**Introduction :**

Au cours de ces dernières années, la technologie a transformé la façon de faire des affaires sous pratiquement toutes ses coutures. Elle nous a libérés de notre bureau. Elle a rendu possible le télétravail. Elle nous a appris que la seule constante c'est le changement. L’internet des objets constitue un des changements récents qui a radicalement transformé le fonctionnement des entreprises tels que les restaurants où les employés gèrent le programme de salubrité alimentaire en mesurant manuellement trois fois par jour la température des aliments conservés et préparés. Ainsi au parc de véhicules un camion dont le moteur tourne au ralenti pendant une heure consomme 4 litres de carburant environ 20 dollars par jour ou 7300 dollars par année on devait penser sérieusement à réduire voire éliminer ces coûts. Grâce à l’internet des objets aujourd’hui les propriétaires de restaurants et d'autres entreprises de service alimentaire peuvent utiliser des objets intelligents pour surveiller automatiquement les températures et les propriétaires de parc de véhicules peuvent suivre leurs véhicules en temps réel et réduire les périodes de fonctionnement au ralenti et assurer la vie de leurs chauffeurs.

**Définitions :**

On peut distinguer plusieurs définitions proposées par des compagnies informatiques diverses qui ont une relation avec l’Internet, la technologie et la communication, vis-à-vis la connectivité à Internet, l’infrastructure ou la connexion entre les différents objets intelligents. Parmi ces définitions on peut citer :

* **IEEE**:(Institute of Electrical and Electronics Engineers) «The IoT is an intelligent network which connects all things to the Internet for the purpose of exchanging information and communicating through the information sensing devices in accordance with agreed protocols. It achieves the goal of intelligent identifying, locating, tracking, monitoring, and managing things» **[1]**
* L'IoT est un réseau intelligent qui connecte tous les objets à Internet dans le but d'échanger des informations et de communiquer via les dispositifs de détection d'informations conformément aux protocoles convenus. Il atteint l'objectif consistant à identifier, localiser, suivre, surveiller et gérer intelligemment les choses
* **ITU**:(International Telecommunication Union) « Internet of things (IoT) is a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies. **» [2]**
* Une infrastructure mondiale pour la société de l'information qui fournit des services avancés en interconnectant des éléments (physiques et virtuels) basés sur des technologies de l'information et de la communication interopérables
* **ETSI :** (European telecommunications standards) « les communications de machine à machine peuvent être définies comme la communication entre des entités (plus d'une) qui ne nécessite pas d'intervention manuelle / humaine. ils sont indépendants, c'est l'automatisation qui permet aux machines de prendre leurs propres décisions sans intervention manuelle » [3]
* **IETF :**(Internet Engineering Task Force) “A world-wide network of interconnected objects uniquely addressable based on standard communication protocols ”. [3]
* Un réseau mondial d'objets interconnectés adressables de manière unique sur la base de protocoles de communication standard
* **CCSA: (**[China Communications Standards Association](https://en.wikipedia.org/wiki/China_Communications_Standards_Association)**)** “a network, which can collect information from the physical world objects through various deployed devices with capability of perception, computation, execution and communication, and support communications between human and things or between things by transmitting, classifying and processing information”. [4]
* un réseau, qui peut collecter des informations à partir des objets du monde physique par le biais de divers dispositifs déployés avec une capacité de perception, de calcul, d'exécution et de communication, et prendre en charge les communications entre l'homme et les objets ou entre les objets en transmettant, classant et traitant des informations
* **CASAGRAS: (Coordination And Support Action for Global RFID-related Activities and Standardisation)** “a global network infrastructure, linking physical and virtual objects through the exploitation of data capture and communication capabilities” [5]
* une infrastructure de réseau mondial, reliant des objets physiques et virtuels grâce à l'exploitation de capacités de capture de données et de communication

D’autre part, on peut simplement dire que l’internet des objets est un réseau connecté à Internet qui regroupe tous les objets (intelligents ou transformés en intelligents) pouvant être connectés entre eux et avec d’autres systèmes connectés à Internet. Cela nous emmène vers la liaison des services à travers la communication sur Internet

**La transformation d’un objet traditionnel à un objet intelligent :**

Un objet dans l’internet des objets, peut-être une personne avec un implant de moniteur cardiaque ou même une automobile qui a des capteurs intégrés pour alerter le conducteur de la distance qui sépare la voiture des autres objets qui l’entourent ou bien tout un autre objet naturel ou artificiel ayant les propriétés suivantes :

L’identifiant : le fait qu’un objet ait un identifiant cela signifie qu’il possède une adresse IP unique de la version v6 du protocole IP propre à lui-même.

Les détecteurs : à travers un ou plusieurs capteurs**,** l’objet intelligent peut rassembler des informations et des changements dans son environnement afin de les envoyer.

L’intelligence : un objet intelligent peut prendre des décisions vis-à-vis les données détectées et rassemblées en lui intégrant des moteurs d’inférence avec une capacité de calcule adéquate.

La sécurité : les objets communiquent via le réseau Internet donc on doit sécuriser les données partagées des attaques et virus avec les méthodes de protection des réseaux et des données.

L’économie d’énergie : un objet intelligent doit consommer une énergie minimale pour qu’il puisse fonctionner pendant une longue durée car on suppose toujours qu’il fonctionne d’une manière permanente et parfois loin de sa source d’énergie.

Le cout minimal : car on a besoin d’une abondance d’objets intelligents pour maximiser le nombre des objets connectés.

La connexion à Internet : pour pouvoir communiquer avec les autres objets intelligents et l’environnement.

La bonne qualité : pour s’assurer que son environnement n’affecte pas sur son traitement d’informations afin de pouvoir se confier aux données et décisions qu’il nous offre.

**Les composants d’un système Iot :**

L’internet des objets est une composition de technologies logicielles et matérielles utilisées dans le but de sauvegarder, extraire, traiter des données en plus de les échanger entre deux ou plusieurs entités. Un système Iot typique doit se composer fondamentalement des parties suivantes :

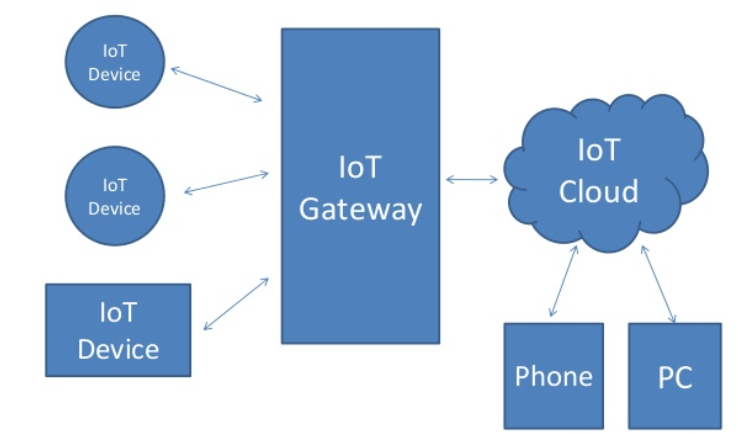
* Les appareils : « chaque appareil possède un ou plusieurs capteurs pour détecter le paramètre environnemental et les envoyer à une plateforme. »[6]. En plus de sa fonction principale, chaque appareil est sensé collecter les informations des autres appareils comme de l’environnement pour les sauvegarder ou les transmettre à une plateforme cible.
* La connectivité à Internet : « le responsable de la connexion des appareils à Internet pour pouvoir se connecter à la plateforme en ligne. Le wifi est l’une des méthodes de connectivité Internet les plus populaires »[6]
* La plateforme Iot : « la plateforme Iot est un logiciel hébergé en ligne. Vous pouvez le considérer comme un réseau auquel tous les appareils sont connectés. La plateforme est suffisamment intelligente pour collecter les données des appareils, analyser, traiter et prendre des décisions en fonctions de ces données. »[6]

Plus précisément une plateforme Iot est responsable de : «

1. Connexion des appareils à une zone en ligne spécifique.
2. Collecte des données reçues des appareils.
3. Surveillance, stockage, traitement, analyse et calcul de ces données.
4. Prendre des décisions sur la base d’un seuil préétabli des données traitées.
5. Travailler avec différents protocoles d’échange de données.
6. Intégration avec des applications (services en ligne, application web, applications mobiles...etc.). »[6]

* Les applications : « L'application est l'interface entre l'utilisateur et la plateforme. Ainsi, chaque fois que l'utilisateur souhaite surveiller, configurer ou contrôler un appareil, il interagit avec l'application. »[6] . Il s’agit d’un ou plusieurs points d’accès aux données, destinés aux utilisateurs finaux. Ces derniers peuvent aborder à l’aide d’un ordinateur, un téléphone ou même une application web

**L’architecture d’un système Iot :**

****

[https://www.slideshare.net/neeveehariharan/internet-of-things-architecture-topology](https://www.slideshare.net/neeveehariharan/internet-of-things-architecture-topologyv) visité le (02/2020)

Par convention, les projets de l’internet des objets n’adoptent pas une architecture formellement identique, néanmoins il est possible de schématiser le parcours suivi de la donnée avec une architecture générale d’un système iot composée de plusieurs niveaux qui communiquent entre eux pour relier le monde physique et le monde virtuel et qui sont présentés comme suit :

capteurs ils convertissent les grandeurs physiques analogiques en signaux numériques qui seront envoyés via le canal de transmission (Gateway) au cloud dans lequel se fait le stockage des données énormes émises par les appareils, les capteurs, les applications ou les smart phones d’une manière non prédictible. Les terminaux par la suite facilitent les interactions pour les utilisateurs non -experts en présentant les informations d’une façon simple et compréhensible.

Couche des appareils (Iot device layer) : Cette couche principale comprend des objets interconnectés sous forme d’appareils intelligents contenant des capteurs et actionnaires. Ces derniers peuvent être connectés avec ou sans fil avec une communication bidirectionnelle via leur correspondante passerelle ou Système d'acquisition de données (DAS). Ils peuvent se reconnaitre, collecter et échanger des informations ainsi que collaborer en temps réel d’où chacun d’eux est défini comme suit :

**Capteur (Sensor) :** c’est unappareil qui peut mesurer des grandeurs physiques analogiques depuis son environnement puis les convertir en données qui peuvent être interprétées par un humain ou bien une machine comme signaux numériques. Un capteur peut collecter des paramètres physiques et détecter d’autres objets intelligents dans leur environnement.

**Actionnaire (Actuator)** : c’est une partie de la machine qui est responsable du déplacement et le contrôle d’un mécanisme ou d’un système. Cette partie peut aussi transformer les données générées par les objets intelligents en action physique.

Couche passerelle Iot (Iot gateway layer): au niveau de cette couche la responsabilité se pose sur la transmission des données via Wi-Fi, des réseaux locaux câblés ou par Internet pour un traitement ultérieur. La passerelle prend en charge la sécurité de ces données à l’aide des outils de cryptage appropriés, ça pourra ainsi empêcher les fuites des informations dans la plateforme Iot dans le but de réduire le risque d’attaques extérieures malveillantes sur les appareils Iot.

Couche de traitement des données (data processing layer): cette couche est sensée s’occuper du stockage, analyse et traitement d’une énorme quantité de données à l’aide de puissants moteurs d’analyse de données (data analytics engines) et de mécanismes d’apprentissage automatique (machine learning). Pour un bon fonctionnement plusieurs technologies sont utilisées telles que les bases de données, le cloud computing et les modules de traitement de données volumineuses (big data).

Application layer: cette couche est responsable de fournir les services spécifiques à l’application aux utilisateurs grâce aux terminaux tels que les smartphones, les ordinateurs et les applications web qui suite facilitent les interactions pour les utilisateurs non -experts en présentant les informations d’une façon simple et compréhensible.

* 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.

**Les avantages de l’Internet des objets :**

Les organisations de divers secteurs utilisent l’internet des objets pour fonctionner plus efficacement, mieux comprendre les clients pour offrir un service client amélioré ainsi qu’améliorer la prise de décision et augmenter la valeur de l’entreprise grâce aux avantages munis par cette révolution technologique dont on peut noter :

* Représenter un lien inévitable entre le monde numérique et le monde physique.
* Une réduction énorme des dépenses en optimisant les ressources et contrôlant l’excès.
* Assistance aux activités professionnelles et personnelles.
* Le contrôle des systèmes et leurs traitements par les utilisateurs avec une grande précision avec des interventions manuelles minimales ou nulles.
* La sensation de la sécurité grâce à la grande quantité de données détectée et assemblée à grande vitesse par les capteurs et prévenir en cas de danger prévu.
* Gagner du temps et d’efforts puisque le contrôle des appareils et des systèmes peut être réalisé à distance.
* Augmenter le rendement des appareils en diminuant les interventions de l’être humain sur les systèmes.
* Améliorer le niveau de vie humaine dans le but de pouvoir opter pour une vie de commodité et confort.
* Augmenter la disponibilité des systèmes en prévenant du danger.
* L’apparition de nouvelles opportunités de travail avec le besoin des nouvelles technologies et des nouveaux services.

**Les inconvénients de l’Internet des objets :**

Comme toute technologie inventée par l’être humain l’internet des objets a apporté de nombreux avantages dans plusieurs domaines malgré ça les objets sont exposés à de nombreux types de menaces qui peuvent causer des types de dommages spécifiques aux entreprises et aux consommateurs dont on peut citer :

* Encourager la dépendance à la technologie résulte l’inactivité humaine engendrant des problèmes physiques et psychiques chez l’homme.
* Perdre la confidentialité des données personnelles en cas d’attaques par pirates par suite du nombre important d’appareils connectés et les informations partagées entre eux.
* L’accès à Internet par les objets fait appel à beaucoup de vulnérabilités concernant la sécurité des systèmes.
* Les entreprises qui fabriquent et distribuent des appareils IoT grand publique pourraient utiliser ces appareils pour obtenir et vendre les données personnelles des utilisateurs.
* Comme il n’y a pas de norme internationale de compatibilité pour l’iot, il est difficile pour les appareils de différents fabricants de communiquer entre eux.
* Le taux de chômage s’élève car les machines font presque tout avec plus d’efficacité.
* S'il y a un bogue dans le système, il est probable que chaque appareil connecté soit corrompu.

**Les domaines d’application des Iots :**

Il existe de nombreuses applications Iot potentielles pénétrées dans la vie quotidienne de différents utilisateurs d’où des individus, des entreprises et de toute la société dans de nombreux domaines d'application divers tels que :

* **Ville intelligente :** circulation routière intelligente, collecte des déchets
* **Environnement intelligent :** prédiction des séismes, détection d’incendies
* **Sécurité et gestion des urgences :** radiations, attentats, explosions
* **Logistique :** suivi en temps réel de la localisation, la température, l’humidité et la vibration
* **Contrôle industriel :** prédiction des pannes, dépannage à distance.
* **Santé :** suivi des paramètres biologiques.
* **Agriculture intelligente :** lumière, humidité, température.

**Les défis des Iots :**

La révolution de l’internet des objets est une technologie récente développée avec un processus pas-à-pas. Il existe encore des problèmes à résoudre et des failles à éliminer tels que :

* La complexité des systèmes à mettre en œuvre nécessite de grandes compétences.
* La mise en place des mécanismes de sécurité pour affronter les tentatives des pirates.
* L’absence des critères unifiés entre les producteurs et les protocoles.
* L’acceptabilité des objets de l’Internet par les gens.

**Conclusion :**

Nous n’avons prédit ni Internet ni le web ni les réseaux sociaux tel que Facebook et Twitter ni les millions d’applications mobile qui ont tout changé qualitativement dans notre mode de vie quotidienne et celui des sociétés donc il serait juste de dire qu’on ne peut pas prédire exactement comment nos vies vont changer. Néanmoins, notre style de vie pourrait être la supposition de qui que ce soit. En ce qui concerne l’internet des objets on remarque que c’est devenu un outil de confort grâce à une sophistication dans la détection, l’actionnement, les communications, le contrôle, et la création de connaissances à partir d’une grande quantité de données. Cela devrait créer des modes de vie qualitativement différents de ceux d’aujourd’hui. Bien que théoriquement il semble être un mécanisme fascinant, il faut tout d’abord envisager des solutions dans le but diminuer voire éliminer les majeurs problèmes de confidentialité et de sécurité des données pour lesquels beaucoup d’utilisateurs auraient pris la fuite. Il faut sérieusement penser à détecter les vulnérabilités et les menaces de sécurité potentielles et de suggérer des solutions qui peuvent atténuer et aider à adapter au maximum les appareils IoT ainsi adopter les bonnes pratiques d’utilisation de cette technologie.

**Références :**

* [1] J. A. Stankovic, "Research directions for the Internet of Things", IEEE Internet of Things J., vol. 1, no. 1, pp. 3-9, Feb. 2014 disponible sur <https://ieeexplore.ieee.org/document/6851114>.
* [2] Recommandations ITU-T Y.2060 (06/2012). Disponible sur : http://www.itu.int/en/ITU-T/gsi/iot.
* [3] G. M. Lee et al., “The IoT—Concept and Problem Statement,” IETF Standard draft-lee-iot-problem-statement-05, Jul. 30, 2012.
* [4] “Terms of the Ubiquitous Network,” CCSA Standard YDB 062-2011, Mar. 2011.
* [5] I. M. Smith et al., “RFID and the inclusive model for the IoT,” CASAGRAS Partnership Rep., West Yorkshire, U.K., Final Rep., 2009, pp. 10–12.
* [6] <https://1sheeld.com/iot-understanding-concepts>