République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université A/Mira de Béjaia
Faculté des Sciences Exactes
Département d'Informatique

MÉMOIRE DE MASTER RECHERCHE

En
Informatique

Option
Réseaux et Systèmes Distribués

Thème

Privacy dans l'Internet des objets. Cas d'étude : la localisation

Présenté par : BOUSSAÏD Nabil
BRAHAMI Rabah

Soutenu le 21 Juin 2017 devant le jury composé de :

Président	**N. DJEBARI**	**MAA**	**U.A.M Béjaia.**
Examinatrice	**N. BERMAD**	**MAB**	**U.A.M Béjaia.**
Examinatrice	**F. CHERIFI**	**Doctorante**	**U.A.M Béjaia.**
Encadreur	**M. OMAR**	**MCA**	**U.A.M Béjaia.**
Co-encadreur	**S. ZEBBOUDJ**	**Doctorante**	**U.A.M Béjaia.**

Béjaia, Juin 2017.

⁕ *Remerciements* ⁕

Nos remerciements les plus sincères vont en premier lieu, à notre encadrant **Dr OMAR Mawloud** pour ses conseils lucides et pertinents, sa patience et son précieux suivi tout au long de la réalisation de ce travail. Sa disponibilité, ses qualités pédagogiques et humaines, et ses compétences nous ont apporté un encadrement déterminant dans toutes les phases de ce travail.

Nos remerciements vont également à notre co-encadrante M^{lle}**. ZEBBOUDJ Sofia** pour sa disponibilité et sa compréhension, son soutien et son suivi nous a permis de mener à bien ce travail.

Nous remercions chacun des membres du jury d'avoir consacré une partie de leur temps à la lecture de ce mémoire et pour l'intérêt qu'ils ont porté à ce travail.

Nos remerciements s'étendent à tous nos enseignants et les membres du département d'Informatique de l'université **ABDERRAHMANE MIRA**.

Ainsi qu'à tous ceux et celles qui ont contribué de près ou de loin à l'accomplissement de ce travail.

⁂ *Dédicaces* ⁂

A nos très chers parents, pour les sacrifices déployés à notre égard, pour leur soutien tous les efforts consentis pour notre éducation et notre formation. Qu'ils trouvent dans ce modeste travail le témoignage de notre reconnaissance, notre profonde affection et notre attachement indéfectible. A nos frères et sœurs et tous nos amis qui nous ont soutenues tout au long de ce travail et à toutes personnes que nous portent fort dans notre cœur et qui sauront se reconnaître.
A chaque main tendue et pour toute attention témoignée.

M. ***BRAHAMI Rabah***
M. ***BOUSSSAÏD Nabil***

Table des matières

Table des figures

Liste des tableaux

Liste des acronymes

AES	Advanced Encryption Standard .
CEI	Consommateur Electrique Intelligent.
CP-ABE	Ciphertext Policy-Attribute Based Encryption.
DLDA	Dynamique Location Divulgate Agent.
DoS	Denial of Service.
ESOT	Enhanced Semantic Obfuscation Technique.
GPS	Global Positioning System.
GSMA	Global System for Mobile Association.
IdO	Internet des Objet.
LBS	Location Based Services.
MK	Master Key.
PK	Public Key.
REI	Réseau Electrique Intelligent.
RFID	Identification par Radio Fréquence.
SOT	Semantic Obfuscation Technique.
SK	Secret Key.

Introduction générale

L'humain dans sa poursuite continue pour l'amélioration de sa condition de vie essaie d'automatiser un maximum de tâches de tous les jours, et cela pour mieux appréhender son environnement en y introduisant des mécanismes qui vont permettre d'obtenir des informations y afférentes, et vont éventuellement réagir automatiquement à ses changements au profit de l'utilisateur. Cela passe par rendre les objets de tous les jours réactifs et capables d'obtenir des informations de l'environnement, et de communiquer avec d'autres objets, et c'est de ce besoin qu'est né l'Internet des objets (IdO).

L'Internet des objets est une technique qui va permettre la connexion d'objets et des capteurs à l'Internet, ou bien plus généralement à des réseaux informatiques, ce qui va donner un tout nouveau type d'application plus tournée vers l'environnement physique, sa perception, et des actions qui peuvent influencer ce dernier. Les applications d'une telle technologie touchent à plusieurs domaines tels que : la santé, l'agriculture, les villes intelligentes, etc. Cependant, il ouvre la voie aussi à beaucoup de dérives en poussant à prendre en considération plusieurs aspects avant le déploiement de cette technologie. L'un des aspects les plus importants est la sécurité et le respect de la vie privée d'utilisateur, car l'application de cette technique permettra de collecter des informations sur l'environnement physique et y appliquer des actions, et donc on peut voir que des failles secrétaires dans ce type de système pouvant être très dangereuses vu les possibilités que donne ce dernier, et des domaines où il peut être appliqué.

À ce fait, la sécurité et la confidentialité de la vie privée des utilisateurs de l'**IdO** ont fait l'objet de plusieurs recherches durant les dernières années. Cependant, la satisfaction des contraintes de cette révolution technologique dans les approches de la sécurité de la vie privée reste un défi à relever. Nous classifions les solutions proposées dans la littérature en trois principales catégories : les solutions au problème de localisation [25, 12], les solutions au problème du système [2] et les solutions au problème d'accès aux d'informations [23, 10]. Ces solutions sont marquées par l'absence de politique de sécurité ce qui les rend vulnérables aux différentes attaques. Ceci présente une menace pour les données privées de l'utilisateur et une atteinte à la sécurité de sa vie privée.

À travers ce mémoire, nous nous sommes focalisés sur le problème de confidentialité de l'emplacement des utilisateurs de l'**IdO**, vu l'importance de cette donnée et son importance pour la préservation de la vie privée des utilisateurs. Nous proposons une architecture permettant de sécuriser cette donnée et limiter l'accès à cette dernière qu'à l'autorité autorisée. Pour cela, notre architecture s'appuie sur l'utilisation de protocole de chiffrement symétrique et asymétrique CP-ABE (Ciphertext Policy-Attribute Based Encryption) qui permet de limiter l'accès à une donnée confidentielle, ainsi que l'utilisation du protocole CHORD afin de permettre de décentraliser notre architecture et d'augmenter sa rapidité d'exécution.

Ce mémoire est organisé en quatre chapitres. Le premier chapitre, "Présentation de l'Internet des objets", portera sur quelques généralités sur l'**IdO** et sur les notions de sécurité et menace. Un état de l'art sur des protocoles fera l'objet du deuxième chapitre, "État de l'art sur la sécurité de la vie privée dans l'**IdO**", où nous établirons des critères d'analyse, puis nous discuterons les points faibles et les points forts de chaque protocole. Dans le troisième chapitre, nous présenterons en détail, les différentes étapes par lesquelles passe l'architecture que nous proposons. Pour prouver l'efficacité de notre solution, nous présenterons dans le quatrième chapitre, les résultats de simulation avec comparaison à un autre protocole concurrent. Enfin, une conclusion suivie de perspectives clôtureront notre mémoire.

Chapitre 1

Présentation de l'Internet des Objets

1.1 Introduction

Le terme Internet des Objets (**IdO**) représente un mécanisme de communication entre des millions d'appareils. Dans l'**IdO**, les objets physiques, les objets virtuels et des dispositifs informatiques sont connectés les uns aux autres permettant à ces dispositifs d'accéder et de contrôler divers services à distance [3]. L'**IdO** désigne une informatique qui se fond dans notre quotidien pour nous simplifier la vie. Toutefois, certaines informations dont disposent les objets sont confidentielles, ce qui impose de grands défis en terme de sécurité des individus et des entreprises.
Dans ce chapitre, nous commencerons par présenter l'**IdO**, ses domaines d'application ainsi que les obstacles ralentissant son déploiement. Ensuite, nous présenterons la vie privée, ses vulnérabilités et ses menaces et nous finirons par quelques notions de sécurité.

1.2 Internet des Objets

L'Internet des Objets (**IdO** ou **IoT** pour l'anglais *Internet of Things*) est défini comme un réseau mondial pour la société de l'information. Il permet de disposer des services évolués en interconnectant des objets physiques et virtuels grâce aux

technologies interopérables de l'information et de la communication existantes ou futures. Ce réseau permet, via des systèmes d'identification électronique normalisés et unifiés, et des dispositifs mobiles sans fil, d'identifier directement et sans ambiguïté des entités numériques et des objets physiques. Ainsi, il est possible de récupérer, stocker, transférer et traiter les données sans discontinuité entre les mondes physiques et virtuels [2].

L'expression « *Internet of Things* » a été introduite pour la première fois par Kevin Ashton durant une présentation en 1999[09]. En 1999, un groupe de recherche au *Massachusetts Institute of Technology* (MIT) a établi les premiers prototypes des identificateurs automatiques (RFID : Identification par Radio Fréquence) qui sont considérés comme un élément clé de la technologie de l'**IdO**. En 2005, L'union internationale de Télécommunications (ITU, *Internation Telecommunication Union*), un organisme de standardisation dans le domaine TELECOM publie un rapport technique consacré à l'**IdO**, qu'elle présente comme une nouvelle révolution de l'Internet.

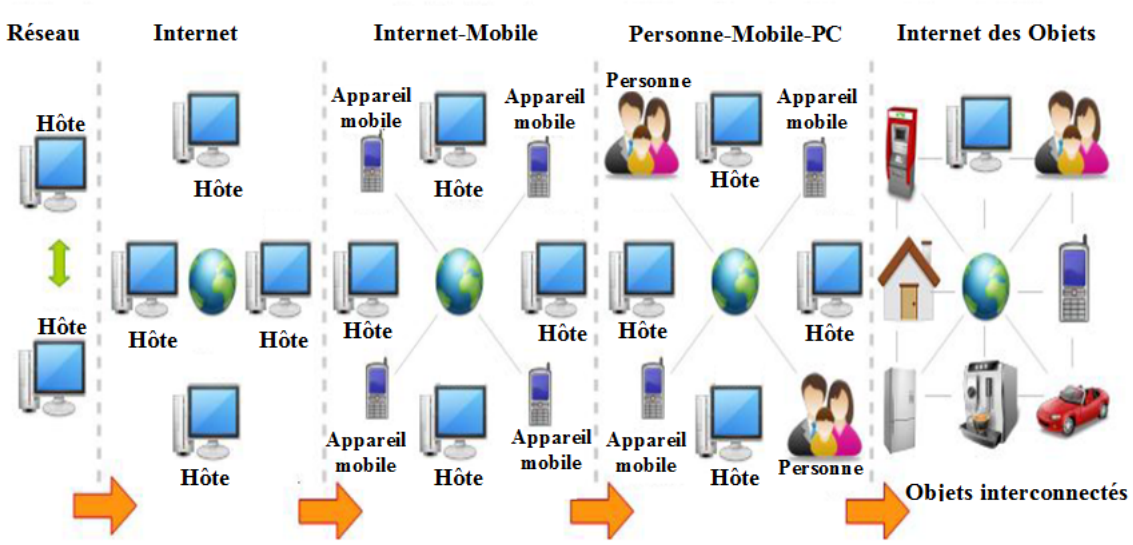

FIGURE 1.1 – Evolution des réseaux informatiques vers l'IdO [13].

Sur le plan économique, l'association GSMA évalue les opportunités de profits reliées à l'**IdO** à 445 milliards de dollars pour l'industrie de l'électronique grand public, 202 milliards pour l'industrie automobile, 69 milliards pour le secteur de la santé et 36 milliards pour les distributeurs d'électricité, d'eau ou de gaz [12].

1.3 Architecture de l'Internet des Objets

L'architecture de l'**IdO** est l'un des sujets les plus mentionnés dans les articles de recherche de ce domaine. L'architecture cinq couches est généralement acceptée comme étant l'architecture qui décrit le mieux l'**IdO** [5-7]. La Figure 1.2 montre la superposition des cinq couches de cette architecture. Ci-dessous une description de chacune d'entre elles [21-23] :

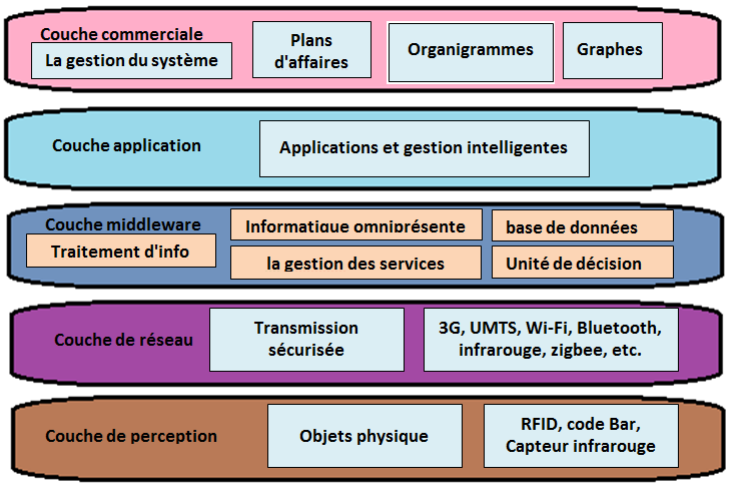

FIGURE 1.2 – L'architecture cinq couches [23].

1.3.1 Couche perception

C'est la première couche, on l'appelle aussi couche objets. Elle représente les objets physiques de l'**IdO** qui ont pour but la collecte et le traitement basique de

l'information, et qui fournissent différentes fonctionnalités comme donner la position physique, la température, le poids, le mouvementent, etc. Cette couche collecte et numérise les données d'un certain environnement et les envoie à la couche supérieure via des canaux sécurisés.

1.3.2 Couche réseau

Elle est aussi appelée couche réseau. Cette couche s'occupe du transport de la donnée vers le centre de traitement de l'information. Le moyen de transmission peut être filaire ou non et les principales technologies utilisées dans cette couche sont la 3G, WiFi, ZigBee, etc. C'est au niveau de cette couche que se trouvent les protocoles de communication, tels que 6LowPan, qui sont nécessaires pour l'adressage de millions d'objets connectés.

1.3.3 Couche traitement

Chaque objet de l'**IdO** offre des services que cette couche (appelée aussi couche Middleware [23]) est responsable de gérer et de lier avec des bases de données les informations collectées, pour ensuite y appliquer des traitements et des calculs, afin de prendre des décisions automatiques. Elle permet aussi au développeurs d'application de l'**IdO** de faire appel à des services sans prendre en considération l'interopérabilité des objets, ou bien une plateforme matérielle spécifique.

1.3.4 Couche application

Cette couche offre la possibilité d'utiliser les informations traitées par la couche traitement et les services des objets présentés par cette dernière, pour développer diverses applications de l'**IdO**. Ces applications seront ensuite directement êtres utilisées par des utilisateurs finaux.

1.3.5 Couche Business

Le but de cette couche est la gestion des différentes applications de l'**IdO**. Les responsabilités de cette couche sont de construire un modèle de gestion, des graphes, des organigrammes, etc. en se basant sur les données reçues de la couche application, et sur le résultat de cette analyse. Cette couche permet de décider le chemin futur et la stratégie de business. La gestion et la surveillance des quatre autres couches se font aussi à son niveau.

1.4 Domaines d'application

Les domaines d'application de l'**IdO** sont très nombreux, et touchent pratiquement tous les axes de la vie quotidienne des individus, ce qui as permis l'émergence d'espace intelligents autour d'une informatique omniprésente [4]. Parmi ces domaines, nous citons quelques exemples :

1.4.1 Santé

Les soins médicaux représentent l'un des domaines d'application de l'**IdO** les plus séduisants. Cette dernière permet de donner lieu à de nombreuses applications médicales telles que la télésurveillance, les programmes de conditionnement physique et les soins pour les personnes âgées [25]. La Figure 1.3 illustre un exemple d'utilisation de l'**IdO** dans la santé.

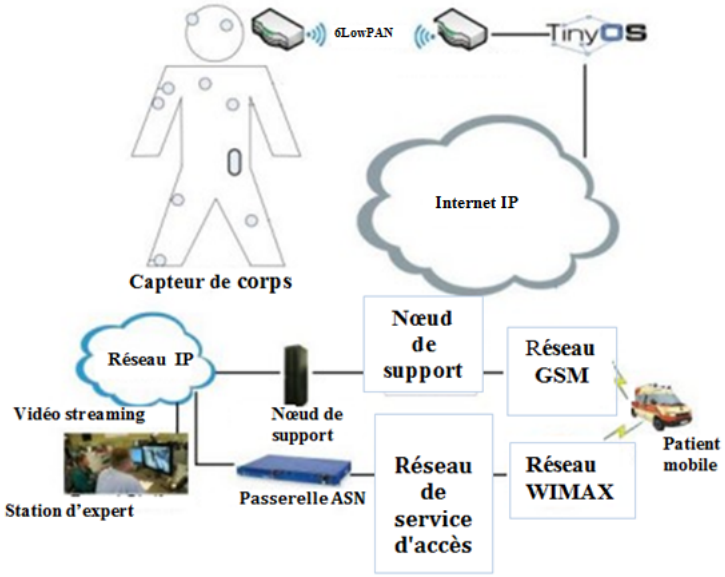

FIGURE 1.3 – La surveillance à distant des soins de santé d'un patient [25].

Dans la Figure 1.3, nous remarquons que le profil de santé du patient et ses signes vitaux sont capturés en utilisant des capteurs attachés à son corps et des appareils médicaux portables. Les données capturées sont ensuite analysées et stockées, et elles deviennent utiles pour l'agrégation (cette agrégation n'est pas forcément nécessaire pour tout type d'application **IdO**). Les soignants peuvent surveiller les patients en tout lieu et réagir en conséquence. En plus, la topologie représentée dans la Figure 1.3 comprend une structure de réseau qui supporte le streaming de vidéos médicales [25].

1.4.2 Transport

Le suivie en temps réel du déplacement des populations, des biens et des moyens de transport dans le monde permettra l'élaboration d'un système de transport intelligent qui a comme objectifs, non seulement le renforcement de la sécurité routière, mais également l'efficacité de la gestion du trafic, l'économie du temps, de l'énergie et le confort des conducteurs.

1.4.3 La domotique en milieux urbains

L'un des domaines d'application les plus intéressants concerne l'intégration des équipements domotiques sur le réseau. Cela permettra un contrôle total sur les équipements de la maison à travers une même interface et permettra leur contrôle à distance. Les champs d'applications de l'**IdO** s'élargit pour toucher le milieu urbain (Villes intelligentes) pour offrir une meilleure gestion de tous les réseaux qui alimentent une ville intelligente (Eaux, gaz, électricité, etc.) ou en utilisant des capteurs afin d'améliorer la gestion des parkings et du trafic urbain, diminuer les embouteillages et les émissions de CO2.

1.4.4 Industrie

Dans le domaine industriel l'**IdO** a permis d'effectuer un suivi global des produits de la chaîne de production jusqu'à la chaîne logistique et assurera la distribution en supervisant l'approvisionnement. Ce suivi total des produit permettra de faciliter la lutte contre la contrefaçon, la fraude et minimiser les déchets.

1.4.5 Agriculture

L'utilisation de l'**IdO** dans le domaine agricole consiste utiliser des capteurs pour la supervision de l'environnement de culture. Ceci, en fournissant un tableau de bord pour faciliter et aider l'agriculteur à faire une prise de décision des besoins imminent de la plantation, permettant ainsi, d'économiser les ressources et préserver l'environnement en diminuant la pollution [4].

1.5 Sécurité dans l'internet des objets

1.5.1 Menaces de Sécurité dans l'IdO

L'**IdO**, a introduit de sérieux soucis en matière de sécurit, qui auparavant étaient peu existant/réalisable dans l'Internet classique. En effet, introduire cette capacité

de pouvoir communiquer avec le monde physique, et même d'agir sur lui à partir du monde numérique, peut mettre en danger la fiabilité et la sécurité de certaines infrastructures qu'on peut classifier comme étant des Infrastructures Critiques (IC). Aussi, vu le nombre important d'objets intelligents qui nous entourent ou que nous utilisons, le problème du respect de la vie privée de l'utilisateur se pose avec force. Ci-dessous, nous donnons une liste non-exhaustive d'attaques et menaces pouvant affecter l'**IdO** en général, en faisant une projection sur le REI [10] :

1.5.1.1 Menace au respect de la vie privée du consommateur

Vu le nombre important d'objets intelligents pouvant être relatifs à une personne, ainsi que le nombre important d'informations échangées par ces objets, il n'est pas difficile qu'un attaquant puisse découvrir des informations qui relèvent du cercle privé de la personne, sans que ce dernier ait explicitement donné son accord pour la divulgation de telles informations. Dans le contexte du REI, un attaquant peut facilement savoir le profit de consommation électrique du consommateur, ces habitudes (Heure de réveil, petit-déjeuner, départ, retour à la maison, etc.), les périodes d'absence du foyer, le nombre et types d'équipements domestiques intelligents dans le foyer, etc.

1.5.1.2 Menace de Compromission

La compromission consiste à avoir un contrôle partiel ou total sur un objet, soit de façon directe (physique) ou indirecte (logiciel). En plus de la tentative de divulgation des informations secrètes et sensibles que renferme l'objet (Clés cryptographiques, codes PIN, etc.), l'attaquant vise aussi à charger l'objet par un programme malveillant, dans le but de perturber le fonctionnement du système dans lequel l'objet prend part. L'objet est sous contrôle total si toutes les actions et outputs de l'objet sont déterminés par l'attaquant, autrement, il est sous contrôle partiel. Dans le contexte du REI, un consommateur malveillant pourrait tout simplement compromettre son CEI afin de minimiser sa facture d'électricité, en sous-estimant sa consommation électrique. De même, un attaquant pourrait compromettre un CEI

afin de prendre contrôle, via celui-ci, des objets domestiques intelligents se trouvant dans le foyer.

1.5.2 Objectifs de la sécurité

La sécurité informatique est l'ensemble des moyens mises en oeuvre pour réduire la vulnérabilité d'un système contre les menaces, et assure que les ressources matérielles et logicielles sont uniquement utilisées dans le carde prévu. Elle permet d'assurer plusieurs objectifs dont les cinq principaux sont : l'authentification, la confidentialité, l'intégrité, la disponibilité et la non-répudiation [2].

1.6 Défis de l'Internet des Objets

Bien que l'**IdO** dessine un future où la vie serait beaucoup plus commode, cet idéal ne sera pas facile à atteindre. Comme pour toute technologie, l'**IdO** fait face à plusieurs challenges dans son évolution. En premier lieu l'**IdO** permet de connecter des milliards d'objets [11] et chaque objet devra être adressé et avoir une identité unique sur Internet. On doit donc avoir un système de gestion de l'application et de l'adressage des objets qui soit efficace et dynamique. Un autre problème actuel pour l'**IdO** est le fait qu'il y ait plusieurs fabricants qui utilisent leurs propres technologies et services, qui ne sont pas forcément accessibles ou bien utilisés par d'autres fabricants. Cela limite grandement les applications possible de l'**IdO** et pose un problème d'interopérabilité. Un travail de standardisation doit donc être mené dans ce domaine. Le fait que les objets connectés ont quelques fois des emplacements retirés et difficiles à surveiller, il faudrait concevoir des systèmes qui empêcheraient qu'un intrus puisse accéder physiquement à ces objets et changer leur fonctionnement. L'un des défis majeur de l'**IdO** consterne la sécurité du réseau et la confidentialité des données. Les données envoyées à partir d'objets connectés passent par des réseaux, filaires ou non, qui doivent être capables de supporter un grand nombre d'objets connectés sans causer de pertes de données à cause de la congestion du réseau. Ils

doivent aussi empêcher la surveillance des données par des éléments externes en ayant, par exemple, de bons mécanismes de chiffrement implémentés dans les objets.

1.7 Vie privée

La vie privée ou la confidentialité est une notion ancienne. Dans la Grèce antique, Socrate et d'autres philosophes ont déjà fait la différence entre le public et le privé [14]. Une définition plus récente de la vie privée a été proposée par Alan Weston en 1960 : « *La vie Privée est la demande des individus, des groupes ou des institutions de déterminer eux-mêmes quand, comment, et dans quelle mesure l'information leur concernant est communiquée aux autres* »[15]. Chaque personne a une compréhension différente de ce qu'est la vie privée. On peut la définir comme étant le droit de garder protégées nos données personnelles comme la date de naissance, le numéro de téléphone personnel, la localisation mais également d'autres données multimédia comme des vidéos et des photos.
La notion de confidentialité varie selon les domaines et peut donc être considérée comme étant une notion subjective. Dans les bases de données classiques, cette notion est très proche de l'anonymat. Ainsi, dans ce contexte, les attaques qui visent à ré-identifier les gens à partir d'une base de données ou lier la même personne présente dans différentes bases de données. La protection de la confidentialité est une tâche difficile et complexe quand les données personnelles sont partagées, que ce soit volontairement ou non.

1.8 Conclusion

Dans ce chapitre, nous avons présenté les notions de base liées à la sécurité de la vie privée dans l'**IdO**, et cela en définissant les concepts rencontrés dans la littérature ou dans le modèle que nous avons étudié. Le chapitre suivant sera consacré à l'étude de quelques travaux récents réalisés dans le contexte de la sécurité de la vie privée dans l'**IdO**.

Chapitre 2

Etat de l'art sur la sécurité de la vie privée dans l'IdO

2.1 Introduction

L'Internet des Objets (**IdO**) prévoit de nouveaux défis qui appellent à une révision. Une innovation substantielle des solutions et des mécanismes déjà existants doit être effectuée afin de s'adapter aux caractéristiques de l'**IdO** et assurer la sécurité de la vie privée de ses utilisateurs.
Dans le chapitre ci-présent, nous avons étudié les différentes solutions proposées pour assurer la sécurité de la vie privée dans l'**IdO** que nous utilisons comme critère de base par la suite dans notre proposition. Pour ce faire, nous avons commencé dans ce chapitre par la définition de critères d'analyse de différentes solutions proposées dans la littérature. Ensuite, nous avons établi une classification des solutions étudiées et avons conclu par une synthèse qui englobe les avantages et les désavantages de ces solutions.

2.2 Critères d'analyse des travaux étudiées

Pour une meilleure évaluation des travaux de recherche étudiés, nous avons établi certains critères jugés pertinents, en tenant compte des besoins et contraintes liés à la sécurité de la vie privée. Nous nous intéresserons, de ce fait, à la sécurité en termes

de consommation d'énergie, de résistance aux attaques (sécurité), la scalabilite de la politique de sécurité.

2.2.1 Consommation d'énergie

La majorité des dispositifs présents dans l'**IdO** sont sévèrement limités en termes de mémoire, CPU ainsi que de capacités énergétiques [19]. De ce fait, le mécanisme de gestion de données privées doit être à moindre consommation d'énergie.

2.2.2 Sécurité

En raison de la variété et la confidentialité des données sensibles échangées par les utilisateurs et par les dispositifs de l'**IdO**, un modèle de sécurité doit être développé pour mieux gérer la vie privée. Ce dernier doit être résistant aux attaques et répondre aux principales exigences de sécurité.

2.2.3 Evolutivité

L'évolutivité dans l'**IdO** désigne la capacité de s'adapter aux nouveaux dispositifs, services et fonctions sans nuire à la performance des services existants. Puisque le volume des données dans l'**IdO** augmente de jour en jour, nous devons prendre en considération ce critère pour avoir un système efficace.

2.3 Etude critique des travaux étudiées

Protéger la vie privée relative aux utilisateurs d'Internet est d'une importance capitale dans l'**IdO**. Plusieurs recherches ont été menées afin de réaliser un mécanisme de sécurité qui répond aux exigences de ces objets.
Après avoir analysé les travaux récoltés, il nous est apparu qu'une classification était nécessaire afin de répertorier les différentes approches. Le tableau suivant représente notre classification des différentes solutions étudiées pour le problème de sécurité de la vie privée dans l'**IdO**.

Classification des travaux étudiés	
Solutions au problème de localisation	Ikram Ullah et al.[25] Mahmoud Elkhodr et al.[16] Patel et al.[12]
Solutions au problème de système	Orlando Arias et al.[2]
Solutions au problème d'accès au flux d'informations	Viorel Negruont et al.[23] Xin Huang et al.[10]

TABLE 2.1 – Classification des travaux étudiés

Dans ce qui suit, nous étudions une partie des travaux réalisées dans ce contexte.

2.3.1 Solutions au problème de localisation

2.3.1.1 A Novel Model for Preserving Location Privacy in Internet of Things

Dans cet article, Ikram Ullah et al. [25] ont proposé une solution au problème de la confidentialité des emplacements dans le contexte de l'**IdO**, la technique d'offuscation sémantique est basée sur la sémantique de l'emplacement de l'utilisateur ou du périphérique. La principale préoccupation de la technique est d'occulter l'emplacement de l'utilisateur à un éventuel adversaire. Cette technique appelée ESOT, est une amélioration de la technique SOT. L'amélioration apportée au SOT est de permettre une application globale de cette dernière, introduire une relation d'équilibre entre la protection de la vie privée et l'utilité des services et réduire les niveaux d'offuscation pour permettre un meilleur service de localisation. Dans la technique d'offuscation nous voulons protéger l'emplacement des LBS, car ils ne sont pas une source de confiance .

2.3.1.2 le fonctionnement du ESOT

Tout d'abord, l'utilisateur doit spécifier la préférence en sa position actuelle. Cette spécification est effectuée avant la demande au LSB et ces préférences sont données en fonction de la sensibilité de l'emplacement. Ces derniers sont classés en

trois niveaux de sensibilité : faible, moyenne ou haute sensibilité. Plus la sensibilité est élevée, plus l'emplacement d'offuscation est pris de large zone. Le modèle du système ESOT est présenté dans la figure2.1, dans la quelle est illustrée la façon avec la quelle l'emplacement original est caché aux LBS. L'emplacement alors reçu par le LBC est obscurci par ESOT.

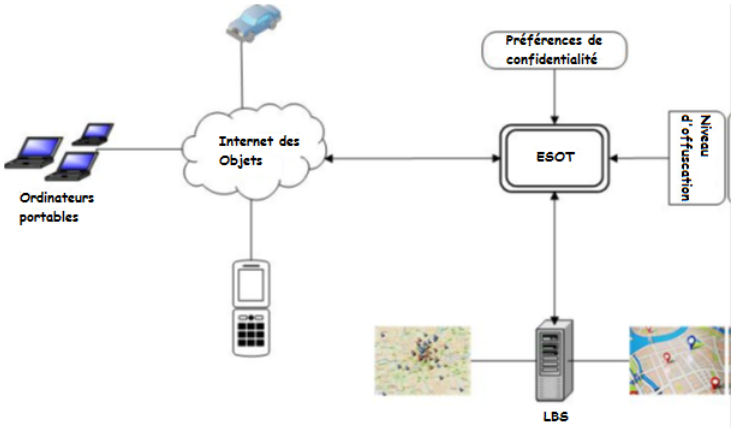

FIGURE 2.1 – Model system du ESOT[25].

La technique **ESOT** proposée par les chercheurs a permis aussi de réduire le nombre de niveaux d'offuscation de 5 à 3 niveaux afin d'éviter la mauvaise affectation des services de localisation, se retrouver à un autre emplacement qui est en dehors de son état ou de son pays. Les niveaux sont divisés en fonction de la distance entre l'emplacement original et l'emplacement d'offuscation.

Discussion et critiques

L'amélioration proposée par Ullah et al ne consomme pas trop d'énergie. Elle a permis de réduire les niveaux d'offuscation et la scalabilité est assurée car cette amélioration a permis une application globale de la technique SOT. La résistance aux attaques n'est cependant pas assurée ; certes l'emplacement du dispositif de l'**IdO** est occulté et protégé, mais aucune politique de sécurité n'a été proposée. Les requêtes échangées

entre les entités, **IdO**, **ESOT**, **LBS** ne sont pas sécurisées, elles sont par conséquent exposées à une éventuelle attaque.

2.3.1.3 A Contextual-adaptive Location Disclosure Agent for General Devices in the Internet of Things

Dans cet article, Mahmoud Elkhodr et al. [16] ont proposé une solution de confidentialité des emplacements dans l'**IdO**. Cette solution est basée sur l'obscurcissement de l'emplacement d'un utilisateur pour protéger et masquer ces informations de localisation. Cependant, certains propriétaires ne souhaitent pas masquer leurs informations à tout moment. La méthode appelée, l'agent de divulgation d'emplacement dynamique (DLDA), est utilisée pour cela. L'agent prend l'emplacement actuel comme entrée et délivre un emplacement obscurci, le DLDA se base sur quatre composants principaux pour obscurcir un tel emplacement qui est : un composant d'analyse de contexte qui permet à l'agent d'être contextuellement conscient de l'emplacement actuel de l'objet. Le second composant est le gestionnaire de confidentialité qui stock les préférences de confidentialité des utilisateurs. Le troisième composant est l'exécuteur de stratégie qui récupère les stratégies pertinentes et exécute des méthodes de contrôle de la divulgation, selon le contexte actuel. Le quatrième composant est le générateur d'emplacement qui applique certaines contraintes spatiales à chaque sortie d'emplacement. L'agent reçoit un emplacement réel actuel d'un dispositif et génère un emplacement fictif à utiliser pour le niveau 5 (L4). L'agent suit un processus pour déterminer les coordonnées des trois points de base.

Discussion et critiques

Cette expérience souffre de deux limitations majeures. Tout d'abord, l'agent DLDA est implémenté de manière centralisée en l'attachant à l'objet. Compte tenu de la nature décentralisée de l'**IdO**, une solution centralisée n'est pas considérée comme l'approche optimale à adopter dans de tels environnements. Par exemple, la solution est considérée peu fiable pour la gestion de plusieurs objets car elle nécessitera l'ins-

tallation de l'agent sur chaque objet. Deuxièmement, parce que l'agent est attaché à l'objet et s'appuie sur ce dernier pour tous les calculs nécessaires ; la scalabilité n'est donc pas assurée, le poids lourd de calcul viole le critère de consommation d'énergie.

2.3.1.4 Enhanced Location Privacy Algorithm for Wireless Sensor Network in Internet of Things

De nous jour, différent types de capteurs recueillent des informations diverses pouvant être privées et contenant l'emplacement d'un objet source. Si un intrus est dans le réseau, alors il est en mesure d'exploiter et de cracker ces informations. Donc l'intrus pourrait déterminer l'emplacement de la source et peut-être de la contrôler. Patel et al. [12] ont proposé un algorithme de multi-routage de marche aléatoire. Dans cet algorithme, plusieurs chemins aléatoires ont été initiés avec un nombre abordable de houblon. Un paquet est transmis au hasard à l'un des voisins, encore et encore jusqu'à ce qu'ils atteignent l'évier. Il est possible qu'un paquet peut être transmis à l'un des voisins de son houblon précédent. Pour éviter le problème de tomber dans une boucle (envoyer un paquet à un voisin déjà dans le chemin). Patel et al ont utilisé un filtre boom qui vérifie ce cas. Ce filtre a réglé une partie de problème et a causé un autre problème ; à chaque fois qu'on suit le filtre, on tombe certainement dans un nœud qui n'a plus de voisins. Alors, le chemin d'accès n'est pas en mesure d'atteindre le nœud destinataire. Une technique est intégrée dans cet algorithme :
La technique de retour arrière, garantie que le chemin mènera toujours à l'évier. Si le chemin réel passe par le nœud intrus et tente de remonter jusqu'à la source, il se trouvera avec plusieurs sources qui rendent difficile de déterminer la source d'origine.

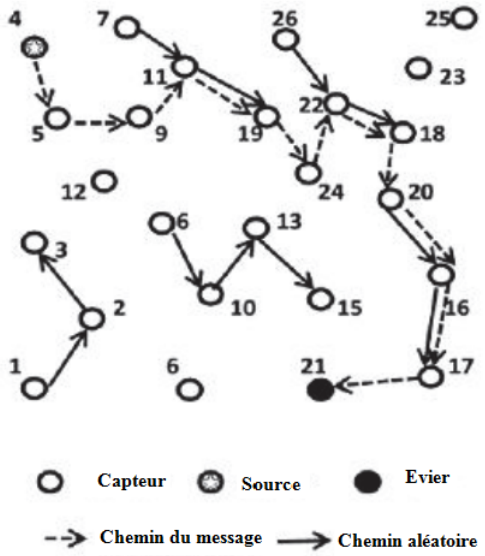

FIGURE 2.2 – Exemple de l'application de l'algorithme multi-routage.

La figure 2.2 illustre un exemple d'application de l'algorithme multi-routage. Dans cet exemple, on a un réseau de 26 objets, l'objet 4 est une source qui veut transmettre le paquet à l'objet 21 qui est le destinataire. Plusieurs chemins sont établis aléatoirement et un seul chemin parmi ces dernier est le chemin réel de paquet. Si le paquet se bloque sur un objet, ce dernier appliquera la technique de retour arrière pour pouvoir continuer la transmission.

Discussion et critiques

Le protocole proposé se base sur un algorithme de multi-routage aléatoire avec une technique de retour arrière. Le critère de scalabilité (évolutivité) est respecté vu que l'algorithme est distribué. Puisque les auteurs n'ont pas défini de politique de sécurité contre les attaques, un intrus peut deviner le nœud source même si il va faire face à plusieurs nœuds source ; le critère de résistance aux attaques n'est pas assure. La technique de routage utilisée provoque une énorme consommation d'énergie chez les objets ne disposant pas de cette quantité d'énergie ; le critère de consommation d'énergie n'est pas assuré non plus.

2.3.2 Solutions au problème de système

2.3.2.1 Privacy and Security in Internet of Things and Wearable Devices

Dans cet article, Orlando Arias et al.[2] se sont focalisés sur la sécurité et la confidentialité de la vie privée dans les dispositifs de l**IdO**. Les chercheurs ont alors proposé des solutions pour faire face au problème de sécurité liés au fait que les dispositifs peuvent stocker et rassembler des informations sur l'utilisateur et créer un profil détaillé aidant à la détermination de la routine quotidienne de l'utilisateur, ce qui représente une atteinte à la vie privée de ce dernier. La première solution proposée consiste en la vérification du firmware au moment de la mise à jour. Cependant, cela est souvent fait par le logiciel qui est considéré comme authentique. La mise en œuvre de cette vérification doit toutefois être valable ; il est insuffisant d'authentifier l'image de mise à jour. La pile logicielle doit également être authentifiée avant de pouvoir déterminer si une mise à jour est valide ou non. Pour ça, les chercheurs ont proposé d'utiliser une chaîne de confiance appropriée dans l'infrastructure matérielle du dispositif afin d'aider le processus à déterminer une pile de logicielle authentique. L'exposition des interfaces de débogage dans les périphériques de l'**IdO** présente un risque lui aussi. Les chercheurs ont alors proposé de limiter l'accès aux unités de débogage. Idéalement, toutes les interfaces de débogage doivent être supprimées de la production ou avoir des protections appropriées, les chercheurs ont proposé une deuxième solution spécifique aux dispositifs de l'**IdO**. Cette solution vise à protéger les périphériques qui chargent des binaires dans l'espace utilisateur. L'approche proposée consiste à charger et exécuter uniquement la binaires cryptographiquement signés. Si la vérification de la signature échoue, le binaire n'est pas exécuté et le périphérique est mis en mode « *failsafe* » , en informant l'utilisateur de l'altération possible.

Discussion et critiques

La solution proposée par les chercheurs, provoque une grande consommation d'énergie. Cela revient au fait de ne charger que les binaires cryptographiquement signés. Il est donc nécessaire d'avoir un chargeur personnalisé pour chaque périphérique afin de permettre de crypter les binaires. La scalabilité n'est pas assurée et cela est dû au fait que les périphériques utilisés doivent être d'une capacité énergétique considérable, ce qui exclu les périphériques à faible consommation d'énergie. La résistance aux attaques est aussi assurée car les chercheurs ont proposé de ne charger que les binaires cryptographiquement signés, permettant ainsi de faire face à différentes attaques.

2.3.3 Solutions au problème d'accès au flux d'informations

2.3.3.1 Considerations Towards Security and Privacy in Internet of Things Based Health Applications

Dans notre vie quotidienne, nous somme souvent mis au défi concernant la confidentialité des données médicales. Viorel Negruont et al [23] ont proposé une solution de confidentialité qui prend en charge la sécurité des données médicales sensibles. L'architecture proposée utilise le contexte de la surveillance des patients à distance. Différents types d'agents de protection des renseignements personnels au courant sont conçus pour collecter, stocker et accéder aux données personnelles du patient. Les données recueillies ne sont visibles que pour le médecin affecté dans le cadre de la relation médecin-patient. Une grande quantité des renseignements personnels recueillis par les capteurs peuvent être stockés sur des serveurs médicaux ce qui peut conduire aux problèmes de sécurité et d'espace de stockage de ces informations.

Discussion et critiques

Le protocole proposé se base sur l'hypothèse qu'un adversaire qui espionne les communications sans fil fait face à des erreurs inévitables qui lui font ainsi manquer

certaines informations transmises dans l'**IdO**. De ce fait, même si l'attaquant obtient le mot de passe et tente de l'utiliser pour se faire passer pour un agent légitime à un moment ultérieur, il ne pourra y arriver car les mots de passe sont cryptés. De plus, l'agent transmet les données récoltées sans crypter l'adresse de ces données ; cela pose un problème de sécurité au système. Le système proposé nécessite tout de même un espace de stockage élevé afin de sauvegarder les données récoltées, ainsi que d'une énergie très élevée.

2.3.3.2 User Interactive Internet of things Privacy Preserved Access control

Dans cet article, Xin Huang et al. [10] ont proposé une amélioration au mécanisme de protection de la vie privée l'**IdO**, qui est constitué principalement de trois entités : l'éditeur **P** qui représente la source de l'information, l'observateur **W** et l'**IdO I** qui est la plateforme où sont partagées les données. Le flux d'information peut être résumé comme suit : $P(PData) \rightarrow I(IData) \rightarrow W(WData)$. Cette amélioration consiste en la conception d'une page de paramètres de confidentialité pour les utilisateurs. Cette dernière inclut les paramètres d'informations personnelles de base et les paramètres généraux d'information du capteur. Chaque capteur peut être réglé dans une page d'information du capteur. Il existe cinq niveaux de protection de la confidentialité par défaut :

- Seulement visible pour moi-même.
- Seulement visible pour mes amis.
- Seulement visible aux gens que je suis.
- Seulement visible aux gens qui me suivent.
- Et visible à tous.

Puisqu'il peut y avoir une chaîne d'observateurs qui souscrivent certaines données de capteurs, les chercheurs fournissent également une chaîne d'abonnement basée sur la fonction de regroupement des observateurs, permettant ainsi à l'éditeur de contrôler facilement le flux d'information à l'aide de cette fonction.

Discussion et critiques

Dans cet article, Xin Huang et al.[10] ont proposé une solution afin d'améliorer le mécanisme de protection de la vie privée. Cette solution permet une faible consommation d'énergie puisque, elle consiste à ajouter une page de paramètres de confidentialité qui n'est pas de grande taille. La scalabilité est aussi assurée car aucune contrainte n'est définie pour les objets et l'amélioration proposée peut-être appliquée pour tous les objets. La résistance aux attaques quant à elle n'est pas assurée car les niveaux de protection de la confidentialité est une politique de sécurité.

2.4 Synthèse

Notre étude des travaux existants nous a permis de classifier ces travaux selon le problème traité : protection de localisation, protection du système, protection du flux d'informations.

La Table 2.2 illustre une étude comparative que nous avons menée sur les différents protocoles analysés précédemment selon les critères d'évaluation.

		Consommation d'énergie	Sécurité	Evolutivité
Solutions au problème de localisation	**Ikram Ullah et al. [25]**	oui	non	oui
	Mahmoud Elkhodr et al. [16]	oui	non	non
	Patel et al. [12]	non	non	oui
Solutions au problème de système	**Orlando Arias et al. [2]**	non	oui	non
Solutions au problème d'accès au flux d'informations	**Viorel Negruont et al. [23]**	non	non	oui
	Xin Huang et al. [10]	oui	non	oui

TABLE 2.2 – Comparaison des protocoles étudiés

2.4.0.3 Modèles pour la protection de localisation

Les modèles proposés permettent d'assurer le critère de consommation d'énergie sauf pour celui de Patel et al. [12] qui utilise une technique de multi-routage, ce qui provoque une grande consommation d'énergie. La scalabilité est aussi assurée par tous les modèles sauf celui de Mahmoud Elkhodr et al. [16] qui utilise une technique DLDA, une technique limitée par le fait d'être centralisée, d'où la non scalabilité du modèle. Pour la résistance aux attaques, aucun des modèles proposés dans cette partie ne l'assure ; aucune politique de sécurité n'est établie.

2.4.0.4 Modèles pour la protection du système

Le modèle proposé dans cette partie, Orlando Arias et al.[2] ne permet pas d'assurer le critère de la consommation d'énergie. Cela revient au fait qu'il utilise la cryptographie. La scalabilité n'est pas assurée non plus car la solution proposée exclu les objets à basse consommation d'énergie, ce qui limite le nombre d'objets auxquels la solution peut être appliquée. Quant à la résistance aux attaques, ce modèle ne permet pas de l'assurer car aucune politique de sécurité n'a été mise en place.

2.4.0.5 Modèles pour la protection du système

Les modèles proposés permettent une bonne consommation d'énergie et ont un réel potentiel pour permettre la décentralisation afin d'assurer la scalabilité. Cependant, cette classe présente une faiblesse car elle n'est pas résistante aux attaques ; aucune politique de sécurité n'est proposée.

On retient de l'ensemble des modèles étudiés que les informations personnelles et privées des utilisateurs de l'**IdO** ne sont pas protégées, que ce soit des données de localisation, des données système ou d'autres données privées car aucune politique de sécurité n'est définie ou mise en œuvre afin de permettre la protection des ces données.

2.5 Conclusion

La sécurité de la vie privée dans l'**IdO** est un domaine important, et un grand nombre de problèmes restent encore à être surmontés. Dans ce chapitre, nous avons établi un état de l'art sur les travaux de recherche existants concernant les mécanismes de sécurité dans l'**IdO**. Nous avons brièvement décrit chaque solution étudiée suivie d'une discussion sur les points forts et les points faibles de chacune d'entre elle. De cette analyse nous avons retenu que de toutes les solutions proposées, aucune ne garantit l'ensemble des critères préalablement définis, surtout celui de la résistance aux attaques. Enfin, nous les avons comparées selon les différents critères retenus. Le chapitre suivant sera consacré à la description détaillée de notre solution.

Chapitre 3

Notre proposition

3.1 Introduction

Après avoir étudié quelques solutions récentes pour assurer la sécurité de la vie privée dans l'**IdO**. Nous avons conclu l'importance de la localisation dans le respect et la confidentialité de la vie privée des utilisateurs de l'**IdO** dans les modèles proposés. D'une autre part, nous avons identifié des faiblesses présentes dans la littérature.

Ce chapitre sera consacré à la présentation de notre architecture qui permet de sécuriser l'emplacement des objets en se basant sur le protocole CHORD qui permet d'exécuter plus rapidement la requête de l'utilisateur. Grâce au chiffrement asymétrique (CP-ABE) et au chiffrement symétrique, nous pouvons sécuriser la transmission et éviter les problèmes d'interférences entre plusieurs utilisateurs. Nous définirons aussi un modèle d'attaque sur lequel nous nous baserons pour démontrer le niveau de sécurité de notre protocole.

3.2 Motivation

L'**IdO** est un mélange de plusieurs technologies qui forment un réseau hétérogène. Les objets d'un tel environnement sont souvent confrontés à effectuer différents services. Cependant, la réalisation de certains de ces services nécessite

beaucoup de ressources dont l'objet ne dispose pas toujours. C'est dans ce contexte que les approches collaboratives sont souvent sollicitées. Le principe de telles approches consiste à trier l'ensemble des objets qui composent un environnement afin de former les communautés d'objets s'aidant mutuellement pour la réalisation de services coûteux. En résume, les objets de l'**IdO** peuvent être en proie à plusieurs menaces et les attaques peuvent être tant bien intentionnelles qu'accidentelles.

Les problèmes de la confidentialité de l'emplacement des utilisateurs de l'**IdO** sont importants pour la simple raison qu'ils peuvent menacer la sécurité personnelle des utilisateurs, et ainsi porte atteinte à la vie privée de ces derniers. Ce qui nous as poussé à proposer une architecture permettant de sécuriser et assurer la confidentialité de l'emplacement et permettre le respect de la vie privée des utilisateurs de l'**IdO**.

3.3 Préliminaires

Demandeur de service : Un demandeur de service est un objet qui a envoyé une demande de service auprès du gestionnaire de localisation.

Point d'accès : un point d'accès est caractérisé par des capacités très élevées en termes d'énergie et de traitement des données. Il permet aussi de récupérer l'emplacement demandé.

Autorité d'attribut : l'autorité d'attribut est une entité qui permet de partager la clé publique et la clé privée entre le point d'accès le plus proche de l'objet à localiser et le point d'accès sollicité par le demandeur de service.

Demande de service : une demande de service est une requête envoyée par un objet au gestionnaire de localisation afin de demander des informations sur un service.

Objet à localiser : autorité que le demandeur de service cherche à localiser.

Cryptage par attribut

Le cryptage basé sur les attributs (ABE, *Attribute Based Encryption*) est une technique relativement nouvelle d'autorisation et de cryptage à clé publique qui a été proposée par Sahai et Waters [21]. Avec ABE, une entité crypte un message vers des récepteurs inconnus en fonction d'une structure d'accès de sa préférence. Cependant, les récepteurs ne peuvent décrypter le message que s'ils possèdent un ensemble d'attributs répondant à la politique d'accès. Donc, ABE est un outil précieux pour fournir l'autorisation et la confidentialité. Il existe deux principaux types d'ABE : *Ciphertext-Policy ABE* (CP-ABE)[5] et *Key-Policy ABE* (KP-ABE) [4]. Dans CP-ABE, les clés secrètes sont associées à un ensemble d'attributs et le texte chiffré spécifie la politique d'accès. Dans KP-ABE, le texte chiffré est associé à l'ensemble des attributs et la politique d'accès est appliquée dans la clé secrète d'un utilisateur. Dans ce travail, nous nous concentrons uniquement sur CP-ABE, car il fournit plus de contrôle sur qui peut avoir accès aux données par rapport à KP-ABE.
CP-ABE consiste en cinq algorithmes principaux. Nous expliquerons chacun de ces algorithmes dans ce qui suit [5] :

- **Algorithme d'installation (Setup) :**

L'algorithme d'installation ne prend aucune entrée autre que les paramètres implicites de sécurité. Il donne en sortie : la clé publique PK (*Public key*) et la clé de maitre MK (*Master key*).

- **Algorithme de chiffrement (Encrypt) :**

L'algorithme prend en entrée la clé publique PK, un message à chiffrer M, et un arbre d'accès A qui définit tous les ensembles d'attributs possibles qui vont permettre le déchiffrement et l'accès au message M. Il donne en résultat le chiffrement du message M, l'arbre d'accès A, et d'autres informations nécessaires au déchiffrement

de la donnée.

- **Algorithme de génération de clé (KeyGen) :**

L'algorithme de génération de clé prend comme entrée la clé de maitre MK, et un ensemble d'attributs S qui définit un utilisateur. Il donne en sortie une clé privée SK.

- **Algorithme de déchiffrement (Decrypt) :**

L'algorithme de déchiffrement prend en entrée la clé publique PK, le message chiffré CT et d'autres informations telles que l'arbre d'accès A et une clé privée SK, qui est spécifique à un certain ensemble S d'attributs. Si ce dernier satisfait l'arbre d'accès A, l'algorithme va être capable de déchiffrer le message.

- **Algorithme de délégation (Delegate) :**

L'algorithme de délégation prend en entrée une clé secrète SK qui est utilisée pour décrire un ensemble d'attributs S, il prend aussi en entrée un ensemble $\overline{S} \subseteq S$, et il donne en sortie la clé secrète SK qui décrit l'ensemble d'attributs S.

Protocole CHORD

Afin de faire face au problème de décentralisation notre architecture utilise le protocole CHORD [9]. Afin d'assurer la scalabilite et décentraliser l'architecture. CHORD repose sur une topologie en anneau ou chaque nœud représente un point d'accès : un nœud CHORD a la connaissance de son prédécesseur et du nœud suivant. Chaque nœud est placé dans l'anneau de manière à ordonner les adresses IP par ordre croissant afin de facilité la recherche du point d'accès le plus proche de l'objet à localiser. En premier lieux, le point d'accès le plus proche de l'utilisateur émet la requête suivie de l'adresse IP de l'objet à localiser au point d'accès successeur. Ce dernier vérifie si la partie réseau de l'adresse IP de l'objet à localiser correspond à la partie réseau de son adresse IP. Si oui, alors ce point d'accès correspond à celui recherché, sinon il consulte la table de routage et cherche le point d'accès qui a l'adresse IP la plus grande et inférieure ou égale à l'adresse IP

de l'objet à localiser et ainsi de suite jusqu'à trouver le point d'accès le plus approprié.

3.4 Notre modèle

L'architecture que nous proposons permet une confidentialité de l'emplacement d'un objet. La figure 3.1 suivante représente les étapes de notre modèle qui se base sur l'utilisation de protocole CHORD, de la cryptographie asymétrique (à base d'attribut CP-ABE) et aussi du chiffrement symétrique afin de permettre une transmission sécurisée de l'emplacement et un contrôle d'accès à l'emplacement des objets qui est lui-même relié a des utilisateurs, ceci permettra d'assurer la confidentialité de la vie privée des utilisateurs de l'**IdO**

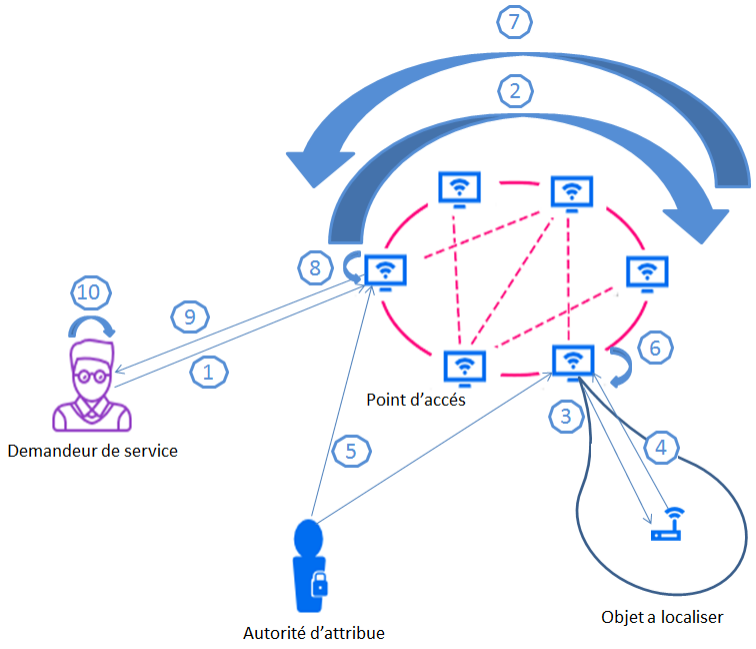

FIGURE 3.1 – Notre modèle

Dans ce qui suit une description des différentes étapes illustrées sur la figure 3.1 :

Étape 1 : Initialement le demandeur de service envoie la requête de recherche au point d'accès le plus proche de lui, accompagnée de la structure d'accès chiffrée et de la date d'émission en clair et chiffrée afin de permettre une authentification.

Étape 2 : Le point d'accès reçoit la requête, déchiffre la date chiffrée et la compare à celle en claire. Si les dates ne correspondent pas, alors la procédure s'arrête, sinon le point d'accès applique le protocole CHORD afin de trouver plus rapidement le point d'accès le plus proche de l'objet à localiser.

Étape 3 : Le point d'accès destinataire transmet la requête du demandeur de service à l'objet à localiser, pour récupérer son emplacement.

Étape 4 : L'objet chiffre son emplacement et sa structure d'accès avec la clé symétrique partagée avec le point d'accès le plus proche de lui et le lui envoie.

Étape 5 : L'autorité d'attribut partage le couple de clé (PK, SK), clé publique et clé secrète entre le point d'accès le plus proche du demandeur de service et le point d'accès le plus proche de l'objet à localiser, leur permettant ainsi de génère une clé privée pour le chiffrement et le déchiffrement.

Étape 6 : Le point d'accès le plus proche de l'objet déchiffre l'emplacement chiffré avec la même clé symétrique et vérifie la validité de l'emplacement reçu et son périmètre de couverture. Si l'emplacement n'est pas valide, alors le point d'accès chiffre son emplacement avec une clé privée générée à partir du couple de clé asymétrique reçu de la part de l'autorité d'attribut et la structure d'accès de l'objet à localiser. Sinon, si l'emplacement est valide,

alors il applique la même procédure toute en chiffrant l'emplacement reçu.

Étape 7 : Après avoir chiffré l'emplacement de l'objet le point d'accès applique le protocole CHORD inverse pour transmettre le résultant au point d'accès source.

Étape 8 : Le résultat étant reçu par le point d'accès source, ce dernier déchiffre le résultat avec la clé asymétrique générer à partir du couple de clé public et clé secrète attribuée par l'autorité d'attribut et la structure d'accès du demandeur de service.Le résultat obtenu est chiffré avec la clé symétrique partagée avec le demandeur de service.

Étape 9 : Le point d'accès source émet alors le résultat de la requête au demandeur de service.

Étape 10 : Le demandeur de service reçoit le résultat, le déchiffre avec la même clé symétrique échangé avec le point d'accès source et obtient l'emplacement de l'objet à localiser.

3.5 Analyse de sécurité de notre modèle

Dans cette section, nous présenterons différentes attaques que peut subir les objets de l'**IdO** afin de mieux démontrer les différents objectifs de sécurité que notre modèle permet d'assurer. Ci-dessous, les principales attaques que l'on peut mener sur une communication dans l'**IdO** et une analyse des propriétés de sécurité de notre architecture :

- **Attaque par déni de service (DoS, *Denial of Service*)**

Souvent les objets déployés dans l'**IdO**, à l'instar des capteurs et tags RFID, peuvent avoir de sévères contraintes des ressources : capacités en calcul et en

stockage limitées, autonomie en énergie limitée (fonctionnement sous batteries). Dans ce cas, le but de l'attaquant et simplement d'épuiser les ressources de ces objets, soit en saturant leur mémoire de stockage, ou en épuisant leur énergie [24]. L'attaque par déni de service n'est pas prise en compte par notre architecture dans le sens où le protocole ne peut pas empêcher cette attaque de survenir. Il permet cependant d'assurer la confidentialité des données échangées lorsque cette attaque se produit ou est combinée à une autre attaque. Un intrus qui effectue une attaque ne pourra pas obtenir une quelconque information confidentielle sur l'emplacement de l'objet à localiser.

- **Attaque par rejoue**

Attaque où un objet qui peut être malveillant, intercepte et enregistre une partie ou bien la totalité d'une session de communication et la rejoue ensuite dans le but d'usurper l'identité d'un objet ou d'un utilisateur quelconque [24]. Cette attaque est difficile à être appliquer dans notre modele grâce à la mobilité des objets utilisés, à l'utilisation du protocole CHORD et au fait d'utiliser une variable temps permettant ainsi de préciser le moment de l'émission des messages échangés entre le demandeur de service et le point d'accès le plus proche de lui.
Par exemple si un attaquant enregistre une session de communication entre un objet et un point d'accès, puis la rejoue après cette attaque n'est pas faisable puisque le point d'accès vérifie la fraicheur de la requête en comparant entre les deux date reçu, alors si les date ne sont pas identiques alors la requête sera annuler.

- **Attaques d'écoutes passives**

Vu que les communications des objets se font souvent en clair via un médium partagé en utilisant une infrastructure de communication publique, un attaquant peut facilement avoir accès aux données échangées. Un attaquant peut facilement avoir accès à la donnée privée concernant l'emplacement d'un objet ou d'un utilisateur quelconque [24]. Notre protocole fait face à ce genre d'attaque en utilisant un chiffrement asymétrique (CP-ABE) et un chiffrement symétrique (AES), ce qui fait que l'emplacement d'un objet est sécurisé et confidentiel.
Par exemple si un attaquant essaye d'accès aux données échangé sur le réseau que ce soit la requête émise par le demandeur de service ou le résultat émis par l'objet a

localise l'attaquant devra faire face au chiffrement symétrique(AES) pour le premier cas et au chiffrement asymétrique (CP-ABE) pour le deuxième cas.

- **Attaque de l'homme du milieu**

C'est une attaque informatique où une personne qui peut être malveillante, intercepte et relaie la communication entre deux entités. Il pourra ensuite par exemple se faire passer pour l'un des partis et avoir des informations confidentielles [20]. Dans notre architecture chaque objet est à proximité d'un point d'accès, alors l'authentification et effectuée automatiquement et directement entre le demandeur de service et le point d'accès le plus proche de lui. Lors de l'émission d'une quelconque requête, cette dernière est accompagnée d'une date chiffrée avec une clé symétrique et une autre en claire, ce qui permet une authentification directe du demandeur de service. Même si un attaquant essaie de s'interposer entre les deux parties, il n'aura aucun moyen de se faire passer pour l'une comme pour l'autre.
Par exemple si un attaquant essaie de s'interposer entre les deux parties communicante, il n'aura aucun moyen de se faire passer pour l'une comme pour l'autre, car une authentification est effectuer entre chaque objet et le point d'accès le plus proche de lui.

3.6 Conclusion

Dans ce chapitre, nous avons proposé un modèle pour la sécurité dans l'**IdO**. Notre modèle introduit l'utilisation du protocole CHORD, qui est un protocole permettant de décentraliser le réseau et de réduire le temps de recherche du point d'accès le plus proche de l'objet à localiser, ainsi que le protocole CP-ABE permettant de garantir la confidentialité des échanges entre les différent points d'accès du réseau. Nous avons aussi dédié une partie de ce chapitre à l'analyse de la sécurité de notre modèle en présentant différentes attaques que l'**IdO** peut subir et comment notre modèle protège ce type de système.
Le chapitre suivant fera l'objet de simulation et d'évaluation de performances de notre modèle.

Chapitre 4

Simulation et évaluation des performances

4.1 Introduction

Après avoir décrit les différentes étapes de notre architecture dans le chapitre précédent, une évaluation des performances s'impose afin de valider notre proposition.
Ce chapitre est consacré à l'évaluation des performances de notre architecture de sécurisation des emplacements et de leurs confidentialités. Nous présenterons en premier lieu l'environnement et les paramètres de simulation considérés pour l'évaluation des performances de notre solution. Nous décrirons par la suite le critère et les métriques de simulation utilisés. Les résultats obtenus à l'issue de ces simulations seront finalement interprétés et comparés avec un protocole récent étudié dans le chapitre de l'état de l'art.

4.2 Environnement de simulation

Dans cette section, nous présentons au préalable les paramètres de simulation, puis nous décrivons le critère et les métriques de simulation utilisés.

4.2.1 Paramètres de simulation

Les simulations ont été réalisées en utilisant le langage de programmation Java. Nous avons simulé les différentes interactions entre le demandeur de service, l'objet à localiser ainsi que l'anneau de CHORD et l'autorité d'attribut. Le demandeur de service chiffre avec une clé symétrique sa requête de taille tr qui sera traitée par le point d'accès le plus proche. Par la suite, le protocole CHORD est exécuté avec une vitesse de transmission vtr et un temps de vérification tv par chaque point d'accès composant l'anneau. Arrivée au point d'accès le plus proche de l'objet à localiser, la requête sera émise à l'objet qui renverra son emplacement chiffré de taille te. Le protocole CHORD inverse et alors appliqué afin de renvoyer le résultat de la requête au demandeur de service.
Les paramètres fixés pour la réalisation des simulations sont définis dans la table 4.1.

Paramètre	Valeur
Vitesse transmission chord vtr	7 bit/ms
Temps de vérification tv	4 ms
Taille de la requête tr	65 bits
Taille de l'emplacement te	15 bits

TABLE 4.1 – Paramètres de simulation.

4.2.2 Critère et métriques de simulation

Dans cette section, nous présentons le critère et les métriques de simulation que nous avons utilisés pour l'évaluation de performances de notre architecture.

Critère de simulation

Le critère de simulation utilisé pour l'évaluation de performance de notre architecture est la taille du réseau. Dans l'**IdO**, le nombre d'objets est très grand. La taille du réseau ou le nombre d'objets connectés se trouve être un paramètre

important à prendre en compte vu son influence sur les temps d'attente et de communication.

Métriques de simulation

Afin d'évaluer les performances de notre architecture, nous utilisons les métriques de simulation suivantes : Temps d'attente et temps de communication.

- Temps de communication

Représente le temps que nécessitent les différentes transmissions effectuées entre les différentes entités de l'architecture.

- Temps d'attente

Représente la durée nécessaire à la requête pour être transmise, traitée et renvoyée. Le temps d'attente inclut ainsi le temps de vérification, le temps de transmission et les temps de chiffrement et de déchiffrement.

4.3 Résultats obtenus

La figure 4.1 illustre les résultats obtenus en matière de temps de communication pour notre architecture et le protocole de Patel et al. [12], nous constatons que le temps de communication augmente en augmentant la taille du réseau pour les deux cas. Les performances de notre architecture sont néanmoins meilleures puisque elle consomme moins de temps de communication comparé au protocole concurrent. Ceci revient au fait d'utiliser le protocole CHORD. En effet, dans notre architecture, l'utilisation de CHORD a permis d'augmenter la rapidité et la facilité de recherche

ainsi que la réduction du temps de communication. Parallèlement, dans le protocole de Zhou et al. [12], le temps de communication augmente considérablement à cause de la technique de routage avec retour arrière.

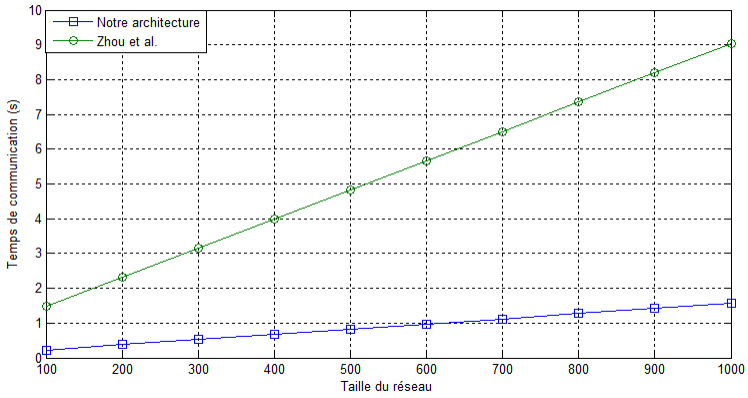

FIGURE 4.1 – Temps de communication en fonction de la taille de réseau.

La figure 4.2 illustre les résultats obtenus en matière de temps d'attente pour notre architecture et le protocole concurrent [12]. Le temps d'attente augmente en augmentant la taille de réseau pour les deux protocoles. Quand la taille du réseau est inférieure à 300 objets, les performances du protocole concurrent sont meilleures que notre architecture. Cela est dû au fait que le protocole concurrent n'a aucune politique de sécurité. Cependant, dès que la taille dépasse 300 objets, le temps d'attente devient plus important pour le protocole concurrent, car la technique de retour arrière nécessite beaucoup plus de temps alors que le protocole CHORD, sur lequel se base notre architecture, permet de réduire ce temps d'attente. Enfin, les performances de notre architecture sont largement meilleures à large échelle, ce qui est plus avantageux compte tenu de l'expansion rapide que connait l'**IdO**.

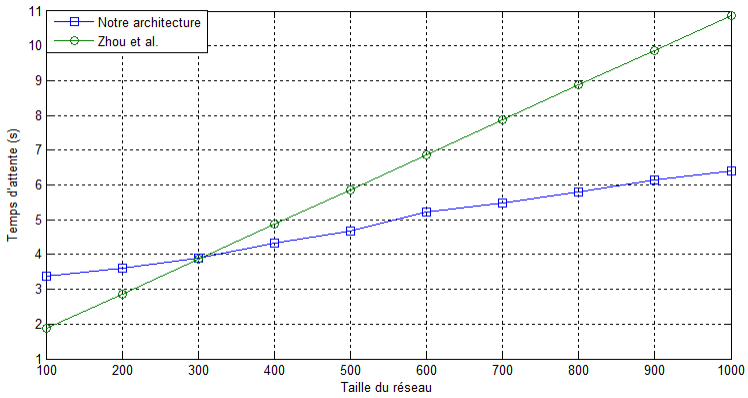

FIGURE 4.2 – Temps d'attente en fonction de la taille de réseau.

4.4 Conclusion

Nous avons conclu dans ce dernier chapitre notre travaille avec une simulation et une évaluation des performances de notre architecture. Nous avons comparé les résultats obtenus avec celle d'un autre protocole de localisation existant dans la littérature. Pour ce faire, nous avons fait varier la taille du réseau afin d'étudier son impact sur les temps de communication et le temps d'attente. Les résultats obtenus montrent que notre architecture est plus performante que le protocole concurrent.

Conclusion générale et perspectives

L'Internet des objets est une technique qui fait couler beaucoup d'encre actuellement, et qui marque le début d'une nouvelle ère en matière de connéctivité et de mobilité dans différents domaines de la vie quotidienne. Cependant, et à l'instar de toute autre nouvelle technologie, l'**IdO** n'est pas dénuée de difficultés et de défis à relever. Un défi très important reste, sans doute, la protection et la confidentialité des données privées et la sécurité des objets connectés. D'où l'importance de la fonction du contrôle d'accès aux données privées des utilisateurs.

Dans ce présent mémoire, nous avons abordé le thème de "privacy dans l'**IdO**. Cas d'étude : la localisation". Nous avons présenté dans un premier chapitre, le concept de l'Internet des objets, ses caractéristiques ainsi que son architecture et ses domaines d'application. Par la suite, nous avons présenté quelques menaces de sécurité. Enfin, nous avons présenté les défis à relever et le concept de la vie privée. Dans le deuxième chapitre, nous avons présenté des critères d'analyse et mené une étude critique des solutions existantes. Ceci nous a permis de dégager les points faibles et forts des différentes solutions afin de proposer une nouvelle solution.

Dans le troisième chapitre, nous avons proposé une architecture qui permet de remédier au problème de la sécurité et la confidentialité de l'emplacement des utilisateurs de l'**IdO**. En premier lieu, nous avons présenté les techniques que nous avons utilisées dans notre architecture (CP-ABE et CHORD) et par la suite nous avons présenté ses différentes étapes. Enfin, nous avons évalué notre solution avec

une analyse de sécurité. Nous avons démontré à travers cette analyse, la robustesse de notre architecture contre les différentes attaques qui menacent la vie privée des utilisateurs de l'**IdO**.

Dans le dernier chapitre, nous avons évalué les performances de notre architecture à travers des simulations en la comparant avec un protocole concurrent et les résultats obtenus sont encourageants.

Comme perspectives pour les futurs travaux, nous envisageons l'implémentation de notre solution, puis par la suite évalué ces performances et les comparer à d'autres protocoles existants dans la littérature, en se basant sur d'autres critères.

Bibliographie

[1] A. Al-Fuqaha, M. Guizani, M. Mohammadiand M. Aledhari, and M. Ayyash. Internet of things : A survey on enabling technologies, protocols and applications. *Communications Surveys and Tutorials, IEEE*, 1, 2015.

[2] O. Arias, J. Wurm, K. Hoang, and Y. Jin. Privacy and security in internet of things and wearable devices. *IEEE TRANSACTIONS ON MULTI-SCALE COMPUTING SYSTEMS*, 1(2) :99–101, 2015.

[3] K. Ashton. that 'internet of things in the real world, things matter more than ideas. *RFID journal*, 22 June 2009.

[4] N. Attrapadung, B. Libert, and E.D. Panafieu. Expressive key-policy attribute-based encryption with constant-size ciphertexts". *Public Key Cryptography - PKC 2011*, pages 90–108, 2011.

[5] J. Bethencourt, A. Sahai, and B. Waters. Ciphertext-policy attribute-based encryption. *Proc. IEEE Symp. Secur. Privacy (SP)*, pages 321–334, May 2007.

[6] Y. Challal. *Sécurités de l'internet des objets : vers une approche cognitive et systématique*. PhD thesis, Universit´e de Technologie de Compiegne, 2012.

[7] B. Dupont. l'environnement de la cybersécurité à l'horizon 2022 tendances, moteurs et implications. *note de recherche no. 14, canada*, pages 18–20, 2012.

[8] M. Elkhodr, S. Shahrestani, and H. Cheung. A contextual-adaptive location disclosure agent for general devices in the internet of things. *IEEE Conf. Local Comput*, (38) :848–855, 2010.

[9] Jan Holvast. History of privacy. in the future of identity in the information society. *IFIP Advances in Information and Communication Technology, Springer Boston*, 298 :13–42, 2009.

[10] X. Huang, R. Fu, B. Chen, T. Zhang, and A. W. Roscoe. User interactive internet of things privacy preserved access control. *The 7th International Conference for Internet Technology and Secured Transactions (ICITST-2012).*, 2012.

[11] S. M. Riazul Islam, K. Daehan, M. Humaun Kabir, M. Hossain, and K. Kyung-Sup. The internet of things for health care : A comprehensive survey. *Access, IEEE*, 3 :678–708, 2015.

[12] D. R. Patel J. Sathishkumar. Enhanced location privacy algorithm for wireless sensor network in internet of things. *2016 International Conference on Internet of Things and Applications (IOTA) Maharashtra Institute of Technology, Pune ,India 22 Jan - 24 Jan*, 2016.

[13] H. j. Zhang and F. Guo. The study of a dual-channel automotive supply chain based on internet of things. *Management Science and Engineering (ICMSE), 2013 International Conference*, pages 650–658, 2013.

[14] R. Khan, S. U. Khan, R. Zaheer, and S. Khan. Future internet : the internet of things architecture, possible applications and key challenges. *Frontiers of Information Technology (FIT), 2012 10th International Conference*, pages 257–260, 2012.

[15] M. Leo, F. Battisti, M. Carli, and A. Neri. A federated architecture approach for internet of things security. *Euro Med Telco Conference (EMTC), 2014*, pages 1–5, 2014.

[16] S. Shahrestani M. Elkhodr and Hon Cheung. A contextual-adaptive location disclosure agent for general devices in the internet of things. *2013 IEEE 38th Conference on Local Computer Networks Workshops (LCN Workshops)*, 2013.

[17] W. Miao, L. Ting-Jie, L. Fei-Yang, S. Jing, and D. Hui-Ying. Research on the architecture of internet of things. *Advanced Computer Theory and Engineering (ICACTE), 2010 3rd International Conference*, pages V5–484–V5–487, 2010.

[18] C. Perera, A. Zaslavsky, P. Christen, and D. Georgakopoulos. Context aware computing for the internet of things : A survey. *IEEE Communications Surveys and Tutorials*, 16(1) :414 – 454, 03 May 2013.

[19] H. Petersen, E. Baccelli, and M. Wahlisch. Interoperable services on constrained devices in the internet of things. *W3C Workshop on the Web of Things*, 2014.

[20] M. Rouse. man-in-the-middle attack (mitm) definition. available. http ://internetofthingsagenda.techtarget.com/definition/man-in-the-middle-attack-MitM., 2015, janvier 2016.

[21] A. Sahai and B. Waters. Fuzzy identity-based encryption. *Advances in Cryptology - EUROCRYPT 2005, Springer*, 3494 :457–473, 2015.

[22] H. Sundmaeker, P. Guillemin, P. Friess, and S. Woelfflé. Vision and challenges for realising the internet of things. *CERP-IoT – Cluster of European Research Projects on the Internet of Things*, 2010.

[23] M. Frincu T. Ivascu and V. Negru. Considerations towards security and privacy in internet of things based ehealth applications. *IEEE 14th International Symposium on Intelligent Systems and Informatics, Subotica, Serbia ,August 29-31*, 2016.

[24] H.C. Van Tilborg and S. Jajodia. Encyclopedia of cryptography and security. *Springer Science and Business Media*, 2011.

[25] I. Ullah and M. A. Shah. A novel model for preserving location privacy in internet of things. *2016 22nd International Conference on Automation and Computing (ICAC), IEEE*, 2016.

[26] A.F. Westin. *Privacy and Freedom.Bodley Head*. Bodley Head, 1970.

[27] M. Zaknoun, Karim, and M. Kanoune Yahia. Applicabilité du protocole de sécurité d'internet tls/dtls dans le contexte de l'internet des objets : Limitations et adaptations dans le contexte de communications de bout-en bout. Mémoire de fin d'études pour l'obtention du diplôme d'ingénieur d'État en informatique, Ecole Supérieur d'Informatique, 2014.

RÉSUMÉ

Au cours des dernières années, nous avons observé le développement de dispositifs connectés et nomades tels que les téléphones mobiles, tablettes ou même les ordinateurs portables, afin de permettre aux individus de les utiliser dans leur quotidien. Néanmoins, ces derniers présentent des risques sur la vie privée qui ne sont pas forcément perçus par les utilisateurs. Le problème est soulevé lorsqu'une entité étrangère peut accéder aux données privées des utilisateurs de l'**IdO** et en déduire des informations personnelles. Quelques solutions ont été proposées au cours des dernières années pour protéger les utilisateurs, mais le problème de sécurité reste toujours d'actualité. Ce travail intervient dans le but d'apporter une solution au problème de la localisation des objets dans l'**IdO**. Dans un premier lieu, un état de l'art de différents travaux existants dans la littérature a été établi. Une proposition vient ensuite apporter une solution au problème de sécurité de la localisation des utilisateurs de l'**IdO**. L'architecture proposée se base sur l'utilisation du chiffrement CP-ABE ainsi que l'utilisation du protocole CHORD, afin de permettre la sécurité de l'emplacement des objets et de ce fait, le respect de la vie privée. Des simulations viennent ensuite valider l'architecture proposée.

Mots clés : IdO, sécurité, localisation, CP-ABE, CHORD.

ABSTRACT

In the recent years, we observe the development of connected devices and nomads such as mobile phones, tablets or even laptops intended for daily usage. However, these developments come with some risks that might not be perceived by the users. These threats are compromising when an outside entity has access to the users private data in the IoT (Internet of Things) and will be able to access to the users personal information. Some solutions have been proposed in the recent years in order to protect the users, but the security remains a challenging issue. This work is carried out with the aim to provide a solution to the localization of objects in the IoT. First, the different existing solutions have been examined. Then, a solution is proposed to address the problem of the users localization security. The proposed architecture is based on the use of CP-ABE encryption as well as CHORD protocol in order to ensure the location security of the objects and thus the respect of privacy. Finally, simulations have been carried out to validate the proposed architecture.

Key words : IoT, security, localization, CP-ABE, CHORD.