I- Question 1 :

D'après les informations communiquées dans l'énoncé, on comprend que l'architecture proposée est une architecture **HUB and SPOKE**, où le hub qui est le siège social est connecté aux différentes villes à travers des liaisons câblées ou sans fil. Chaque ville possède de plus de cette liaison avec le hub, une connexion vers Internet et d'autres connexions vers les différentes succursales. Ci-dessous l'architecture du siège social et ses liaisons avec les différentes villes avec les spécifications suivantes :

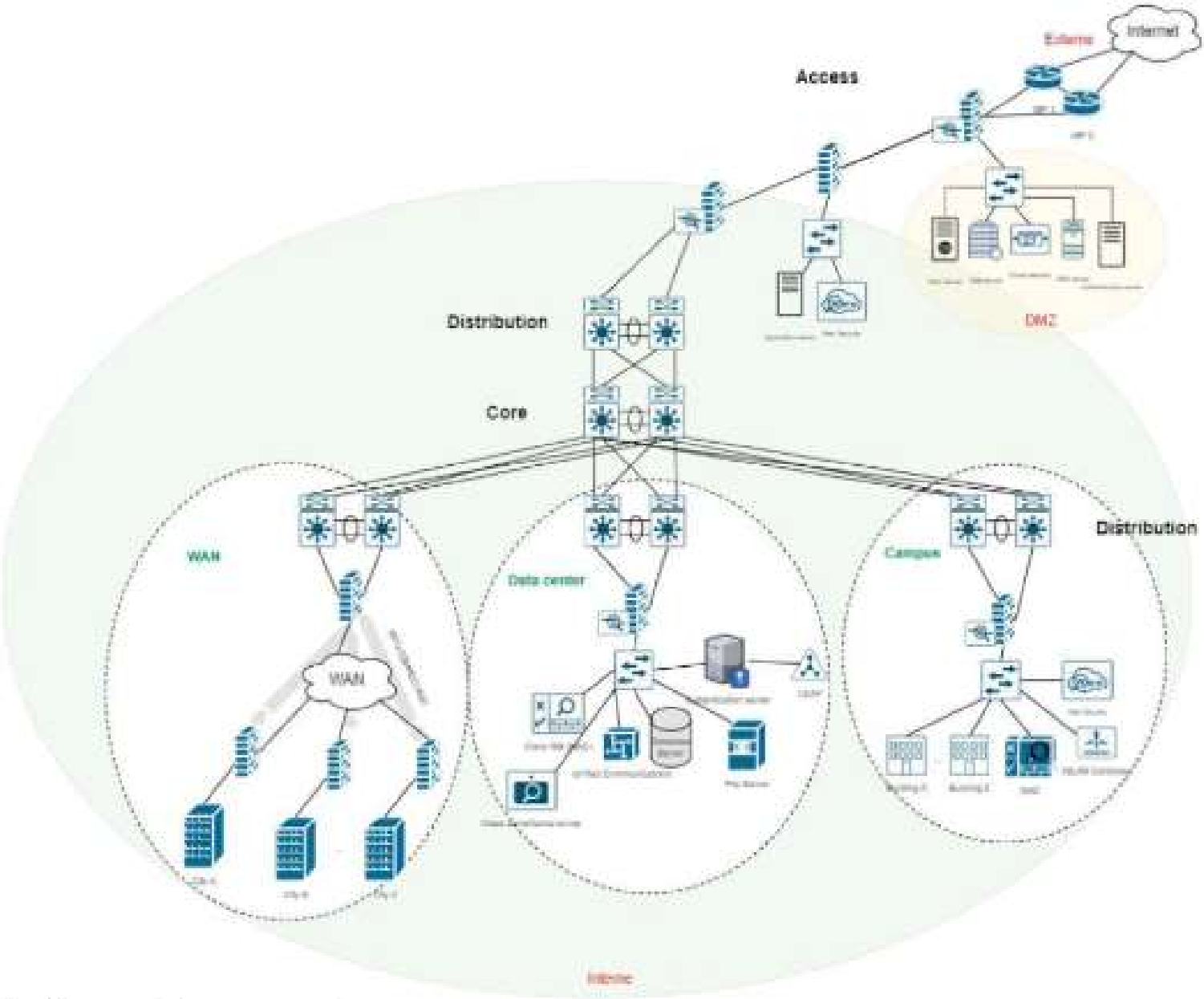
- Le siège qui est le point central de l'architecture doit avoir une connexion redondante vers Internet à travers deux ISP différents et en utilisant deux technologies d'accès différentes, par exemple ils peuvent utiliser la fibre optique pour la connexion principale et une connexion backup avec la technologie faisceaux hertzien ou LTE/ 5G.
- Comme mentionné dans l'énoncé, le siège a une architecture trois tiers, on peut distinguer sur le diagramme les trois couches (Accès, Distribution et Cœur)
- L'utilisation d'un pare-feu combiné avec un IPS est nécessaire pour la protection des services qui sont dans la DMZ.
- La zone DMZ comprend les éléments suivants : le serveur Web, le serveur mail, Email Security pour la protection contre les attaques liées au serveur mail, le serveur DNS et DHCP et un serveur d'authentification lié à l'application Web (transaction bancaire).
- L'application Web a une architecture 3 tiers, il est nécessaire pour assurer un niveau de sécurité élevé, d'ajouter un autre pare-feu entre le serveur web et le serveur d'application. On a ajouté également un Web Security Appliance pour bloquer les connexions malicieuses.
- Il est nécessaire d'ajouter une autre couche de protection (pare-feu et IPS) pour protéger le réseau interne de la banque au cas où le serveur d'application sera compromis.
- On a divisé le réseau interne du siège en trois blocs :
    - WAN : Une liaison VPN site to site sera déployé pour connecter chaque ville au siège. Un pare-feu est obligatoire à l'entrée du siège et à chaque sortie d'une ville. Le VPN est limité à l'extérieur du pare-feu pour rendre l'inspection de ce dernier plus facile (trafic non crypté)
    - Data Center : C'est la partie de l'architecture la plus sensible, c'est pour cette raison qu'on a ajouté un autre pare feu et IPS pour une protection même contre les attaques internes. Cette partie comprend plusieurs serveurs : le serveur

d'authentification de la banque combiné avec l'Active Directory, le serveur de base de données, le serveur des fichiers, surveillance …

- Campus : C'est le réseau d'accès de la banque, il regroupe les différentes installations réseaux dans les différents sites du siège (commutateurs, points d'accès …) ainsi qu'un NAC pour l'application de la politique de sécurité, un contrôleur WIFI et un Web Security pour filtrer les sites web malveillants.

- Afin de répondre au besoin de la banque en termes de **BYOD**, on a décidé d'implémenter la solution **Cisco ISE** qui va nous permettre de contrôler les appareils des utilisateurs, vérifier leurs conformités aux politiques de sécurité appliquées et prendre les décision adéquates pour protéger le réseau. Par exemple, pour un client qui utilise son propre laptop qui n'a pas été mise à jour et qui n'a aucun antivirus installé, Cisco ISE peut mettre cet utilisateur dans un VLAN isolé et lui donner un accès restreint aux ressources de l'entreprise (accès internet seulement par exemple).
- Pour assurer une haute disponibilité et une tolérance au faute, tous les éléments de l'architecture réseau doivent être redondants. Sur le diagramme ci-dessous, j'ai essayé de montrer cette redondance au niveau des liens et des commutateurs modulaires mais il reste quelques SPOF (Single Point Of Failure) que j'ai gardé pour simplifier l'architecture.
- Dans un réseau redondant il est nécessaire d'utiliser des technologies comme l'agrégation de lien (**Etherchannel**), le protocole de redondance **HSRP** et le protocole Spanning Tree (**STP**) pour bénéficier de toutes les ressources disponibles.
- Dans la partie Campus, il est nécessaire d'appliquer la solution **NAT** avec un adressage privé adéquat et des protocoles réseaux sécurisés par exemple : **OSPF** pour le routage, des **VLANs** par secteur et par technologie (VLAN WIFI, VLAN MANAGEMENT, …) pour limiter les domaines de broadcast, **NTP** pour la synchronisation du temps, **SNMP** pour la supervision…
- Il est obligatoire d'utiliser **HTTPS/TLS** au niveau du serveur Web. Et le protocole **SSH** pour le management des équipements réseau à distance.

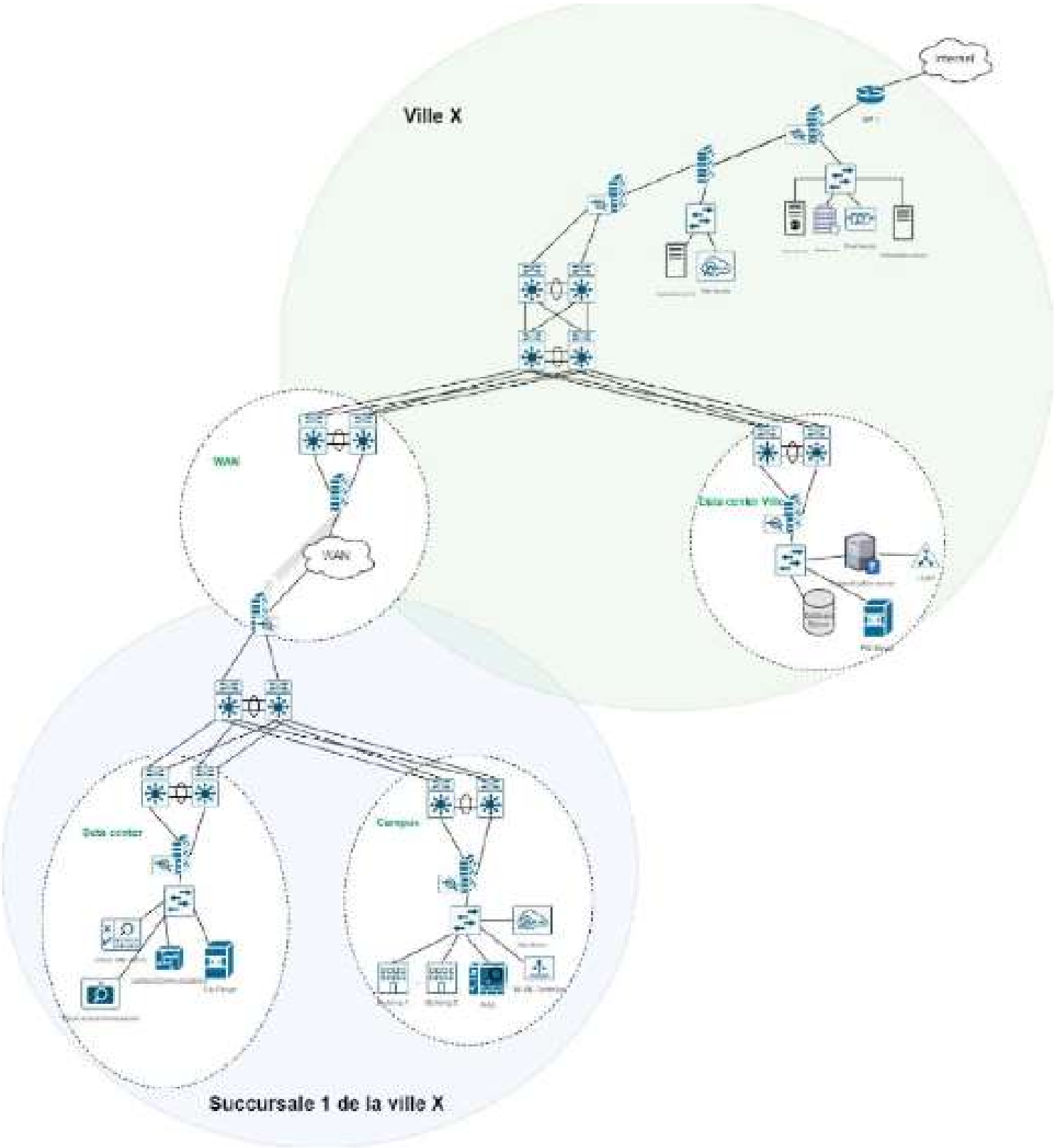
<u>Architecture du siège sociale + connexion avec les villes :</u>



Architecture ville et succursale :

D'après l'énoncé, chaque ville regroupe plusieurs succursales et possède un accès à Internet et un serveur avec BD centralisée. C'est ce que nous avons essayé de montrer dans le diagramme ci-dessous avec une seule succursale.

Les mêmes explications mentionnées ci-dessus sur le choix des équipements restent valables pour ce deuxième diagramme avec des petites modifications au niveau des équipements déployés (serveurs, connexion entre ville et succursale, ...).



II- Question 2 :

Article 1: Decentralized Self-Enforcing Trust Management System for Social Internet of Things

Article 2: On Designing Context-Aware Trust Model and Service Delegation for Social Internet of Things

Article 3: A Comprehensive Study on the Trust Management Techniques in the Internet of Things

1-

A)

Le premier article présente l'un des modèles de confiance de SIoT, il a été publié en avril 2020 par des chercheurs dans la revue IoT de IEEE.

Cet article détaille un nouveau modèle de gestion de la confiance au niveau des infrastructure SIoT. Ce modèle se base principalement sur la communication directe entre les périphériques du réseau IoT appartenant à un ensemble d'utilisateurs connectés entre eux à travers un réseau social.

Dans ce modèle, les périphériques utilisent un algorithme spécifique pour calculer le score de confiance de chaque élément participant. Ce score est calculé et stocké d'une manière sécurisée dans une base de données (PBB) publique accessible à tous pour des besoins de vérification. Seuls les éléments authentifiés peuvent écrire dans cette base de données et toutes les communications sont chiffrées en utilisant la méthode 'Noninteractive Zero Knowledge Proof (NIZKP)' ce qui permet d'avoir un niveau de confidentialité élevé.

Le modèle décrit dans cet article se caractérise par les points suivants :

- Il garantit que les informations sensibles des participants ainsi que leurs réseaux privés de communication ne sont pas exposées aux autres utilisateurs du système.
- Aucun système de confiance de tiers (Trusted third party system) n'est utilisé pour recueillir les informations et les feedbacks des utilisateurs.
- Le système est capable de mettre à jour le score de confiance par lui-même de manière vérifiable sans impliquer un tiers.
- Le calcul des scores finaux est vérifiable par les utilisateurs du système.

Dans le deuxième article, on trouve une deuxième méthode d'évaluation de la confiance dans les SIoT. Cette méthode se caractérise par l'utilisation d'un ensemble de SR (service requester) et SP (Service provider) et un modèle de confiance centralisé qui permet de stocker les informations sur les éléments du réseau et les scores correspondants à ces éléments. Le modèle permet une communication SR – SP pour la demande d'exécution des tâches et le partage des résultats, et une communication SR-modèle de confiance pour vérifier le score du SP choisi avant de lui affecter une tâche.

Si on se base sur les critères : **Confidentialité**, **Précision**, **Fiabilité et Intégrité,** il est clair que le premier modèle est plus souhaitable par rapport aux deuxièmes vu qu'il s'intéresse plus à la confidentialité des données et des systèmes. Les tests ont montré qu'il est très difficile de toucher à l'intégrité des données. Ainsi que l'accès publique aux informations de confiance de la BD PBB permet d'assurer un niveau de précision élevé avec une haute disponibilité vu que le modèle ne se base pas sur un système de confiance de tiers centralisé.

B)

Les véhicules connectés sont la tendance aujourd'hui dans le monde des IoT surtout avec l'apparition de la nouvelle génération de réseau 5G qui va rendre la communication plus facile entre véhicules et entre le véhicule et son environnement. Dans ce cadre et afin d'assurer une communication et un partage d'informations sécurisés entre ces véhicules, il est nécessaire d'implémenter un modèle de confiance adapté à ce type de besoin. Ce modèle devra répondre aux plusieurs exigences :

- La nature de communication véhicule to véhicule sans aucune intervention externe

- La sécurité et la confidentialité des données partagées
- La mobilité des véhicules
- L'évolutivité (Scalability) du réseau
- La capacité énergétique
- …

Afin de répondre à ce besoin et en se basant sur les deux articles communiqués, le modèle le plus adapté à ce type de besoin est celui du premier article et ce pour les raisons suivantes :

- Ce modèle assure une communication Device to Device sans avoir besoin d'un système de tiers, au contraire du modèle de l'article 2 qui permet une communication entre SR et SP, le véhicule devra contacter un service provider à chaque fois qu'il aura besoin d'une nouvelle information.
- Le modèle de l'article 1 utilise des méthodes de communication et de partage d'informations sécurisé et le degré de confiance d'un objet pourra être vérifié en tout moment à travers une base de données publique. Le modèle a également des résultats satisfaisants face aux plusieurs types d'attaques auxquelles il a pu faire face dans la phase des tests : *Malicious Adversary* et *Honest-But-Curious Adversary*.
- Le modèle 1 nécessite une bonne capacité de calcul et une bonne quantité d'énergie pour exécuter les opérations de cryptographie à chaque transaction. Ces performances sont beaucoup plus disponibles dans les véhicules que dans les petits objets connectés.
- L'article 2 présente une solution basée sur l'utilisation d'un modèle centralisé de confiance de tiers, le dimensionnement de ce modèle devra être refait si le nombre de véhicules dans le réseau augmente et dépasse la capacité de ce dernier. L'article 1 présente un modèle plus évolutif.
- La mobilité des véhicules ne pose aucun problème dans le cas où les communications sont de nature Device to Device, le véhicule va à chaque fois établir des communications avec les véhicules qui sont dans la même zone géographique.

2-

L'article trois présente huit critères utilisés pour la gestion de la confiance, dans ce qui suit, on va essayer de détailler chaque critère et voir comment les deux modèles dans les articles 1 et 2 répondent à ces critères :

Précision (Accuracy) : La confiance et la réputation dans le SIoT doivent être gérées avec précision.

Adaptabilité : Dans les réseaux IoT on a souvent beaucoup de changement de manière dynamique, la méthode de gestion de confiance doit être capable de gérer ces changements.

Disponibilité : Le modèle doit garantir la disponibilité des services malgré les attaques

Hétérogénéité : l'environnement hétérogène de l'IoT est un défi essentiel dans le développement des techniques de gestion de confiance. Le modèle doit prendre en considération que les objets de l'IoT ont des capacités différentes (exemples : portée de détection, puissance de calcul et la quantité d'énergie)

Intégrité : Le système doit protéger les données lors de la transmission entre l'expéditeur et le récepteur

Confidentialité : Le modèle de gestion de la confiance doit protéger la vie privée des utilisateurs et la confidentialité des données qui sont partagées entre les objets.

Fiabilité : La fiabilité garantit le fonctionnement correct du réseau sans interruption et sans défaut dans le temps spécifié.

Evolutivité : les réseaux de IoT sont évolutifs au niveau de certaines caractéristiques comme le nombre de nœuds et le nombre de requêtes dans le réseau.

Article 1 :

Précision	Comme déjà discuté dans les questions précédentes, le modèle de l'article 1 permet d'avoir une précision élevée pour deux raisons, la première c'est que tous les objets peuvent fonctionner soit en mode utilisateur soit vérificateur des données, des poids sont affecté à chaque objet selon son degré de précision, la valeur du poids de confiance peut augmenter ou diminuer à chaque nouvelle itération selon la précision du comportement de l'objet. La deuxième raison c'est que les scores de confiance sont stockés dans une BD publique accessible et vérifiable par tout le monde.
Adaptabilité	La relation Device to Device permet aux objets de s'adapter à leur environnement après chaque changement effectué.
Disponibilité	Les tests effectués sur ce modèle ont montré qu'il résiste à un grand nombre d'attaque. La disponibilité est donc garantie.
Hétérogénéité	Ce critère n'a pas été traité dans l'article
Intégrité	La solution a donné des bons résultats en matière d'intégrité des données, exemple : résultat contre l'attaque *Malicious Adversary*
Confidentialité	Le modèle utilise de la cryptographie NIZKP pour assurer la confidentialité des données et pour protéger la vie privée des utilisateurs.
Fiabilité	Face aux attaques testées, la solution a pu répondre correctement mais d'autres tests devront être effectués pour s'assurer du niveau de fiabilité de la solution notamment face aux attaques DOS.
Evolutivité	La solution n'utilise aucune plateforme centralisé, seuls des liaisons entre les périphériques, on peut dire que ce critère est assuré

Article 2 :

Précision	Dans le modèle présenté dans le deuxième article, la précision est basée principalement sur le modèle de confiance centralisé qui calcule le degré de confiance des objets en se basant sur plusieurs paramètres liés aux différents objets et aux itérations précédentes. La précision d'un objet/périphérique est liée à ce score de confiance.
Adaptabilité	A travers les méthodes de calcul du niveau de confiance qui prennent en compte le contexte (context aware) que l'article présente, la solution est adaptable aux environnements dynamiques.
Disponibilité	Plusieurs attaques ont été testées sur ce modèle, les impacts sur la performance sont généralement négligeables sauf par rapport à l'attaque BMA qui a eu un

	impact remarquable sur le modèle proposé.
Hétérogénéité	Le système supporte l'hétérogénéité parce que le calcul du degré de confiance prend en compte les caractéristiques de chaque périphérique (set of features Hv)
Intégrité	L'article ne donne pas beaucoup de détails sur la transmission des données.
Confidentialité	Des attaques contre la confidentialité n'ont pas été testés et l'article ne mentionne aucun algorithme de cryptographie utilisé.
Fiabilité	Les attaques testées ciblent le processus de calcul des scores de confiance et l'élection des SP, d'autres tests sont à faire pour s'assurer de la confidentialité, la fiabilité et l'intégrité de la solution.
Evolutivité	L'évolutivité de cette solution est faible vu qu'elle se base sur une plateforme centralisée qui a des capacités limitées. Des upgrades seront nécessaires pour suivre l'évolutivité du réseau.