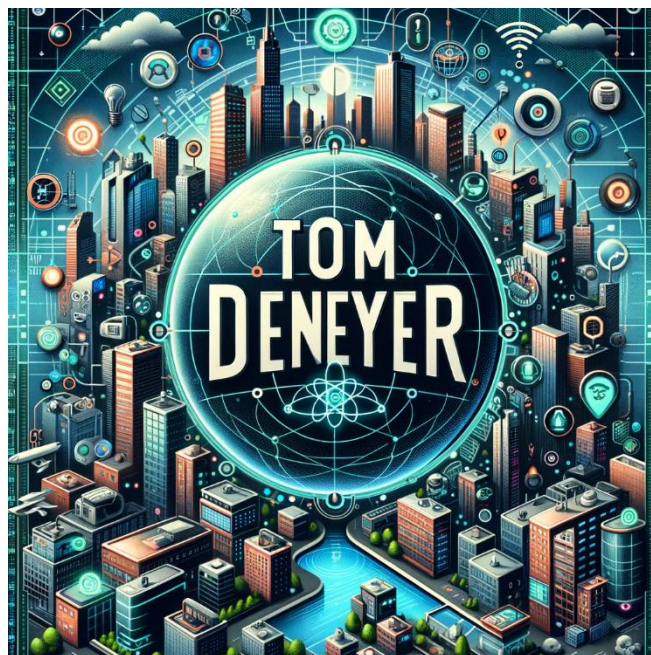


Synthèse

Internet Of Everything

Tom Deneyer

(paypal : tomdeney@gmail.com) lol



IoE

Généralités Internet.....	4
Internet of Things	4
Définition IoT	4
Digitalisation	4
Digitalisation des entreprises	4
Digitalisation des gouvernement	4
Digitalisation des villes.....	5
Réseaux.....	5
Structures	5
Périphériques	6
Types de réseaux	6
Protocoles.....	7
Cloud	7

IBN (Intend-Based Network)	7
IBN avancé.....	8
The Edge	8
Fog Computing.....	8
IoT informations complémentaires	8
Capteurs et Activeurs.....	9
Programmation	9
Peps (gpt4 résumé)	9
Prototypage.....	10
Ressources.....	10
BIG DATA (data ain't the only big thing)	10
5v.....	10
Les challenges.....	10
Solutions	11
Les entreprises et le Big DATA.....	11
Leaks en BIG DATA.....	11
Sources de données	11
Cloud Computing.....	12
Types de clouds	12
Principe.....	12
Comparaison Cloud/Fog.....	13
Data Center	14
Emplacement.....	14
Facteurs importants.....	14
Virtualisation	14
Hadoop	14
Automatisation	14
Technologies avancées.....	15
Blockchain	15
AI	15
Machine Learning	15
Deep Learning	15
Dans L'IOT... ..	15
Sécurité	16
Types de données	16

Hackers.....	16
Sécurité physique/réseau.....	16
Défi de la sécurisation des dispositifs IoT.....	17
Maisons intelligentes.....	17
Transition vers IoE	18
Definition IoE.....	18
Architecture d'approche de l'IOE.....	18
Informations complémentaires.....	19
Lois	19
Data storage	19
Présentations orales	19
Cryptographie / stéganographie	19
Voitures autonomes	20
Cryptage de données + militaire.....	21
OS	21

Généralités Internet

- Le réseau des réseaux. Toile qui relie tous les appareils connecté sur terre, via câbles ou wireless.

Table 1 Four phases of the internet

Phase 1	Phase 2	Phase 3	Phase 4
Connectivity	Networked economy	Collaborative experiences	Internet of everything
Digitise access to information	Digitise business process	Digitise interactions (business and social)	Digitise the world, connecting
<ul style="list-style-type: none"> • email • web browser • search 	<ul style="list-style-type: none"> • e-commerce • digital supply chain • collaboration 	<ul style="list-style-type: none"> • social • mobility • cloud • video 	<ul style="list-style-type: none"> • people • process • data • things

Internet of Things

- Connecte le monde physique au monde réseau, l'utilisation de la digitalisation des objets et leur connexion à la toile internet.
- Les objets « intelligents » sont capables de penser, càd modifier leurs comportements, leurs options etc en fonctions des données qu'ils analysent. S'il y a assez de données ils peuvent **apprendre** et modifier leur propre code.

Définition IoT

- La connections de millions d'objets intelligents à internet qui échangent des données aux autres réseaux ou appareils, qui les utilisent et analysent.

Digitalisation

- (statistique qui date un peu...) 2020 chaque consommateur aura une moyenne de 6.58 appareils connectés intelligents.
- Internet, la digitalisation, IoT, etc augmente de façon **exponentielle**

Digitalisation des entreprises

- Services en ligne, dans tous les domaines. C'est devenu la norme.
- Les données sont utilisées et analysées pour :
 - Déterminer des paternes d'achats
 - Nouvelles tendances
 - Optimiser les productions

Digitalisation des gouvernement

- Données analysées et utilisées pour :
 - Visualiser et gérer l'environnement
 - Prévoir les tendances des populations
 - Prédire la criminalité

- Planifier des services sociaux

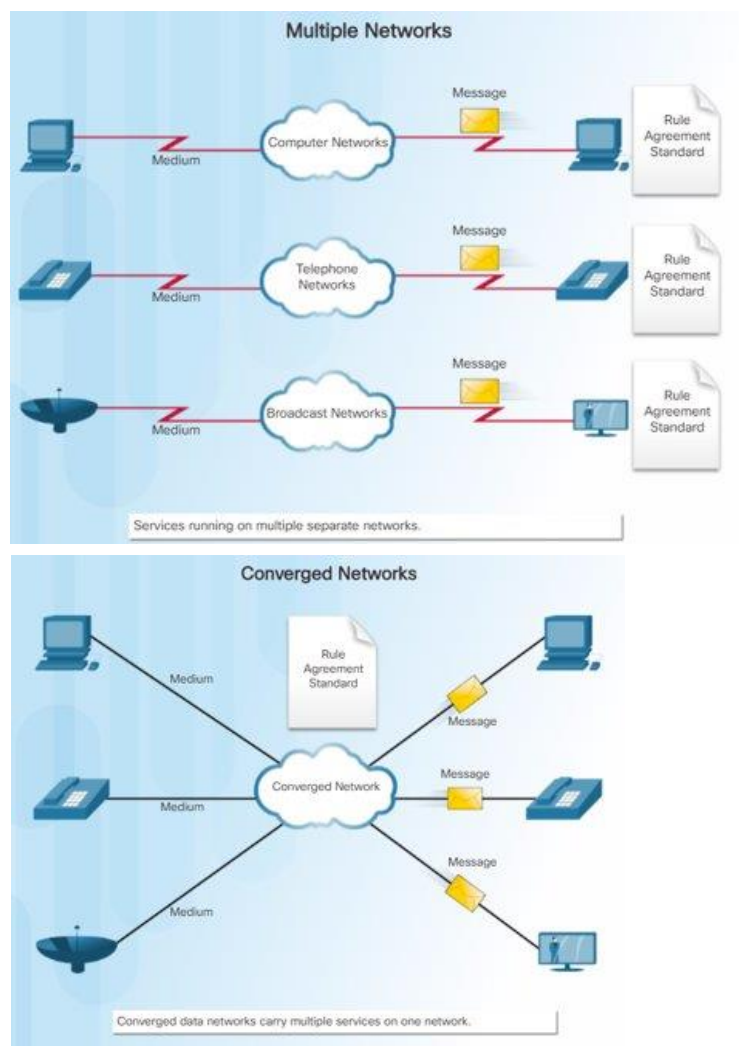
Digitalisation des villes

- Données analysées et utilisées pour ;
 - Contrôler le trafic automobile
 - Visualiser et optimiser les parkings
 - Déployer la police et pompiers plus vite
 - Contrôler les déchets

Réseaux

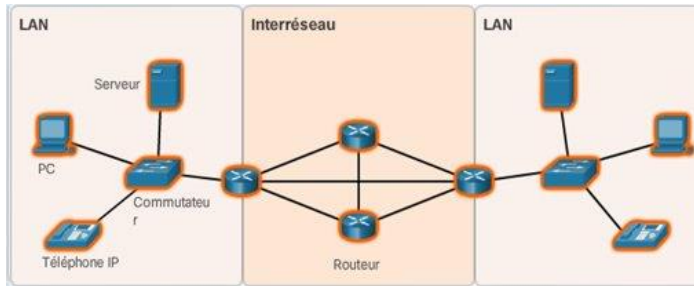
Structures

- Multiple (lignes téléphonique, Tv et réseau sont séparés)
- Convergent (toutes les lignes passent dans un seul système avec des normes, et protocoles qui sont en approuvés)

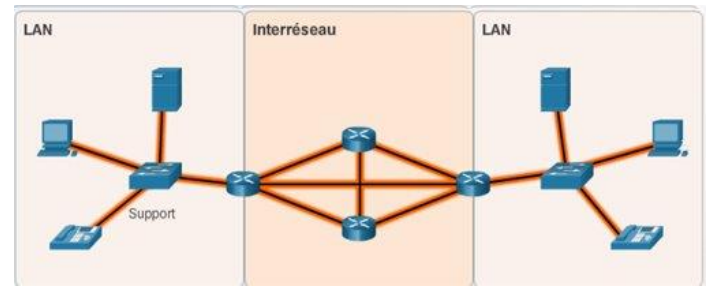


Périphériques

Périphériques (finaux et intermédiaires)¹



Supports (câbles, et Wireless)²

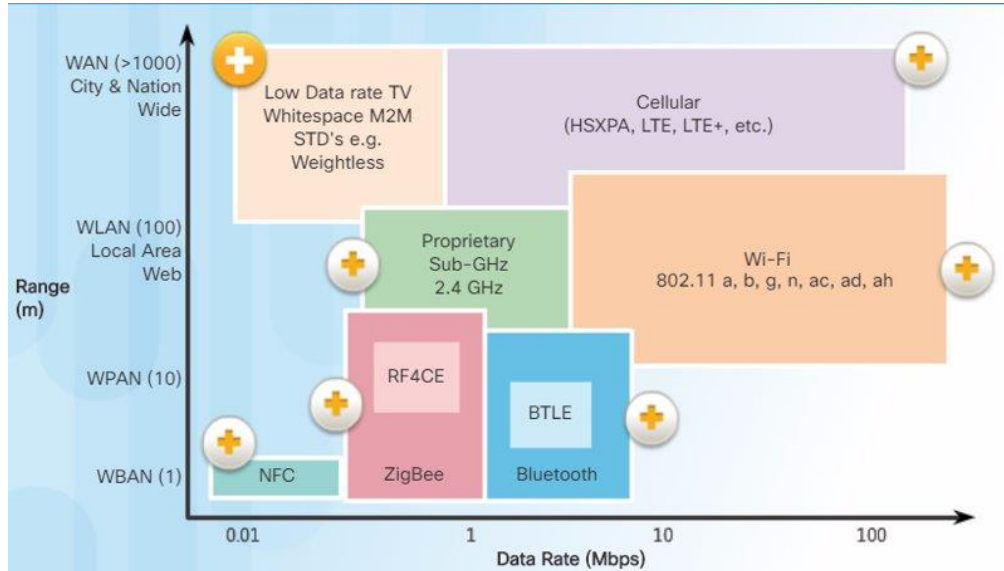


- 1) Finaux : Pc, laptops, téléphones, caméras, capteurs, ...
intermédiaires : switchs, routeurs, firewalls, ...
- 2) Câbles cuivre, optiques (plastique ou verre), wireless (ex 802.11 wifi)

Types de réseaux

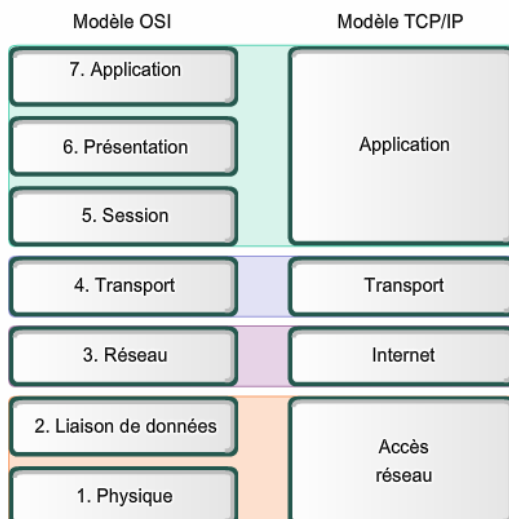
- PAN (personal Area Network)
Distance : faible (quelques centimètres à quelques mètres)
Débit : assez limité ➔ *quelques Mbit/s MAX*
Exemples : Bluetooth, Zigbee(domotique), Nfc. (tous des standards low power) ➔ IEEE802.15
- LAN (Local Area Network)
Distance : un département ou bâtiment
Débit : assez élevé
Exemple : Wifi (IEEE 802.11)
- MAN (Metropolitan Area Network)
Distance : Une ville, donc grande.
Débit : assez limité car utilisation de norme basse énergie ex Wimax, 802.16
- WAN (Wide Area Network)
Distance : très grande, voir "worldwide"
Débit : assez élevé, cela dépend des normes.
Exemple : Cellular (téléphone), LTE, UMTS...
- Internet
Distance : définit par la toile comme tout autour du monde. Réunion de tous les réseaux
Pas de propriétaire, cela est pour tout le monde.
- Les réseaux qui -commencent par « w » comme wPAN, wLAN, wWAN, etc. Sont des réseaux sans fils.

- Weightless = low power ex tv, NFC = carte bancaire, Zigbee = domotique...



Protocoles

- TCP/IP ou OSI. Voir synthèse Télécom car flemme de tout remettre ici...



Cloud

- Ensemble de Data Centers, de groupes de serveurs connectés.
- Utilisé pour des services en lignes, backups, organisations et accès de fichiers, etc...

IBN (Intend-Based Network)

- Software qui permet de modifier et gérer un réseaux facilement, basé sur les intentions de l'utilisateur, exemple : vouloir donner l'accès seulement à certains logiciels pour un ensemble d'utilisateurs dans un réseau et le logiciel modifie les paramètres par lui-même pour s'adapter à la demande.

IBN avancé

- Avec de l'IA, il est possible donc de transformer de simples phrases en l'organisation/configuration d'un réseau. Ou bien même l'auto modification d'un réseau selon les besoins.
Cela s'applique en 3 parties :
 - Assurance (trouver les modifications en permanence, via AI et ML)
 - Translation (passer des modifications à faire en configurations)
 - Activation (configurations apportées au réseau)
- Ex : Cisco DNA

The Edge

- C'est la limite physique d'un réseau. Là où il s'arrête. Ex un pc jusqu'à un routeur. L'Edge c'est le routeur, car après le réseau change.

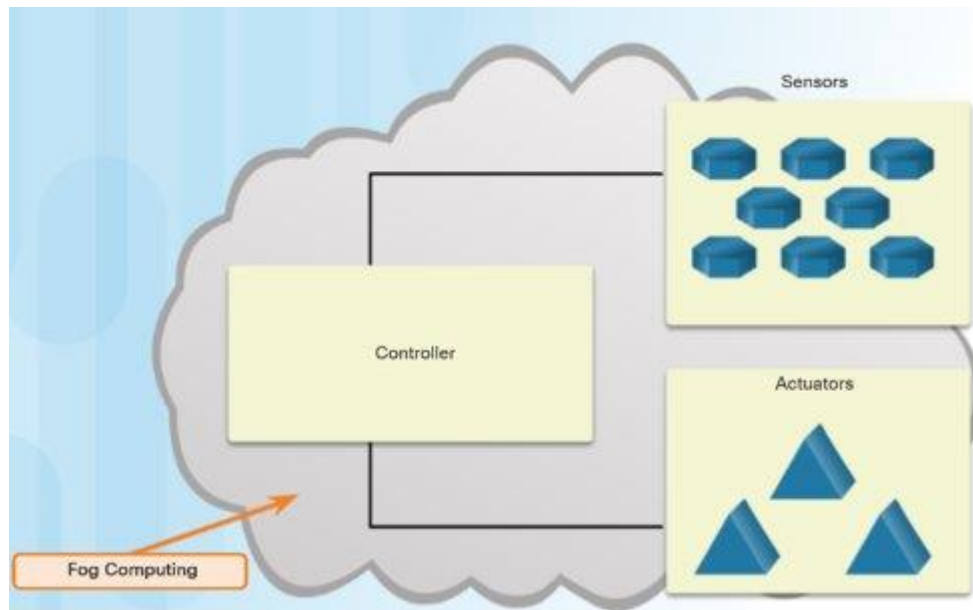
Fog Computing

- Le « FOG » c'est le réseau jusqu'à l'Edge.
- Le principe est de pré-analyser les données de manière locale pour accélérer le processus mis en place. Généralement les données sont utilisées localement et/ou envoyées sur un cloud. La pré-analyse de celles-ci est donc une décentralisation de l'analyse ce qui de 1) Rend moins lourd l'analyse finale sur un cloud et de 2) Permet d'utiliser les données plus rapidement de manière locale.

IoT informations complémentaires

- Les appareils et capteurs qui collectent et partagent les données sont utilisés par des entreprises, villes, gouvernements, hôpitaux et individus dans un but d'optimiser notre monde.
- Un tiers seulement des appareils sont des périphériques finaux utilisés par des humains, les 2 autres tiers sont des capteurs et « activateurs ».

Capteurs et Activateurs



- Dans un fog computing, les capteurs analysent les données qui peuvent entraîner l'activation d'actuateurs qui modifient physiquement quelque chose.
- Les capteurs sont absolument partout, dans les villes, les routes, les maisons, les hôpitaux, les aéroports, etc...

Programmation

Je pars du principe que ce sont des bases de programmation de ma synthèse base de prog, donc pas la peine de mettre dans cette synthèse.



SyntheseProgramma
tionTHTomDeneyer23

Peps (gpt4 résumé)

Les **Python Enhancement Proposals** (PEP) sont une collection de directives et pratiques importantes pour Python. Voici un résumé de trois PEP clés :

1. **PEP 20 - Le Zen de Python** : Il s'agit de principes de conception pour Python, mettant en avant la lisibilité, la simplicité et la clarté. Les principes clés incluent la préférence pour la beauté sur la laideur, l'explicité sur l'implicite, la simplicité sur la complexité, et la valeur de la lisibilité. Il souligne qu'il devrait y avoir une manière évidente de faire les choses.
2. **PEP 8 - Les meilleures pratiques et conventions** : Ce PEP établit des conventions de codage pour assurer la cohérence et la lisibilité du code Python. Les recommandations comprennent la lisibilité du code, le suivi des

conventions d'appellation, l'évitement des espaces inutiles, l'utilisation judicieuse des commentaires et une mise en page cohérente.

3. **PEP 257 - Conventions de docstring** : Il fournit des lignes directrices pour les docstrings dans le code Python, soulignant leur importance pour documenter le code. Il recommande que les docstrings soient clairs, concis et informatifs, avec des conventions spécifiques pour leur rédaction.

Ces PEP sont fondamentaux pour maintenir la qualité et la cohérence du code Python et faciliter la collaboration au sein de la communauté des développeurs.

Prototypage



- Is fully functional, but not fault-proof.
- Is an actual, working version of the product.
- Is used for performance evaluation and further improvement of product.
- Has a complete interior and exterior.
- May be relatively expensive to produce.
- In the IoT, is often used as a technology demonstrator.

Ressources

- Arduino, raspberry Pi, LEGO, Meccano, Imprimantes 3D, etc...

BIG DATA (data ain't the only big thing)

- C'est quoi (FEUR) ?
Lorsqu'une organisation, société ou autre analyse et utilise des données qui respectent certaines conditions, cela est considéré comme BIG DATA, càd les conditions 5v qui suivent ci-dessous.

5v

- Volume (beaucoup de données)
- Velocity (Vitesse, il faut que les données arrivent rapidement)
- Variety (variété, différents types de données)
- Value (valeur, il faut que les données aient une certaine utilité...)
- Veracity (vérité, il faut que les données soient exactes)

Les challenges

- Management (savoir organiser les données à utiliser, ce qui est complexe avec une grande quantité et variance de donnée)

- Sécurité (Pour les entreprises, il faut pouvoir garder les données sécurisées, et accessibles seulement aux personnes, appareils autorisés)
- Redondance (Il faut être certain de ne pas perdre les données, grâce à différentes manières, backups, etc...)
- Analyse (Le big data analyse les données structurées et non structurées, il faut pouvoir les analyser de différentes manières)
- Accessibilité (Il faut pouvoir accéder aux données de n'importe où, n'importe quand, peu importe le nombre de demande d'accès)

Solutions

- Utilisation du FOG COMPUTING, ce qui est donc une décentralisation des processus d'analyse.
- Données sauvegardées sur plusieurs serveurs, data centers... CLOUD

Les entreprises et le Big DATA

- Les entreprises peuvent analyser les données récupérées de leurs clients pour mieux optimiser les ventes, publicités, l'organisation...

Leaks en BIG DATA

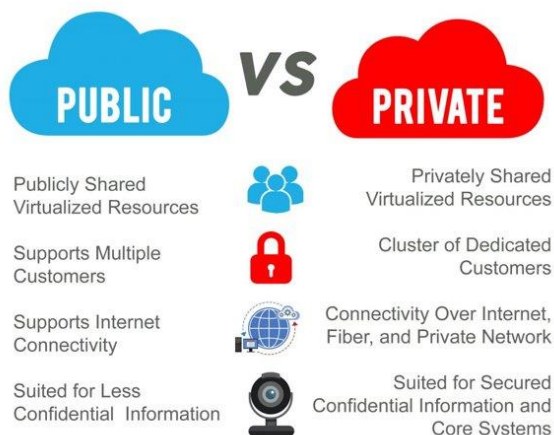
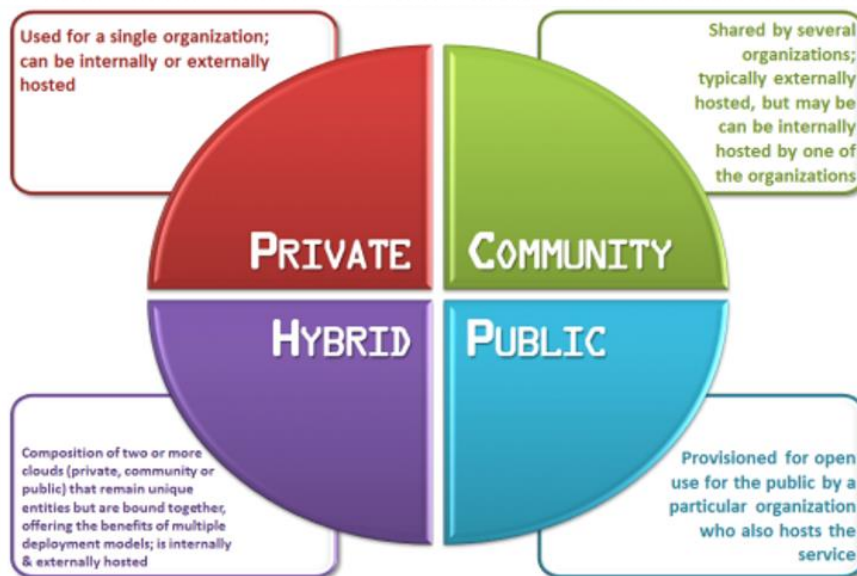
- Yahoo (2013-2014) affectant 3 milliards de comptes utilisateurs
- Facebook 2018 avec une faille qui affecte les infos de 50millions de comptes

Sources de données

- Depuis capteurs, etc... c'est fort répétitif au final
- Les données sont après structurés sous différentes formes tableaux, csv, graphiques...

Cloud Computing

Types de clouds



- Accéder de n'importe où n'importe quand aux données via le cloud

Principe

- Accès aux données, applications et services depuis un cloud
- Les services sont gérés par un tiers, et les entreprises payent en fonction de leurs besoins un certain type de service, ci-dessous listés
 - SaaS (Software as a service)
Accès à des logiciels depuis un navigateur par exemple, office 365...
 - PaaS (Platform as a service)
Accès à une plateforme qui permet de développer le projet, parfois avec un service de host de serveur web ou autre, exemple Google app Engine

- IaaS (Infrastructure as a service)
Un service de ressources virtuelles est donné, c'est le bébé du cloud computing. Avec IaaS, sont inclus : Infrastructures serveurs, machines virtuelles, stockages réseaux, système d'exploitations...
- ITaaS (IT as a service)
IT = technologie d'informations.
Cela couvre l'ensemble de tous les besoins. Cela inclus généralement tous les autres services ci-dessus.

Comparaison Cloud/Fog

	CLOUD	FOG
Architecture	Centralized	Distributed
Communication with devices	From a distance	Directly from the edge
Data processing	Far from the source of information	Close to the source of information
Computing capabilities	Higher	Lower
Number of nodes	Few	Very large
Analysis	Long-term	Short-term
Latency	High	Low
Connectivity	Internet	Various protocols and standards
Security	Lower	Higher

Data Center

Emplacement

- Environnement sans problème de risque de désastre naturels.
- Situé non loin d'une source électrique nécessaire
- Une source d'eau à distance d'utilisation pour le refroidissement
- Climat pas trop chaud

Facteurs importants

- Le réseau doit pouvoir être suffisant pour augmenter le datacenter si besoin et supporter la bande passante
- La sécurité du site doit être une priorité (sécurité physique du data center)

Virtualisation

- Le fait de mettre plusieurs OS, applications... Dans le même serveur physique (Voir partie virtualisation de la synthèse Architecture système



Synthese_ArchiSyste
mes_2023-2024_Tom

Hadoop

- En big Data surtout, il est important de distribuer les données pour les traiter, de manière horizontale. En utilisant donc plusieurs machines.
- Hadoop est un système de traitement de fichier tolérant aux fautes qui permet facilement d'être agrandi autant que voulu sur autant de machines possibles... de 1 serveur à plusieurs milliers de machines !
HDFS (Hadoop Distributed File System)
- Tolérant aux fautes veut dire que Hadoop réplique automatiquement les données endommagées pour être certain qu'elles ne sont pas perdues. Si il y a une panne, les données sont safe.

Automatisation

- Le fait de réduire ou bien d'éliminer le besoin d'une intervention humaine dans un processus.
- Il y a de l'automatisation dans la vie de tous les jours
 - Automatisation dans des situations dangereuses
 - Les self-checkouts aux magasins
 - Les voitures autonomes
 - Dans les lignes de productions, les robots
 - Des bâtiments intelligents
 - Les diagnostics médicaux

Technologies avancées

Blockchain

La blockchain est un ensemble de « blocs » qui sont des listes d'actions ayant été effectuées. La blockchain est un système décentralisé de paire à paire dont chaque utilisateur fait partie et peut vérifier la validité des blocs en comparant les « hash » de chaque bloc. Les hash sont les identités uniques d'une longueur donnée d'un bloc, qui commence d'une certaine façon si il est valide, le bloc suivant se base sur le bloc d'avant, donc si on essaye de modifier un bloc, il faut aussi modifier tous les blocs suivant. Mais même avec ça il faudrait que +50% des utilisateurs de la blockchain valide le changement ce qui en réalité n'est pas vraiment possible.

- A l'opposé d'un système centralisé dont les utilisateurs se reposent sur un individu ou système au centre, le système décentralisé demande à chaque utilisateur de faire ce travail, pour avoir une confiance totale dans la validité du système.

AI

- Des programmes qui recréent l'intelligence humaine, la manière de « réfléchir » pour répondre à certaines instructions ou éléments qui les entourent

Machine Learning

- C'est aussi des IA, qui eux sont capables d'apprendre de leurs environnements

Deep Learning

- Type de Machine Learning qui est plus poussé, qui fonctionne avec un système de neurones complexe sur plusieurs couches... Le plus proche de l'humain.

Dans L'IOT...

- AI :
 - Systèmes de recommandation
 - Assistants virtuels
- ML :
 - Détections de fraudes de carte de débits
 - Diagnostics médicaux
 - Reconnaissances vocales
- Deep Learning :
 - Reconnaissance d'images
 - Voitures autonomes
 - Traductions automatiques (avancés)

Sécurité

Types de données

- PII (Personally identifiable information)
- SPI (Sensitive personal information)
- Information Data

PII	Informational
Social security number	Rain gauge value
Email address	Number of cars through an intersection
Bank account numbers	Hospital emergency use per state
Student tuition bill	Average plane capacity
Credit rating	House thermometer reading
Debit card number	Census data
Fingerprints	Immigration values
Birth date	Average potato crops per province
Username/password	Next train time per station
Vehicle identification number (VIN)	Average gas consumption per flight
Mortgage information	
Home address	
Facebook photographs	

Hackers

- White hat
Les gentils qui trouvent les failles de sécurités pour des entreprises, gouvernements, etc
- Black hat
Les méchants, ils volent des informations personnels, pour les vendre, en tirer de l'argent, etc...
- Grey hat
Ils sont souvent dans l'ilégalité ou contre la morale mais ne font pas ça dans un but de nuire, juste pour le défi de le faire.

Sécurité physique/réseau

- Il faut prévoir différents systèmes physique dans les data centers ou autres lieux sensibles contenant des données pour éviter des attaques et fuites de données.
 - Un périmètre de sécurité extérieur, des barrières, clôtures, vidéo permanente
 - Périmètre de sécurité intérieur, vidéo permanente, accès biométriques, détecteurs de mouvements...
- Il faut aussi protéger les risques d'attaques de l'extérieurs sur le réseaux, en utilisant des par feux, du chiffrement, régulariser les accès au réseau, etc...
- Utilisation d'un VPN sur les wifi publiques, aussi applicable aux téléphones
- Sécurisation d'un wifi :
 - Modifier le mdp de base administrateur
 - Modifier le SSID (identifiant de l'ensemble du service reseau)
 - Ne pas publier son SSID

- Avoir un réseau sans fil pour invité
- Protéger physiquement son routeur
- Mettre à jour le routeur (modifié)
- Protection des dispositifs :
 - mettre le pare-feu
 - Mettre à jour tout
 - Sécuriser tout (pas seulement le routeur mais tous les appareils)
 - Utiliser anti-Virus et Anti logiciel espion
- Meilleures pratiques de sécurité :

Security Best Practices		
Perform Risk Assessment	+	Regularly Test Incident Response
Create a Security Policy	+	Implement a Network Monitoring, Analytics and Management Tool
Physical Security Measures	+	Implement Network Security Devices
Human Resource Security Measures	+	Implement a Comprehensive Endpoint Security Solution
Perform and Test Backups	+	Educate Users
Maintain Security Patches and Updates	+	Encrypt data
Employ Access Controls	+	

Défi de la sécurisation des dispositifs IoT

- Augmentation du nombre de dispositifs
La croissance exponentielle du nombre d'appareils augmente aussi les possibilités de failles et d'attaques
- Emplacement des appareils
Certains appareils IoT sont capables d'interagir avec le monde physique. Faille potentielle aussi sur ce point.
- Manque d'évolutivité
Les appareils connectés à des capteurs peuvent être situés à des endroits éloignés et/ou inaccessibles où l'intervention humaine ou la configuration est presque impossible.

Maisons intelligentes

- Avoir de plus en plus d'appareils connectés dans nos maisons augmente le nombre de failles, des accès à notre réseau. C'est comme notre talon d'Achille.

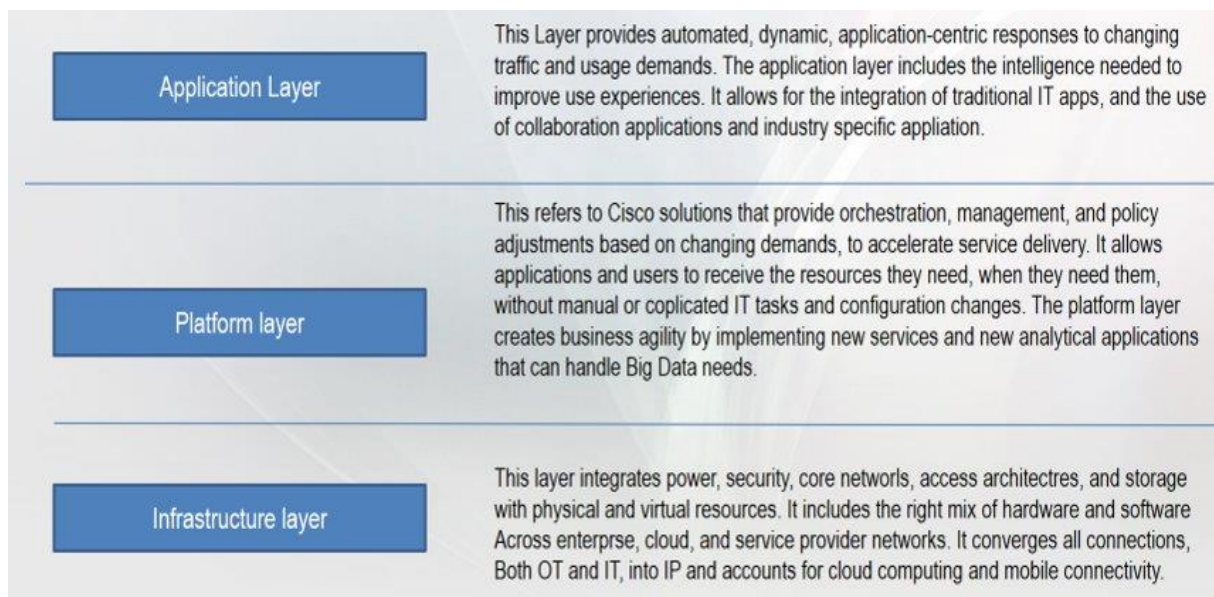
Transition vers IoE



Definition IoE

Concept technologique basé sur l'IoT. Là où l'IoT se base sur la connexion des appareils et des systèmes, L'IoE va plus loin en englobant tout ce qui est connectable; machines, processus, les personnes...

Architecture d'approche de l'IOE



- Besoin de plus de sécurité car plus d'appareils connectés
 - Des architectures de sécurité qui grandissent
 - Des systèmes de préventions d'attaques et d'intrusions (IPS)
 - De la redondance
 - Les gens sont le point faible...

Informations complémentaires

Lois

- Moore's law : le nombre de transistors des cpu double chaque année, ensuite c'est la finesse de gravure...
- Metcalfe's law : nombre de liens entre périphériques = $n(n-1)/2$
- Reed's law : les réseaux grandissent de manière exponentielle.

Data storage

- De manière local = sur un périphérique donné avec un matériel physique ex HDD...
- Centralisé = tous les périphériques sont reliés à un stockage central.
- Distribué = les données sont stockées dans plusieurs endroits différents (DDBMS)




















Présentations orales


Cryptographie / stéganographie

- Cryptographie = chiffrer le visible pour rendre illisible
 - Manuelle, ex : signaux de fumées, morses.... Qui nécessite une action physique et un code.
 - Mécanique, il y a un processus mécanique derrière qui chiffre, ex : Enigma
 - Numérique, des algorithmes qui chiffrent, ex : RSA (système de chiffrement asymétrique, une clef privée de déchiffrement, une clef publique de chiffrement)
 - Quantique, processus utilisant des ordinateurs quantiques pour chiffrer ou déchiffrer.
- Stéganographie = cacher dans le visible pour rendre illisible
 - Exemple prendre la première lettre de chaque mot dans une phrase.
- Il y a du chiffrement dans la vie de tous les jours, même si beaucoup d'applications ne sont pas assez sécurisées par rapport aux infos potentiellement trouvable (nos infos perso)
- Alan Turing = Mathématicien qui déchiffre Enigma pendant la guerre (super bon film sur le sujet. Avec Benedict Cumberbatch qui s'appelle « The Imitation Game » je vous conseille de regarder.)

Voitures autonomes

- Utilisations de capteurs en masses pour la détections de l'environnement
- Il y a 5 stades d'autonomies qui vont de pas du tout autonomes à pouvoir rouler sans chauffeurs, sur toutes les routes possibles.
- Aujourd'hui nous sommes seulement au niveau 2

LES 6 NIVEAUX D'AUTONOMIE D'UN VÉHICULE				
	ACCÉLÉRATION FREINAGE & VOLANT	SURVEILLANCE DE LA ROUTE	CONTRÔLE EN CAS DE PROBLÈME	QUELLES CONDITIONS
Niveau 0				
Niveau 1				Certaines routes
Niveau 2				Certaines routes
Niveau 3				Certaines routes
Niveau 4				Certaines routes
Niveau 5				Toutes les routes





Cryptage de données + militaire

Comparison										
Has refused to cooperate with intelligence agencies	✗	✗	✓	✗	✓	✓	✓	—	—	—
Provides transparency reports	✓	✓	✗	✓	✓	✓	✓	✓	✗	—
Abstains from collecting user data	✗	✗	✗	✗	✓	✓	✓	✓	✗	✓
Default encryption	✗	✓	✗	✓	✓	✓	✓	✓	✓	✓
Open source apps	✗	✗	✗	✗	✓	✓	✓	✓	✗	✓
Open source servers	✗	✗	✗	✗	✓	✓	✓	✗	✗	✗
Personal information is hashed	✗	✗	✗	✗	—	✓	—	✓	—	—
Encrypts metadata	✗	✗	✗	✗	—	✓	✓	—	—	—
Doesn't log timestamps and IP addresses	✗	✗	✗	✗	—	✓	✓	✓	—	—

- Les applications les plus populaires sont les moins sécurisées.
 - Signal et Wickr sont les plus sécurisés
- En période de guerre (Ukraine), Développement d'outils sécurisés de communication.
 - Digitalisation de la guerre via des outils numériques (Diia, bot eEnemy, TOPO, UKropSoft,...)
- En gros, grande importance du chiffrement de données dans les communications car données sensibles pouvant être volées par l'ennemi et utilisées...

OS

- Je tiens à dire que c'était une très bonne présentation mais j'ai 0 notes donc désolé à l'avance lol
- Les systèmes d'exploitations sont le liens entre l'humain et la machine. Il transforme des lignes de commandes en communication directe avec le CPU, la RAM, HDD, périphériques etc... (en assembleur par exemple)
- Ces commandes sont répertoriées dans une interface utilisateur
- L'OS gère aussi les fichiers, leurs accès...
- Il est composé de plusieurs parties importantes, des modules qui ont tous leurs propres rôles. Comme par exemple un « boot loader », qui initialise l'OS, et charge celui-ci en mémoire.