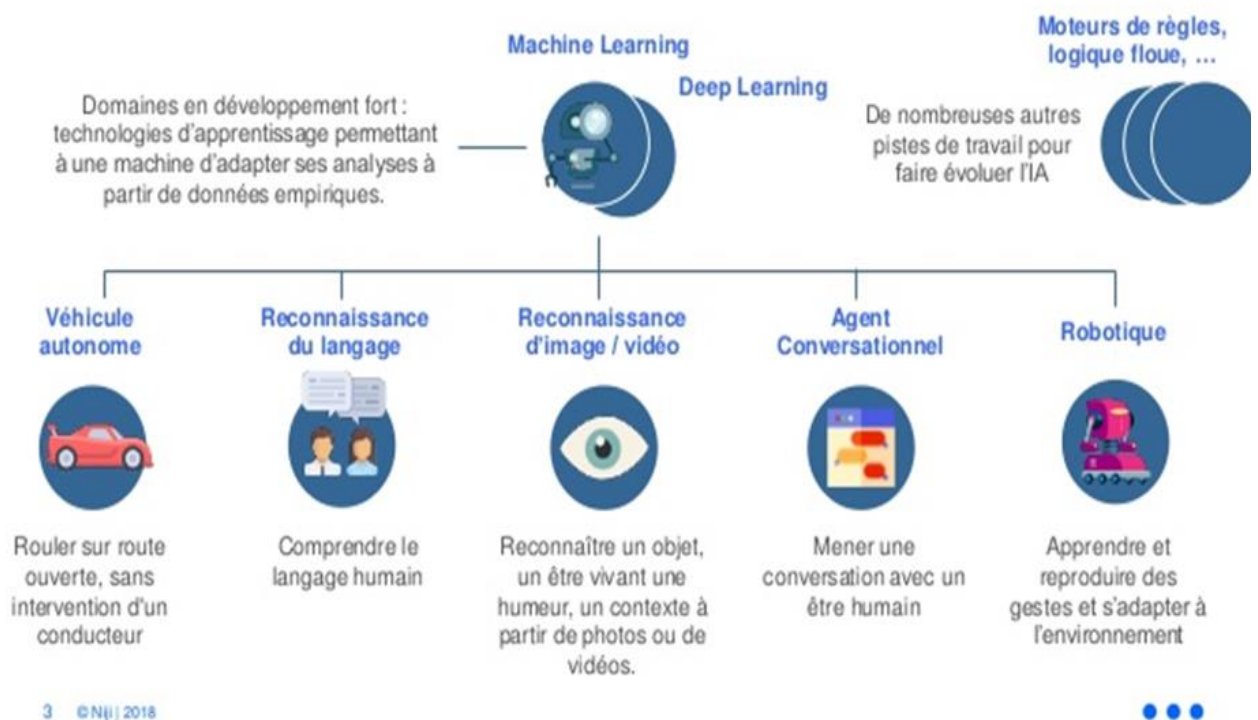


Figure 17 : Domaines d'application de l'IA

IV.2.MACHINE LEARNING

IV.2.1.DEFINITION

Deux définitions de Machine Learning (apprentissage automatique) sont proposées :

Définition 1 :

Arthur Samuel l'a décrit comme « Le domaine d'étude qui donne aux ordinateurs la capacité d'apprendre sans être explicitement programme ». C'est une définition plus ancienne et informelle.

Définition 2 :

Tom Mitchell fournit une définition plus moderne : « Un programme informatique est réputé apprendre de l'expérience E en ce qui concerne certaines classes de tâches T et de la mesure de performance P, si sa performance aux tâches en T, mesurée par P, s'améliore avec l'expérience E. »

IV.2.2.LES DIFFERENTS TYPES DE MACHINE LEARNING

L'apprentissage automatique peut être divisé en trois sous-catégories principales en fonction de la manière dont la machine est "enseignée" :

➤ **Apprentissage supervisé :**

En apprentissage supervisé, nous recevons un ensemble de données et savons déjà à quoi devrait ressembler notre sortie correcte, en ayant l'idée qu'il existe une relation entre l'entrée et la sortie.

Les problèmes d'apprentissage supervisé sont classés en problèmes de « régression » et de « classification ». Dans un problème de régression, nous essayons de prédire les résultats dans une sortie continue, ce qui signifie que nous essayons de mapper les variables d'entrée à une fonction continue. Dans un problème de classification, nous essayons plutôt de prédire les résultats dans une sortie discrète. En d'autres termes, nous essayons de mapper les variables d'entrée en catégories distinctes.

Exemple : pour apprendre à un enfant à écrire il faut lui dessiner une lettre puis le laisser la reproduire

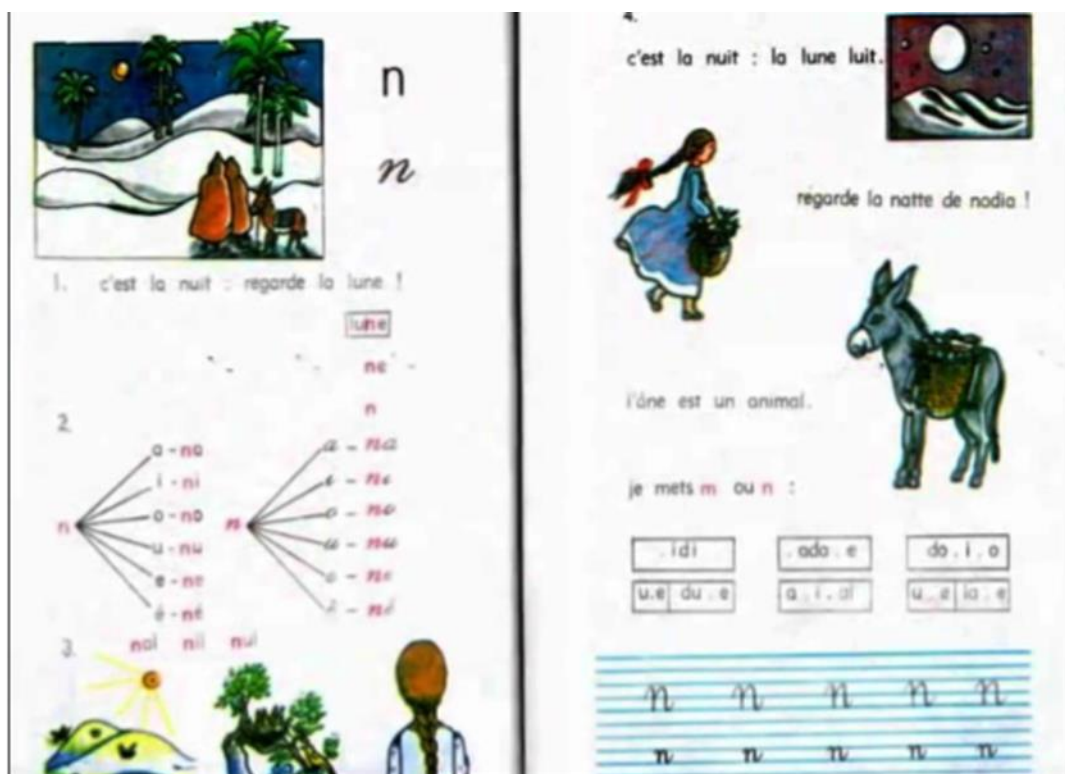


Figure 18 : Image qui représente l'apprentissage supervisé

➤ Apprentissage non supervisé :

L'apprentissage non supervisé nous permet d'aborder les problèmes sans aucune idée de nos résultats. Nous pouvons tirer de la structure des données pour lesquelles nous ne connaissons pas nécessairement l'effet des variables.

Nous pouvons dériver cette structure en regroupant les données en fonction des relations entre les variables contenues dans les données.

Avec l'apprentissage non supervisé, il n'y a pas de retour d'informations basé sur les résultats de la prédiction.

Exemple : L'une des particularités les plus surprenantes de Ludwig van Beethoven est qu'il était sourd. Comment un musicien, un compositeur, peut-il ne plus posséder le sens que l'on imagine le plus important pour lui ?

Il ne connaissait pas les sens mais il a fait des merveilles avec, il ne combinait pas les musiques dans sa tête (variables) pour créer une nouvelle musique (prédire les résultats).

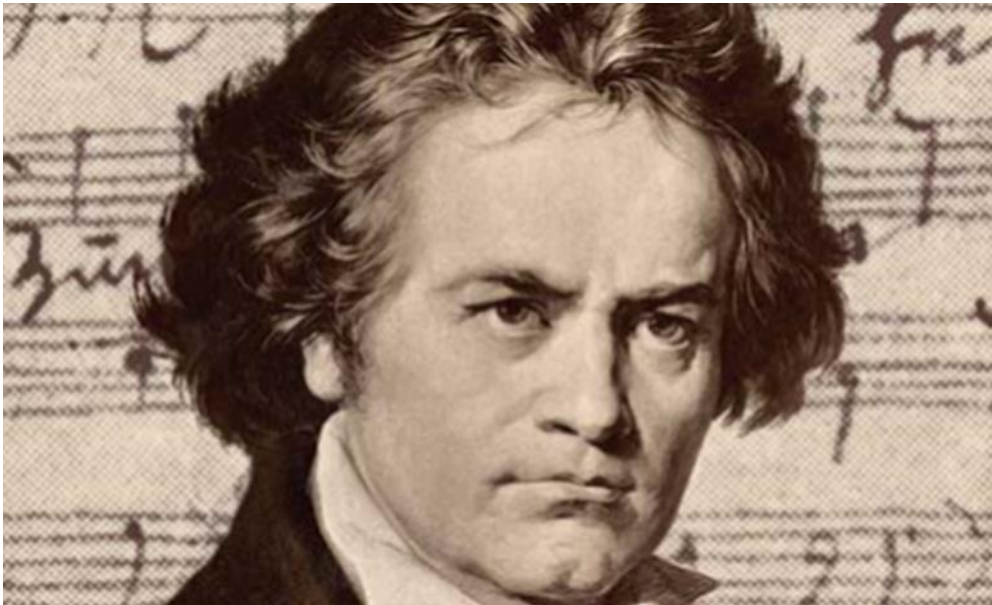


Figure 19: Image qui représente l'apprentissage non supervisé

➤ **Apprentissage par renforcement :**

L'apprentissage par renforcement est un domaine de l'apprentissage automatique inspiré de la psychologie comportementaliste, qui s'intéresse à la façon dont les agents logiciels devraient agir dans un environnement afin de maximiser la notion de récompense cumulative.

Exemple : L'apprentissage par renforcement s'explique mieux en utilisant l'analogie de la formation d'un animal de compagnie, comme un chien. Lorsque vous souhaitez encourager un comportement, vous récompensez le chien. Inversement, lorsque le chien est en panne, il

est puni. Bien que le chien ignore initialement si ses actions sont bonnes ou mauvaises, il apprend avec le temps à associer la récompense ou la punition à ses actions. Ainsi, le chien « apprend » le bien du mal. De même, les ordinateurs peuvent être formés pour exécuter certaines tâches.



récompenser un chien



punir un chien

Figure 20 : Image qui représente l'apprentissage par renforcement

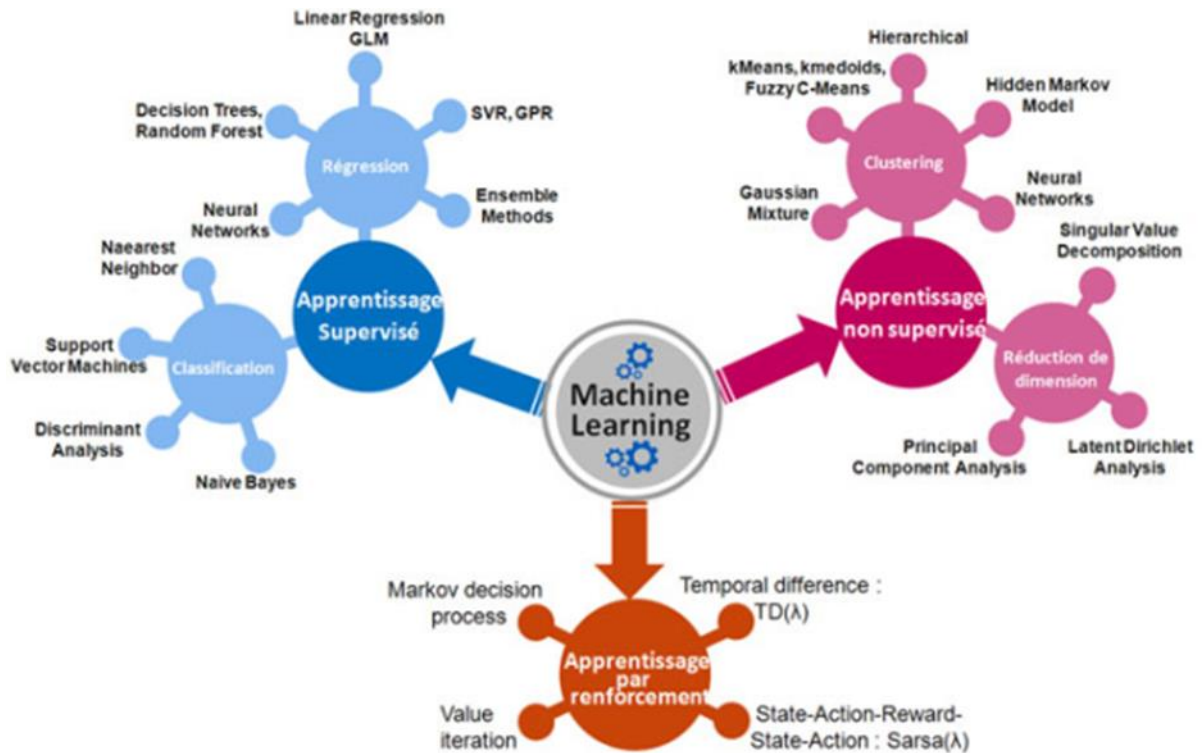


Figure 21 : Image qui résume le machine learning

IV.2.3. APPLICATIONS DE L'APPRENTISSAGE AUTOMATIQUE

- Traitement de la langue
- Jeux
- Filtrer les spams
- Diagnostic médical
- Prévission météo
- Comprendre le discours

IV.3. LE DEEP LEARNING

IV.3.1.DEFINITION

L'apprentissage en profondeur est une fonction d'intelligence artificielle qui imite le fonctionnement du cerveau humain lors du traitement de données et de la création de modèles à utiliser dans la prise de décision. L'apprentissage en profondeur est un sous-ensemble de l'apprentissage automatique en intelligence artificielle (IA) doté de réseaux capables d'apprendre sans surveillance à partir de données non structurées ou non étiquetées. Aussi appelé apprentissage neuronal profond ou réseau neuronal profond.

IV.3.2.FONCTIONNEMENT DU DEEP LEARNING

Au sein du cerveau humain, chaque neurone reçoit environ 100 000 signaux électriques des autres neurones. Chaque neurone en activité peut produire un effet excitant ou inhibiteur sur ceux auxquels il est connecté. Au sein d'un réseau artificiel, le principe est similaire. Les signaux voyagent entre les neurones. Toutefois, au lieu d'un signal électrique, le réseau de neurones assigne un certain poids à différents neurones. Un neurone qui reçoit plus de charge exercera plus d'effet sur les neurones adjacents. La couche finale de neurones émet une réponse à ces signaux.

Pour comprendre comment fonctionne le Deep Learning, prenons un exemple concret de reconnaissance d'images. Imaginons que le réseau de neurones soit utilisé pour reconnaître les photos qui comportent au moins un chat. Pour pouvoir identifier les chats sur les photos, l'algorithme doit être en mesure de distinguer les différents types de chats, et de reconnaître un chat de manière précise quel que soit l'angle sous lequel il est photographié.

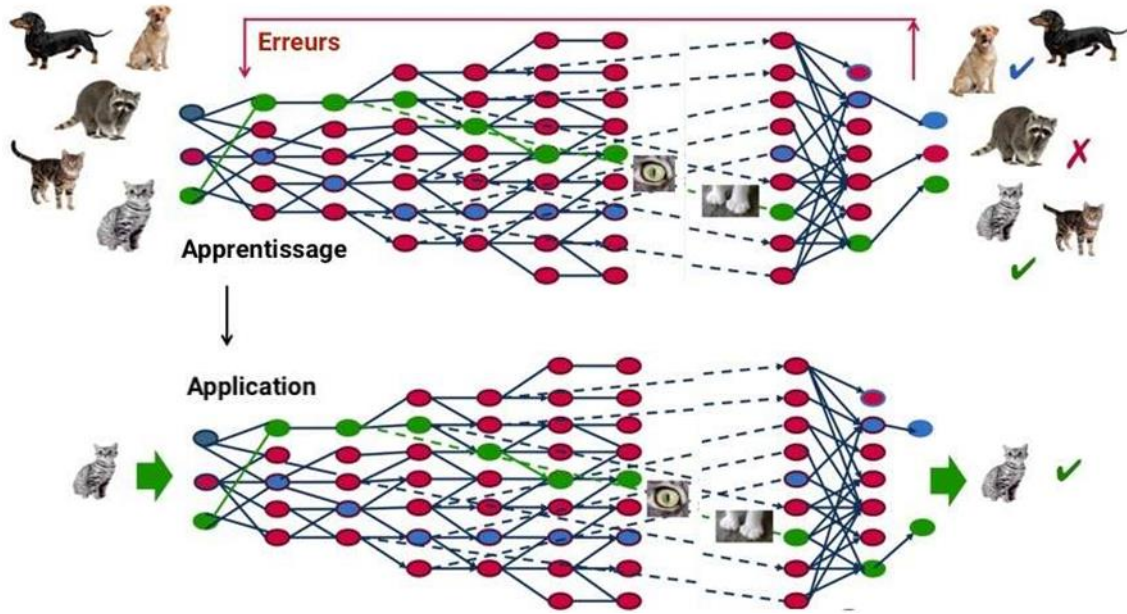


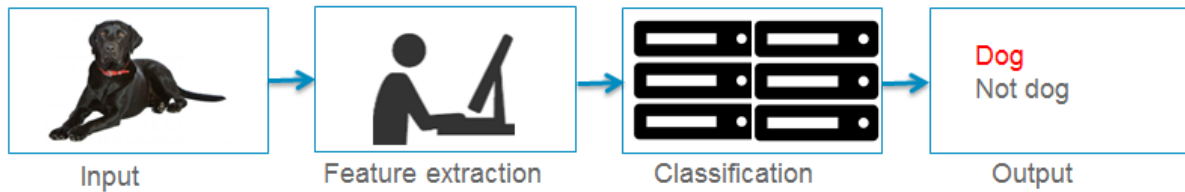
Figure 22 : Exemple de Deep Learning

IV.3.3.DOMAINES D'APPLICATION DE DEEP LEARNING

- Reconnaissance d'image.
- Reconnaissance faciale.
- Traduction automatique.
- Voiture autonome.
- Diagnostic médical.
- Recommandations personnalisées.
- Modération automatique des réseaux sociaux.
- Prédiction financière et trading automatisé.
- Identification de pièces défectueuses.
- Détection de malwares ou de fraudes.
- Chatbots (agents conversationnels).
- Exploration spatiale.
- Robots intelligents.

IV.4.LA DIFFERENCE ENTRE LE MACHINE LEARNING TRADITIONNEL ET LE DEEP LEARNING

Traditional machine learning



Deep learning

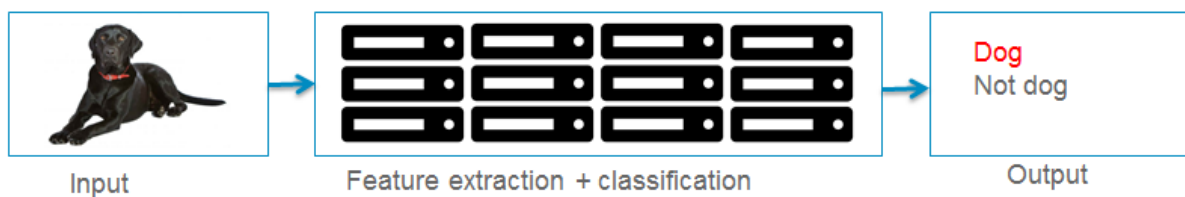


Figure 23 : Différence entre le Machine Learning traditionnel et le Deep Learning

Contrairement aux méthodes plus traditionnelles de techniques d'apprentissage automatique, les classificateurs d'apprentissage en profondeur sont formés par apprentissage de fonctions plutôt que par des algorithmes spécifiques à une tâche. Cela signifie que la machine apprendra des motifs dans les images qui lui sont présentées plutôt que de demander à l'opérateur humain de définir les motifs que la machine devrait rechercher dans l'image. La technique d'apprentissage des fonctionnalités est utilisée quotidiennement pour apprendre à un enfant à reconnaître différents objets.

CONCLUSION

Il convient donc d'anticiper ces changements. En particulier, il faudra apprendre à décider avec esprit critique face aux informations traitées avec l'aide de la technologie. Son rôle n'étant pas de prendre des décisions à notre place, mais de nous aider, tout en tenant compte de nos valeurs éthiques, morales et légales.

L'anticipation sera donc la clé de la bonne utilisation de l'Intelligence Artificielle et Augmentée. Dans le passé, et ce dès les prémises de l'automatisation et de la bureautique, nos sociétés et nos métiers ont dû et ont su se transformer. Et nous devons donc dès maintenant nous préparer à l'avènement de l'IAA, par l'éducation et la formation, afin que la technologie assiste l'Homme dans ses tâches et son développement quotidien.

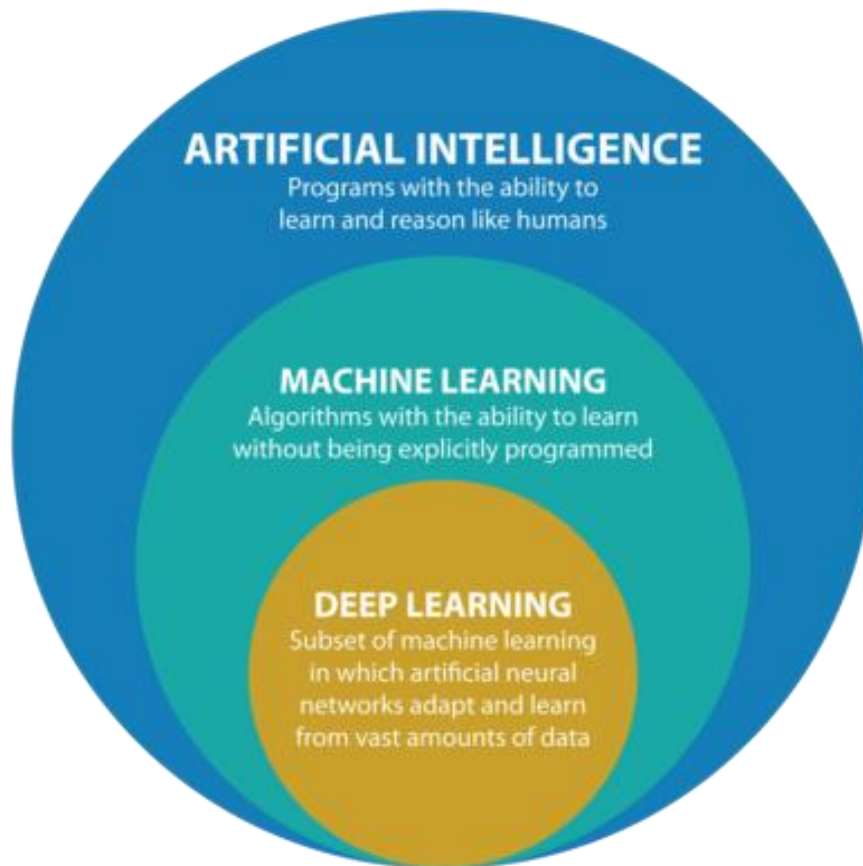


Figure 24 : IA, Machine Learning, Deep Learning

LA RECONNAISSANCE FACIALE



SOMMAIRE

<i>V.1. QU'EST-CE QUE LA RECONNAISSANCE FACIALE</i>	60
<i>V.2. HISTOIRE DE LA RECONNAISSANCE FACIALE</i>	60
<i>V.3. AVANTAGES</i>	61
<i>V.4. INCONVENIENTS</i>	61
<i>V.5. LES ETAPES DE LA RECONNAISSANCE FACIALE</i>	62
<i>V.6. LES PRINCIPALES DIFFICULTES DE LA RECONNAISSANCE FACIALE</i>	64
<i>CONCLUSION</i>	66

La reconnaissance faciale est un des problèmes les plus étudiés de l'apprentissage automatique. Grâce à sa popularité ce problème a été bien exploré pendant les 50 dernières années.

Récemment la reconnaissance faciale attire de plus en plus d'attention. La sécurité reste le domaine d'application principal. Dans ce domaine la reconnaissance de visage est responsable de l'identification et de l'authentification.

Trottoir, route, gare : Tous ou presque, nous traversons quotidiennement au moins un espace public. Convaincus, pour la plupart, que l'historique détaillé de nos déplacements et la liste des personnes qui nous accompagnent restent privés. Une confidentialité que la reconnaissance faciale, mise en œuvre sur les réseaux de caméras déjà en place dans la plupart des grandes villes, vient menacer.

Dans ce chapitre, nous abordons la reconnaissance faciale, sa définition, son histoire. Nous verrons quels sont ses avantages et inconvénients, ses étapes ainsi que ses principales difficultés.

V.1. QU'EST-CE QUE LA RECONNAISSANCE FACIALE

La reconnaissance faciale est une technique qui permet à partir des traits de visage :

- D'authentifier une personne : c'est-à-dire, vérifier qu'une personne est bien celle qu'elle prétend être (dans le cadre d'un contrôle d'accès)
- D'identifier une personne : c'est-à-dire, de retrouver une personne au sein d'un groupe d'individus, dans un lieu, une image ou une base de données.

V.2. HISTOIRE DE LA RECONNAISSANCE FACIALE

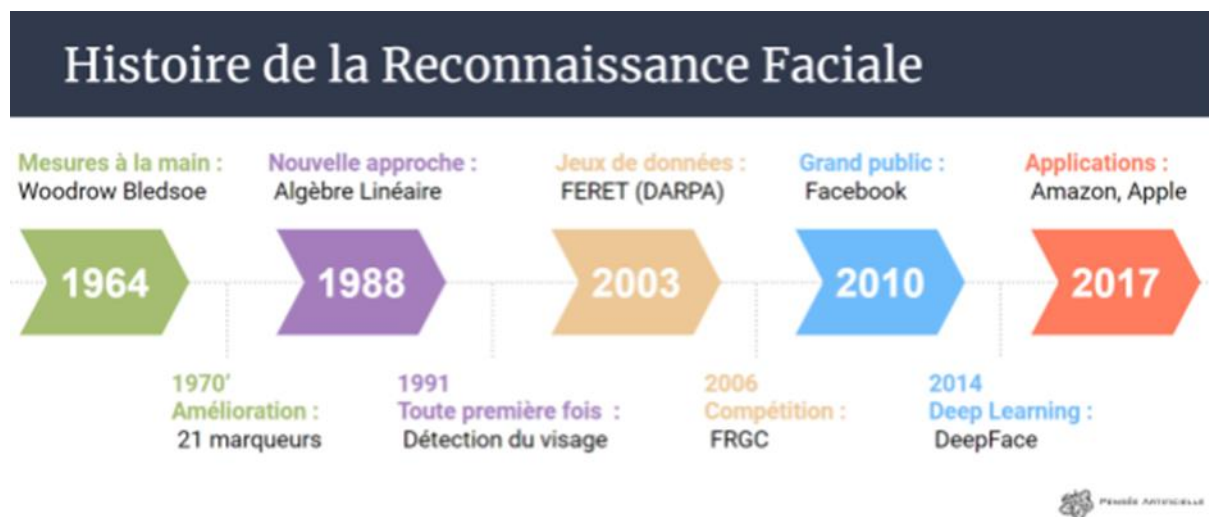


Figure 25 : Histoire de la reconnaissance faciale

V.3.AVANTAGES

Si les chercheurs ont souhaité voir la reconnaissance faciale s'améliorer, c'est parce qu'elle présente de nombreux avantages :

Elle est sans-contact : potentiellement, l'utilisateur ne saura jamais qu'il a fait l'objet de reconnaissance faciale, comme par exemple lors du **SuperBowl de 2001**.

Elle utilise le matériel déjà existant : les caméras qui servent à la circulation ou pour la sécurité de certains lieux. Par exemple, en Chine, la reconnaissance faciale est utilisée pour réprimander les cyclistes et les gestes d'incivilité dans la rue.

Les vidéos qui servent pour la reconnaissance faciale peuvent, d'ailleurs servir à beaucoup d'autres choses dont de l'analyse du comportement. A l'inverse, de l'ADN ne permettra « que » de faire un test ADN...

Enfin, elle est très rapide (0.1s pour une identification en général avec un ordinateur récent).

V.4.INCONVENIENTS

D'un point de vue éthique, la reconnaissance faciale pose beaucoup de problèmes et est très contrôlée. Beaucoup, dont Brad Smith, Président de Microsoft, ont peur qu'en 2024 on se retrouve dans la situation du livre **1984 de Georges Orwell** : un monde totalitariste contrôlé par Big Brother.

De plus, elle reste sensible à l'angle (il faut que le visage à reconnaître soit en face de la caméra autant que possible) et à la lumière.

Elle n'est pas aussi précise que ce que l'on pourrait croire ! Concernant les polices qui l'utilisent pour traquer les criminels (San Diego, Dallas, Los Angeles...), il faut savoir que le taux de prédiction de leurs IA est de... 3%. Autrement dit, sur 100 personnes, elles n'en reconnaissent bien que 3. Ne vous attendez donc pas à ce qu'elles retrouvent des criminels, même si par effet de peur, le taux de criminalité a chuté de 25%.

Ni aussi fiable : si pour certaines applications les scores de prédictions atteignent 96%, il est « facile » de tromper un système de reconnaissance faciale et elle n'est donc pas recommandée pour des applications de sécurité. A noter que le hack le plus connu (mettre une photo imprimée de la personne dont on veut usurper l'identité) ne fonctionne plus, car des

algorithmes peuvent maintenant dire si une vraie personne est devant la caméra (on parle de Spoof Detection, et le MIT ou TrueFace.ai par exemple est bien avancé sur le sujet).

V.5. ETAPES DE LA RECONNAISSANCE FACIALE

Pour être identifié, l'image d'une personne dans un système de reconnaissance faciale suit les étapes suivantes :

a) Le monde physique (l'extérieur)

C'est le monde réel en dehors du système avant l'acquisition de l'image. Dans cette étape, on tient compte généralement de trois paramètres essentiels : L'éclairage, la posture et l'échelle. La variation de l'un de ces trois paramètres peut conduire à une distance entre deux images du même individu, supérieure à celle séparant deux images de deux individus différents, et par conséquent une fausse identification.

b) L'Acquisition de l'image

Cette étape consiste à capturer l'image de l'utilisateur du monde extérieur dans un état statique à l'aide d'un appareil photo ou dynamique à l'aide d'une caméra. Après, l'image extraite sera digitalisée ce qui donne lieu à une représentation bidimensionnelle au visage. L'image dans cette étape est dans un état brut ce qui engendre un risque de bruit qui peut dégrader les performances du système.

c) Les prétraitements

Le rôle de cette étape est d'éliminer les parasites causés par la qualité des dispositifs optiques ou électroniques lors de l'acquisition de l'image en entrée, dans le but de ne conserver que les informations essentielles et donc préparer l'image à l'étape suivante. Elle est indispensable car on ne peut jamais avoir une image sans bruit à cause du background et de la lumière qui est généralement inconnue. Il existe plusieurs types de traitement et d'amélioration de la qualité de l'image, telle que : la normalisation, l'égalisation et le filtre médian. Cette étape peut également contenir la détection et la localisation du visage dans une image, surtout là où le décor est très complexe.

d) L'extraction de paramètres

L'étape de l'extraction des paramètres représente le cœur du système de reconnaissance, elle consiste à effectuer le traitement de l'image dans un autre espace de travail plus simple et qui assure une meilleure exploitation de données, et donc permettre l'utilisation, seulement, des informations utiles, discriminantes et non redondantes.

e) La classification (Modélisation)

Cette étape consiste à modéliser les paramètres extraits d'un visage ou d'un ensemble de visages d'un individu en se basant sur leurs caractéristiques communes. Un modèle est un ensemble d'informations utiles, discriminantes et non redondantes qui caractérise un ou plusieurs individus ayant des similarités.

f) L'apprentissage

C'est l'étape où on fait apprendre les individus au système, elle consiste à mémoriser les paramètres, après extraction et classification, dans une base de données bien ordonnée pour faciliter la phase de reconnaissance et la prise d'une décision, elle est en quelque sorte la mémoire du système.

g) La décision

C'est l'étape qui fait la différence entre un système d'identification d'individus et un autre de vérification. Dans cette étape, un système d'identification consiste à trouver le modèle qui correspond le mieux au visage pris en entrée à partir de ceux stockés dans la base de données, il est caractérisé par son taux de reconnaissance. Par contre, dans un système de vérification il s'agit de décider si le visage en entrée est bien celui de l'individu (modèle) proclamé ou il s'agit d'un imposteur, il est caractérisé par son EER (Equal Error Rate).

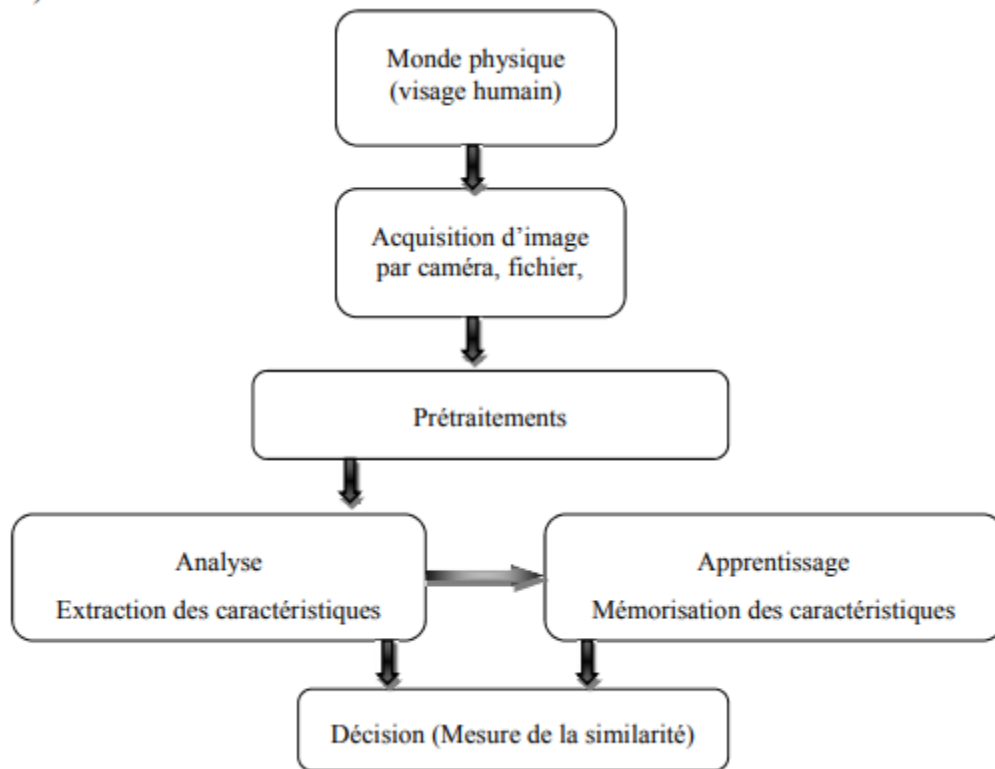


Figure 26 : Schéma qui résume le fonctionnement de la reconnaissance faciale

V.6.LES PRINCIPALES DIFFICULTES DE LA RECONNAISSANCE FACIALE

Pour le cerveau humain, le processus de la reconnaissance de visages est une tâche visuelle de haut niveau. Bien que les êtres humains puissent détecter et identifier des visages dans une scène sans beaucoup de peine, construire un système automatique qui accomplit de telles tâches représente un sérieux défi. Ce défi est d'autant plus grand lorsque les conditions d'acquisition des images sont très variables. Il existe deux types de variations associées aux images de visages : inter et intra sujet. La variation inter-sujet est limitée à cause de la ressemblance physique entre les individus. Par contre la variation intra-sujet est plus vaste. Elle peut être attribuée à plusieurs facteurs que nous analysons ci-dessous.

➤ **Changement d'illumination :**

Les variations d'éclairage rendent la tâche de reconnaissance de visage très difficile. En effet, le changement d'apparence d'un visage dû à l'illumination, se révèle parfois plus

critique que la différence physique entre les individus, et peut entraîner une mauvaise classification des images d'entrée.

➤ **Variation de pose :**

Le taux de reconnaissance de visage baisse considérablement quand des variations de pose sont présentes dans les images. La variation de pose est considérée comme un problème majeur pour les systèmes de reconnaissance faciale. Quand le visage est de profil dans le plan image (orientation $< 30^\circ$), il peut être normalisé en détectant au moins deux traits faciaux (passant par les yeux). Cependant, lorsque la rotation est supérieure à 30° , la normalisation géométrique n'est plus possible.

➤ **Présence ou absence des composants structurels :**

La présence des composants structurels telle que la barbe, la moustache, ou bien les lunettes peut modifier énormément les caractéristiques faciales telles que la forme, la couleur, ou la taille du visage. De plus, ces composants peuvent cacher les caractéristiques faciales de base causant ainsi une défaillance du système de reconnaissance.

➤ **Les vrais jumeaux :**

Qui ont le même indicatif d'ADN, peuvent tromper les personnes qui ne les connaissent pas (les personnes familières avec les jumeaux ont reçu une grande quantité d'information sur ces derniers et sont donc beaucoup plus qualifiés à distinguer les jumeaux.).

➤ **Expressions faciales :**

La déformation du visage qui est due aux expressions faciales est localisée principalement sur la partie inférieure du visage. L'information faciale se situant dans la partie supérieure du visage reste quasi invariable. Elle est généralement suffisante pour effectuer une identification. Toutefois, étant donné que l'expression faciale modifie l'aspect du visage, elle entraîne forcément une diminution du taux de reconnaissance. L'identification de visage avec expression faciale est un problème difficile qui est toujours d'actualité et qui reste non résolu.

CONCLUSION

Les jours à venir annoncent de nombreux changements. Nous ne pouvons évidemment pas prétendre prévoir l'avenir de la reconnaissance faciale et savoir quels seront les enjeux majeurs qui émergeront à l'avenir

La reconnaissance d'individus demeure un problème complexe et non parfaitement résolu, malgré tous les travaux réalisés au cours des dernières années. Plusieurs problèmes incombent à cette tâche d'identification et chacun d'eux est non trivial. De nombreuses conditions réelles affectent la performance d'un système, cependant la détection automatique des visages influence énormément la performance du module d'identification.

PARTIE 1. CONTRIBUTION

ORGANISME D'ACCEUIL

I

SOMMAIRE

I.1.PRESENTATION DE L'ENTREPRISE	69
I.2.PRESENTATION DU CENTRE TIZI-OUZOU	69
I.3.SA SITUATION GEOGRAPHIQUE.....	70
I.4.SON IMPORTANCE ET SA CLASSIFICATION.....	70
PROBLEMATIQUE.....	71

Algérie télécom au statut d'une entreprise publique économique. La naissance de cette entreprise remonte au 5 août 2000, après une restructuration visant le secteur des postes et télécommunications algérien afin de séparer les domaines d'activités postales de celles des Télécommunications.

Entrée officiellement en activité à partir du 1er janvier 2003, elle s'engage dans le monde des technologies de l'information et de la communication avec trois objectifs :

« Rentabilité, Efficacité et Qualité de service ».

L'activité majeure en Algérie Télécom est :

- Fournir des services de télécommunication permettant le transport et l'échange de la voix, de messages écrits, de données numériques, d'informations audiovisuelles ...
- Développer, exploiter et gérer des réseaux publics et privés de télécommunication.
- Établir, exploiter et gérer les interconnexions avec tous les opérateurs des réseaux.

Algérie Télécom a trois filiales :

- Mobile (MOBILIS).
- Internet (DJAWEB).
- Télécommunications spatiales (REVAST).



Figure 27 : Algérie Télécom

I.1.PRESENTATION DE L'ENTREPRISE

ATM MOBILIS filiale du groupe Algérie Télécom spécialisée dans le domaine de la téléphonie mobile de type GSM. Mobilis est le premier opérateur téléphonique mobile en Algérie, il couvre tout le territoire national qui est très large pour cela MOBILIS s'organise en huit directions régionales, celle d'Alger est la centrale. Chacune d'elle est constituée de plusieurs sous directions.

MOBILIS propose à ses clients une large gamme de produits et de services innovants et de haute qualité : offres des post payées et prépayées, SMS vers tous les opérateurs et vers l'étranger, le ROAMING international, facture en ligne, communication en ligne ...

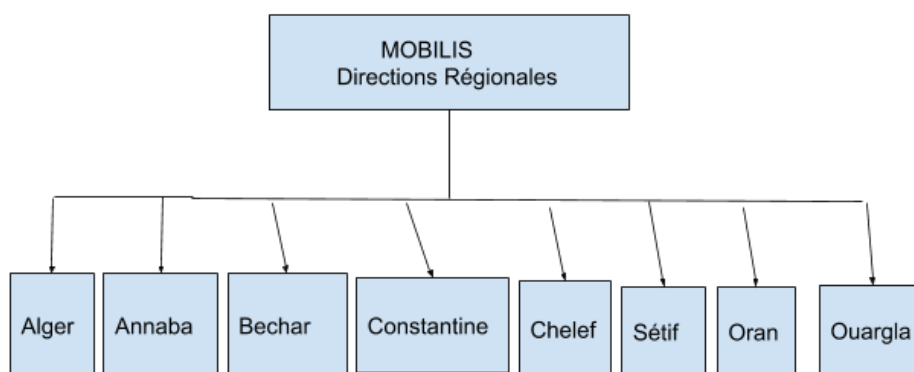


Figure 28 : Les directions régionales de Mobilis

I.2.PRESENTATION DU CENTRE DE TIZI-OUZOU

Le MSC (Mobile Switching Center), et parfois appelé centre de communication des mobiles ou commutateur du service mobile, il gère l'établissement des communications entre un mobile et un autre MSC, l'exécution d'un handover entre deux BSC différentes.

Il est composé de trois salles :

1. **Salle du chef de centre** : Elle abrite le bureau du chef de centre.
2. **Salle de contrôle** : C'est la salle où sont installées les positions de travail des techniciens faisant la supervision et la maintenance des différents équipements du centre, essentiellement cette salle est composée d'AT (Alphanumeric Terminal ; Micro-ordinateur) connecté à une interface permettant la communication Homme-Machine.
3. **Salle des équipements** : Elle comporte tous les équipements du système GSM (commutation 'MSC, BSC').

I.3.SA SITUATION GEOGRAPHIQUE

La wilaya de Tizi-Ouzou se trouve au centre du pays (Algérie) et qui possède un centre de communication mobile (MSC) qui se situe à la nouvelle ville au sud de la wilaya de Tizi-Ouzou.

I.4.SON IMPORTANCE ET SA CLASSIFICATION

Grâce à l'importance du service qu'il assure, le MSC de Tizi-Ouzou, est classé parmi les centraux de première classe. Il est le centre de communication le plus important de la région, car il couvre aussi la wilaya de BOUIRA. Ce dernier à 145 mille abonnés.



Figure 29 : Logo Mobilis

PROBLEMATIQUE

Lors de notre première visite rendue au datacenter de l'entreprise MOBILIS, nous constatons la présence de quelques points de sécurité qui garantissent le bon fonctionnement du datacenter, comme la présence de trois capteurs de température placés sur le plafond du centre : Dans le cas où la température du datacenter dépasse la température recommandée, un message d'alerte sera envoyé au responsable technique, mais l'alerte n'est pas prise en considération sauf si celle-ci est confirmée par les deux autres capteurs.

Ceci pose problème car en cas de panne d'un des capteurs et dépassement de normes de la température c'est tout l'équipement du datacenter qui est mis en danger.

Toutefois nous constatons qu'en cas de fuite de gaz ou d'incendie durant la nuit, le personnel ne pourra être alerté jusqu'à la destruction totale du data center.

S'intéressant à l'accès au data center, nous remarquons que cela est œuvré par autre que les ingénieurs et les techniciens, ce qui entraîne l'insécurité du data center.

Comment est-ce que le responsable du centre peut donc bien monitorer et contrôler ce dernier ?

Pour cela nous proposons plusieurs solutions pour aider l'ingénieur responsable à contrôler et surveiller son datacenter 24 /7, parmi elles :

- L'autorisation d'accès au datacenter avec la reconnaissance faciale.
- Le contrôle de la température et de l'humidité.
- Le contrôle de gaz et de fumé.
- Le contrôle de la qualité de l'air.

OUTILS ET TECHNOLOGIES UTILISES

II

SOMMAIRE

II.1.LA CARTE RASPBERRY	75
<i>II.1.1.PRESENTATION DE LA CARTE</i>	75
<i>II.1.2.LES MODELES DE LA CARTE RASPBERRY</i>	75
<i>II.1.3.RASPBERRY PI B+</i>	77
<i>II.2.LE RASPBERRY CAMERA MODULE</i>	78
<i>II.2.1.PRESENTATION</i>	78
II.2.2.CARACTERISTIQUES	79
II.2.3.DETAILS DE LA CAMERA	79
II.3.CONVERTISSEUR ANALOGIQUE ADC ADS1115	80
II.3.1.PRESENTATION	80
II.3.2.UTILISATION	81
II.3.3.SPECIFICATIONS TECHNIQUES	81
II.4.CAPTEURES UTILISES	81
II.4.1.DETECTEUR DE GAZ ET DE FUME MQ-2	81
II.4.1.1.PRESENTATION	81
II.4.1.2.SPECIFICATIONS	82
II.4.1.3.CABLAGE	83

II.4.2.DETECTEUR DE LA QUALITE DE L'AIR MQ-135.....	83
II.4.2.1.PRESENTATION.....	83
II.4.2.2.SPECIFICATIONS.....	84
II.4.2.3.CABLAGE.....	84
II.4.3.CAPTEUR D'HUMIDITE ET DE TEMPERATURE DHT-11.....	84
II.4.3.1.PRESENTATION	84
II.4.3.2.SPECIFICATIONS.....	84
II.4.3.3.CABLAGE.....	85
II.5.PUBNUB.....	86
II.6.EON.....	87
II.7.OPENCV.....	87
II.7.1.PRESENTATION.....	87
II.7.2.APPLICATIONS OPENCV.....	88
II.7.3.FONCTIONNALITES OPENCV.....	89
II.8.FRITZING.....	89
II.9.GOOGLE DOC.....	89
II.10.APPLICATION WEB.....	90
II.10.1.FLASK PYTHON.....	90
II.10.2.GOOGLE DRIVE.....	90
II.10.3.SQLITE.....	91

Pour réussir la réalisation de notre projet et mettre en place la solution que nous avons proposé, nous avons opté à utiliser plusieurs outils et technologies que nous allons définir et présenter en détail dans cette partie.

Matériels :

- Une carte Raspberry pi B3+
- Un Raspberry Pi camera module.
- Un convertisseur analogique ADC ADS1115.
- Trois capteurs :
 - Un détecteur de gaz et de fumé MQ-2.
 - Un détecteur de la qualité de l'air MQ-135.
 - Un capteur d'humidité et de température DHT-11.

Logiciels :

- Pubnub (Cloud PaaS).
- OpenCV (Pour la reconnaissance faciale).
- EON (EyesOfNetwork) (pour la supervision des capteurs).
- Fritzing (Pour les schémas de câblage).
- API Spreadsheets.
- Flask Python (Application web).
- Base de données (SQLite).



II.1.LA CARTE RASPBERRY

II.1.1.PRESENTATION DE LA CARTE RASPBERRY

Raspberry est une carte mère d'un mini-ordinateur qui peut être branchée à n'importe quel périphérique (souris, clavier...). Cette carte est fabriquée pour aider à étudier les ordinateurs et pour représenter un moyen d'apprentissage de la programmation informatique en plusieurs langages (python, scratch...). Elle est aussi capable de lire les vidéos à haute définition et même à installer des jeux vidéo. L'intérêt d'utiliser le Raspberry Pi est sa capacité d'interaction avec le monde extérieur et d'exécuter plusieurs variantes du système d'exploitation libre (GNU/Linux, Raspbian Debian ...) et des autres logiciels compatibles [Raspberry Pi 2017].

II.1.2.LES MODELES RASPBERRY PI

➤ **Le modèle A** : Il existe deux types A et A+.



Figure 30 : Modèle A+



Figure 31 : Modèle A

- **Le modèle B :** Il existe cinq types B1, B1+, B2, B3 et B3+.

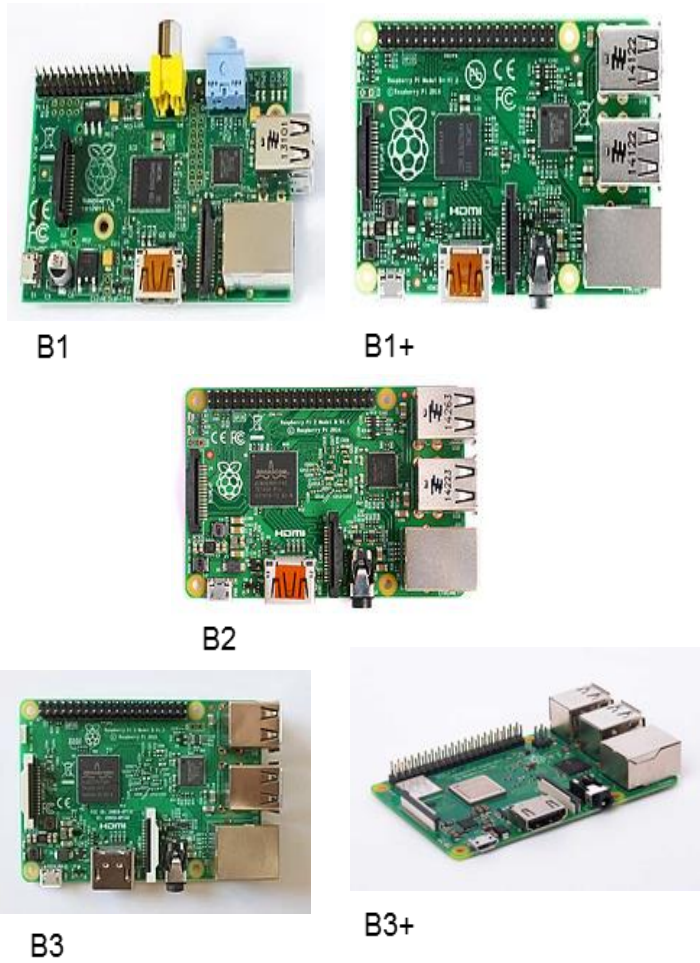


Figure 32 : Types du modèle B

- **Le modèle zéro :** Un seul modèle.

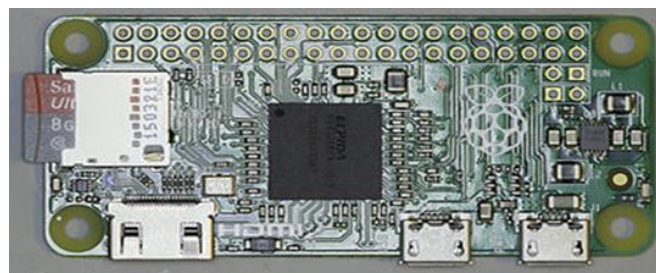


Figure 33 : Le modèle zéro

II.1.3.RASPBERRY PI B+

Pour notre projet, nous avons opté pour Raspberry Pi B3+ pour beaucoup de raisons notamment sa puissance et sa rapidité par rapport au Raspberry Pi Type B. Raspberry Pi Type B3+ est la carte mère idéale pour un système d'architecture ARM.

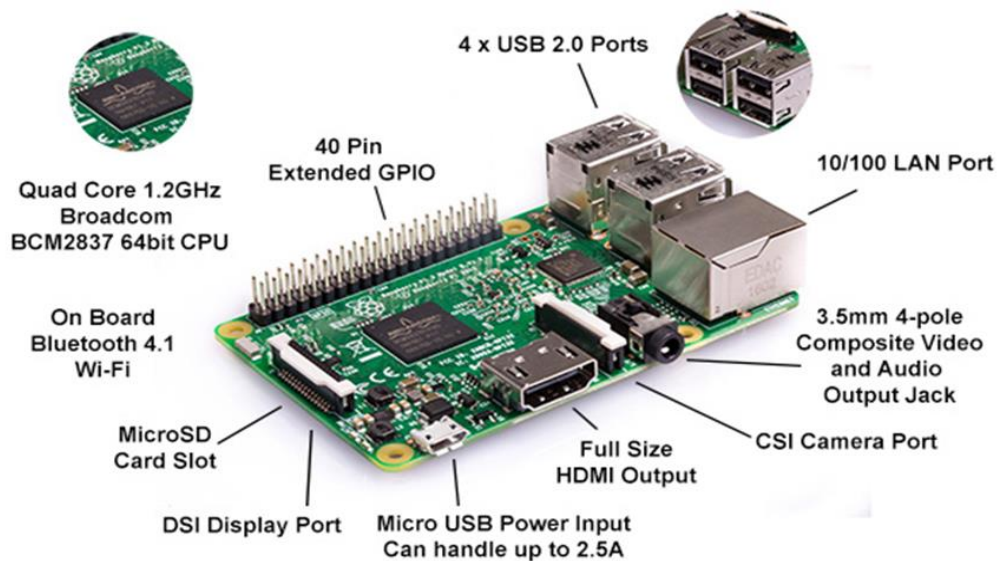


Figure 34 : Raspberry Pi B+

Une des caractéristiques de la Raspberry Pi, est le nombre de ses GPIOs, qui peuvent être entrées/sorties.

Il y'a 40 broches, disposés tout au long, du bord supérieur, de la carte.

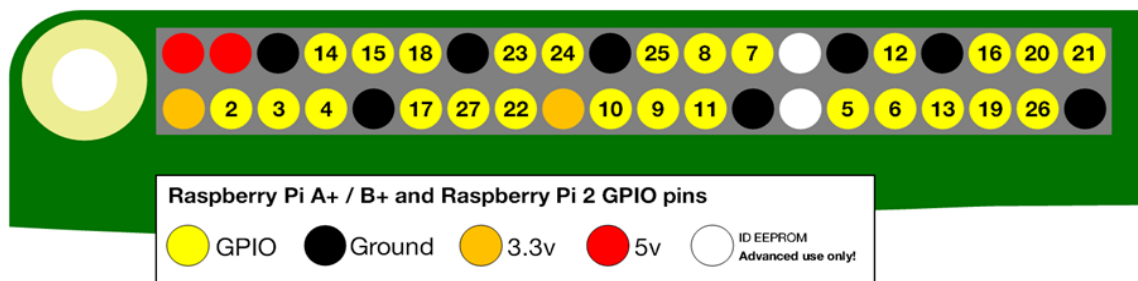


Figure 35 : GPIOs de la Raspberry Pi

Dans notre cas, nous l'avons utilisé pour la détection et la reconnaissance faciale dans le but d'autoriser l'accès au data center.

II.2.2.CARACTERISTIQUES

- Capteur 5MP
- Image plus large, capable d'images fixes 2592x1944, vidéo 1080p30
- Vidéo 1080p pris en charge
- CSI
- Taille : 25 x 20 x 9 mm

II.2.3.DETAILS DE LA CAMERA

La caméra consiste en une petite carte de circuit imprimé (25 mm sur 20 mm sur 9 mm), qui se connecte au connecteur de bus CSI (interface série) de Raspberry Pi via un câble ruban souple. Le capteur d'image de l'appareil photo a une résolution native de cinq mégapixels et un objectif à focale fixe. Le logiciel de la caméra prend en charge des images fixes haute résolution jusqu'à **2592x1944** et des résolutions vidéo de **1080p30**, **720p60** et **640x480p60 / 90**.

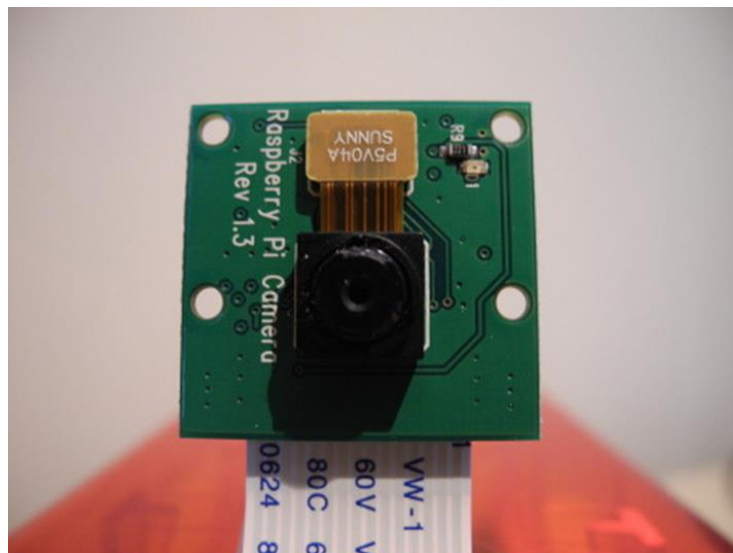


Figure 37 : caméra rev 1.3

II.3.CONVERTISSEUR ANALOGIQUE ADC

ADS1015

II.3.1.PRESENTATION

L'idée maîtresse de l'ADS1015 16-Bit ADC 4 canaux est de nous offrir un convertisseur analogique-numérique de faible consommation, puissant, précis et adaptable aux conversions à réaliser.

On peut profiter ainsi d'un excellent débit de données maximum (860 SPS), mais qui peut être programmé pour être beaucoup plus faible. L'amplificateur de gain programmable interne nous permet également d'adapter nos mesures à l'intensité du signal en diminuant ou en augmentant la tension d'alimentation (à partir de 256 mV).

Quant aux canaux de transmission, ils peuvent être utilisés comme canaux d'entrée unidirectionnels (4) ou canaux différentiels (2). Enfin, l'interface I2C nous permet de sélectionner jusqu'à 4 adresses esclaves, et donc de connecter simultanément 4 ADC 16-Bit à notre microcontrôleur.



Figure 38 : ADC ADS1015

II.3.2.UTILISATION

Ce convertisseur est bien évidemment utile à tous ceux qui ne disposent pas d'un microcontrôleur avec convertisseur analogique-numérique. Il peut également être ajouté à un CAN existant pour des mesures plus précises sur petits et grands signaux.

Un tel dispositif peut être utilisé pour créer un appareil de mesure de la température, un système automatique ou de contrôle des processus, ou bien encore un indicateur de niveau de charge des batteries. Sa très petite taille lui permet de prendre place dans des projets portables très réduits.

II.3.3.SPECIFICATIONS TECHNIQUES

- Précision : 16 bits.
- Tension de fonctionnement : 2-5,5 V.
- Consommation : 150 uA en mode continu (Mode impulsion par impulsion : arrêt automatique).
- Débit de données programmable : 8SPS à 860SPS (échantillons par seconde).
- Tension de référence à faible dérive.
- Oscillateur interne.
- Amplificateur de gain programmable interne.
- Interface I2C : Jusqu'à 4 adresses sélectionnables par broche.
- 4 canaux unidirectionnels ou 2 canaux différentiels.
- Comparateur programmable.

II.4.LES CAPTEURS UTILISES

II.4.1.LE DETECTEUR DE GAZ ET DE FUME : MQ-2

II.4.1.1.PRESENTATION

Le **MQ-2 Capteur de Gaz/Fumée** est un semi-conducteur capteur de gaz/fumée qui détecte la présence du gaz/fumée à des concentrations de 300 ppm à 10000 ppm. La simple

interface de tension analogique du capteur ne nécessite qu'une seule broche d'entrée analogique du microcontrôleur.

La concentration de détection gamme de 300 ppm à 10000 ppm est approprié pour la détection des fuites. Le capteur peut fonctionner à des températures allant de -10 à 50 ° C et consomme moins de 150 mA à 5 V.

Le capteur de gaz MQ2 est utilisé pour la détection des fuites de gaz pour les équipements des marchés de grandes consommations et industriel. Ce capteur est conçu pour détecter le LPG, i-butane, propane, méthane, alcool, hydrogène et la fumée. Il a une grande sensibilité et un temps de réponse rapide. Sa sensibilité peut d'ailleurs être ajustée par potentiomètre.

Il possède deux types de sorties :

- Une sortie analogique, dont la tension de sortie varie en fonction de la concentration globale d'élément détecté (tous les gaz à la fois)
- Une sortie numérique, réglable à l'aide d'un potentiomètre à l'arrière du composant. L'utilisateur règle le seuil de détection du module, et ce dernier se déclenche si la concentration dépasse le seuil.

II.4.1.2.SPECIFICATIONS

- Alimentation : 5V
- Type d'Interface : Analogique
- Connectique : 1-Sortie 2-GND 3-VCC
- Large panel de détection
- Réponse rapide et haute sensibilité
- Circuit de Contrôle Simple
- Système stable à longue durée de vie
- Dimensions : 40x20mm

II.4.1.3.CABLAGE

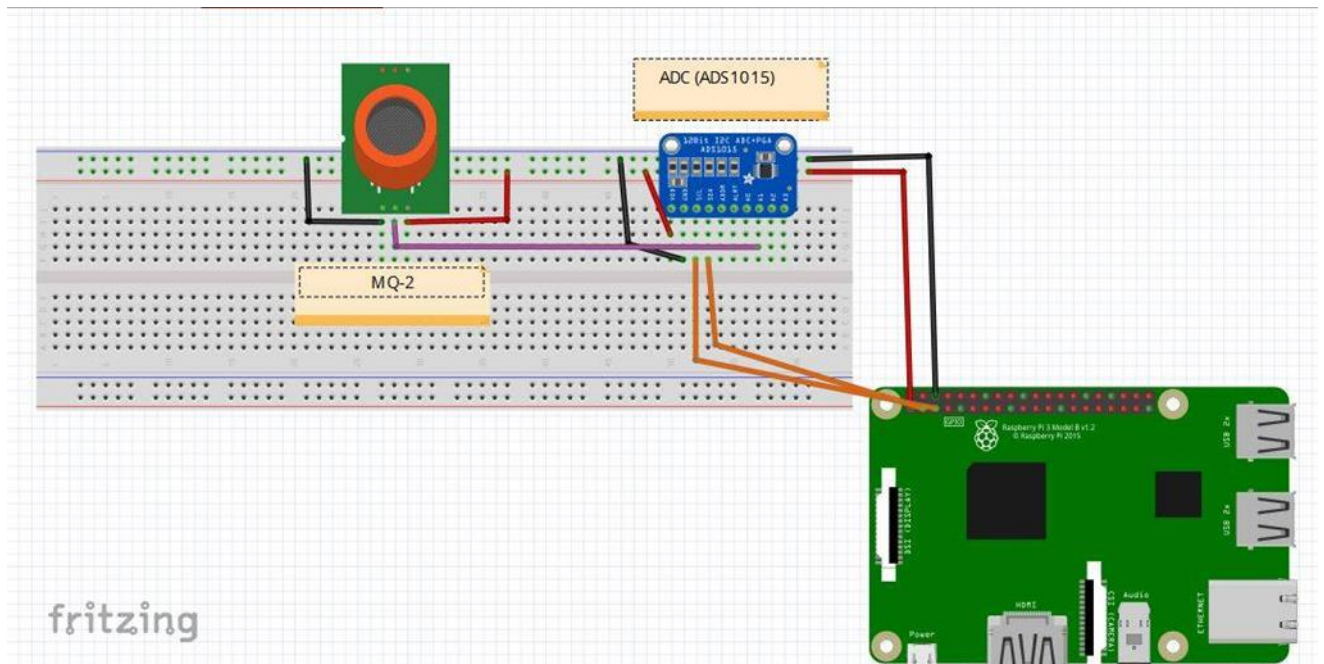


Figure 39 : Câblage de MQ-2

Broche 1 .. 3v3
Broche 2 .. branchée à la broche A1 du ADS1015
Broche 3 .. Gnd

II.4.2.DETECTEUR DE LA QUALITE DE L'AIR MQ-135

II.4.2.1.PRESENTATION

Le MQ135 est un capteur qui permet de mesurer la qualité de l'air. Le **MQ135** est sensible à aux principaux polluants présents dans l'atmosphère de la maison. Ce capteur est sensible au CO₂, à l'alcool, au Benzène, à l'oxyde d'azote (NO_x) et à l'ammoniac (NH₃).



Figure 40 : MQ-135

II.4.2.2.SPECIFICATIONS

- Tension nominale : 5V.
- 2 Sorties : Analogiques et numérique tout ou rien selon un seuil réglable.
- Le module possède un indicateur LED de l'état de la sortie numérique.
- Détecte NH3, NOx, alcool, benzène, fumée et CO2.
- Haute sensibilité : 10 - 300 ppm NH3, 10 - 1000 ppm Benzène, 10 - 300 Alcool.
- Plus la concentration est importante plus la sortie analogique est élevée.
- Stable.
- Longue durée de vie.

II.4.2.3.CABLAGE

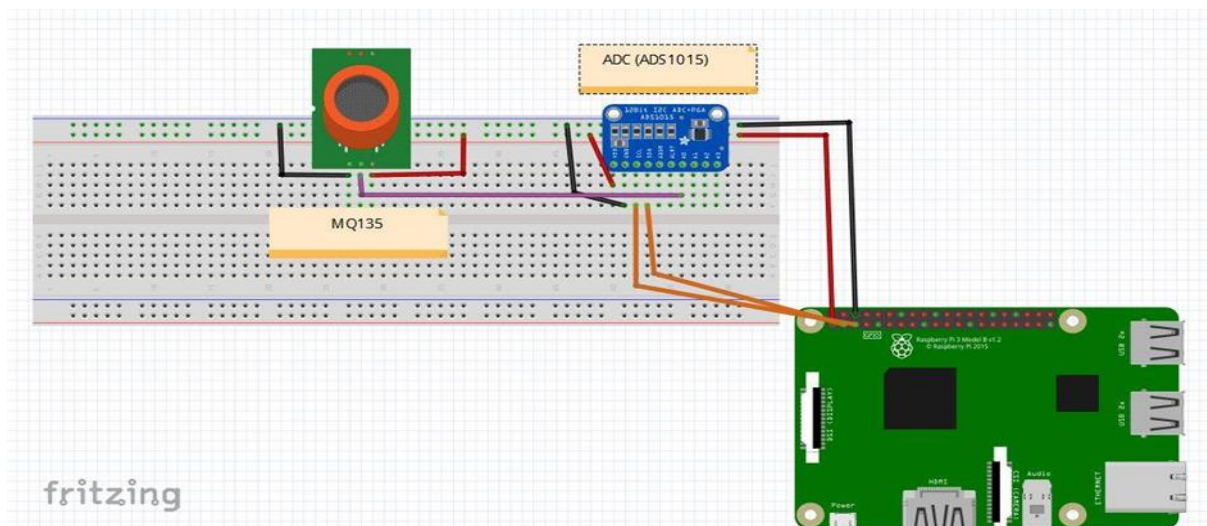


Figure 41 : Câblage MQ-135

Broche 1 .. 3v3
Broche 2 .. branchée à la broche A0 du ADS1015
Broche 3 .. Gnd

II.4.3.CAPTEUR D'HUMIDITE ET DE TEMPERATURE

DHT-1

II.4.3.1.PRESENTATION

Le DHT-11 Un capteur numérique idéal pour mesurer la température et l'humidité.

Le capteur DHT11 fournit une sortie numérique proportionnelle à la température et à l'humidité mesurées par le capteur. La technologie utilisée pour produire le capteur DHT11 garantit une grande fiabilité, une excellente stabilité à long terme et un temps de réponse très rapide.

Le DHT11 est étalonné avec précision en laboratoire. Le coefficient d'étalonnage est mémorisé dans la mémoire interne de l'OTP et cette valeur est utilisée par le processus de détection du signal interne du capteur. L'interface série monofilaire permet une intégration rapide et simple de ce capteur dans le système numérique.

L'interface physique du capteur est réalisée par un connecteur à 3 broches: +5V, GND et DATA. Les deux premières broches sont l'alimentation et la terre et elles sont utilisées pour alimenter le capteur, la troisième est le signal de sortie numérique du capteur.

Sa petite taille physique (1.05 "x0.7") et son poids très léger (seulement 0.1oz) font de cette carte un choix idéal pour la mise en œuvre de petits robots et de systèmes de surveillance d'ambiance.

II.4.3.2.SPECIFICATIONS

- Alimentation : 3 à 5 Vcc
- Consommation maxi : 2,5 mA
- Plage de mesure :
 - Température : 0 à +50 °C
 - Humidité : 20 à 100 % HR
- Précision :
 - Température : ± 2 °C
 - Humidité : ± 5 % HR
- Dimensions : 16 x 12 x 7 mm

II.4.3.3.CABLAGE

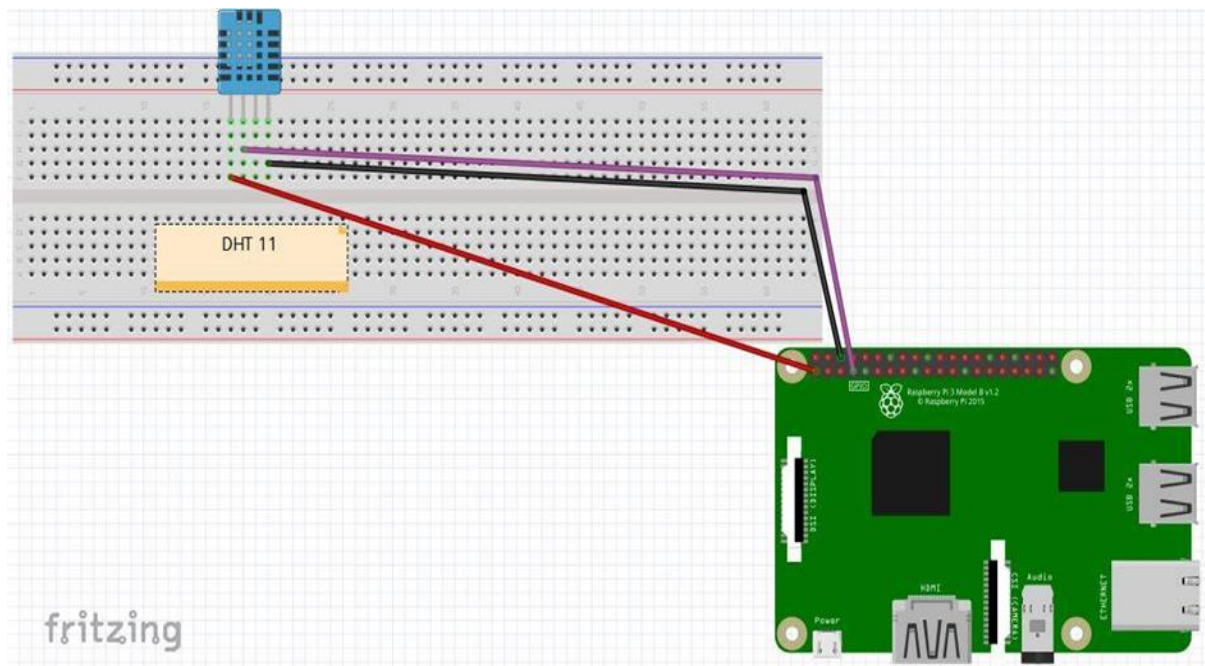


Figure 42 : Câblage DH-11

Broche 1 .. 3v3
Broche 2 .. Gpio 4
Broche 3 .. Gnd

II.5.PUBNUB

PubNub est un réseau de données en temps réel, il permet à ses utilisateurs de s'inscrire gratuitement et de développer des applications en temps réel, en réduisant le coût de développement et la complexité de la tâche. Il fournit en effet une API (interface) de services web pour les entreprises leur permettant de créer des applications de données évolutives sur les mobiles, les tablettes et le web.

Ce service Push en temps réel sur le Cloud prend en charge plusieurs kits de développement de logiciels, tels que iOS, Android, JavaScript, Python, Ruby on Rail et pleins d'autres.

Ainsi, PubNub propose des services de base pour répondre aux besoins des développeurs afin qu'ils développent n'importe quelle application en temps réel. Rapide,

fiable et sécurisé, il permet également d'obtenir des fonctionnalités instantanément et en temps réel, sur n'importe quel dispositif.



Figure 43 : Logo PubNub

est un projet lancé par PubNub, c'est un diagramme open source et un cadre cartographique pour les données en temps réel ; IoT Device Control pour surveiller, contrôler, fournir et diffuser des données entre des périphériques connectés à Internet ; et des API et des infrastructures permettant d'alimenter la messagerie en temps réel pour l'innovation des soins de santé ; API et infrastructure pour divers cas d'utilisation de la crypto-monnaie. La société fournit également WebRTC et VoIP, une solution pour la signalisation en temps réel..

II.6.EON

EON(EyesOfNetwork) est un projet lancé par PubNub ,c'est un diagramme open source et un cadre cartographique pour les données en temps réel; IoT Device Control pour surveiller, contrôler, fournir et diffuser des données entre des périphériques connectés à Internet; et des API et des infrastructures permettant d'alimenter la messagerie en temps réel pour l'innovation des soins de santé; API et infrastructure pour divers cas d'utilisation de la crypto-monnaie. La société fournit également WebRTC et VoIP, une solution pour la signalisation en temps réel ..



Figure 44 : Logo EON

II.7.OPENCV

II.7.1.PRESENTATION

OpenCV est la principale bibliothèque open source dédiée à la vision par ordinateur, au traitement d'images et à l'apprentissage automatique. Il offre désormais une accélération GPU pour un fonctionnement en temps réel.

OpenCV est publié sous licence BSD et est donc gratuit pour un usage académique et commercial. Il a des interfaces C ++, C, Python et Java et supporte Windows, Linux, Mac OS, iOS et Android. OpenCV a été conçu pour l'efficacité informatique et se concentre sur les applications en temps réel. Écrit en C / C ++ optimisé, la bibliothèque peut tirer parti du traitement multicœur. Adopté dans le monde entier, OpenCV compte plus de 47 000 utilisateurs et un nombre de téléchargements estimé à plus de 6 millions. L'utilisation va de l'art interactif à l'inspection des mines, en passant par l'assemblage de cartes sur le Web ou par la robotique avancée.

Dans notre projet, pour la reconnaissance faciale on a utilisé l'algorithme Haar Cascade offert par OpenCV.

HaarCascade est un algorithme de détection d'objets d'apprentissage automatique utilisé pour identifier des objets dans une image ou une vidéo. Il repose sur le concept de fonctionnalités proposé par Paul Viola et Michael Jones dans son article "Détection d'objet rapide à l'aide d'une cascade optimisée de fonctionnalités simples" dans 2001.

C'est une approche basée sur l'apprentissage machine où une fonction en cascade est formée à partir de nombreuses images positives et négatives. Il est ensuite utilisé pour détecter des objets dans d'autres images.



Figure 45 : Logo OpenCV

II.7.2.APPLICATIONS OPENCV

OpenCV est utilisé pour un très large éventail d'applications, notamment :

- Assemblage d'images Street View.
- Inspection et surveillance automatisées.
- Navigation et contrôle de voiture robot et sans conducteur.
- Analyse d'images médicales.
- Recherche et récupération de vidéos / images.

- Films - Structure 3D du mouvement.
- Installations d'art interactives.

II.7.3.FONCTIONNALITE OPENCV

- E / S image / vidéo, traitement, affichage (*core, imgproc, highgui*).
- Détection d'objets / fonctionnalités (*objdetect, features2d, nonfree*).
- Vision par ordinateur monoculaire ou stéréo basée sur la géométrie (*calibré, couture, vidéostab*).
- Photographie numérique (*photo, vidéo, superres*).
- Apprentissage et regroupement (*ml, flann*).
- Accélération CUDA (*gpu*).

II.8.FRITZING

Fritzing est un logiciel open-source multi-plateforme permettant de construire des schémas des circuits que nous utilisons avec Arduino. Plusieurs vues sont disponibles : platine d'essai, schémas électriques et circuit imprimé. Il permet aussi l'export en image pour figurer sur internet.



Figure 46 : Logo FRITZING

II.9.GOOGLE DOC

Google Documents est un traitement de texte inclus dans le cadre d'une suite logicielle bureautique Web gratuite proposée par Google dans le cadre de son service Google Drive. Ce

service inclut également Google Sheets et Google Slides, un tableur et un programme de présentation.



Figure 47 : Logo Google Doc

II.10.APPLICATION WEB

Afin de réaliser notre application web nous avons utilisé :

- Flask python.
- API spreadsheet.
- SQLite.

II.10.1.FLASK PYTHON

Flask est un Framework open-source de développement web en Python. Son but principal est d'être léger, afin de garder la souplesse de la programmation Python, associé à un système de templates. Il est distribué sous licence BSD.



Figure 48 : Logo Flask

II.10.2.GOOGLE DRIVE

Google Drive est un service de stockage et de partage de fichiers dans le cloud lancé par la société Google. Google Drive, qui regroupe Google Docs, Sheets et Slides, Drawings, est une suite bureautique permettant de modifier des documents, des feuilles de calcul, des présentations, des dessins, des formulaires.



Figure 49: Logo Google Drive

Dans notre projet nous avons utilisé l'un de ses services qui est le **Spreadsheet API**. Spreadsheet API permet de :

- Lire, écrire et formater des données dans des feuilles. La dernière version de l'API Sheets permet aux développeurs de programmer :
- Lire et écrire des données
- Mettre en forme le texte et les chiffres
- Construire des tableaux croisés dynamiques
- Appliquer la validation de cellule
- Définir les lignes gelées
- Ajuster la taille des colonnes
- Appliquer des formules
- Créez des graphiques ... et plus encore !

II.10.3.SQLITE

SQLite est une bibliothèque C qui fournit une base de données légère sur disque qui ne nécessite pas de processus serveur distinct et permet d'accéder à la base de données à l'aide d'une variante non standard du langage de requête SQL. Certaines applications peuvent utiliser SQLite pour le stockage de données interne. Il est également possible de prototyper une application à l'aide de SQLite, puis de transférer le code dans une base de données plus grande telle que PostgreSQL ou Oracle.



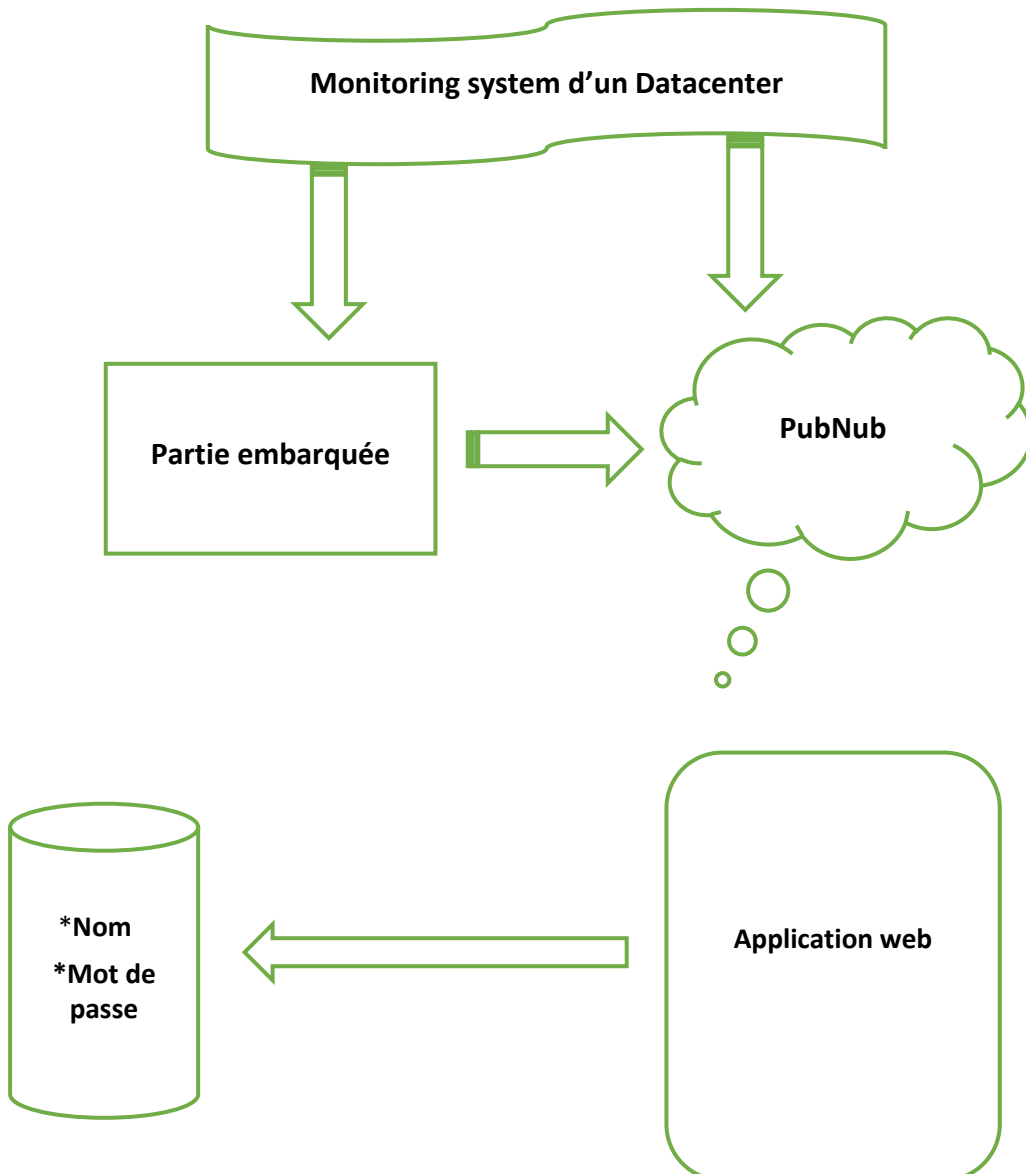
Figure 50 : Logo SQLite

CONCEPTION ET REALISATION

III

Dans ce chapitre on s'intéresse à la réalisation de notre système de monitoring d'un datacenter.

On commence par présenter l'idée globale de notre solution par le schéma suivant :



III.1.PARTIE EMBARQUEE :

Dans cette partie on trouve tous les composants physiques tels :

- La carte Raspberry
- Les capteurs
- La caméra
- Les câbles

Ces composants sont reliés comme suit :

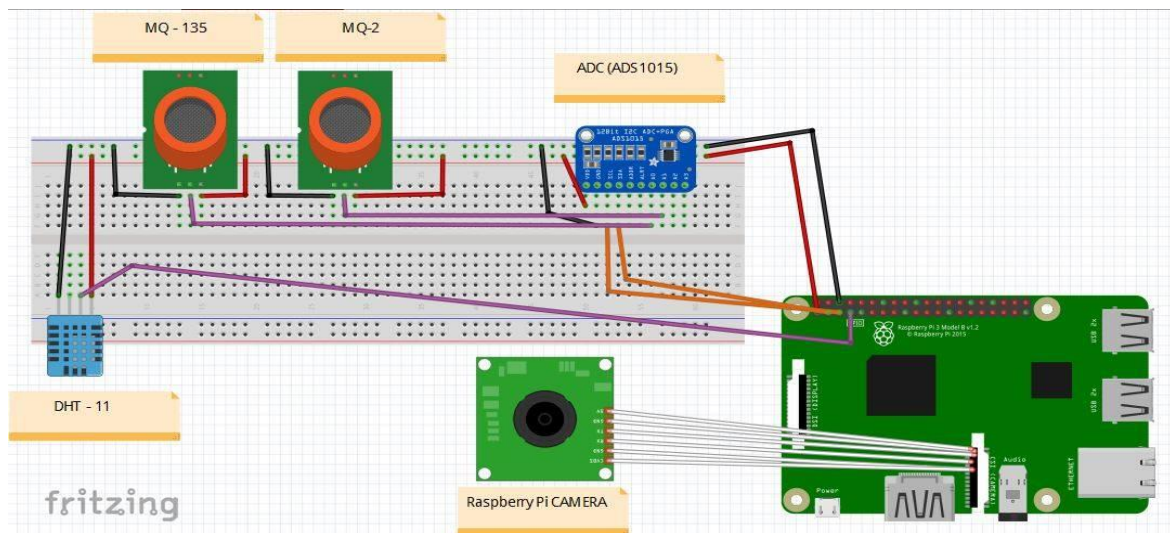


Figure 51 : Schéma qui représente le câblage de notre système embarqué

DHT11	MQ-2	MQ-135	ADC(ADS1015)
Broche1 : 3v3	Broche1 :3v3	Broche1 : 3v3	Broche1 : 3v3
Broche2 : GPIO4	Broche 2 : broche A1 de ads 1015	Broche 2 : broche A1 de ads 1015	Broche2:GND
Broche3 :GND	Broche3 :GND	Broche3 :GND	Broche3 : scl
			Broche 4 :Sda

Tableau 1: numéro des broches

III.2.PARTIE LOGICIELLE

Cette partie est composée de deux parties :

- Partie développeur : PubNub.

➤ Partie Utilisateur : Application web.

La partie développeur est décrite comme suit :

Les résultats récupérés par la carte Raspberry sont directement envoyés vers notre service cloud qui est PubNub où ils seront traités et analysés puis transformés en des graphes et des statistiques comme le montre la figure suivante :

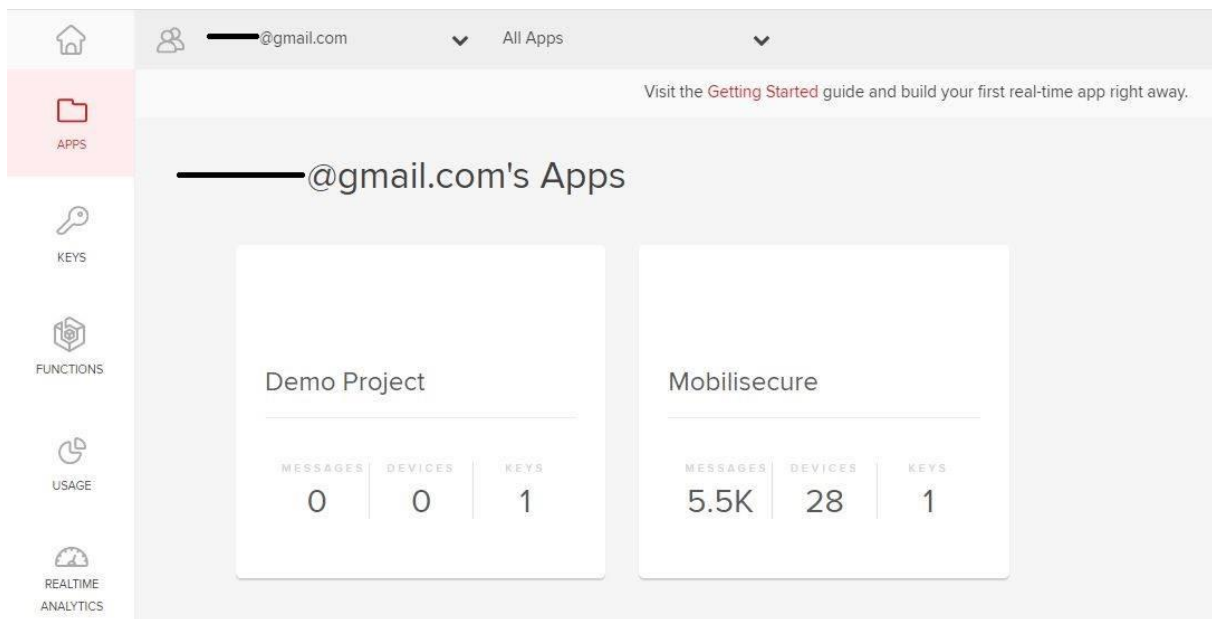


Figure 52 : Interface PubNub

Une fois le traitement et l'analyse seront fait, les résultats seront envoyés à l'application web. Celle-ci propose 4 services :

1. Connexion
2. Monitoring
3. Ajouter un utilisateur
4. Liste des gens reconnus avec la caméra.

Cette application est reliée vers une base de données SQLite.

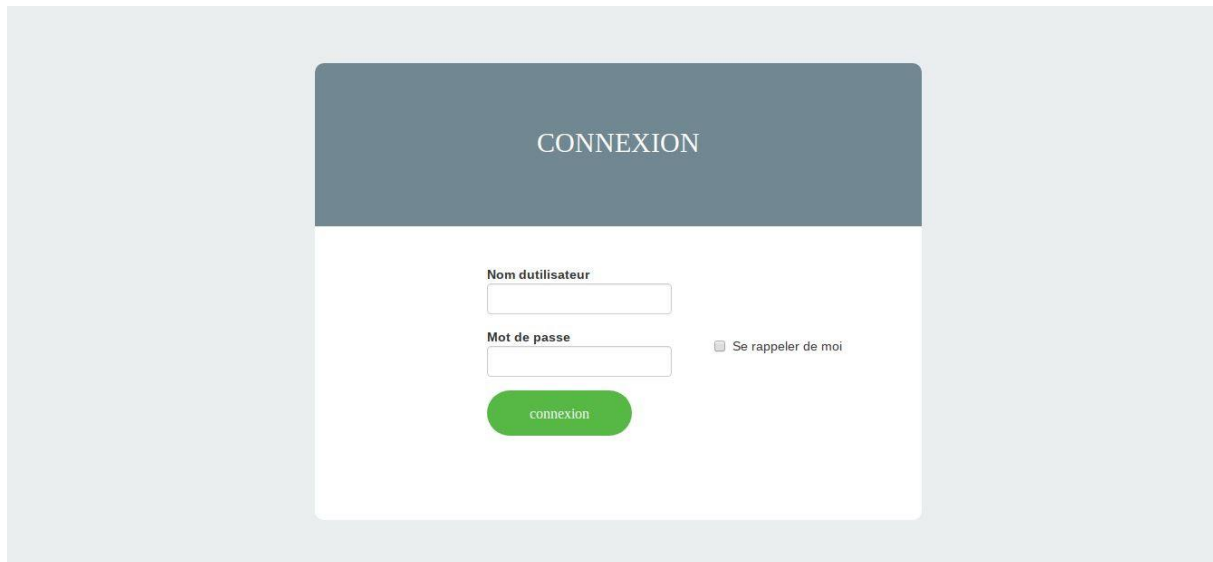


Figure 53: l'interface principale de l'application web

```
pi@raspberrypi:~/Documents/applications/BMS $ sqlite3 database.db
SQLite version 3.16.2 2017-01-06 16:32:41
Enter ".help" for usage hints.
sqlite> select * from user;
1|Mazen|sha256$0ghVVap8$93e0b65c5ff2205bef72fed7cf43358f0fc71df7888e4172e19c0dc346950245
2|Nelya|sha256$FeC09F6I$9d1a99a17d09911c5bdd36416b371a6768da45d0fc98bc65c4a7d7321edbe4ce
3|Djou|sha256$hyyp0JDx$04cf4782a1cbc69483c0ae1224db0bebf13f499c01dac0c0d6db7e12783ab08e
```

Figure 54: la table SQLite.

Pour mieux comprendre le fonctionnement de notre application on a décidé de réaliser un diagramme de cas d'utilisation

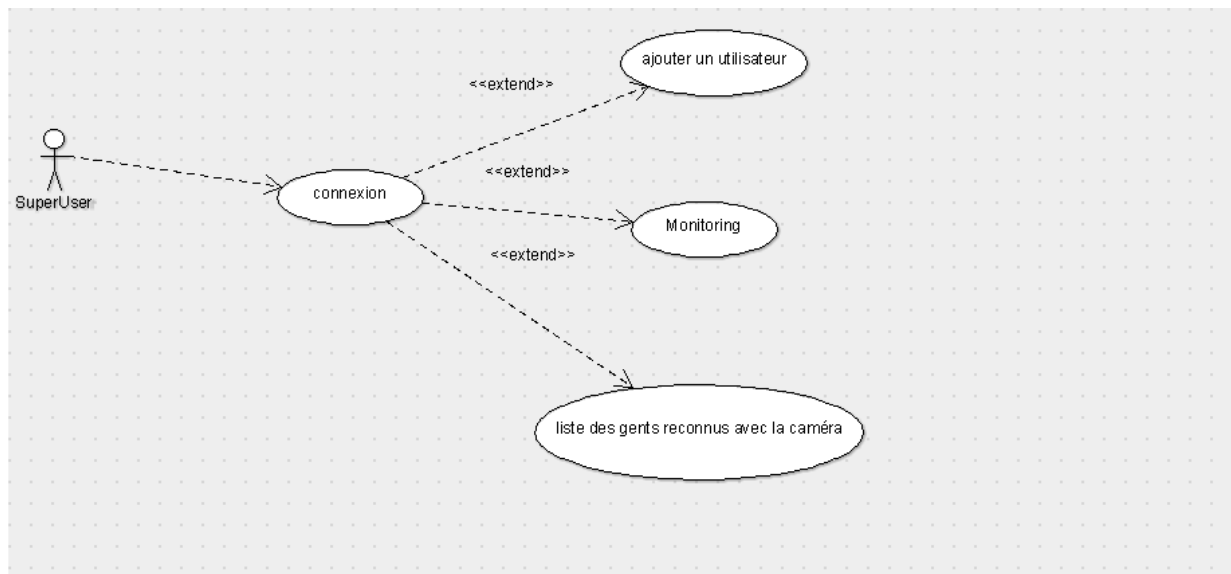


Figure 55 : diagramme de cas d'utilisation.



: Acteur

Acteur	Tâche
SuperUser	T1 : se connecter
	T2 : ajouter un utilisateur
	T3 : surveiller ses équipements (monitoring)
	T4 : voir la liste des gens reconnus avec la caméra

Tableau 2 : Les taches des cas d'utilisation

Une fois l'utilisateur connecté, celui-ci peut effectuer les tâches citées ci-dessus.

1. MONITORING :

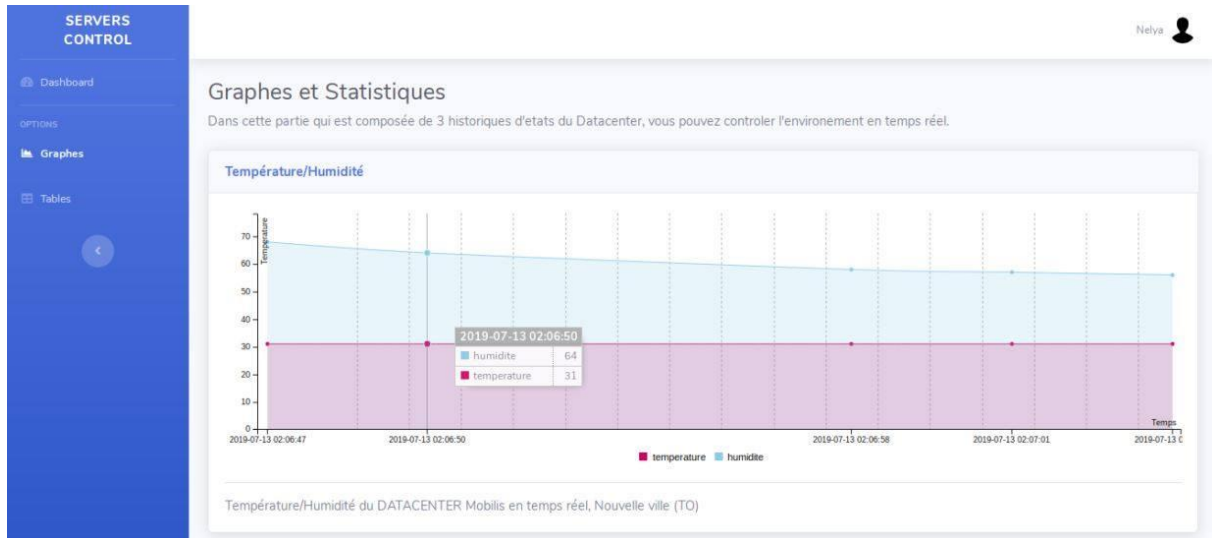


Figure 56: Transformation des valeurs de la température et de l'humidité en un graphe

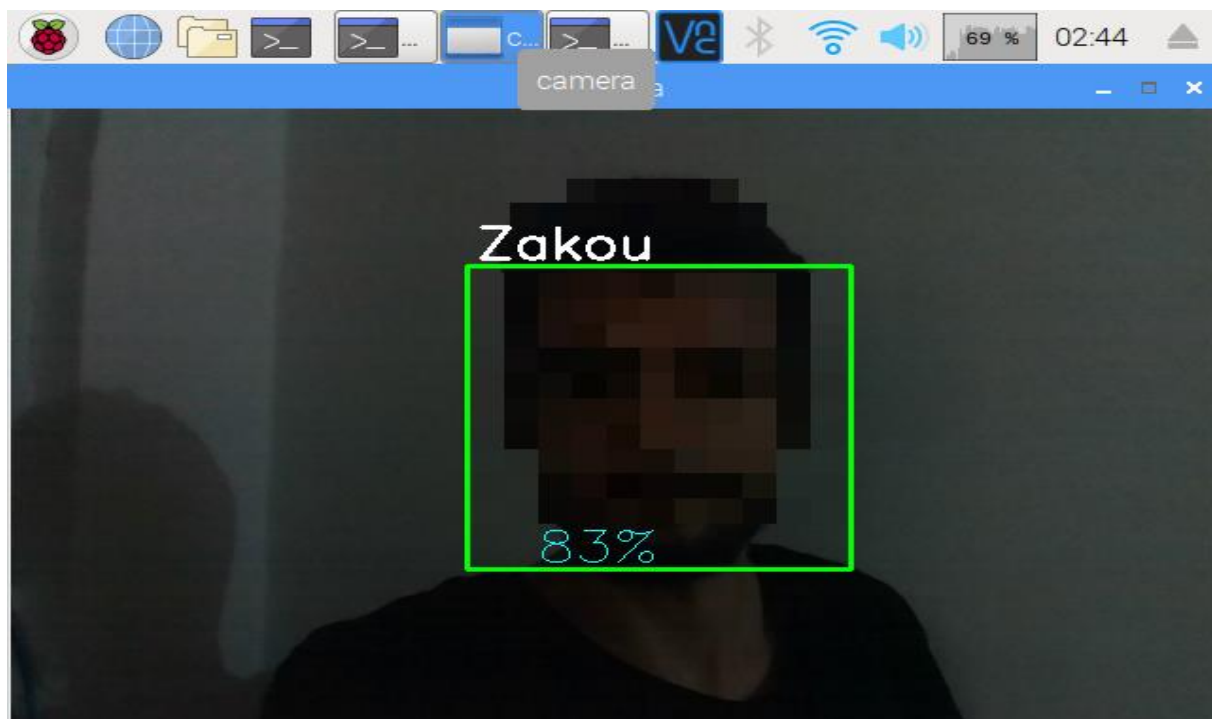


Figure 57 : Reconnaissance faciale avec caméra rev 1.3

SERVERS CONTROL

Nelya

Liste des personnels

Cette liste affiche les personnes ayant procédé à la reconnaissance faciale pour l'accès au DataCenter, elle se mettera automatiquement à jour avec les informations sur la personne

Liste des personnes

Heure	Nom et prénom
13/07/2019 20:00	Madjid -B
13/07/2019 20:13	Omar -B

Developement © Djouher/Zak 2019

Figure 58 : Enregistrement du nom de la personne reconnue

CONCLUSION Gnérale

Ce travail a été principalement axé sur l'implémentation de plusieurs solutions sécurisées dans une architecture d'un Data center. L'objectif de ce travail consiste en le déploiement d'une politique de monitoring et de contrôle au sein d'un datacenter en explorant de nouvelles technologies qui assurent le bon fonctionnement du Datacenter en facilitant le contrôle et le monitoring, telles que le contrôle d'accès au centre à l'aide de la reconnaissance faciale, le contrôle des grandeurs physiques grâce aux schémas et aux statistiques réalisés par EON (Le projet lancé par PubNub).

Pour mener à terme notre application, nous avons donné un aperçu général sur l'IoT, le Data center, le Cloud Computing, l'IA, le Machine Learning, le Deep Learning, la reconnaissance faciale + une annexe sur les généralités sur les capteurs. En plus de tout ça, nous avons présenté brièvement l'architecture de l'organisme d'accueil « **MOBILIS TO** », afin de cerner la problématique, ce qui nous a permis d'en tirer les objectifs de notre Système.

La réalisation de ce projet était une occasion pour nous d'emprunter de nouveau chemins dans le monde complexe de l'informatique :

- Ce stage nous a permis de mettre en pratique et de consolider les connaissances acquises durant notre cursus universitaire et de nos recherches personnelles.
- L'implémentation de notre système, nous a été un moyen de cerner aussi des connaissances pratiques qui nous étaient inconnues auparavant.
- Grâce à ce travail, nous avons pu nous familiariser avec le monde du travail en entreprise car connaître les pressions et les occupations des employés nous donnent l'opportunité de nous préparer psychologiquement pour faire face à cette réalité.

Cette expérience enrichissante représente pour notre future professionnel un atout majeur auquel on ne manquerait pas de nous référer.

Nous espérons que ce modeste travail sera d'un grand intérêt pour les futurs utilisateurs et qu'ils y trouveront satisfaction.

BIBLIOGRAPHIE ET WEBOGRAPHIE

BIBLIOGRAPHIE

- ❖ Mémoire Master réalisé par Mr : Bouharoua Abderrahim et Mr : Boukeli Hacene Mohammed Imad de l'université de Tlemcen qui a pour thème : Automatisation d'une maison intelligente Via une application Android.
- ❖ Thèse Doctorat, réalisée par Mr : Elodie Morin de l'université de Grenoble Alpes, qui a pour thème : Interopérabilité de protocoles de communication adaptatifs basse-consommation pour des réseaux de capteurs.
- ❖ Livre sur L'Internet des objets « *Deux technologies clés : les réseaux de communication et les protocoles* » de Jean-Pierre Hauet.
- ❖ Livre Blanc 102 sur « le contrôle physique des menaces dans un datacenter » de Christian Cowan et Chris Gaskins.
- ❖ Livre sur le « Monitoring d'un Datacenter du concept à la réalisation » de Norbert Andrey.
- ❖ Mémoire de fin de Cycle Master 2 Informatique Professionnel Option : ASR Administration et Sécurité des Réseaux réalisé par Mr : Hijeb Ali qui a pour thème : implémentation d'un protocole d'élections d'un serveur d'authentification dans l'internet des objets.

W E B O G R A P H I E

- ❖ www.cisco.com/c/fr_fr/solutions/data-center-virtualization/what-is-a-data-center.html
- ❖ <https://www.cisco.com/c/dam/assets/global/FR/offers/sc10/secure-dc-wp/pdfs/sc-10-5-steps-wp-fr.pdf>
- ❖ <https://lipn.univ-paris13.fr/~gerard/uml-s2/uml-cours04.html>
- ❖ www.developpez.com
- ❖ www.openclassroom.com
- ❖ <https://www.sunbirdcim.com/what-data-center-monitoring>
- ❖ <https://pandorafms.com/blog/data-center-monitoring/>
- ❖ https://syntec-numerique.fr/sites/default/files/Documents/livre_vert_vol.5_datacenters_etat_de_lart_et_perspectives.pdf
- ❖ <https://www.memoireonline.com/04/12/5604/Monitoring-dune-infrastructure-informatique-sur-base-doutils-libres.html>
- ❖ <https://www.memoireonline.com/04/12/5604/Monitoring-dune-infrastructure-informatique-sur-base-doutils-libres.html>
- ❖ <https://cloudcomputing-world.com/cloud-datacenter-des-march>
- ❖ <https://cloudcomputing-world.com/cloud-datacenter-des-march>
- ❖ <http://www.leparisien.fr/economie/business/data-centers-mais-ou-se-trouvent-vos-donnees-20-02-2017-6694767.php>
- ❖ https://www.lemonde.fr/pixels/article/2016/06/03/les-datas-du-grand-froid_4932566_4408996.html
- ❖ <https://www.1min30.com/dictionnaire-du-web/datacenter>
- ❖ <https://searchitoperations.techtarget.com/tip/Data-center-monitoring-system-considerations>

ANNEXE

LES CAPTEURS

A.INTRODUCTION

Dans de nombreux domaines (industrie, recherche scientifique, services, loisirs...), on a besoin de contrôler des paramètres physiques (température, force, position, vitesse, luminosité...). Le capteur est l'élément indispensable à la détection de ces grandeurs physiques. Un capteur est un organe de prélèvement d'informations qui élabore à partir d'une grandeur physique, une autre grandeur physique de nature différente (souvent électrique). Cette grandeur représentative de la grandeur prélevée est utilisable à des fins de mesure ou de commande.

B.DEFINITION

Un capteur est un organe de prélèvement d'informations qui élabore, à partir d'une grandeur physique, une autre grandeur physique de nature différente (généralement électrique) représentative de la grandeur prélevée, et utilisable à des fins de mesure.

C.REPRESENTATION FONCTIONNELLE

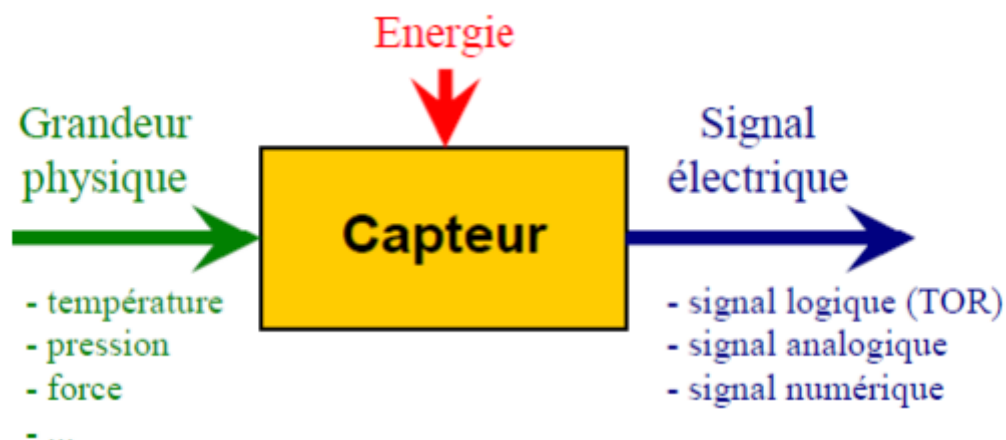


Figure 59: Représentation fonctionnelle d'un capteur

D.ROLE DU CAPTEUR

Parmi les informations de toutes natures issues de notre environnement, on distingue les grandeurs physiques associées à des événements climatiques, géométriques ou encore lumineux ou temporels. Le rôle du capteur est de rendre exploitable ces différentes grandeurs physiques en vue de leur traitement ultérieur.

- Mesure de présence : indique la présence d'un "objet" à proximité immédiate.
- Mesure de position, de déplacement ou de niveau : indique la position courante d'un objet animé d'un mouvement de rotation ou de translation.
- Mesure de vitesse : indique la vitesse linéaire ou angulaire d'un "objet".
- Mesure d'accélération, de vibrations ou de chocs.
- Mesure de débit, de force, de couples, de pressions.
- Mesure de température, d'humidité.

E.ELEMENTS CONSTITUTIFS D'UN CAPTEUR

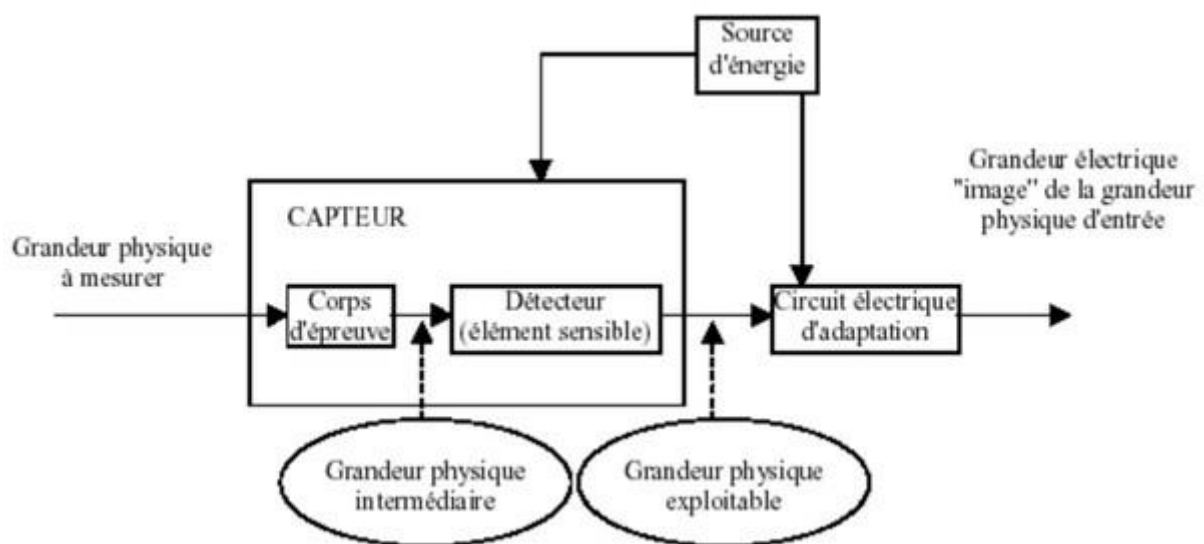


Figure 60 : éléments constitutifs d'un capteur

F. CLASSIFICATIONS DES CAPTEURS :

On peut classer les capteurs en 3 groupes en fonction de la nature de l'information délivrée en sortie :

- ❖ **Les capteurs analogiques** : Dans la pratique industrielle, on donne à ce type de matériel le nom de capteurs. Type de signal de sortie : 0 – 10V ou 4 – 20mA.
- ❖ **Les capteurs numériques** : Souvent nommés codeurs ou compteurs. Type de signal de sortie : 0011 ou 0001.
- ❖ **Les capteurs logiques ou Tout Ou Rien (TOR)** : Ils portent le nom de détecteurs. Type de signal de sortie 0V ou 5V

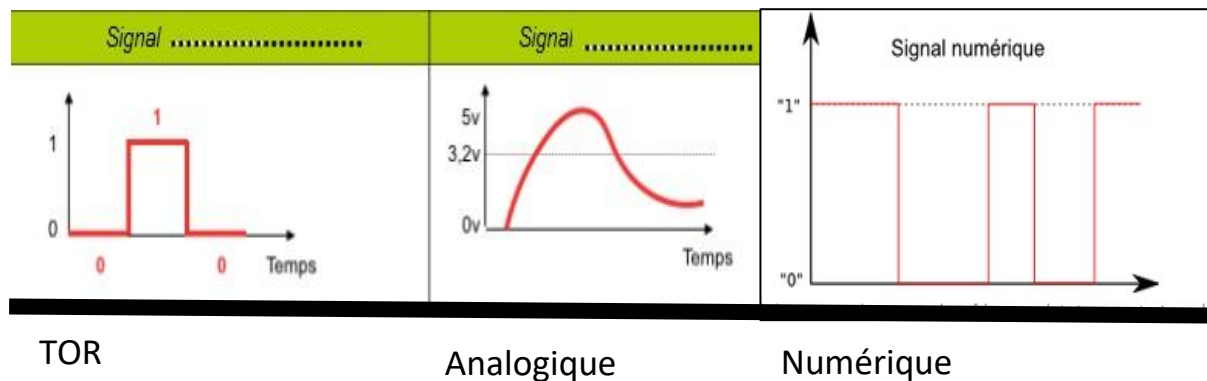


Figure 61: classification des capteurs

G.LISTE DES CAPTEURS LES PLUS FREQUENTS

LES CAPTEURS LES PLUS FREQUENTS	
NOM DU CAPTEUR	DESCRIPTION
	Très sensible aux rayons infrarouges de 750 à 1100 nm, le capteur de flamme permet de détecter une flamme devant lui. Pratique pour les applications de sécurité par exemple.

Capteur de flamme	
	Permet de connaître la pression ambiante et l'altitude. Ce type de capteur permet également de calculer la température.
Capteur d'altitude et de pression	
	Permet d'obtenir une sortie binaire pour savoir si un son est présent ou non et d'analyser son amplitude.
Capteur de son	
	Détecte la couleur des objets. Multiples applications de reconnaissances et de commande. Exemple : un robot qui réagit en fonction de la couleur des objets qu'on lui présente
Capteur lumière RGB	

 <i>Capteur d'angle</i>	Ne payez pas ce capteur plus de 1€, il s'agit en réalité d'un potentiomètre... Il permet néanmoins de savoir précisément un angle en calculant sa résistance. C'est le principe de tous les boutons qui se tournent
 <i>Capteurs de gaz</i>	Au pluriel car il existe beaucoup de capteurs différents pour les gaz : Méthane, Butane, LPG, Ethanol, fumée, hydrogène, monoxyde de carbone, CO2, Ozone, qualité de l'air ... Les plus connus sont les MQ.
 <i>Capteur d'obstacles et de proximité</i>	Ce capteur émet en permanence une lumière infrarouge et analyse la lumière renvoyée par les objets. Lorsqu'un objet se rapproche, il renvoie plus de lumière et le capteur le détecte. Avec ce petit capteur vous pouvez diriger un robot, donner des croquettes à votre chien quand il pointe le bout de sa truffe



Module RFID

Traçabilité, antivols, carte d'accès...Les tags RFID sont partout !

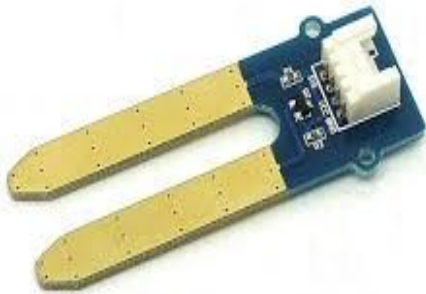
L'identification par radiofréquence consiste à échanger des données à très courte distance entre un lecteur et un tag RFID. S'ils sont autant utilisés, c'est notamment parce que seul le lecteur a besoin d'une source d'énergie pour fonctionner : le lecteur est composé d'un bobinage qui va générer un champ magnétique et alimenter le tag par induction. Chaque tag possède une micro puce radio capable d'émettre un numéro d'identification UID unique ainsi qu'une petite mémoire de quelques ko.

Le module le plus utilisé est le RC 522 car il est très peu cher. Il existe de super librairies qui permettent de lire facilement ces tags avec un microcontrôleur.



Capteur de pulsations

Placés au bon endroit sur le corps, ces capteurs permettent de capter les pulsations du cœur.

 <i>Capteur musculaire</i>	Ce capteur filtre et redresse les signaux électriques de nos muscles. Permet de contrôler des objets avec ses muscles en passant par un Arduino. Il suffit de placer les "patches" sur ses bras par exemple.
 <i>Ultrason</i>	Le capteur ultrason est un capteur de distance. Il comporte un émetteur et un récepteur d'onde et permet de calculer la distance d'un objet en face de lui en comparant les temps d'émission et de réception de l'écho (en connaissant la vitesse de propagation du son). Le modèle HC-SR04 (moins de 3€...) est précis à 3mm près sur une ouverture de 30° : relativement imbattable.
 <i>Capteur d'humidité des sols</i>	La conductivité entre les deux broches de ces capteurs est proportionnelle à l'humidité des sols dans lesquels on les plante. Pratique pour savoir quand arroser ses plantes.

 Accéléromètre	Les accéléromètres sont souvent une combinaison de gyroscopes (qui permettent de détecter la rotation) et d'accéléromètres (qui permettent de détecter l'accélération). Ils ont plus ou moins de "degrés de liberté" ce qui définit le nombre de directions pour lesquelles ils peuvent détecter une accélération. Ils sont utilisés pour de multiples applications : construire un objet qui s'équilibre seul (type segway), contrôler des objets avec des mouvements (des gants qui font de la musique), calculer une vitesse.
 Capteur IR suiveur de ligne	Fonctionne de la même manière que le capteur d'obstacles (en analysant sa propre lumière renvoyée). Ce capteur est utilisé sur certains robots pour suivre des tracés prédéfinis

Tableau 3 : Liste des capteurs les plus fréquents.

