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

Université Mohamed Sadik Benyahia de Jijel
Faculté des Sciences Exactes et informatique
Département d'Informatique

Mémoire de fin d'étude

pour obtention du diplôme de Master de Recherche en Informatique

Option: ***Informatique légale et multimédia***

Thème

Gstion de la confidentialité des données pour les dispositifs IOT (Internet of Things)

Présenté par:
Droua sohib.
Terir Karim.

Encadré par:
Bouchaib Fazia.

Promotion: 2020.

⁂ *Remerciements* ⁂

Avant tout, nous remercions Allah tout puissant qu'il nous a guidré tout au long de nous vie, qu'il nous a donnré courage et patience pour passer tous les moments difficiles, qu'il nous a permis d'achever ce travail et de pouvoir le mettre entre vos mains aujourd'hui.

Tout d'abord, nous tenons á remercier l'encadreur.MM fazia bouchaib, qui ont confiance en nous et ils nous ont permis de travailler sur un sujet de mémoire. Nous adressons également nos sincéres remerciements et notre gratitude aux A tous mes amis.

Nous remercions par ailleurs vivement les membres du jury de nous avoir fait l'honneur de juger notre travail et d'assister á la soutenance.

Nous remerciements á tous les enseignants du département de Sciences.

Finalement, nous remercions toutes les personnes qui ont participé de prés ou de loin á la concrétisation de ce mémoire.

⁂ *Déicaces* ⁂

A mes parents pour votre énorme sacrifice á m'offrir

le repos et le bonheur, pour l'éducation que vous m'avez

inculquée, pour votre entier engagement á étre á mes cotés á chaque

fois que j'ai besoin d'un soutien moral et matériel.Trés chers parents

je ne vous remercierai jamais assez pour vos actes.
A mes chers fréres **houssem karroud** et **salah bounar** et **rami**
et **Roufaida Belatreche** et **Amina Boudjlida**

A qui m'a encouragé et m'a soutenu.
A tous mes collégues de la promotion de 2020.

Contents

List of Tables

List of Figures

Liste des abréviations

AES Advanced Encryption Standard

ADSL Asymmetric Digital Subscriber Line

API Application Programming Interface

CBC Cipher Block Chaining

CDMA Code Division Multiple Access

CDDL Common Development and Distribution License

CEI Communauté des États Indépendants

CMM Chromatographie couche mince

CTR CounTeR

DES Data Encryption Standard

DDos Distributed Denial of service

DDs Dénie de service

DSS Digital Signature Standard

EPS Evolved Packet System

ETSI European Telecommunications Standards Institute

EUMTS Evolved Universal Mobile Telecommunications System

E-UTRA Evolved Universal Terrestrial Radio Access

FDMA Frequency Division Multiple Accés

FS Forward Secrecy

FRMPay Financial Risk ManagerPay

GPS Global Positioning System

GSM Global System for Mobile

GPRS General Packet Radio Service

IOd Internet des objets

IOT Internet of things

IDO Investment Development Office

IDO Integrated Development Environment

IPv6 Internet Protocol Version 6

6lowPAN IPv6 over Low -Power Wireless Personal Area Networks

IETF6L low PAN IPv6 Low power Wireless Personal Area Networks ou IPv6 LoW Inter-PAN

IETFRPL Internet Engineering Task Force

IP Internet Protocol

IOS International Organization for Standardization

JDK Java Development Kit

LLC Logical Link Control

LTE Long Term Evolution

LORAWAN Low Power Wide Area Network

M2M Machine à Machine

MAA Message Authenticator Algorithm

MAC Media Access Control

MHz Megahertz

MITM Man In The Middle

MIC Message Integrity Code

MS Mobile Station

NIST le National Institute for Standards and Technology

NFC Near Field Communication

NFB National Federation of the Blind

NSA National Security Agency

OCARI Open Communication protocol for Ad hoc Reliable industrial Instrumentation

PAN Personal Area Network

PDH Porteuse Digital Health

PDA Personal Digital Assistant

PIN Personal Identification Number

PSK Pre-Shared Key

RFID Radio Frequency Identification

RPL Routing Protocol for LLNs

RSA Rivest, Shamir, Adleman

TC Trust Center

TCP Transmission Control Protocol

TDMA Time Division Multiple) Access

TK Tool Kit

TKIP Temporal Key Integrity Protocol

SA Spoofing Attack

SA Software-Defined Networking

SHA Secure Hash Algorithm

SS Subscriber Station

SSL SecureSockets Layer

SIOT Service internet of things

UIT Union Internationale des Télécommunications

UMTS (Universal Mobile Telecommunication System)

xDSL x Digital Subscriber Line

VoIP Voice Over Internet Protocol

WEB Worker Education Program

WCDMA Wide Band Code Division Accès multiple

WLAN Wireless Local Area Network

WIMAX Worldwide Interoperability for Microwave Access

WPAN Wireless Personal Area Network

WWAN Wireless Wide Area Network

WMAN Wireless Metropolitan Area Network

4G Quatrième Génération

3G Troisième Génération

Introduction générale

L'internet des objets a été introduit pour la première fois par kevin ashton. Il désigne l'omniprésence autour de nous d'une variété d'objets qui, à travers des schémas d'adressage uniques, sont capables d'interagir les uns avec les autres et de coopérer avec leurs voisin pour atteindre des objectifs communs. Les objets, qui sont considéré comme la plateforme de base de l'IOT, sont les objets de la vie quotidienne (réfrigérateur, téléviseur, portables, Smartphone, .etc.). Ces objets sont équipés de composants électronique tels que des supports de communication radio, des processeurs pour le traitement, des capteurs et/ou actionneurs etc.

La grande puissance de l'IoT repose sur le fait que ses objets communiquent, analysent, traitent et gèrent des données d'une manière autonome. Cependant, les problèmes liés à la sécurité freinent considérablement l'évolution et le déploiement rapide de cette haute technologie. L'usurpation d'identité, les vols d'information et la modification des données représentent un vrai danger pour ce type des systèmes.

La prospérité de l'IoT ne peut être réalisée que lorsqu'on assure une bonne sécurité aux objets et aux réseaux de communication utilisés. Il est primordial de mettre en place une politique de sécurité qui empêche tout objet malicieux ou non autorisé d'avoir accès aux systèmes IoT, de lire leurs données ou de les modifier. Pour qu'un objet ait la possibilité d'exploiter un service ou de s'associer à un réseau, il doit d'abord prouver son identité et avoir les droits d'accès nécessaires.

L'objectif de ce travail est la protection des données échangées entre les objets communicants en assurant une gestion de confidentialité avec l'algorithme AES avec des clés de taille 128, 192, 256 bits ce qui nous permet d'atteint le niveau top sécurité. L'algorithme AES (Advanced Encryption Standard) qui est le plus récent algorithme à clé symétrique, en plus, c'est le plus fiable, efficace et fort des algorithmes de chiffrement disponibles aujourd'hui.

Ce mémoire est structuré en quatre chapitres encadrés par une introduction générale et une conclusion et perspectives:

Le premier chapitre sera consacré à la présentation de l'internet des objets, ainsi que l'introduction de quelques notions fondamentales utilisées dans le domaine de l'IOT.

Dans le deuxième chapitre, nous l'avons consacré pour la gestion de la confidentialité dans des technologies de communication IoT. Le troisième chapitre est une étude détaillée de l'algorithme cryptographique symétrique AES (Advanced Encryption Standard). Cette étude constitue une plateforme pour pouvoir implémenter l'application de chiffrement de données échangées entre les objets communicants.

Dans le quatrième chapitre, nous l'avons consacré pour la réalisation, c'est-à-dire, l'implémentation de l'algorithme AES pour sécuriser les données circulent dans un réseau d'objets (téléphones mobiles, micro portables).

Chapitre 1

Concepts fondamentaux de l'Internet des objets

1.1 Introduction

Dans ce chapitre, nous présentons l'IoT (Internet of things) définition, ses composantes, ses domaines d'application, son architecture, son fonctionnement, ainsi que ses axes de recherche, et nous consacrons par la suite le reste du chapitre à la définition de quelques notions utilisées dans le domaine de la sécurité.

1.2 Internet Of Thing (IOT)

1.2.1 Définition

L'IOT est l'acronyme de Internet Of Thing (Internet des Objets en français). Le terme IoT est apparu la première fois en 1999 dans un discours de l'ingénieur britannique **Kevin ASHTON**. Il servait à désigner un système où les objets physiques sont connectés à internet. Il s'agit également de systèmes capables de créer et transmettre des données afin de créer de la valeur pour ses utilisateurs à travers divers services (agrégation, analytique, etc).

Selon l'**UIT** (Union Internationale des Télécommunications), l'Internet des Objets est défini comme (une infrastructure mondiale pour la société de l'information, qui permet de disposer de services évolués en interconnectant des objets (physique ou virtuels) grâce aux technologies de l'information et de la communication interopérables existantes ou en évolution). Au fil du temps, le terme a évolué et il englobe maintenant tout l'écosystème des objets connectés. Cet écosystème englobe, des fabricants de capteurs, des éditeurs de logiciels, des opérateurs historiques ou nouveaux sur le marché, des intégrateurs, etc. Cet éclectisme en fait sa richesse.

Inspére de [4], la figure (**Figure 1.1**) montre l'architecture passée, présente et future de l'IOT. À l'avenir, les appareils ne devraient pas seulement être connectés à Internet et à

d'autres appareils locaux, mais devraient également communiquer directement avec d'autres appareils sur Internet. Outre les appareils ou les objets connectés, le concept d'IOT social (SIoT[1]) émerge également.

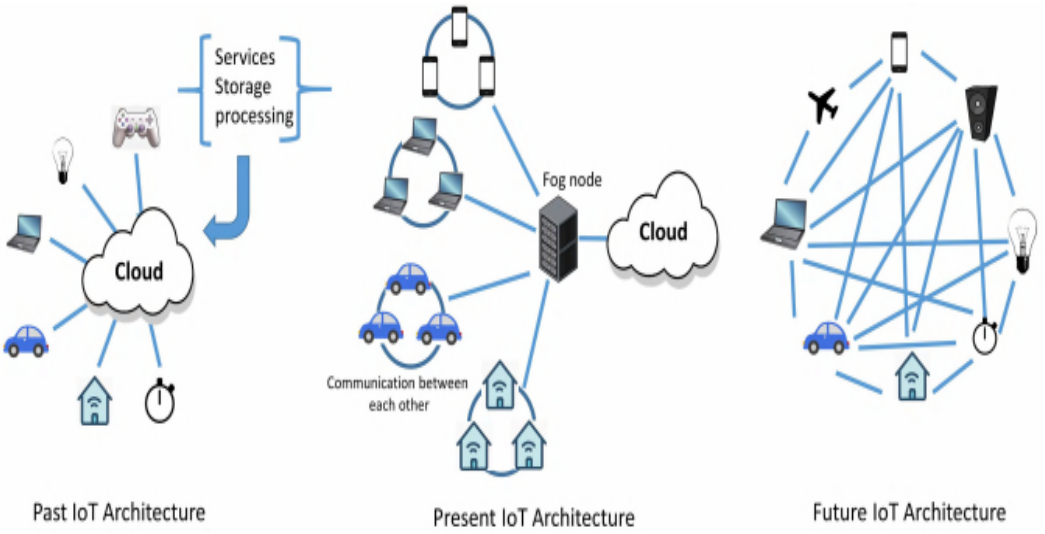

Figure 1.1: Architecture actuelle et future de l'IoT.[4]

1.2.2 Composantes de l'IOT

Les composant iot est cinq. L'objet connecté est d'abord un objet qui a une fonction mécanique et/ou électrique propre, il peut soit être conçu directement connectable, soit il est déjà existant et la connectivité est rajoutée à postériori. L'objet connecté a pour fonction de collecter des données de capteurs, de traiter ces données et de les communiquer à l'aide de d'une fonction de connectivité et de recevoir des instructions pour exécuter une action. Généralement ces fonctions de l'objet connecté nécessitent une source d'énergie, surtout quand les données sont prétraitées directement dans l'objet[5].

1.2.2.1 Les capteurs

Les capteurs sont des dispositifs permettant de transformer une grandeur physique observée (température, luminosité, mouvement etc) en une grandeur digitale utilisable par des logiciels. Il existe une très grande variété de capteurs de tous types, les objets connectés ont souvent la fonction de captation de ces grandeurs physiques sur leurs lieux d'utilisation.

Exemple de capteurs: lumière, présence, proximité, position, déplacement, accélération, rotation, température, humidité, son, vibration, électrique, magnétique, chimique, gaz, flux, force, pression, niveau[5].

[1]SIoT permettra à différents utilisateurs de réseaux sociaux d'être connectés aux appareils et les utilisateurs pourront partager les appareils sur Internet [4].

1.2.2.2 Les réseaux de capteurs

Afin de satisfaire les besoins de communication entre eux, les capteurs sont équi- pés de dispositifs sans fil pour l'émission et la réception de données. Cela ne sufit cependant pas å rendre un ensemble de capteurs accessibles ou du moins de m anière inter-opérable, transparente et simplifiée Pour cela, les capteurs doivent aussi s'organiser Ce qui c aractérise un réseau de capteurs, c'est que ses éléments sont de très petits appareils, dotés de capacités de transmission sans fil[6].

1.2.2.3 L'énerie

La plus import ante contrainte à laquelle sont soumis les rése aux capteurs concernant l'énergie. L'autonomie temporelle des noeuds s'évalue en termes d'années[12].

1.2.2.4 Les actionneurs

Les actionneurs sont des dispositifs qui transforment une donnée digitale en phénomène physique pour créer une action, ils sont en quelque sorte l'inverse du capteur. Exemple d'actionneurs: Afficheurs, Alarmes, Caméras, Haut-parleurs, Interrupteurs, Lampes, Moteurs, Pompes, Serrures, Vannes, Ventilateur, Vérins[5].

1.2.2.5 La connectivité

La connectivité de l'objet est assurée par une petite antenne Radio Fréquence qui va permettre la communication de l'objet vers un ou plusieurs réseaux (qui sont détaillés dans la section *réseaux IOT*). Les objets pourront d'une part remonter des informations telles que leur identité, leur état, une alerte ou les données de capteurs, et d'autre part recevoir des informations telles que des commandes d'action et des données. Le module de connectivité permet aussi de gérer le *cycle de vie de l'objet*, c'est-à-dire, l'authentification et l'enregistrement dans le réseau, la mise en service, la mise à jour et la suppression de l'objet du réseau[5].

1.3 Domaines d'application de l'Internet des objets

On n'en entendait à peine parler il y a quelques années, et ils sont maintenant partout. Les objets connectés ont envahi notre quotidien sans même que nous y prêtions attention.
De la télé intelligente à la voiture connectée, nos loisirs, nos déplacements sont facilités par ces nouveaux outils qui augmentent grandement notre confort.
Le potentiel des objets connectés est énorme. Une étude de 2016 du cabinet **Gartner** prévoit qu'en 2020, plus de la moitié des outils et processus métiers feront appels à l'Internet des Objets. Les applications sont variées et recouvrent de nombreux domaines: industrie, sciences, santé,...

Figure 1.2: Domains d'application de l'IOT[7].

L'utilisation de l'IOT permettra le développement de plusieurs applications intelligentes qui toucheront essentiellement ceux qu'on citera dans ce qui suit, nous citrons brièvement des exemples d'applications de l'IOT:

1.3.1 La domotique

La domotique regroupe l'ensemble des technologies informatique, électrotechnique et électronique, qui permettant l'automatisation des équipements d'un habitat et transforment une maison en une mais intelligente. C'est l'ensemble des techniques visant à intégrer à l'habitant tous les automatismes en matière de sécurité (comme les alarmes), de gestion de l'énergie (optimisation de l'éclairage et du chauffage etc.), de communication (contacts et discussion avec des personnes extérieures), etc[7].

1.3.2 Automobile

Avec le nombre croissant de véhicules intelligents, presque tous les véhicules vendus aujourd'hui dans le monde contiennent des capteurs et des moyens de communication pour faire face aux embouteillages, à la sécurité et au trafic[7].

L'objectif est que le véhicule puisse communiquer de manière autonome avec d'autres véhicules ou une station de surveillance pour éviter les accidents, réduire le trafic et sauver des vies[7].

Par exemple: si la voiture a un accident, elle demande automatiquement de l'aide et explique son emplacement et sa capacité à communiquer avec les utilisateurs[7].

Aujourd'hui, Les constructeurs automobiles travaillent sur des projets de véhicules autonomes (sans conducteur) capables de se déplacer d'un point A à un point B sans aucune intervention humaine[7].

1.3.3 La sante

Le secteur de la santé a connu un très grand nombre d'applications permettant à un patient et à son docteur de recevoir des informations, parfois même en temps réels, qu'il aurait été impossible de connaître avant l'apparition d'IoT[7].

Par exemple, il existe un médicament qu'il s'appelle **Porteuse Digital Health** qui est le premier médicament connecté sur le marché grâce à un capteur directement intégré dans l'être humain qui permet après ça le suivi des patients à distance[7].

Aussi, Il existe Plusieurs autres dispositifs sont disponibles, fixé autour du poignet et permettent également de suivre l'activité physique quotidienne du patient, mesurer le taux de sucre, compter le nombre de pas et les kms parcourus, le nombre de calories brûlées, le dispositif lui envoie une alerte dans les cas anormaux[7].

1.3.4 L'agriculture

L'agriculture intelligente a pour objet de renforcer la capacité des systèmes agricoles, de contribuer à la sécurité alimentaire en intégrant le besoin d'adaptation et le potentiel d'atténuation dans les stratégies de développement de l'agriculture durable[7].

Cet objectif a été atteint enfin par l'utilisation des nouvelles technologies, telles que l'imagerie satellitaire et l'informatique, les systèmes de positionnement par satellite de comme GPS, aussi par l'utilisation des capteurs qui vont s'occuper de récolter les informations utiles sur l'état du sol, taux d'humidité, taux des sels minéraux, etc. Et envoyer ces informations au fermier pour prendre les mesures nécessaires garantissant la bonne production[7].

1.3.5 Les villes intelligentes

Les villes intelligentes ou smart city sont en croissance dans les pays qui connaissent une avancée technologique. Il existe dans ce cas, des systèmes qui permettent de contrôler le fonctionnement de ville, les activités des populations, la gestion des bâtiments, la sécurité. Pour la sécurité, l'internet des objets permet d'effectuer la gestion du trafic dans les lieux de grande affluence, le suivi des caméras de télésurveillance publiques, l'éclairage connecté. Les enjeux d'une ville connectés sont entre autres, l'optimisation des ressources économiques, la gestion de la population et l'assainissement de la ville[8].

1.3.6 L'industrie

Le déploiement de l'IoT dans l'industrie sera certainement un support pour le développement de l'économie et du secteur des services, puisque. L'IOT il permettra d'assurer un suivi total des produits, de la production à la distribution, par la gestion automatisée, la surveillance

à distance, et le renforcement de la comptabilité. Ce travaille compte de développer les techniques de production en entreprises ainsi que le renforcement des capacités de gestion[8].

Donc La technologie IOT permet aux usines d'améliorer l'efficacité de ses opérations, d'optimiser la production et en plus améliorer la sécurité des employés[8].

1.3.7 IOT dans le domaine du sport

De nombreux objets connectés comme des montres ou des bracelets connectés vous permettrons pendant la journée de calculer le nombre de pas effectuée, la distance par courue, votre temps d'activités, les calories brulées, ainsi pendant la nuit en calculant vos heurs de sommeil. Pour les passionnés de High-tech, c'est un grand marché qui s'ouvre à eux! De la montre connectée au téléviseur connecté en passant par les appareils photos, les montre, les drones, les lunettes (Google glass)[26].

1.3.8 IOT dans le domaine de la sécurité

Pour le cabinet en stratégie, ces entreprises vont rapidement se positionner comme des alliés des personnes qui résident dans leur domicile. En fournissant des données relatives à la consommation d'énergie aux foyers, ces groupes vont apparaitre comme des arguments contre le facteur EDF pour les fournisseurs d'énergie la précision sera difficile à tenir car ils seront probablement contraints d'accompagner leurs clients dans une baisse de leurs facteurs énergétique[27].

1.4 Les étapes pour la mise en place de l'IOT

Pour simplifier le cadrage d'un projet IoT, nous avons modélisé en 6 étapes incontournables la construction déun objet connecté. Avec une solution IOT simple et pratique, facilement utilisable, pour aider tous les entrepreneurs souhaitant se lancer dans le monde de l'Internet des objets[29]:

1.4.1 Elément central du projet IoT

l'objet Boitier inséré dans un véhicule pour surveiller les déplacements, capteur permettant de mesurer les éléments de température ou de pression d'un équipement industriel, ou encore pour gérer des matériels médicaux dans les hopitaux (maintenance, taux d'utilisation), l'objet connecté peut être représentatif d'éléments extrémement différents et diversifiés. La première étape est donc d'acquérir, ou de construire le cas échéant, l'objet adapté aux contraintes physiques du cas d'usage de l'entreprise.

1.4.2 Connectivité pour la communication des objets connectés

Une fois cette problématique de l'objet traitée, l'objectif est de le rendre communiquant. Si l'objet capte les données, elles n'ont aucun sens si elles ne sont pas transférées. Un ensemble de solutions de connectivité existe pour faire 'parler' l'objet. En fonction de la nature de l'objet et des données qu'il capte, il faudra choisir le bon réseau: 2G/3G/4G, réseaux bas débit et basse consommation (type Sigfox, NB-IoT).

1.4.3 Collecte de l'ensemble des données

Face à la multitude des objets, la collecte et la modélisation de l'ensemble des données produites est un point crucial. Pour les traiter, toutes les données doivent etre collectées et traitées afin d'étre exploitable et ce à travers un seul outil simple et ergonomique.

1.4.4 Hébergement et le stockage des données

Les données doivent étre stockées, gérées et administrées en toute sécurité. Face à la criticité des données (exemple données de santé ou de géolocalisation), il est important de bénéficier d'une infrastructure qui garantit la sécurité des données et qui soit en mesure de s'adapter à la montée en charge du projet.

1.4.5 Développement de logiques applicatives

Pour donner un sens aux données collectées et en dégager toute la valeur (optimisation de l'activité de l'entreprise, fidélisation de ses clients ou encore proposition de nouveaux services innovants), il faut pouvoir les utiliser et les lier entre elles. Cela se traduit par le développement et la mise en oeuvre d'une application IoT. Au travers d'une telle application, l'entreprise peut utiliser au mieux ces données et piloter les objets ou les processus.

1.4.6 Restitution des données captées par les objets connectés

Pour proposer ces nouveaux services innovants à ses clients, l'entreprise doit mettre une interface à leur disposition pour interagir avec eux. Cette application IoT, proposée sous forme d'interface web, d'application mobile permet de partager les données avec ses clients ou ses fournisseurs, en toute simplicité et d'améliorer l'expérience client par exemple.

1.5 Architecture de l'Internet des objets

Le développement rapide l'IdO, il devenait nécessaire architecture de référence qui permettrait d'un iformiser la conception des systèmes et favoriserait l'interopérabilité? et la communication entre les différents écosystèmes de l'IdO[28].

1.5.1 Architecture et Standardisation

Les racines de l'IdO remontent aux technologies M2M (machine à machine) pour le contrôle des processus à distance. L'IdO qui est aujourd'hui un mélange de plusieurs technologies telles que la RFID, NFC, les capteurs et actionneurs sans fil, le M2M, l'ultrage bande ou 3/4G, IPv6, 6lowPAN, et RPL nécessite la définition d'une architecture et des standards afin de faciliter son développement dans le futur. L'ETSI propose une architecture découpée en trois domaines distincts, le domaine du réseau d'objets, le domaine du réseau coeur d'accès et le domaine des applications M2M et applications clientes[9].

1.5.2 Le domaine du réseau d'objets

Dans ce domaine nous trouvons les différentes technologies d'interconnexion des objets M2M, RFID, Bluetooth, IETF6L low PAN, IETFRPL et des passerelles vers les réseaux coeur de transport[10].

1.5.3 Le domain du réseau cœur

Dans ce domaine nous trouverons les différentes technologies de réseaux de transport et d'accès comme xDSL, WIMAX, WLAN, 3/4G, etc[11].

1.5.4 Le domaine des applications M2M et applications clientes

Ce domaine est composé de plateformes M2M, les Middlewares et API des applications M2M, processus métiers exploitant l'IDO, etc[11].

1.6 Notions de base de la sécurité

On peut définir la sécurité informatique comme étant le fait d'assurer le bon fonctionnement d'un système et de garantir les résultats attendus de sa conception. Autrement dit, la sécurité représente l'ensemble de politiques et pratiques adoptées pour prévenir et surveiller l'accès non autorisé, l'utilisation abusive, la modification ou le refus d'une opération informatique. A partir de cette définition, on peut extraire les bases de la sécurité qui sont décrites dans ce qui suit[27]:

1. **Authentification:** l'authentification est le mécanisme de sécurité qui permet de prouver l'identité d'une entité. En effet, il existe plusieurs méthodes d'authentification qu'on peut classer en quatre catégories[27].

   L'authentification avec ce qu'on sait, c'est à dire que l'entité prouve son identité avec une information secrète, qui n'est connue que par un nombre limité d'objets légitimes. Généralement le nombre d'objets concernés ne dépasse pas deux (ex. un client et un

serveur). Les mécanismes les plus utilisés dans cette catégorie sont les mots de passe et les numéros personnels d'identité (Personal Identity Number (PIN))[27].

- ✔ Authentification avec ce qu'on possède. Dans cette catégorie, une entité s'authentifier grâce à une donnée stockée. Cette donnée peut être secrète comme les clé pré-partagé (Pre-Shared Key (PSK)), ou publique comme les certificats numériques et les jetons[27].

- ✔ L'authentification avec ce qu'on est. Ça concerne généralement les utilisateurs humains, qui ont des caractéristiques biométriques qui leurs sont uniques telle que la voix, l'empreinte digitale, l'iris, et les veines[27].

- ✔ Authentification avec comment on se comporte. Cette dernière catégorie est basée sur les profiles comportementaux de chaque utilisateurs. Chaque entité à une façon de travaille particulière, par exemple, sa façon de taper sur un clavier, les horaires de travail habituels, l'environnement de travail habituel, etc[27].

❷ **Confidentialité:** la confidentialité est le mécanisme qui permet de cacher une donnée, et de cacher même l'information de son existence. Ainsi, empêcher toutes entité(s) non autorisée(s) d'avoir accès à cette donnée. Généralement, on assure ce service en utilisant le chiffrement de données. Ce dernier est basé sur des algorithmes mathématiques permettant de déformer un texte en clair est le remettre à sa forme initiale grâce au à une ou plusieurs clés cryptographiques[27].

❸ **Intégrité:** l'intégrité est un mécanisme assurant qu'une donnée ne soit pas: falsifiée, modifiée, altérée ou supprimée par une entité non autorisée. Dans la plupart des cas, ce service est réalisé en utilisant des fonctions de hachages avec des propriétés de signature de données[27].

❹ **Disponibilité:** la disponibilité est le mécanisme qui permet de garantir la bonne exécution d'un service, et le bon fonctionnement du système. Afin de garantir la disponibilité d'un service, on utilise des mécanismes qui le protègent contre les arrêts intentionnels telles que les attaques de dénies de service et dénies de service distribués (Denial/Distributed Denial of service(Dos/DDos)), et non intentionnels (ex. les erreurs humaines). En outre, on duplique et distribue ce service sur plusieurs serveurs. De cette façon, si l'un des serveurs ne fonctionne plus, les autres maintiennent le service[27].

❺ **Non répudiation:** la non répudiation est un mécanisme permettant de garantir qu'une opération ne peut être niée par celui qui l'avait établis. On garantie ce service grâce

aux signatures numériques combinées avec desmécanismes qui assurent le non rejeu de données[27].

❻ **Non rejeu:** le non rejeu est un mécanisme garantissant qu'un message échangé entre deux entités A et B, ne doit pas être réutilisé par une entité non autorisée C. La plus part des systèmes intègrent des compteurs et des numéros de séquence différents au niveau des messages échangés, ce qui fait qu'un message ne peut pas avoir le même numéro de séquence que ses n messages précédents (n un nombre de message qui varie selon la politique de sécurité utilisée), sinon il sera automatiquement rejeté[27].

❼ **Résilience:** on peut définir la résilience par la capacité d'un système à surmonter une altération de son environnement. Par exemple dans le cas de l'IoT, si un objet est compromis, cela ne devrait pas influencer l'ensemble du réseau.
La confidentialité persistante (forward secrecy) La confidentialité persistante est une caractéristique cryptographique qui garantit que la découverte d'une information secrète (ex. clé privée) d'un objet légitime par un utilisateur malicieux ne compromet pas la confidentialité des communications passées[27].

❽ **Èvolutivité:** l'évolutivité représente l'aptitude d'un système à maintenir des bonnes performances lorsque des ressources (notamment ressources matérielles) lui sont ajoutées[27].

❾ **Tolérance aux fautes:** la tolérance aux fautes est un mécanisme permettant à un système de continuer à fonctionner lorsque l'un de ses composants tombe en panne (ex. en dupliquant les serveurs)[27].

L'objectif de la sécurité est de protéger les systèmes informatiques contre les différentes menaces et attaques qui les ciblent. Ces attaquent consistent en l'exploitation d'une faille au niveau d'un système afin d'atteindre un objectif précis. Ces objectifs peuvent être l'obtention illégale d'un accès au système, le vol des données confidentielles d'une entreprise, l'obtention des informations personnelles sur un utilisateur, récupérer des codes de carte bancaires, etc. Ces attaques peuvent également avoir comme objectif l'interruption ou la perturbation d'un service, la falsification des données, ou l'exploitation des ressources du système[27].

❿ **Catégories d'attaques:**

- Attaques d'usurpation d'identité (spoofing attack): c'est lorsqu'une entité malveillante réussit à se faire passer pour une autre, obtenant ainsi les droits d'accès et les avantages de la victime[30].
- Attaques de rejeu: c'est quand un utilisateur malicieux copie et renvoie un ou plusieurs message(s) déjà transmis afin d'exploiter les vulnérabilités du système[30].
- Attaques par force brute: en effet le principe de ces attaques consiste à tester un grand nombre de mots de passe dans l'espoir de deviner le bon. Il peut également s'agir d'une opération de déchiffrement de données où l'attaquant essaie toutes les clés possibles jusqu'à ce que la clé correcte soit trouvée (recherche de clé exhaustive)[30].
- Attaques par cryptanalyse: cette catégorie concerne l'étude du flux de chiffrement (cipher), du texte chiffré, ou des crypto-systèmes, afin de trouver des vulnérabilités qui permettent de récupérer le texte en clair à partir du texte chiffré[30].
- Attaques de l'homme au milieu (Man In The Middle (MITM)): c'est lorsqu'une entité non autorisée se met entre deux ou plusieurs entités communicantes afin d'écouter une communication confidentielle, ou modifier/supprimer des données échangées, voire interrompre le trafic (dénie de service)[30].
- Attaques par dénie de service / dénie de service distribué (Dos/DDos) elle vise à rendre une ressource ou une information indisponible. Elle peut être réalisée (1) en inondant la machine source ou le réseau par un grand nombre de messages (ex. attaque d'inondation), ou (2) en exploitant une vulnérabilité dans le protocole. Comparé aux objets utilisés dans l'Internet classique qui représentent majoritairement Des ordinateurs- les objets dans l'IoT représentent tout équipement électronique Ayant une capacité de calcul et de mémorisation, qu'il s'agisse d'un capteur très limité en Performances et en consommation d'énergie, ou d'un grand data-center alimenté, avec des capacités ultra-puissantes. À cause de cette diversité d'objets, il est difficile de concevoir un protocole de sécurité robuste et au même temps adapté à ces objets variés. En plus, le faite que la tendance dans l'IoT est d'utiliser les technologies de communication sans fil rend le système IoT encore plus vulnérable et plus exposé à toute sorte de cyberattaque[30].

Afin de sécuriser les systèmes IoT, et d'assurer les propriétés vu ci-dessus. Il faut concevoir un protocole basé sur des algorithmes robustes, mais aux même temps légers et flexibles. Ce protocole doit être adapté aux différents types d'objet, du plus puissant au plus faible, sans qu'il y aie une dégradation en terme de performance sécuritaire.

1.7 Travaux connexes sur la sécurité IoT

Année	Auteurs	contributions
2016	Arslan Mosenia. al	Une brève discussion de la vulnérabilité rencontrée par la couche côté bord de l'IOT.
2017	YU Wei .al	Survey sur l'utilisation de l'informatique de périphérie pour sécuriser l'IOT.
2017	Jei Lin .al	Discussion sur la relation entre l'IOT et le calcul du brouillard (fog computing).
2017	Y Yang .al	Une brève discussion sur les limitations les plus pertinentes des dispositifs IOT.
2017	L chen, S, Thombre .al	Problèmes de sécurité spécifiques aux services basés sur la localisation dans l'IOT.
2017	A H Ngu, V.Metsis .al	Problèmes de sécurité liés au middleware IOT.
2018	I Farris, T Taleb .al	Mécanisme de sécurité pour la sécurité IOT comme SDN et NFB.
2019	Ikram Ud din, M. Guizani .al	Technique de gestion de la confiance pour l'Internet des objets.

Table 1.1: Travaux connexes sur la sécurité IoT[4]

1.8 Conclusion

Dans ce chapitre nous avons exposé l'Internet des objets (IOT) d'une manière générale, ces différents composantes, on s'est focalisé sur ses concepts de base, ses applications, et ses caractéristiques.
Bien que le IOT a permis le développement de nouveaux usages qui sont de plus en plus appréciés par les utilisateurs, mais malheureusement beaucoup de problèmes restent à résoudre. La sécurité et la protection des données privées des objets connectés soulèvent cependant plusieurs problèmes qui peuvent constituer des obstacles sérieux au déploiement ou à l'acceptation de l'IoT.

Après avoir présenté l'architecture IOT et les travaux connexes sur la sécurité IoT , une étude sur la confidentialité dans cet environnement IOT sera faite dans le prochain chapitre.

Chapitre 2

Technologies de communication de l'IOT et leurs mécanismes de sécurité

2.1 Introduction

L'IoT (Internet of Things) est un système décentralisé et faiblement couplé d'objets (appareils physiques, véhicules, appareils électroménagers, ...) capables de détecter ou d'exploiter, stocker et interpréter les informations créées en eux-mêmes et autour du monde extérieur voisin où ils se trouvent.

Enfait que la tendance dans l'IoT est d'utiliser les technologies de communicationsans fil,l'objectif de ce chapitre est de fournir un état de l'art sur différentes technologies decommunication et domaines utilisés par l'IoT et expliquer leurs architectures et modede fonctionnement. On va étudier principalement les aspects de sécurités, notamment l'aspect confidentialité.

2.2 Sécurité IOT

On peut définir la sécurité informatique comme étant le fait d'assurer le bon fonctionnement d'un système et de garantir les résultats attendus de sa conception. Autrementdit, la sécurité représente l'ensemble de politiques et pratiques adoptées pour prévenir etsurveiller l'accès non autorisé, l'utilisation abusive, la modification ou le refus d'une opération informatique. A partir de cette définition, on peut extraire les bases de la sécuritéqui sont (Authentification, Confidentialité, Intégrité, ..).

Dans ce travail comme il est déjà mentionné on s'intéresse seulement à la gestion confidentialité dans un environnement IoT. [13].

2.2.1 Confidantialite IOT

La confidentialité est le mécanisme qui permet de cacher une donnée, et de cacher même l'information de son existence. Ainsi, empêcher toutes entité(s) nonautorisée(s) d'avoiraccès

à cette donnée. Généralement, on assure ce service en utilisant le chiffrement dedonnées. Ce dernier est basé sur des algorithmes mathématiques (AES, DES, RSA) permettant de déformer un texte en clair est le remettre à sa forme initiale grâce au à une ou plusieurs cléscryptographiques. Dans ce qui suit, nous étudions la confidentialité dans quelques technologies de communication IoT. [14].

2.3 Technologies IOT

Les technologies IoT ne sont pas tous d'un seul et même type de réseau, ils sontclassés par catégorie, par rapport à un ensemble de caractéristiques communes, tel que le débit, la portée et la bande de fréquences dans laquelle ils opèrent[15].

2.3.1 Réseaux etandus sans fil (WWAN)

Ces réseaux sont considérés comme étant les réseaux les plus étendus. Ils représentent généralement les réseauxà liaisons sans fil à faible consommation énergétique (LoRaWAN et Sigfox), et les réseaux cellulaires tels que GSM, UMTS, et LTE. Les WWANs incluent aussi les réseaux satellitaires telsque le (GPS)[16]:

2.3.1.1 LORAWAN

LoRAWAN est l'une des technologies de réseau étendu à faible puissance (LPWAN) qui a reçu une attention considérable de la communauté des chercheurs au cours des dernières années. Il offre une communication à faible puissance et faible débit sur une large gamme de zones couvertes[17].

Elle possèdeune architecture totalement adaptée à l'IoT, lui permettant de localiser facilement les objets mobiles. Elle est déployée pour des réseaux nationaux par des grands opérateurs detélécommunications (ex. Orange). Les réseaux LoRaWAN sont généralement présentés par une topologie en étoile dans laquelle des passerelles relient des terminaux (ex.capteurs, ordinateurs, etc) à un serveur réseau central, qui est relié à son tour à un serveur d'applications.

❒ **Architecture**

L'architecture LoRaWAN est composée de nœuds d'extrémité, de passerelles, d'un serveur de réseau et d'un serveur d'applications comme présenté dans la **figure2.1** ci-dessous[18]:

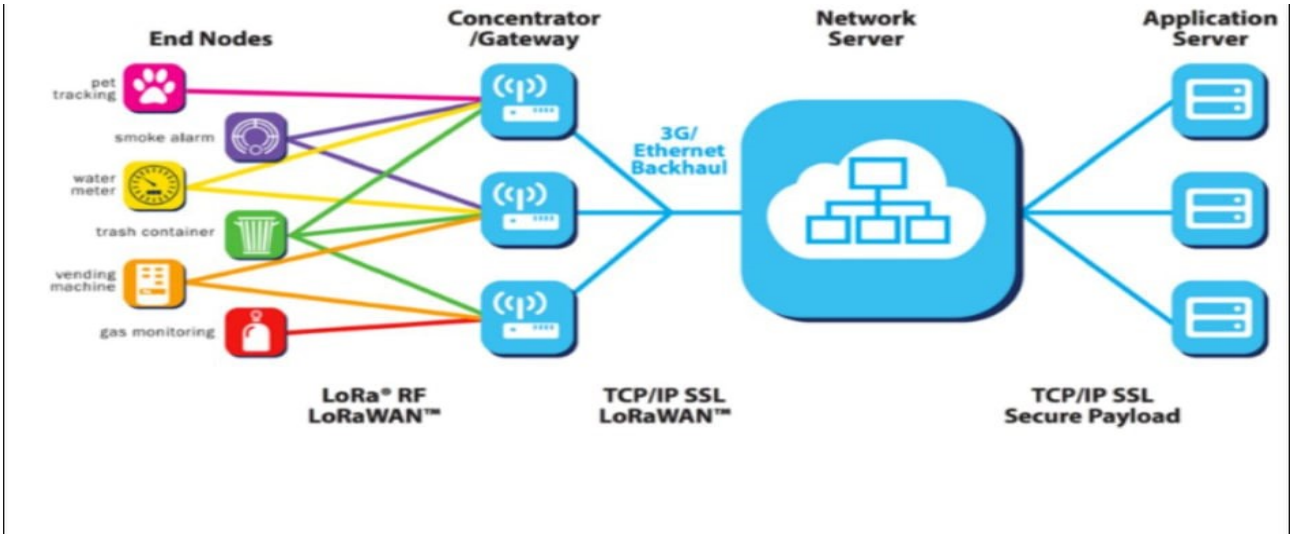

Figure 2.1: Architecure de LORAWAN[18].

Premeirment, le nœud d'éxtrimité envoie les données recueillies à une plusieurs passerelles à l'aide de la couche physique LoRa. Ensuit chaque passerelle enverra les données reçus des nœuds d'éxtrimité aux serveur de réseau en utilisant une liaison (Wi-Fi, cellulaire ethernet ou satellite). Le serveur réseau est l'entité intellegente qui va gérer le réseau, effectuer les controles de sécurité, effectuer des débits de données adaptatifs, filtrer les paquets reçus redondants, etc[18].

❒ **Sécurité**

La politique de sécurité de LoRaWAN assure les mécanismes de base qui sont l'authentification des objets, la confidentialité et l'intégrité des données. Cette politique définie également des techniques de partage de clés[27].

❒ **Confidantialite**

Une fois que l'objet soit associé au réseau de LoRaWAN, tous les messages échangés doivent étre chiffrés pour assurer la confidentialité en utilisant les clés de session connus uniquement par le serveur réseau et l'objet concerné. Le chiffrement de message est établis via le standard AES128[20] avec le mode d'opération à compteur (CounTeR (CTR))[31].

2.3.1.2 Technologies Cellulaire

Ce sont des réseaux longue portée (de quelques kilométrés en ville à 30 km en zone rurale) et consommateurs d'énergie. A l'image des réseaux GSM, 2G, 3G ou 4G, ils permettent le transport de grands volumes de données (vidéos, images, etc.) et ont une bonne couverture

au niveau national et international[22].

A. technologies 2G

La 2G est basée sur le GSM (Global System for Mobile technologie de la communication). Systéme 2G utilisé combinaison de TDMA (Time Division Multiple) Access) et FDMA (Frequency Division Multiple Accés). Grace à cela, un plus grand nombre d'utilisateurs ont pu se connecter à un moment donné dans une bande de fréquence donnée[22].

B. Les technologies 3G

Le systéme 3G utilise le CDMA (Code Division Multiple Access) et WCDMA (Wide Band Code Division Accès multiple). Le CDMA est une technique dans laquelle un un code unique est attribué a chaque utilisateur utilisant lea ce momentlà. Après avoir attribué un code unique, la largeur de bande entiérement disponible est utilisée efficacement en elle. De ce fait, un trés grand nombre d'utilisateurs peuvent utiliser la chaine en meme temps par rapport à la TDMA et FDMA[22].

C. Les technologies 4G

La technologie LTE (Long Term Evolution) ou la 4G s'appuie sur un réseau de transport commutation de paquet IP. Elle nia pas prévu de mode d'acheminement pour la voix, autre que la VoIP, contrairement à la 3G qui transporte la voix en mode circuit. Le LTE utilise des bandes de fréquences hertziennes d'une largeur pouvant varier de 1,4 MHz, 20 MHz,permettant ainsi d'obtenir (pour une bande 20 MHz) un débit binaire théorique pouvant atteindre 300 Mbit/s en downlink a, alors que la *vraie 4G* offre un débit descendant atteignant 1 Gbit/s[22].

- **Architecture LTE**

L'architecture générale du système LTE comme le montre la figure2.2 [24].

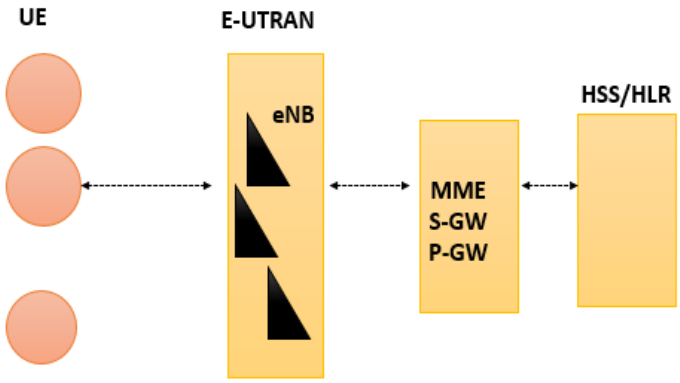

Figure 2.2: Architecture du système LTE[25].

- **UE**: terminal mobile.
- **E-UTRAN**: réseau d'accès radio terrestre universel évolué.
- **eNB**: station de base de la E-UTRAN.
- **MME**: entité de gestion de la mobilité.
- **S-GW**: passerelle de service.
- **P-GW**: passerelle réseau de données par paquets.
- **HLR**: enregistreur de localisation géographique des abonnés.
- **HSS**: sur-ensemble du HLR intégrant des nouveaux protocoles de cœur de réseau (Diameter et SIP) propres aux réseaux 4G.
- communiquentavec les MMEs -en passant par des passerelles si nécessaire- qui sont connectées aux HSS/ HLR[32].

- **Sécurité**

  On s'intéresse uniquement au LTE, car à partir de l'année 2012, ce dernier est devenu la technologie la plus déployée. Le LTE assure les services principaux de la sécurité, qui sont l'authentification des objets, la confidentialité et l'intégrité de données[27].

- **Confidantialite**

  Le LTE utilise un standardde confidentialité appelé Evolved Packet System Encryption-Algorithm (128-EEA3). L'algorithme de confidentialité 128-EEA3 fournit un chiffrement par flux utilisé pourchiffrer/déchiffrer des blocs de données via une clé symétrique (ex. CK). Le bloc de données peut avoir une longueur comprise entre 1 et 32 bits[42].

2.3.1.3 Technologie Satilitaire

Un systéme de communication par satellite hybride fournit des communications, en particulier un accès Internet, aux utilisateurs d'ordinateurs. Le système de communication hybride par satellite comprend un système par satellite et un système de communication terrestre. Le système satellite comprend deux émetteurs récepteurs[43].

Le premier émetteur récepteur reçoit et transmet un premier ensemble de signaux reçus du système de communication terrestre à une pluralité d'unités d'utilisateur. A l'inverse, le deuxième émetteur récepteur du système a satellites reçoit un deuxieme ensemble de signaux dans une deuxième bande de fréquences de l'utilisateur[44].

❒ **Architecture**

L'intégration des réseaux par satellite dans les réseaux terrestres peut étre faite de plusieurs manières. De nombreuses solutions techniques peuvent étre envisagées à ce propos mais le critère principal d'intégration sera principalement dicté par les modèles de role et de business qui en découlent[33].

Il est toutefois possible de définir trois types d'intégrations génériques:

1. Une intégration a fort couplage, dans laquelle le systeme mobile (3G, LTE, WIMAX) est étendu pour prendre en charge le media satellite comme un canal d'accès alternatif, demanière complétement transparente[33].
2. Une intégration relai, dans laquelle le satellite est intégré à l'infrastructure du réseau mobile, non pas directement au niveau de l'interface air mais à travers un relai spécifique (gateway) permettant l'accès au cœur de l'infrastructure mobile[33].
3. Une intégration a faible couplage, ou une interface spécifique au système satellite est ajoutée au terminal mobile satellite afin de permettre aussi l'accès à un réseau IP terrestre par cette interface. Des terminaux multimodaux et multi technologies capables de gérer plusieurs interfaces et leurs protocoles spécifiques (par exemple DVB-RCS+M) sont donc nécessaires[33].

❒ **Sécurité**

Il existe plusieurs travaux qui visent à sécuriser les réseaux de communication satellitaire. D'après[45], il étudie le service de la confidentialité dans un réseau satellitaire bidirectionnel composé de deux utilisateurs mobiles qui souhaitent échanger des messages via un satellite multi-faisceaux. D'autres travaux[46] proposent l'utilisation du protocole Satellite Secure Sockets Layer (SSL)[47] qui représente l'utilisation du protocole SSL dans les

réseaux satellitaires afin d'assurer l'authentification des utilisateurs, la confidentialité et l'intégrité de données.

❒ **Confidantialite**

La confidentialité dans la technologie satellitaire est assurée par le Data Encryption Standard (DES)[44].

2.3.2 Réseaux métropolitains sans fil (WMAN)

Le réseau métropolitain sans fil (WMAN pour Wireless Metropolitan Area Network) est connu sous le nom de Boucle Locale Radio (BLR). Les WMAN sont basés sur la norme IEEE 802.16. La boucle locale radio offre un débit utile de 1 à 10 Mbit/s pour une portée de 4 à 10 kilomètres, ce qui destine principalement cette technologie aux opérateurs de télécommunication[16].

2.3.2.1 WIMAX

Le WiMAX ou WorldwideInteroperability for Microwave Access est une famille de normes, définissant des connexions à haut-débit par voie hertzienne, développée par le Consortium WiMAX Forum et ratifié en 2001 par l'IEEE sous le nom IEEE-802.16. Le WiMAX est aussi le nom commercial délivré par le WiMAX Forum aux équipements conformes à la norme IEEE 802.16, afin de garantir un haut niveau d'interopérabilité entre ces différents équipements[46].

❒ **Architecture**

L'architecture du réseau WIMAX se compose de stations de base et des stations mobiles ou clientes (SS, Subscriber Station). La station de base joue le rôle d'une antenne centrale chargée de communiquer et de desservir les stations mobiles qui, à leur tour, servent les clients utilisant le WIFI ou l'ADSL. La station de base est constitué de deux modules[46]:

1. Module ≪ indoor ≫ qui contient le processeur, le modem, l'interface Ethernet et un module radio.
2. Module ≪ outdoor ≫ qui contient un module radio et une antenne d'émission-réception.

En plus de la station cliente qui contient les deux modules avec les mêmes rôles que pour la BS, il faudra avoir un terminal similaire au modem ADSL pour assurer la connexion.

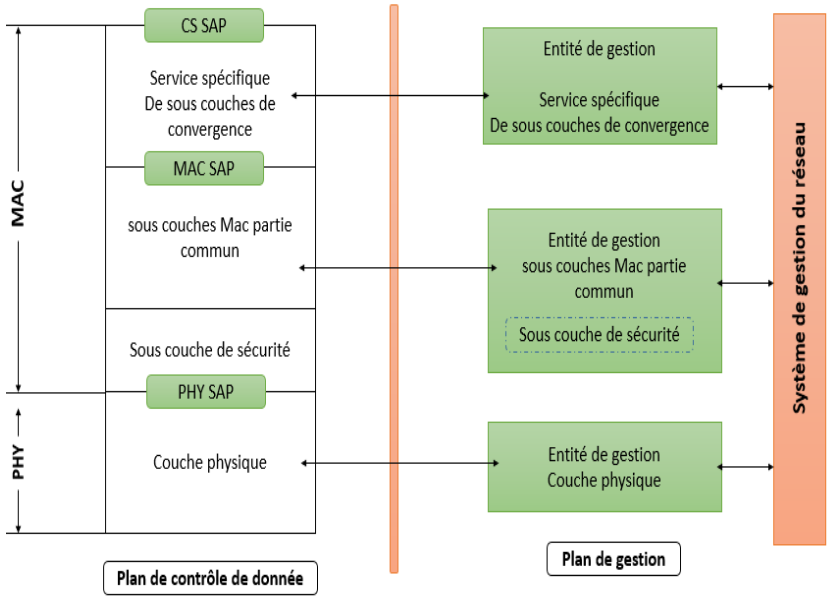

Figure 2.3: Architecture en couche de la norme 802.16[35].

La figure2.3 représente un exemple d'architecture générale d'un réseau d'accès à large bande Il s'agissait au départ dans la version 802.16a et 802.16d de liaisons point à multi-points qui offrent la possibilité de se déplacer dans un secteur donné[35].

❒ **Sécurité**

L'aspect sécurité fut reconnu comme une des principales faiblesses des premières versions. Le dernier 802.16e a amélioré ces aspects en introduisant intégrité, authentification et confidentialité sur les réseaux sans fil haut débit[48].

De plus, la sous-couche sécurité apporte aux utilisateurs une protection forte contre le détournement du service. La station émettrice (BS Base Station) se protège des accès illicites en sécurisant les flux de service associés dans le réseau. La sous-couche sécurité introduit également des mécanismes d'authentification dans le protocole client/serveur de gestion des clés, par lequel la BS contrôle la distribution des éléments de chiffrement aux stations mobiles (MS Mobile Station). En plus, les mécanismes de sécurité de base sont renforcés en ajoutant une authentification des équipements basée sur un certificat numérique[48].

❒ **Confidantialité**

Le Wimax permet de garantir une fiabilité, de segmenter les communications pour garantir la confidentialité. Il utilise un type plus solide, l'AES avec le Protocol CCMP[49].

2.3.3 Réseaux locaux sans fil (WLAN)

Le réseau local sans fil (noté WLAN pour Wireless Local Area Network) est un réseau permettant de couvrir l'équivalent d'un réseau local d'entreprise, soit une portée d'environ une centaine de mètres. Il permet de relier entre-eux les terminaux présents dans la zone de couverture. Il existe plusieurs technologies concurrentes exemple: wifi; hepperlan[16].

2.3.3.1 Wi-Fi

Le Wi-Fi (contraction de Wireless-Fidelity) est un standard international décrivant les caractéristiques d'un réseau local sans fil (WLAN). Le principe de cette technologie est d'établir des liaisons radio entre, par exemple, des terminaux et des points d'accès pour se connecter sur un réseau local ou sur Internet. Dans la pratique, le Wi-Fi permet de relier des ordinateurs portables, des machines de bureau, des assistants personnels (PDA) ainsi que des périphériques mobiles a une liaison haut débit oua des appareils électroniques communiquant sur un rayon de plusieurs dizaines de mètres en intérieur, a plusieurs centaines de metres en environnement ouvert[16].

❒ **Architecture**

La norme IEEE 802.11 s'attache a définir les couches basses du modele OSI pour une liaison sans fil utilisant des ondes électromagnétiques, c'est-à-dire[50]:

- La couche physique: proposant trois types de codages de l'information.
- La couche liaison de données: constitué de deux sous-couches: le controle de la liaison logique (Logical Link Control, ou LLC) et le controle d'accés au support (Media Access Control, ou MAC).

Le WiFi définit les deux premières couches (basses) du modèle OSI, à savoir la couche physique et la couche liaison de données. Elle introduit des modifications sur la couche basse du niveau lien (donc niveau MAC) et sur le niveau physique avec le support de plusieurs méthodes d'accès radio et les règles de communication entre les différentes stations. Il est à noter que la nouvelle couche MAC est commune à toutes les couches physiques. La figure2.4 suivante illustre l'architecture en couches de la norme IEEE802.11[37].

Figure 2.4: L'architecture en couches de la norme IEEE802.11[37].

❒ **Sécurité / Confidantialite**

La sécurisation de wi-fi est basée sur le standard 802.11i qui supporte trois protocoles de sécurité[38][51]:

- ✈ *WEP*, importé de la norme 802.11 originale.
- ✈ *TKIP* (Temporal Key Integrity Protocol), ce protocole est le successeur de WEP. Il met en œuvre l'algorithme dechiffrement RC4, et ajoute à chaque SDU11 MAC une signature de 64 bits baptisée MIC (Message Integrity Code). La clé RC4 (128 bits) est déduite d'un compteur de 48 bits (Transmit Sequence) transmis en clair et d'une clé TK (Temporal Key).
- ✈ *CCMP* (Counter-Mode/CBC-MAC), ce protocole utilise l'algorithme de chiffrement AES en mode CCM et une signature MIC. Les paramètres de chiffrement (bloc initial?) sont déduits d'un compteur de 48 bits (PacketNumber) transmis en clair et d?une clé TK[38].

2.3.4 Réseaux personnels sans fil (WPAN)

Concernent les réseaux sans fil à faible portée, de l'ordre de quelques dizaines de mètres. Tout commela portée qui varie d'une technologie WPAN à une autre, le débit varie aussi. Ce dernierpeut être à 250 Kbits/S (ZigBee) jusqu'à 1 Mbits/S (cas du Bluetooth). Ces technologiessuivent la famille IEEE 802.15, les plus connues celles de la sous norme IEEE 802.15.1(Bluetooth), et celles qui sont utilisées dans le domaine des réseaux de capteurs sans fil(WSN pour WirlessSensor Networks) qui suivent principalement la sous norme IEEE802.15.4 tel que ZigBee, OCARI, 6LoWPAN, etc[27].

2.3.4.1 6LoWPAN

6LoWPAN est une spécification d'un réseau personnel sans fil à faiblepuissance. Il peut être déployé avec une topologie en mode étoile ou maillage. Il est basésur le protocole IPv6, ce qui

lui permet d'avoir plusieurs avantages, tel que la possibilité d'utiliser des infrastructures et technologies IP existantes qui sont testées et approuvées. On outre, les objets basée IP, peuvent être connectés facilement à d'autres réseauxIP, sans avoir besoin d'entités intermédiaires comme les passerelles[39].

❒ Architecture

La figure2.5 montre un exemple d'un réseau IPv6, y compris un maillage 6LoWPAN[52].

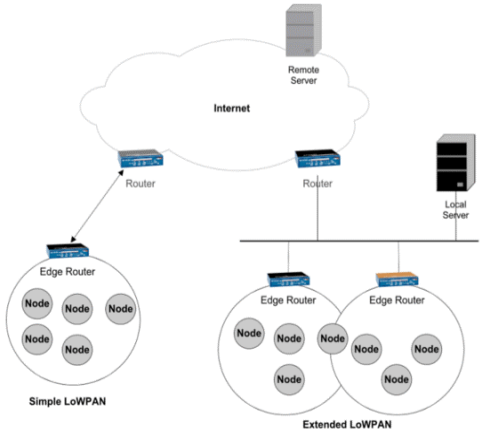

Figure 2.5: Une architecture d'un réseau 6LoWPAN[52].

Dans les réseaux 6LoWPAN, les données vont dans le réseau est destiné à l'un des appareils à l'intérieur le 6LoWPAN. Un réseau 6LoWPAN peut être connecté à d'autres réseaux IP via un ou plus de routeurs de périphérie qui transfèrent les datagrammes IP entre différents médias. [53].

❒ Sécurité

Comme dans le cas de la plupart des technologies IEEE 802.15.4, 6LoWPAN assure la confidentialité. En revanche, elle ne définit pas une méthode spécifique pour l'authentification, ni pour la gestion desclés[39]. Un travail intéressant était proposé par[39]définit une méthode d'authentification qui utilise le protocole Extensible Authentication Protocol GeneralizedPre-SharedKey (EAP-GPSK), qui est basé sur la cryptographie symétrique.

❒ Confidantialite

Afin de protéger les données échangées, [39] recommande l'utilisation du standard AESCCM, qui est un algorithme qui assure à la fois les services d'intégrité et confidentialité.

2.3.4.2 ZIGBee

Le Zigbee est une technologie WPAN à faible débit et à faible consommation de ressources (énergie, calcul, et mémorisation) qui peut être déployé avec une topologie enmode étoile ou maillée[54].

La bande de fréquences 2,4 GHz, les débits de données peuvent atteindre 250 Kb/s, tandis que dans la bande de fréquences 868 MHz, il n'a que20 Kb/s[55].

❒ **Architecture**

La structure du système Zigbee comprend trois types différents de périphériques, tels que le coordinateur Zigbee, le routeur et le périphérique final. Chaque réseau Zigbee doit comporter au moins un coordinateur qui agit en tant que racine et pont du réseau. Le coordinateur est responsable du traitement et du stockage des informations lors des opérations de réception et de transmission des données. Les routeurs Zigbee agissent comme des périphériques intermédiaires qui permettent aux données de les transmettre à d'autres périphériques[56].

Les périphériques finaux ont une fonctionnalité limité pour communiquer avec les nœuds parents, de sorte que la batterie est économisée ,comme indiqué sur la **figure2.6** suivante[56]:

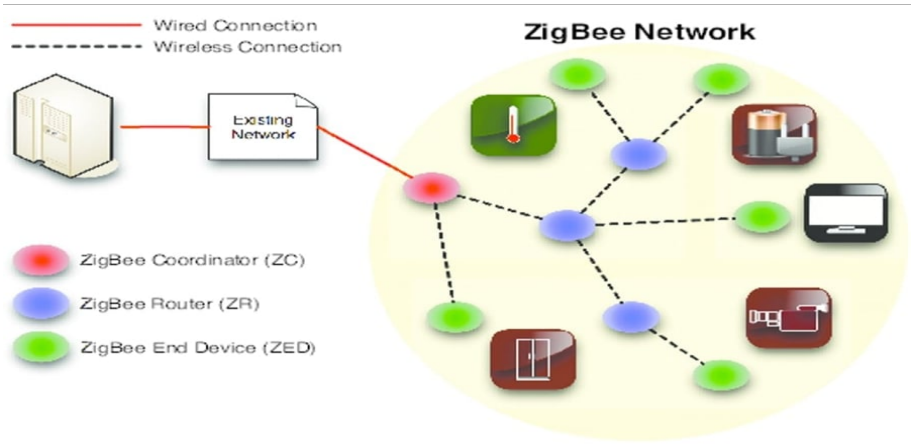

Figure 2.6: L'architecture du ZigBee[56].

❒ **Sécurité**

La sécurité est déployée au niveau de la couche application et la couche réseau. Chaque couche est responsable de sécuriser l'échange de ses données[57].

❒ Confidantialite

Les services de confidentialité et d'intégrité sont assurés grâce au chiffrement authentifié déployé au niveau de la couche application et la couche réseau. En effet, les messagessont doublement protégés au niveau des deux couches séparément, en utilisant le standard AES-CCM[58].

2.3.4.3 OCARI

OCARI (Optimisation de la communication pour un réseau industriel fiable ad hoc) est un protocole éco énergétique qui cible les réseaux de capteurs sans fil industriels. Il est adapté à applications de collecte de données où un puits, appelé CPAN, collecte les données générées par le capteur nœuds. Pour atteindre le puits, les données sont acheminées selon un arbre de collecte de données enraciné auévier[40].

❒ Architecture

figure2.7 présente un exemple d'un réseau OCARI avec trois ilots interconnectés par le biais de passerelles reliées à une unité de contrôle. Le rôle de cette unité de contrôle est de surveiller l'activité industrielle et mettre à jour les paramètres du réseau. Nous remarquons aussi un rondier qui se déplace entre les ilots et qui se connecte de manière ponctuelle à l'un de ces ilots afin d'effectuer des interventions localisées ou de collecter des informations[41].

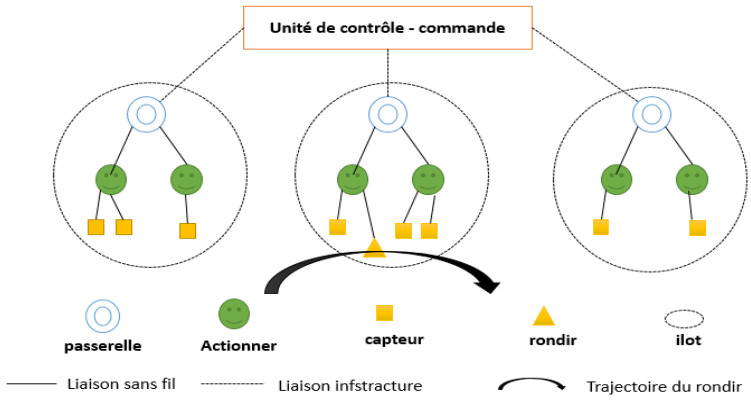

Figure 2.7: Topologie du réseau industriel OCARI[41].

❒ Sécurité

La sécurité dans OCARI En raison de la nouveauté d'OCARI, la version actuelle du protocole ne définit pas des services de sécurité. Dans[27], un protocole de sécurité robuste,

léger, rapide et économique en énergie a été proposé. Il est désigné spécialement pour être déployé sur des objets ayant des capacités limités. Il implémente ce protocole de sécurité sur la plateforme d'OCARI, et il a déployé sur des vrais capteurs.

❒ **Confidentialité**

En raison de la nouveauté d'OCARI ,la version actuelle du protocole ne définie pas des services qui assure la confidentialité[27].

2.4 Discussion

Dans ce chapitre nous avons présenté les différentes technologies de communications sans fil utilisées dans le cadre de l'IOT. Nous sommes focalisés principalement sur leurs approches de sécurités, et plus précisément sur leurs mécanismes de gestion de confidentialité.

Dans cette section, nous allons faire une comparaison entre ces différents protocoles de sécurité afin de pouvoir définir un modèle de confidentialité général.

Tableau de comparative

Type de réseau	**La technologie de communication**	**La confidentialité**
Réseaux étendus sans fil (WWAN)	LoraWAN Technologies cellulaires Technologies satellitaires	AES 128 128-EEA3 DES
Réseaux métropolitains sans fil (WMAN)	WiMax	AES CCMP (128)
Réseaux locaux sans fil (WLAN)	Wi-Fi	AES CCM (128)
Réseaux personnels sans fil (WPAN)	6LoWPANs ZigBee OCARI	AES-CCM (128) AES-CCM (128) N'est pas assurée

Table 2.1: Tableau de comparative les protocoles de sécurité.

D'après le tableau comparatif, nous concluons que la gestion de la confidentialité dans la plupart de ces technologies de communication IOT est basée sur le standard de chiffrement AES avec une clé de chiffrement de 128bits, et cela bien sûre pour plusieurs raisons, parmi lesquelles:

☛ Grande sécurité résistance à toutes les attaques connues.

☛ Large portabilité: carte à puces.

☛ processeurs dédiés.

- Rapidité.
- Lecture facile de l'algorithme Blocs de 128 bits et clés de 128/192/256 bits.
- Durée de vie de 20 à 30 ans.

2.5 Conclusion

Le long de ce chapitre, nous avons présenté quelques technologies de communications. Nous avons focalisé sur leur approche de sécurité et plus précisément sur leur confidentialité.

Donc, le but du prochain chapitre est de présenter le standard de chiffrement AES qui assure la confidentialité dans la plus part de ces technologies de communications dans le cadre de l'IOT.

Chapitre 3

Standard d'encryptage avancé(AES)

3.1 Introduction

Les algorithmes de chiffrement symétrique sont ceux qui utilisent la même clé pour chiffrer et déchiffrer un message. Ils sont souvent basés sur des techniques de substitutions et de transpositions. Cela offre un moyen rapide et efficace pour chiffrer un message. Les algorithmes les plus utilisés sont DES (Data Encryption Standard) et l'AES (Advanced Encryption Standard).

Dans ce chapitre, nous allons détailler l'algorithme cryptographique AES, en présentant les définitions utilisés dans ce standard ainsi que ses préliminaires mathématiques. Ensuite, nous allons aborder sa méthode de chiffrement, de déchiffrement ainsi que l'opération de génération de clé, nous allons présenter aussi l'ensemble de cryptanalyse qui peut menacer cet algorithme. Le chapitre se termine par une présentation du travail réalisé.

3.2 Historique

En 2002, AES est entrée en vigueur comme norme du gouvernement fédéral. Elle est également incluse dans la norme ISO/CEI 18033-3, qui préconise le chiffrement par blocs pour la confidentialité des données[59].

En juin 2003, le gouvernement des Etats-Unis a annoncé qu'AES pouvait être utilisé pour protéger les informations confidentielles. Dans la foulée, c'est devenu l'algorithme de chiffrement par défaut pour protéger ce type d'information et le premier algorithme publiquement accessible et ouvert approuvé par la NSA pour les informations ultrasecrètes. AES est l'un des algorithmes de chiffrement Suite B utilisés par l'Information Assurance Directorat de la NSA dans les technologies approuvées pour la protection des systèmes de sécurité nationaux[59].

Son utilisation éprouvée par le gouvernement des Etats-Unis a favorisé son expansion dans le secteur privé, et AES est devenu l'algorithme le plus utilisé dans le domaine de la

cryptographie à clé symétrique[59].

Le processus de sélection transparent d'AES a contribué à inspirer un haut degré de confiance chez les experts. AES est plus sûr que ses prédécesseurs - DES et 3DES -, grâce à un algorithme plus fort et à des clés plus longues. Il permet un chiffrement plus rapide que DES et 3DES, ce qui le rend parfaitement adapté pour les applications, les microprogrammes et le matériel qui exigent une faible latence ou un haut débit, comme les pare-feu et les routeurs. Il est utilisé dans de nombreux protocoles, tel SSL/TLS, ainsi que dans les applications et les périphériques récents qui utilisent le chiffrement[59].

3.3 Définition

AES est un algorithme symétrique de chiffrement par blocs utilisé dans le monde entier sur des supports matériels et logiciels pour protéger les données sensibles[59].

- L'AES est un standard, donc libre d'utilisation, sans restriction d'usage ni brevet[60].
- C'est un algorithme de type symétrique (comme le DES)[60].
- C'est un algorithme de chiffrement par blocs (comme le DES)[60].
- Il supporte différentes combinaisons [longueur de clé]-[longueur de bloc]: 128-128, 192-128 et 256-128 bits (en fait, Rijndael supporte également des tailles de blocs variables, mais cela n'est pas retenu dans le standard)[60].
- En termes décimaux, ces différentes tailles possibles signifient concrètement que[60]:

3.4 x 1038 clés de 128-bit possibles.
6.2 x 1057 clés de 192-bit possibles.
1.1 x 1077 clés de 256-bit possibles.

3.4 Natation et la structure des données

3.4.1 Entrés et Sortie

L'entrée et la sortie pour l'algorithme AES est une séquence de 128 bits (bit binaire). Les bits de ces séquences seront numérotés à partir de zéro. A chaque bit on associe un index i qui sera dans l'une des plages $0 \leq i$ ¡ 128, $0 \leq i$ ¡192, ou $0 \leq i$ ¡256 [61].

3.4.2 Octet

L'unité de base de traitement dans l'algorithme AES est l'octet qui est une séquence de huit bits et qui est traitée comme une seule entité. L'entrée, la sortie et la clé de chiffrement qui sont notée par 'a', sont traitées comme des tableaux d'octets. Chaque octet sera référencé par an, où n sera être dans l'une des plages suivantes[60]:

Longueur de bloc = 128 bits, 0 ≤ n ¡ 16
Longueur de clé = 128 bits, 0 ≤ n ¡ 16
Longueur de clé = 192 bits, 0 ≤ n ¡ 24
Longueur de clé = 256 bits, 0 ≤ n ¡ 32

Chaque octet an sera présenté comme la concaténation de 8 bits dans l'ordre b_7, b_6, b_5, b_4, b_3, b_2, b_1, b_0. Ces octets sont interprétés comme des éléments de corps finis en utilisant un polynôme de représentation[62]:

$$b_7x^7 + b_6x^6 + b_5x^5 + b_4x^4 + b_3x^3 + b_2x^2 + b_1 + b_0 = \sum_{i=0}^{7} b_ix^i$$

Par exemple, 01100011 identifie l'élément de corps fini x6 + x5 + x +1. Ainsi, l'élément 01100011 peut être représentée en hexadécimale[62].

3.4.3 Tableau d'octet

On a la séquence d'entrée de 128-bits suivante[61]:

$$input_0\ input_1\ input_2.....input_{126}\ input_{127}$$

Un tableau d'octets est représenté par la forme suivante (pour un bloc de taille 128 bits)[61]:

$$a_0\ a_1.....a_{15}$$

ou:

$$a_0 = input_0, input_1,..., input_7;\ a_1 = input_8, input_9,....,a_{15};$$
$$.....$$
$$input_{15} = input_{120}, input_{121},..., input_{127};$$

D'une façon générale:

Sequence de bit d'entrée	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Numéro d'octet	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
Numéro de bit d'octet	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0

Sequence de bit d'entrée	...	22	23		..
Numéro d'octet	2	2	2	2	..
Numéro de bit d'octet	7		0		..

Table 3.1: Travaux connexes sur la sécurité IoT[61]

3.4.4 L'état

Les opérations de l'algorithme AES sont effectuées sur une matrice de quatre lignes et Nb=4 colonnes d'octets appelée l'état, où Nb est la longueur de bloc (128 bits), divisée par 32. Dans l'état désignée par le symbole s, chaque octet i,j a deux indices, l'indice i pour désigner le numéro de ligne 0 ≤ i ¡ 4 et l'indice j pour désigner le numéro de colonne 0 ≤ j ¡ (Nb=4). Les octets lus en entrée in_0, in_1, ... in_{15} y sont copiés colonne après colonne dans la matrice. A la fin des opérations de chiffrement ou déchiffrement, la valeur finale de la matrice d'état est copié dans la sortie les octets de sortie out_0 out_1, ... out_{15} [61].

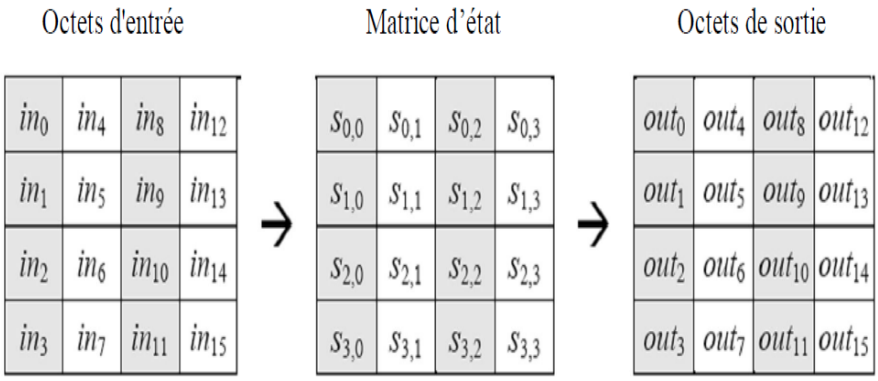

Figure 3.1: Matrice d'état, l'entrée et sortie[61]

Le tableau d'entrée est copié à l'état selon le schéma:

$$s[i, j] = in[i + 4j] \text{ pour } 0 \leq i ¡ 4 \text{ et } 0 \leq j ¡ Nb$$

L'état est copié au tableau de sortie comme suit:

$$out[i + 4j] = s[i, j] \text{ pour } 0 \leq i ¡ 4 \text{ et } 0 \leq j ¡ Nb.$$

Par conséquent, l'état peut être considéré comme un tableau de quatre mots de 32 bits, comme suit:

$$W0 = S_{0,0}\ S_{1,0}\ S_{2,0}\ S_{3,0}$$
$$W2 = S_{0,2}\ S_{1,2}\ S_{2,2}\ S_{3,2}$$
$$W1 = S_{0,1}\ S_{1,1}\ S_{2,1}\ S_{3,1}$$
$$W3 = S_{0,3}\ S_{1,3}\ S_{2,3}\ S_{3,3}$$

3.5 Algorithm AES

3.5.1 Spécification de l'algorithme AES

Dans l'algorithme AES, la taille du bloc (sois d'entré, de sortie ou d'état) est 128 bits, c'est-à-dire, il est composé de quatre mot de 32 bits d'où Nb (nombre de colonne) = 4. La clé de chiffrement, possède trois taille différentes 128, 192 ou 256 bits, d'où elle est composé de Nk (nombre de colonne) = 4, 6 ou 8 respectivement de mot de 32 bits. Chaque bloc de 128 bits subit une séquence de transformations, ces différentes transformations, définissant un tour Nr, sont répétées plusieurs fois. Pour une clé de 128, 192 ou 256, AES nécessite respectivement 10, 12 ou 14 tours, comme le résume ce tableau suivant[61].

	Nb	Nk	Nombre de tour (Nr)
AES-128	4	4	10
AES-192	4	6	12
AES-256	4	8	14

Table 3.2: Combinaison bloc, clé, tour[61]

3.5.2 Chiffrement

Le chiffrement commence par le copiage de l'entrée au tableau d'état. Ensuite, un tour initial est appliqué en ajoutant la clé de chiffrement à cet état, qui sera après transformé en itérant 10, 12 ou 14 fois (selon la longueur de clé) quatre transformations sur les octets:

SubBytes(),**SubBytes()**, **ShiftRows()**, **MixColumns()** et **AddRoundKey()** en utilisant le cadencement de clé , avec le tour final différant du premier (Nr-1) où la transformation MixColumns() n'est pas inclus. Le résultat final est ensuite copié dans la sortie[61].

figure3.2 suivante résume le principe de fonctionnement de cet algorithme de chiffrement[62]:

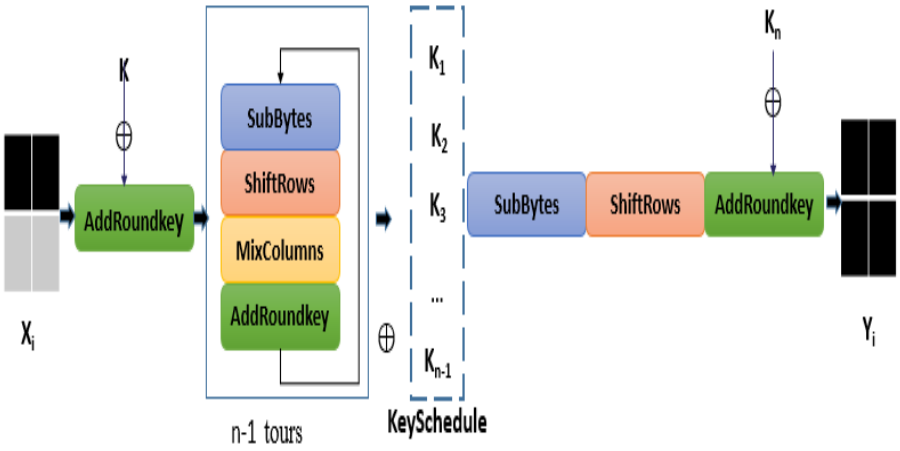

Figure 3.2: Schéma général de l'AES[61].

- **SubBytes:** chaque entrée est remplacé par un autre mot de 8 bits donné par un tableau de correspondance[62].
- **ShiftRows:**les entrées sont décalées suivant un décalage circulaire à gauche d'un nombre de cases dépendant de la ligne[62].
- **MixColumns:**chaque colonne est remplacée par une nouvelle colonne[62], obtenue en transformant la colonne en un polynôme et en multipliant par un polynôme fixé[62].
- **AddRoundKey:** chaque entrée est remplacée par le ou exclusif entre cette entrée et l'entrée correspondante dans une matrice 4 * 4 construit à partir de la clé[62].

3.5.3 Déchiffrement

Le déchiffrement est l'inverse de chiffrement, où les transformations de ce dernier peuvent être inversés et implémentés dans l'ordre inverse et avec des sous-clés également dans l'ordre inverse. L'inverse des transformations de chiffrement sont: **InvSubBytes()**, **InvShiftRows()**, **InvMixColumns()**, avec **AddRoundKey()** reste la même[61].

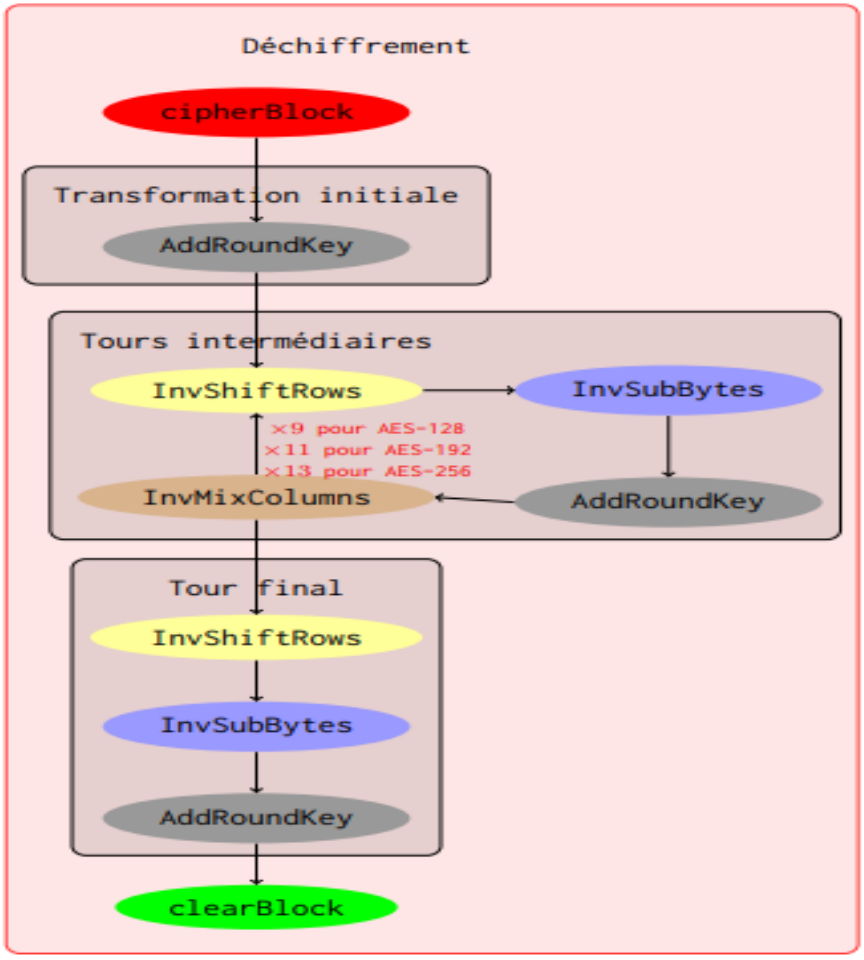

Figure 3.3: Déchiffrement de AES[63].

3.5.4 La génération des sous-clés

La planification des clés génère les clés rondes à partir de la clé AES K en utilisant 2 fonctions: *l'extension de clé* et *la sélection de clé ronde[63].*

1. *L'extension de clé:* cette fonction calcule à partir de la clé AES, une clé étendue de longueur égale à la longueur du bloc de message multipliée par le nombre de tours plus 1. La clé développée est un tableau linéaire de mots de 4 octets et est notée EK [4 * (Nk +1)] où Nk est la longueur de clé en mots. L'extension de clé est décrite ci-dessous pseudo code:

```
KeyExpansion(byte Key[4 * Nk], word EK[4 * (Nr + 1)])
{
word temp;
for (i = 0 ; i < Nk ; i + +)
EK[i] = (Key[4 * i], Key[4 * i + 1], Key[4 * i + 2], Key[4 * i + 3]);
for (i = Nk ; i < 4 * (Nr + 1) ; i + +)
temp = EK[i − 1];
if (i mod Nk = 0)
temp = SubWord(RotWord(temp)) ⊕ Rcon[i/Nk];
else if ((Nk > 6) and (i mod Nk = 4))
temp = SubWord(temp);
EK[i] = EK[i − Nk] ⊕ temp;
}
```

Figure 3.4: pseudo code[63].

où:

- **SubWord ()** est une fonction qui applique la S-box AES à chaque octet du 4 octets entrée pour produire un mot de sortie[64].

- **RotWord ()** est une rotation cyclique telle qu'une entrée de 4 octets (a, b, c, d) produit le Sortie 4 octets (b, c, d, a)[65].

le tableau de mots constants ronds, Rcon [i], est défini par Rcon [i] = (x^{i-1}, 00, 00, 00) avec x^{i-1} étant des puissances de x (x est noté 02) dans le champ F_2^8[64].

2. *La sélection de clé ronde(la sélection des sous-clés générées):* cette routine extrait les clés rondes de 128 bits de la clé étendue[64].
   - Exemple de planification de clé pour un AES-128 (voir ci-dessous **fig3.5**):

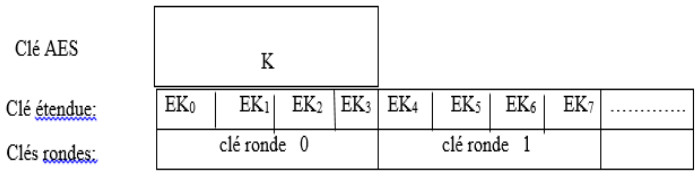

Figure 3.5: Exemple de planification de clé[64].

Ou:
- $(EK_0,...,EK_3)$ est la clé AES 128 bits K.
- $EK_4 = EK_0 \oplus \text{SubWord}(\text{RotWord}(EK_3)) \oplus \text{Rcon}[1]$,
- $EK_5 = EK_1 \oplus EK_4$,
- $EK_6 = EK_2 \oplus EK_5$,
- $EK_7 = EK_3 \oplus EK_6$, ...

3.6 Cryptanalyse de AES

L'AES n'a pour l'instant pas été cassé, même théoriquement, au sens où il n'existe pas d'attaque significativement plus efficace que la recherche exhaustive quand le chiffrement est correctement utilisé[65].

3.6.1 Attaques sur des versions simplifiées

Des attaques existent sur des versions simplifiées d'AES. Niels Ferguson et son équipe ont proposé en 2000 une attaque sur une version à 7 tours de l'AES 128 bits. Une attaque similaire casse un AES de 192 ou 256 bits contenant 8 tours. Un AES de 256 bits peut être cassé s'il est réduit à 9 tours avec une contrainte supplémentaire. En effet, cette dernière attaque repose sur le principe des ≪ related-keys ≫ (clés apparentées). Dans une telle attaque, la clé demeure secrète mais l'attaquant peut spécifier des transformations sur la clé et chiffrer des textes à sa guise. Il peut donc légèrement modifier la clé et regarder comment la sortie de l'AES se comporte[65].

3.6.2 Attaques sur la version complète

La simplicité algébrique de l'AES a été mise en avant, par exemple en 2001 par Niels Ferguson, comme une potentielle faiblesse. Elle n'a cependant pu être exploitée jusqu'à présent. En 2002 *Nicolas Courtois et Josef Pieprzyk* avaient présenté une attaque algébrique théorique l'attaque XSL, dont ils estimaient qu'elle était plus efficace que l'attaque par force brute, mais cela a été infirmé par des travaux ultérieurs[65].

En 2011, des chercheurs de Microsoft publient une attaque sur la version complète d'AES. Cette attaque permet de trouver la clef d'AES-128 en $2^{126.1}$ opérations (contre 2^{128}) pour une attaque par force brute, soit presque 4 fois plus rapide que cette dernière). La même attaque s'applique à une version simplifiée (à 8 tours) d'AES-128, réduisant la complexité de l'attaque à $2^{124.9}$. Cette attaque, fondée sur une amélioration de l'attaque par rencontre au milieu, reste impraticable[65].

3.6.3 La force brute

Cette attaque consiste à tester toutes les combinaisons possibles d'un mot de passe. Plus il existe de combinaisons possibles pour former un mot de passe, plus le temps moyen nécessaire pour retrouver ce mot de passe sera long. Un mot de passe, d'une longueur minimale de douze caractères et constitué d'au moins trois des quatre groupes de caractères énoncés ci-dessus (minuscules, majuscules, caractères spéciaux et chiffres), ne pourra pas en général être découvert par cette attaque dans un temps raisonnable [65].

3.6.4 Attaques par canal auxiliaire

Les attaques par canal auxiliaire exploitent les faiblesses du système implémentant l'algorithme de chiffrement et ne le visent donc pas directement. Il existe plusieurs attaques connues de ce type pour l'AES[65].

En avril 2005, *Daniel J. Bernstein* a publié une attaque temporelle utilisée pour casser une clé AES sur un serveur spécifique tournant avec OpenSSL[66].

En novembre 2010, *Endre Bangerter, David Gullasch et Stephan Krenn* ont publié un article décrivant la récupération d'une clé secrète AES-128 quasiment en temps réel qui fonctionne sur certaines implémentations. Comme les précédentes attaques de ce type, elle nécessite de lancer un programme sur la machine qui effectue le chiffrement[65].

3.7 Les Avantage du AES

- L'AES a été choisi pour être totalement sûr et opérationnel sur tout type d'environnement. Il répond effectivement à ces obligations, puisqu'une recherche exhaustive de la clé n'est absolument pas envisageable en un temps limité (on parle de près de 149 milliards d'années) et aucune ne lui est connue à ce jour.
- Il est très efficace en terme de rapidité (nettement plus que le DES)[66].
- Ses besoins en ressources mémoires sont également très faibles[66].
- La même clé est utilisée pour le chiffrement et le déchiffrement.

- Il est très flexible d'implémentation. Cela induit une grande variété de plateformes et d'applications[66].
- Il est possible de l'implémenter aussi bien sous forme logicielle que matérielle (câblé)[66].
- Enfin, nous pouvons ajouter que l'algorithme de l'AES est relativement simple.
- Sécurité ou l'effort nécessaire pour une éventuelle cryptanalyse[66].

3.8 Les incontinents du AES

- Le décryptage est plus difficile à implanter en *"Smart Card"*[66].
- Code et tables différents pour l'encryptage et le décryptage[66].
- Dans une réalisation en matériel, il y a peu de réutilisation des circuits d'encryptage pour effectuer le décryptage gestion des clés difficiles (plusieurs clé) échange d'un secret[66].
- Gestion des clés difficiles (plusieurs clés) échange d'un secret.
- Le temps d'exécution est assez élevé, sans doute incompatible avec les exigences des protocoles de communication les plus courants[67].

3.9 Le travail réalisé

L'objectif de notre travail consiste en la création d'un système de sécurité permettant d'assurer le service de confidentialité des données échangées entre des objets connectés. Pour réaliser ce travail, nous avons opté pour l'architecture suivante:

3.9.1 Architecture

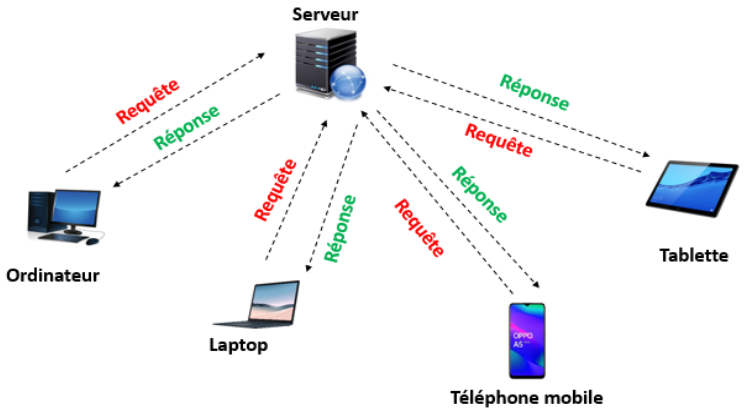

Figure 3.6: Architecture.

Où nos objets représente soit des portatifs, des téléphones mobile, connecté qui peut communiquer avec d'autre équipement connecté dans le réseau par l'envoie des messages, fichiers, images et vidéos en envoyant des demandes a un serveur, ce serveur un dispositif (matériel et logiciel) qui offre des services a un ou plusieurs objets (parfois des milliers), il répond automatiquement a des requêtes provenant d'autres objets, selon le principe dit client-serveur.

Problématique:

Maintenant, le problème d'envoi de messages secrets à travers un canal non sécurisé est lesouci le plus ancien en cryptographie. Les deux objets envoient leurs messages à travers un moyen de communication tout en essayant de garder l'adversaire loin. Un schéma de cryptage appelé aussi un crypto système permet à ces deux parties de communiquer entre eux secrètement en utilisant des algorithmes de chiffrement et de déchiffrement pour obtenir un texte crypté et un autre décrypté. Les deux objets communicants devront avoir un truc secret entre eux qui est la clé de cryptage et de décryptage afin de pouvoir crypter les messages clairs et décrypter les messages cryptés. Donc, une clé de cryptage est une clé utilisée pour le chiffrement et le déchiffrement des messages. Dans notre cas, elle est unique parce que le cryptage est symétrique.

D'après une recommandation de la NSA L'architecture et la longueur de toutes les tailles de clés de l'algorithme AES (128, 192 et 256 bits) sont suffisantes pour protéger des documents classifiés jusqu'au niveau *SECRET*. Le niveau *TOP SECRET* nécessite des clés de 192 ou 256 bits.

De ce fait, une fois que l'objet soit associé au réseau, tous les messages échangés doivent être chiffrés pour assurer la confidentialité en utilisant les clés de session connus uniquement par le serveur réseau et l'objet concerné. Le chiffrement de message est établi via le standard AES (128, 192, 256 bits).

La confidentialité aide à renforcer la confiance entre les deux objets connectés. Par conséquent, le cryptage de l'AES garantir l'intégrité des informations entre l'objet émetteur et l'objet récepteur:

1. L'objet émetteur chiffrer les données avec une clé secret,

2. L'objet récepteur reçoit des données chiffrées, et les déchiffre avec la même clé secret.

La clé de chiffrement/déchiffrement doit être connue par les deux objets communicants, de ce fait l'objet émetteur doit envoyer la clé secrète à l'objet récepteur et ça de façon sécurisé. Pour cela, il faut passer par une étape de gestion de clé.

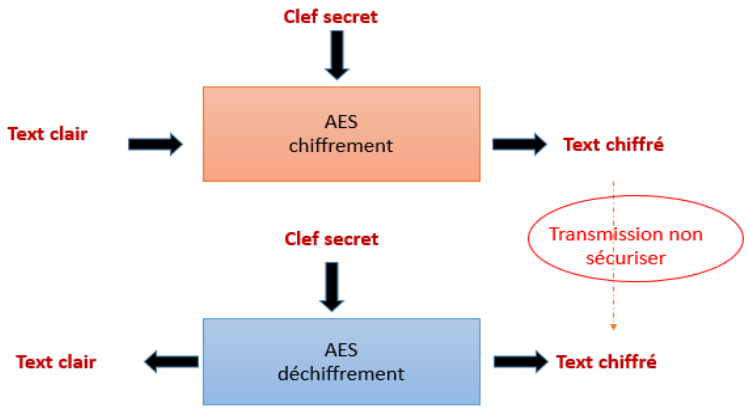

Figure 3.7: L'echange des données entre deux objets connecté

3.9.2 La gestion de clé

L'aspect le plus difficile à configurer dans un système cryptographique est la gestion des clés. Toutes les parties communicantes doivent disposer de clés cryptographiques ou paires de clés qui sert au chiffrement et de déchiffrement des messages. Le protocole dans sa totalité doit être capable de générer et de distribuer d'une manière sécurisée les clés et chacune de ces parties capable de vérifier et de stocker ces clés.

La solution la plus performante en cryptographie est celle à clé publique (cryptographie asymétrique) car elle fournit des mécanismes fiables pour l'authentification et la distribution des clés (malgré que cette solution nécessite une capacité de calcul et un espace mémoire importants).

Pour envoyer un message d'un objet à un autre:

- L'objet expéditeur génère une clé de communication (pour AES) d'une manière aléatoire, le mécanisme du partage de clé basé sur le cryptage asymétrique (algorithme RSA). Il commence par une demande de clé publique de l'objet destinataire, aprè.s
- L'objet le destinataire répond avec son clé publique,
- L'objet expéditeur chiffre la clé de communication par l'algorithme RSA en utilisant la clé publique du destinataire comme une clé de chiffrement. Lorsque la clé de communication est chiffrée, l'expéditeur envoi la clé de communication chiffrée au destinataire,
- Le destinataire fait le déchiffrement de la clé de communication par l'algorithme RSA en utilisant son clé privé.

Donc, les deux objets possèdent la clé de communication, et ils peuvent communiquer entre eux.

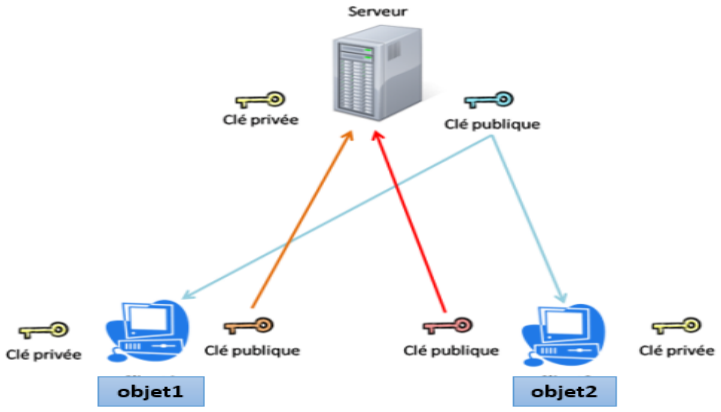

Figure 3.8: Deux objets communiquant entre eux

3.9.3 Panne du serveur

Dans le cas de la panne du serveur, le système reste à fonctionner, c'est-à-dire un des objets connectés prend le rôle du serveur. La question qui se pose quel objet devient le nouveau serveur?.

Chaque client envoie une donnée au serveur et le dernier ne réponds pas ,les clients comprennent que y a pas de connexion entre eux , cela veut dire que le serveur est en panne.

- A chaque connexion d'un nouveau objet, le serveur lui affecté un numéro aléatoire appelé numéro de priorité (généré au niveau du serveur), c'est-à-dire chaque objet connecté a un numéro de priorité.
- Si le serveur tombe en panne, l'objet avec le numéro de priorité maximal digues un message contient deux informations: son adresse IP avec son numéro de priorité, puis il commence d'écouter sur le port 3000 (le même port de serveur).
- Les objets qui recevaient ce message utilisent la nouvelle adresse IP pour les nouvelles communications.

3.9.4 Les attaques réalisées

3.9.4.1 La recherche exhaustive

C'est une application desktop, qui utilise la méthode de la recherche exhaustive pour casser l'AES.
La recherche exhaustive est une méthode algorithmique qui consiste principalement à essayer toutes les solutions possibles. Nous avons besoin du texte clair et du texte Chiffré après on génère une clé et essayée de décrypter le texte chiffré et voir s'il est correspond au texte clair, cette opération effectuer plusieurs fois jusqu'à trouver la clé. La recherche exhaustive prend

beaucoup de temps pour trouver la clé, un temps déraisonnable[68].
Dans notre cas (AES), La clé K est prise dans un espace suffisamment grand ce qui permet de prémunir contre la recherche exhaustive (essayer toutes les clés). K est de taille 128, 192 ou 256 bits, ce qui fait que la recherche exhaustive nécessite 2^{128}, 2^{192} ou 2^{256} essais.

3.9.4.2 Man in the middle

L'attaque man-in-the-middle (MITM) ou *attaque de l'homme du milieu* est une technique de piratage informatique consistant à intercepter des échanges cryptés entre deux personnes ou deux ordinateurs pour décoder les messages[69].

Dans notre cas, l'attaquant doit pirater un compte depuis le serveur, pour envoyer des messages illégitime aux autres objets connectés.

La première étape l'attaquant sniffer le réseau et attend le partage de clé entre les deux objets.

Si un objet envoi une demande de clé public à un entre objet, l'attaquant envoi leur clé publique avant l'autre objet. .

- Le premier objet qui demande la clé publique receviez la clé publique de l'attaquant, donc il chiffre la clé de communication avec la clé de communication de l'attaquant et envoi le à l'attaquant.
- L'attaquant peut déchiffrer la clé de communication, mais ne fais rien au système parce que l'objet qui demande il registre la clé de communication comme une clé de communication entre lui et l'attaquant n'est pas entre lui et le deuxième objet.

Donc nous conclurons que pour une attaque Man in de Middle, la sécurité ne peut être pas cassée.

3.10 Conclusion

Le choix d'AES est toujours le meilleur, cependant, de tels types. C'est un critère important et que son utilisation et sa compréhension augmentent significativement la fiabilité et la sécurité de nos systèmes informatiques.

En premier lieu, nous avons appris d'importants concepts de AES, y compris leur définition et un petite historique , et après nous avons touché le principe de chiffrements et déchiffrements (détaille commet fonctionner) de AES. Nous avons mentionné le architecture proposer, et enfin les avantages et les inconvénients de L'AES.

L'étude de ces technique ou AES nous dirigé vers leur l'implémentation, dans le prochain chapitre, nous avons détailler notre l'implémentation.

Chapitre 4

L'implémentation

4.1 Introduction

Dans ce chapitre, nous allons développer une application basée sur l'algorithme AES qui permet le chiffrement et le déchiffrement des données (message texte, fichiers, images, vidéos, audio,?) échangées entres les objets connectés sur un réseau.

Pour développer n'importe quelle application nous avons besoin de certains outils qui nous facilitent la réalisation de certaines tâches. Dans ce qui suit nous allons faire une présentation de ce que nous avons utilisé pour la réalisation de notre application.

4.2 Langages de programmation

Nous avons utilisé Java comme langage de programmation. Java est un langage de programmation largement utilisé, spécialement conçu pour être utilisé dans l'environnement distribué d'Internet. C'est le langage de programmation le plus populaire pour les applications de Smartphone Androide, il est également l'un des plus utilisés pour le développement des appareils de pointe et de l'Internet des objets. On cite les avantages principaux de java[70]:

- Java est un langage orienté objets.
- Portable: pris en charge par différents matériels et offre une connectivité sécurisée, ce qui le rend plus préférable pour le système IoT.
- Créer des applications complètes s'exécutant sur un seul ordinateur ou être réparties entre des serveurs et des clients d'un réseau.
- Créer un petit module d'application ou une applet a utilisé dans le cadre d'une page Web.
- Développer des applications pour les appareils mobiles. Tout d'abord, pour faire la programmation en Java, il faut télécharger et installer le kit de développement Java(JDK).

4.3 JDK

JDK (Java Development Kit) est un environnement de développement utilisé pour le développer des applications Java. Il inclut Java Runtime Environment (JRE), un compilateur (javac), un généerateur de documentation (javadoc) et d'autres outils nécessaires au développement Java.

Pour exécuter des applications Java, télécharger simplement le JRE. Cependant, pour développer des applications Java ainsi que les exécuter, le JDK est nécessaire. [71].

4.4 IDE

4.4.1 NetBeans

Nous avons utilisé l'IDE NetBeans. NetBeans est un environnement de développement intégré (EDI), placé en open source par Sun en juin 2000 sous licence CDDL (Common Development and Distribution License) et GPL v2. En plus de Java, NetBeans permet la prise en charge native de divers langages tels le C, le C++, le JavaScript, le XML, le Groovy, le PHP et le HTML, ou d'autres (dont Python et Ruby) par l'ajout de greffons. Il offre toutes les facilités d'un IDE moderne (éditeur avec coloration syntaxique, projets multi-langage, refactoring, éditeur graphique d'interface set de pages Web)[72].

4.4.2 Android Studio

Android Studio est l'environnement de développement intégré officiel (IDE) pour le développement des applications Android. Il a été annoncé pour la première fois à Google I / O en mai 2013 et la première version stable a été publiée en décembre 2014. Il est basé sur IntelliJ IDEA, un environnement de développement intégré pour les logiciels et intégre ses outils d'édition et de développement de code. Android Studio utilise un système de construction basé sur Gradle, un émulateur, des modéles de code et l'intégration de Github pour prendre en charge le développement des applications dans le système d'exploitation Android[71]. Il permet de voir chacun des changements visuels que vous effectuez sur votre application et en temps réel, vous pourrez voir aussi son effet sur différents appareils Android, chacune avec différentes con

gurations et con

gurations simultanément. Android Studio offre aussi d'autres choses[74]:

- Un environnement de développement robuste.
- Une manière simple pour tester les performances sur d'autres types d'appareils.
- Un éditeur complet avec une panoplie d'outils pour accélérer le développement de votre application.

4.5 Bibliothèques utilisés

4.5.1 Cipher

La classe Cipher utiliser pour la méthode de cryptage RSA Java Cryptography Extension (JCE) est la partie de la JCA (Java Cryptography Architecture) qui fournit une application avec des chiffrements cryptographiques pour le cryptage et le décryptage des données, ainsi que le hachage de données privées. La classe Cipher située dans le package javax.crypto constitue le noyau du framework JCE et fournit les fonctionnalités[72].

pour le cryptage et le décryptage. L'interface Key représente les clés des opérations cryptographiques. Les clés sont des conteneurs opaques contenant une clé codé, son format de codage et son algorithme cryptographique. Les clés sont généralement obtenues via des certificats ou spécifications de clé à l'aide d'une fabriquec[73].

4.5.1.1 MessageDigest

On a utiliser la classe MessageDigest pour le hashage des mots de passes (SHA-256des) lorsque on va les envoyer à travers le réseau, Cette classe fournit aux applications la fonctionnalité d'un algorithme de résumé de message, tel que SHA-1 ou SHA-256. Les résumés de messages sont des fonctions de hachage unidirectionnelles sécurisées qui prennent des données de taille arbitraire et produisent une valeur de hachage de longueur fixe. Un objet MessageDigest démarre initialisé. Les données y sont traitées en utilisant les méthodes de mise à jour. A tout moment, la réinitialisation peut étre appelée pour réinitialiser le résumé. Une fois que toutes les données à mettre à jour ont été mises à jour, l'une des méthodes de résumé doit étre appelée pour terminer le calcul de hachage. La méthode digest peut étre appelée une fois pour un nombre donné de mises à jour. Aprés l'appel de digest, l'objet MessageDigest est réinitialisé à son état initialisé[74].

4.6 Composants de l'application

Notre application est basée sur l'architecture objet/serveur des machines, dont l'objet envoie des requétes au serveur, ce dernier attend les requétes du client et y repend ou il fournit des services(des programmes fournissant des données). Les clients sont des machines de différent type (PC et smartphone).

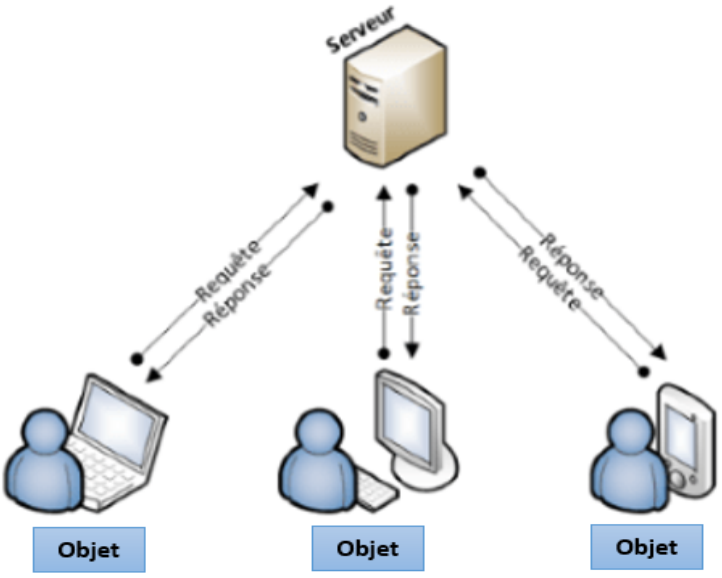

Figure 4.1: Les catégories des réseaux sansfils.

4.6.1 Objet

L'objet c'est l'entité connecté qui peut communiquer avec d'autre objet connecté dans le réseau par l'envoie des données chiffrées, en voyant des demandes au serveur. Cet objet peut être (une application desktop ou application mobile, Smartphone).

4.6.2 Serveur

C'est un dispositif (matériel et logiciel) qui offre des services à un ou plusieurs objets, il répond automatiquement à des requêtes provenant d?autres objets, selon le principe dit client-serveur.

4.6.3 Attaquant

C'est une application desktop, qui utilise soit:

- La méthode de la recherche exhaustive pour casser l'AES, l'attaquant doit avoir besoin d'un texte claire et un texte chiffré, après testé tous les possibilités pour trouver la clé de l'AES. En utilise l'application de l'attaquant pour vérifier l?efficacité de notre système de sécurité.
- L'attaque de l'homme du milieu (HDM) ou man in the middle attack (MITM) est une attaque qui a pour but d'intercepter les communications entre deux objets, sans que ni l'une ni l'autre ne puisse se douter que le canal de communication entre elles a été compromis.

4.7 Le système proposé

- Le but de notre application est de protégé les données (texte, fichiers, images, audio) échangées entre les objets connectés en appliquant le chiffrement AES 128, 192 et 256 bits comme taille de la clé de chiffrement. Ces différentes tailles, c'est pour assurer un niveau de sécurité plus élevé.
- Les objets se communiquent entre eux à travers le réseau via le serveur.
- Chaque objet doit connecter au serveur via un compte (nom d'utilisateur et le mot de passe), dont les mots de passes sont sauvegardés dans le serveur sous forme de hash en utilisant SHA-256, pour éviter l'inspiration du mot de passe par les Sniffer.
- Chaque objet a une paire de clé (une clé publique et une clé privé), si un objet1 souhaite communiquer avec un autre objet2, l'objet1 génère une clé de communication aléatoire (pour AES de taille 128, 192 ou 256 bits selon le choix) et alors les deux objets partagent la même clé de communication à l'aide de l'algorithme RSA.

4.7.1 Démarrer Serveur

Pour démarrer le serveur il suffit de cliquer sur le bouton **démarrer serveur**(voir la figure 4.2), le serveur commence à écouter sur le port 3000, crée une socket server(ServerSocket), donc les autres objets peuvent connecter à travers ce port.

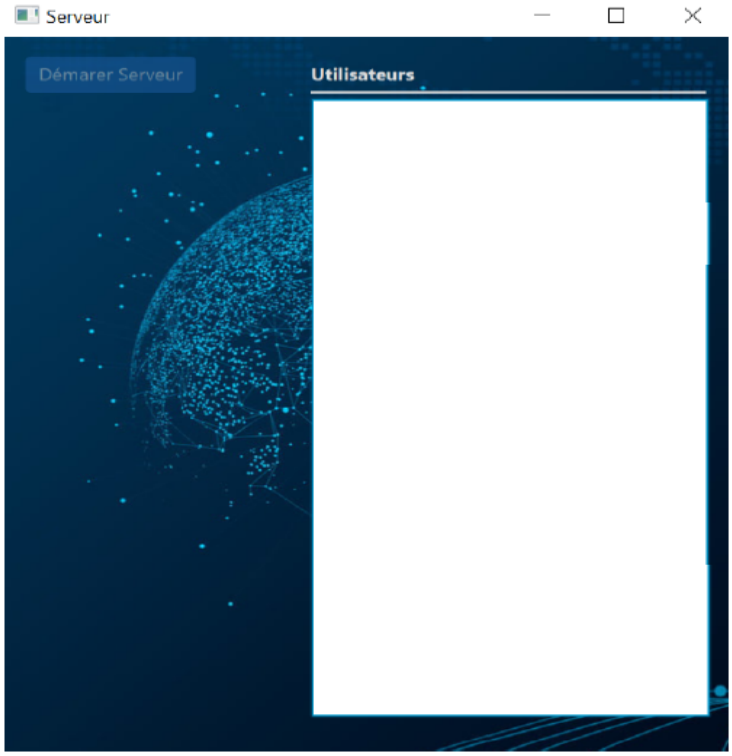

Figure 4.2: Le démarrage du serveur

4.7.2 Connecter objet

La figure 4.3 suivante représente la fenêtre qui permet à un objet de se connecter au serveur:

Figure 4.3: Connecter objet

Pour connecter un objet:

- Cliquer sur connecter, léobjet doit crée une socket client (un objet de la class Socket), la socket utilise le port 3000 et l'adresse IP du serveur pour connecter, une fois que l'objet est connecte, il calcule le HASH du mot de passe par utilisation de la fonction *SHA256* du la classe MessageDigest.
- Ensuite, l'objet doit envoyer leur authentification (le nom d'utilisateur et le hash du mot de passe) au serveur. Le serveur vérifie la correspondance des noms d'utilisateurs et le HASH du mot de passe, si il y a une correspondance le serveur répond avec un message de confirmation **connect**.

Figure 4.4: Entrée des informations pour un objet.

- Le serveur vérifie la correspondance des noms d'objets et le HASH du mot de passe, si il y a une correspondance le serveur répond avec un message de confirmation *connect*, sinon répond avec un message de refus *wrong user name psw*. Si l?objet reçoit un message *wrong user name psw*, il affiche un message d'erreur comme le montre la fenêtre de la figure 4.5:

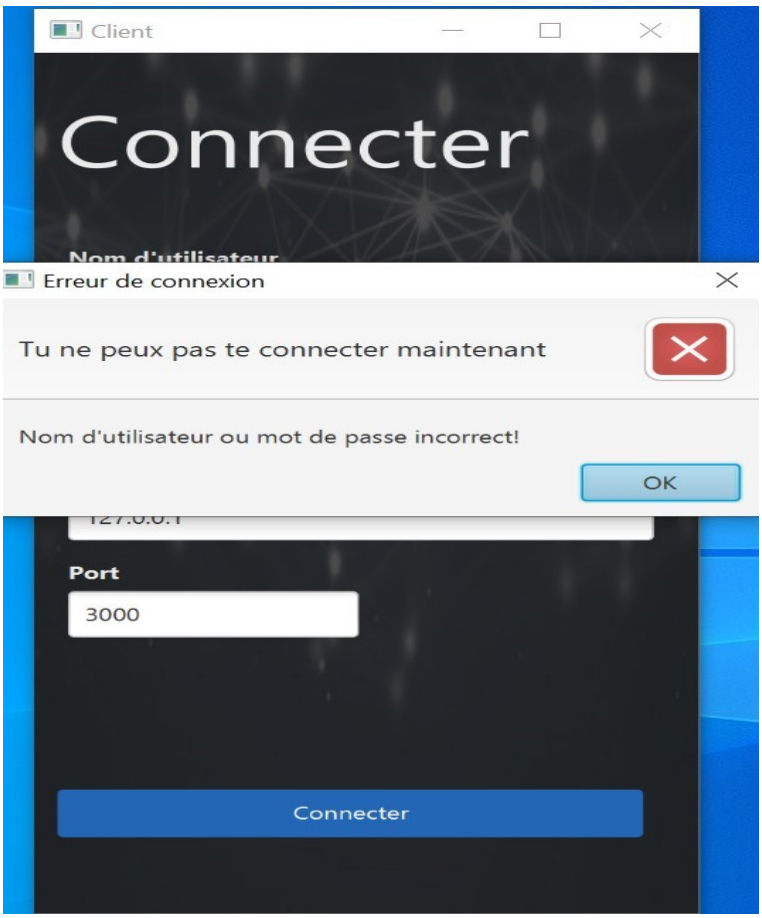

Figure 4.5: connexion objet échouée

Sinon, Si l'objet reçoit un message **connect** , il passe à la fenêtre de communication comme le montre la figure 4.6 suivante:

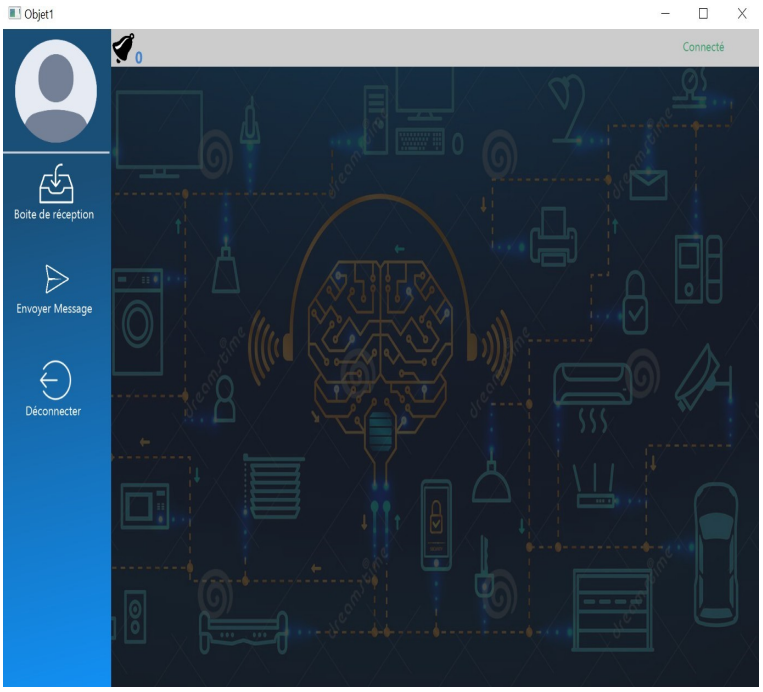

Figure 4.6: connexion objet avec succès.

Le serveur à son tour affiche la liste d'objets connectés comme montre la fenêtre de la figure 4.7 suivante:

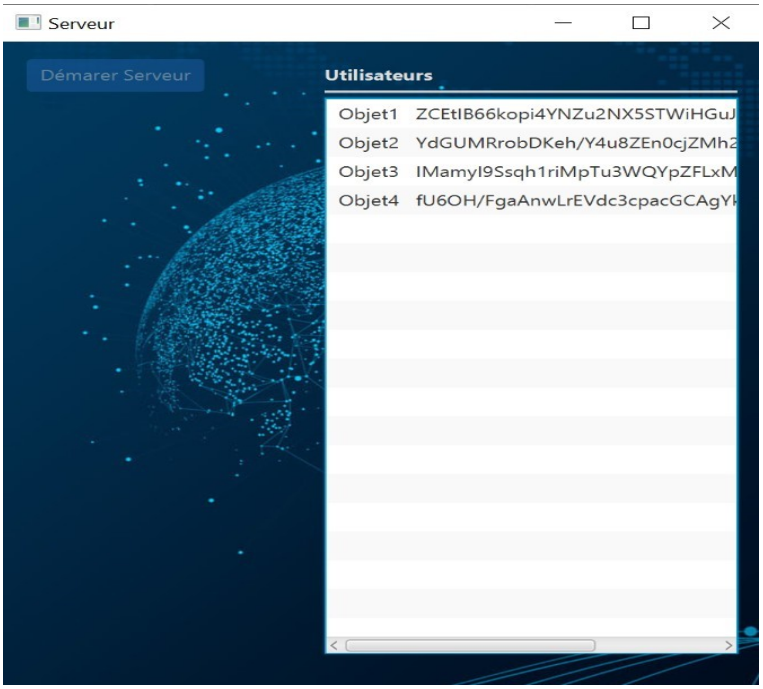

Figure 4.7: La liste des objets connectés.

Pour chaque ligne, le serveur affiche le nom d'objet connecté et le HASH du mot de passe. Maintenant la liste des objets connectés affichés au niveau du serveur peuvent faire des communications entre eux.

4.7.3 Communication entre objets

4.7.3.1 Envoyer une données

Pour envoyer des données (message texte, fichiers, images, vidéo, audio) d'un objet à l'autre, l'objet émetteur doit sélectionner l'objet récepteur, comme montre la figure 4.6:

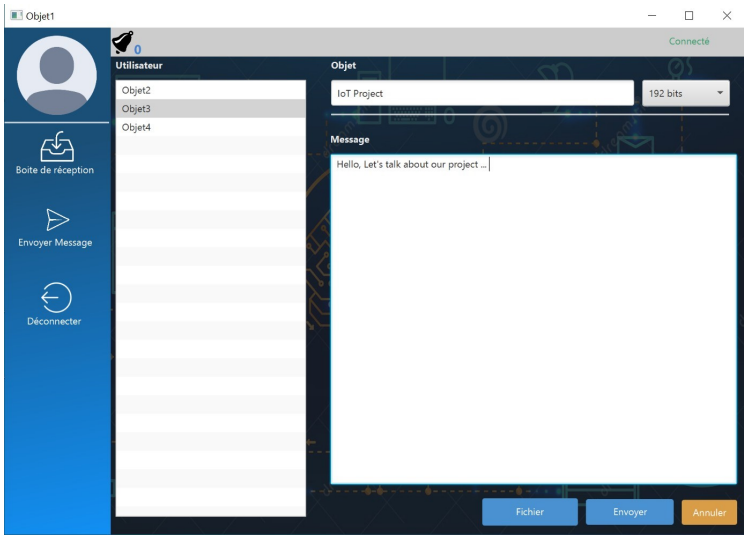

Figure 4.8: Sélectionner l'objet destinataire.

Donc pour envoyer un message une fenêtre s'affiche (figure 4.8). Cette fenêtre se compose des champs suivants:

- Le nom de l'objet destinataire.
- Choix de la taille de la clé parmi 128, 192 et 256 bits.
- Objet: l'objet du message.
- Message: le message à envoyer.

En suite cliquer sur la flèche en dessus de la fenêtre pour l'envoie du message. L'envoi assure le chiffrement et l'envoi de la donnée chiffrée.

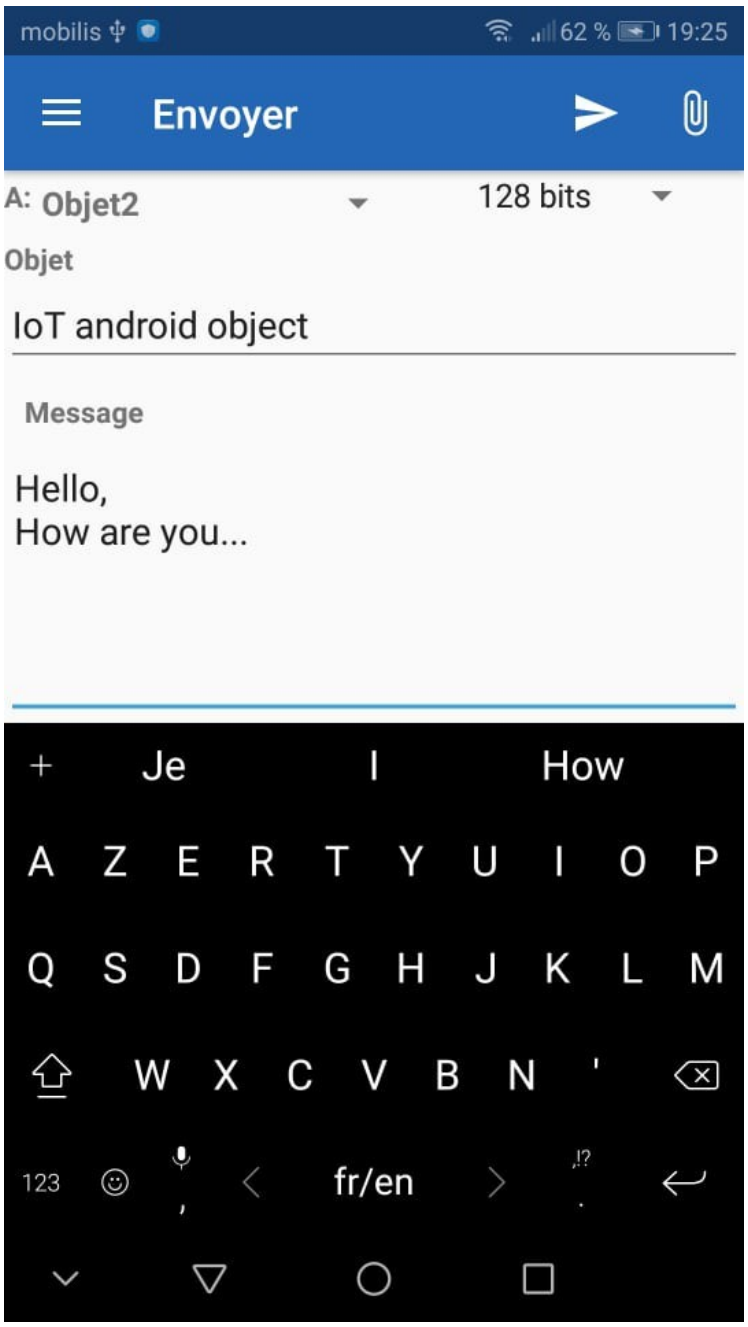

Figure 4.9: Envoyer un message chiffré.

Pour envoyer un fichier, une image ou un vidéo on suivie la même méthode précédente, sauf ici on clique sur le bouton fichier pour choisi le fichier concerné, comme montre la figure 4.10 suivante:

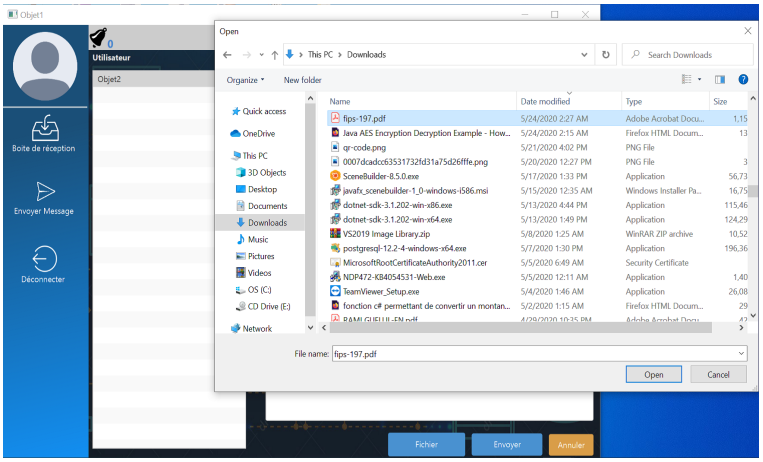

Figure 4.10: Envoyer un fichier chiffré.

Pour sauvegarder un fichier, cliquer sur le fichier reçu, une fenêtre est apparait on choisit l'emplacement pour sauvegarder le fichier, enfin cliquer sur sauvegarder (figure 4.11):

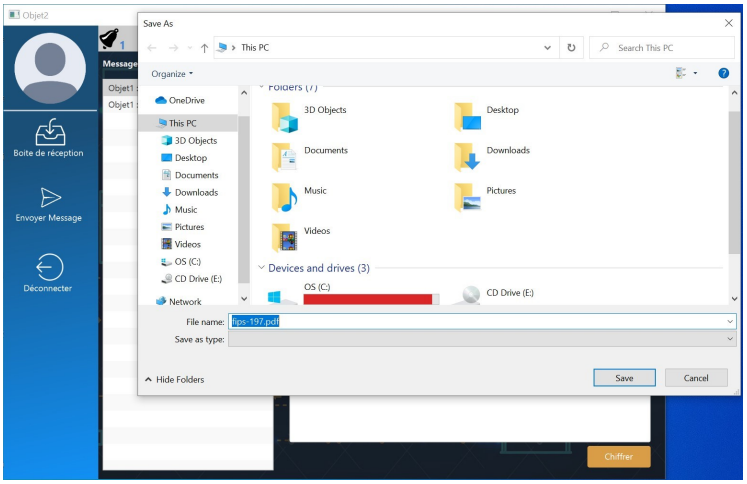

Figure 4.11: L'enregistrement du fichier

4.7.3.2 Recevoir une donnée

La figure 4.12 montre la boite de réception des messages chez un objet android où elle contient la liste des noms des objets émetteurs et les objets des messages.

Pour lire n'importe quel message de la boite de réception :

- Cliquer sur le message souhaité,
- La fenêtre de figure 4.12 s'affiche, où elle contient le nom de l'expéditeur, le message et un bouton **DECHIFRER** pour le déchiffrement du message reçu. De même pour les fichiers, images, ?.

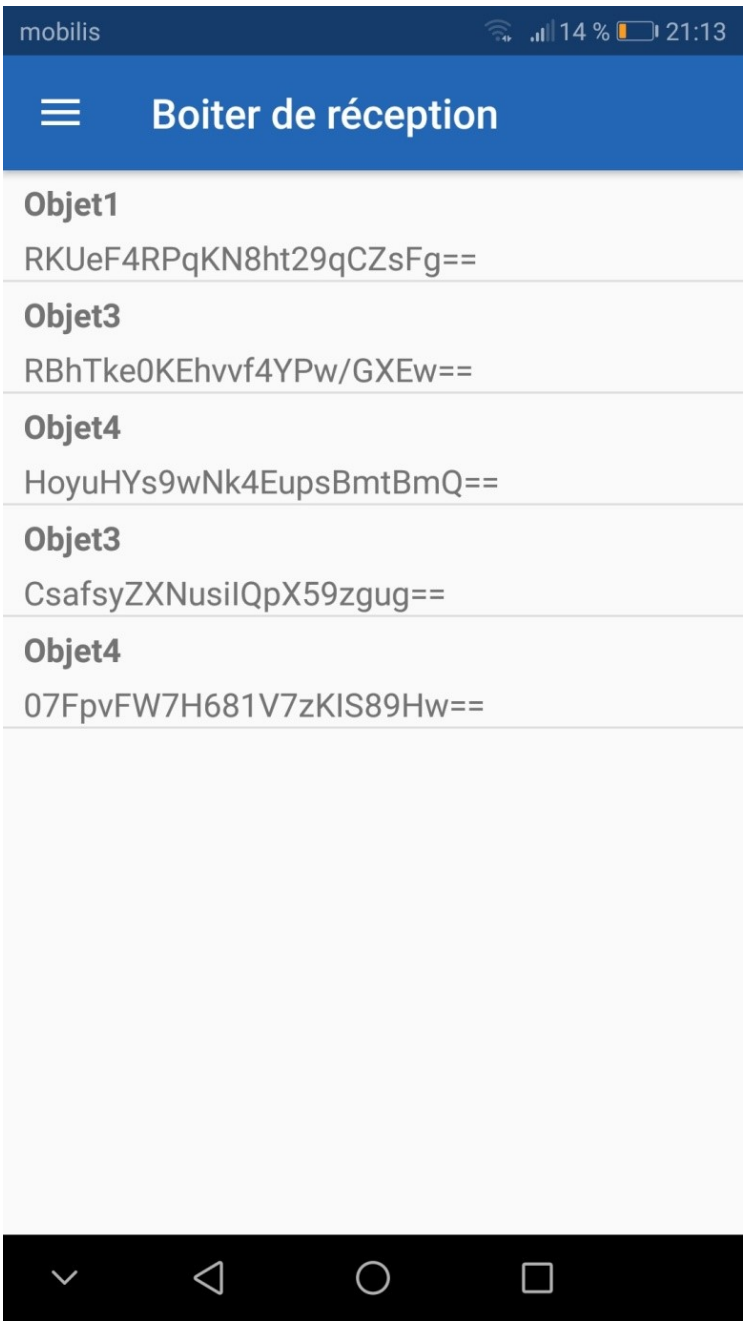

Figure 4.12: La boite de réception des messages chez un objet.

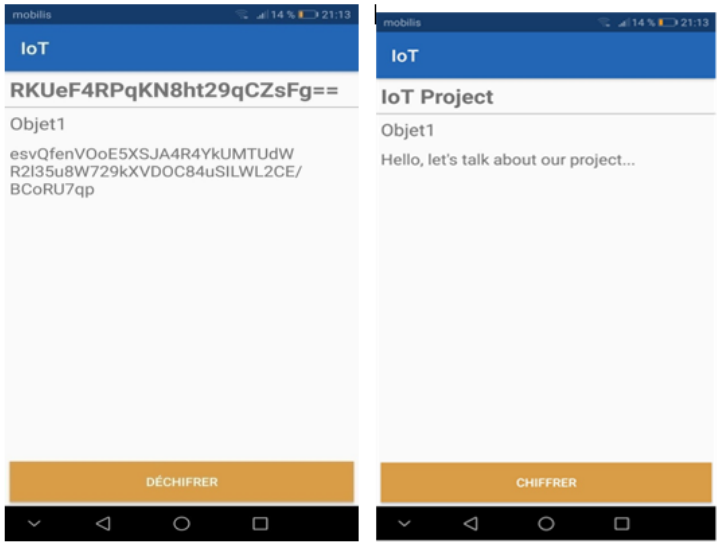

Figure 4.13: Le déchiffrement et l'affichage du message envoyé.

4.7.4 Les attaques

Dans la recherche exhaustive (figure 4.14), nous avons besoin du texte clair et du texte crypté après on génère une clé et essayé de décrypter le texte chiffré. Cette opération est répétée plusieurs fois jusqu' à trouver la clé (elle prend beaucoup de temps pour trouver la clé et ce temps dépend de la taille de la clé).

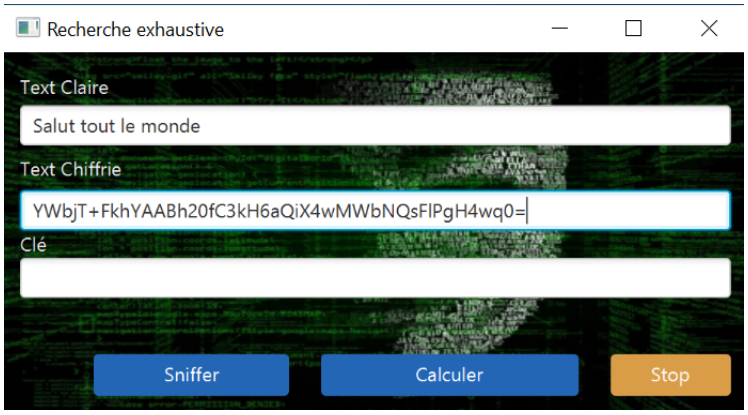

Figure 4.14: La recherche exhaustive

4.7.5 Man in the middle

La fenêtre de la figure 4.15 suivante représente l'exécution de l'attaque man in the middle.

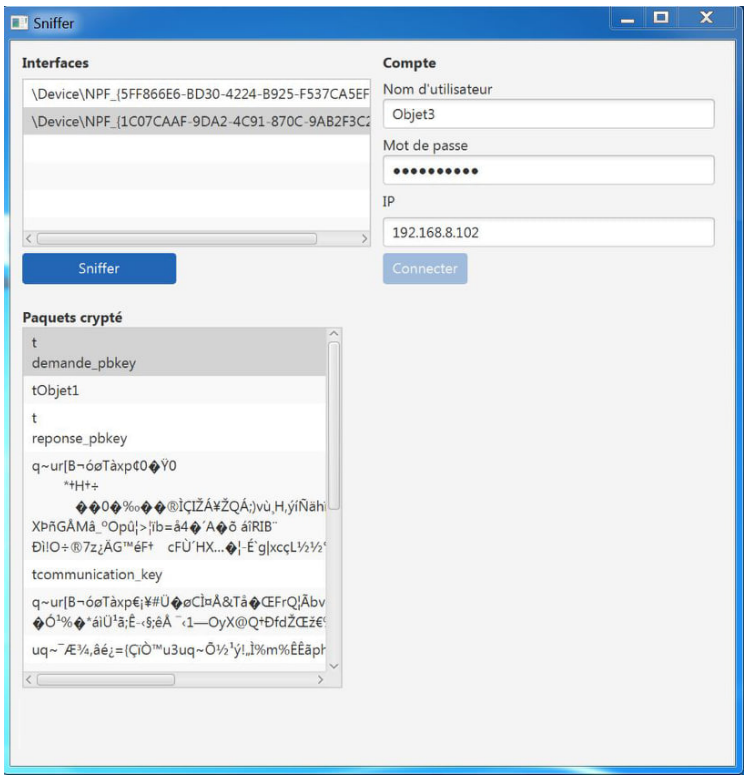

Figure 4.15: L'attaque MIDM.

4.8 Tolérance à la panne

Si le serveur tombe en panne, il sera remplacé par des objets qui a le numéro de priorité le plus élevé.

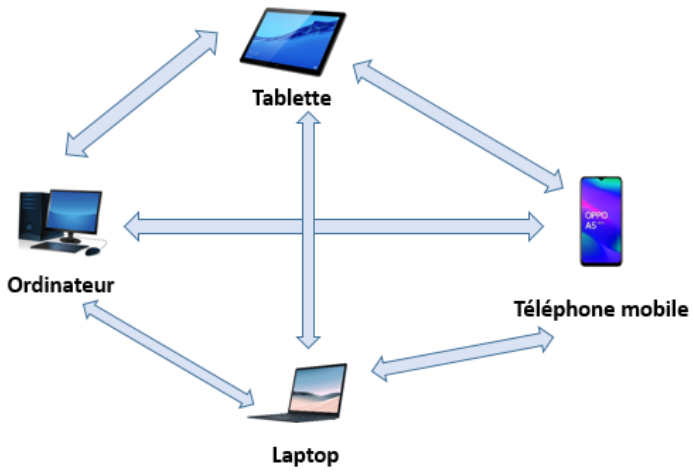

Figure 4.16: Objet comme un serveur.

4.9 Conclusion

Dans ce chapitre, nous avons présenté la mise en œuvre de notre application, la configuration matérielle et logicielle utilisée. Puis nous définissons les composantes de notre application, et son fonctionnement.

Ensuite, nous avons présenté, les deux types d'attaques utilisées pour l'évaluation d'application suivie par une gestion de la panne du serveur.

A la fin, Les résultats de ce travail montrent que le chiffrement des données est très important pour les objets connectés malgré qu'elle démunie les ressources des objets (en terme de temps d'exécution, ..) et elle consomme leur énergie.

Conclusion générale

L'internet des objets est un concept qui repose sur l'idée que tous les objets seront connectés un jour á l'internet de l'information et éventuellement de recevoir des commandes. En quelques années seulement depuis son apparition, il est fut adopté dans divers secteurs et cela grace á son potentiel énorme. Cependant, sa forte intégration souléve plusieurs interrogations dont le principal est comment assurer une sécurité robuste pour cette nouvelle technologie.

Dans ce travail, nous avons mis en avant les concepts essentiels de l'IOT, ainsi que les besoin et les défis de la sécurité dans l'IOT. Ensuite, nous avons présenté la sécurité et particuliérement la gestion de la confidentialité dans les différentes technologies de communication classifiée par le réseau sans fil. Dans le but de réaliser un systéme de sécurité permettant d'assurer le service de confidentialité des données.

Pour assurer la confidentialité nous avons choisi le standard de chiffrement AES qui vise á sécuriser les communications entre les différents objets connectés (telephone mobile, tablette, lapto....Ets) sur un réseau wiFi ou bien entre les objets et le serveur. Nous avons aussi sélectionné un autre serveur parmi un ensemble d'objets connectés pouvant assurer cette fonction en cas de panne.

Le systéme reste solide á deux types d'attaques: la recherche exhaustive et l'attaque MIDM.

Finalement, en guise de perspective, nous souhaitons une amélioration du travail implémenté, ou faire une simulation ou il y a différents types d'objets et en prenant en considération plusieurs aspects tel que la consommation d'énergie, l'espace mémoire, etc. Ce travail nous a été bénéfique sur le plan théorique et pratique, avec lequel on a amélioré nos connaissances déjá acquises, et acquérir de nouvelles connaissances.

Bibliography

[1] Potvin Jean-Yves Michel Gendreau. *Handbook of Metaheuristics*. Springer US, (2010).

[2] Saeed et Kurauchi. Enhancing the service quality of transit systems in rural areas by flexible transport services. (2015).

[3] Mahjoub A Quilliot A Kerivin H, Lacroix M. The splittable pickup and delivery problem with reloads, european journal of industrial engineering, (2008).

[4] Vikas Hassija, Vinay Chamola, Vikas Saxena, Divyansh Jain, Pranav Goyal, and Biplab Sikdar. A survey on iot security: application areas, security threats, and solution architectures. *IEEE Access*, 7:82721–82743, 2019.

[5] https://www.connectwave.fr/techno-appli-iot/iot/reseaux-et-infrastructures-iot.

[6] Jennifer Yick, Biswanath Mukherjee, and Dipak Ghosal. Wireless sensor network survey. *Computer networks*, 52(12):2292–2330, 2008.

[7] https://wikimemoires.net/2019/09/domaines-d-applications-de-l-iot/.

[8] http://taneleo.fr/internet-des-objets-application/.

[9] Yacine Challal. *Sécurité de l'Internet des Objets: vers une approche cognitive et systémique*. PhD thesis, 2012.

[10] Ala Al-Fuqaha, Mohsen Guizani, Mehdi Mohammadi, Mohammed Aledhari, and Moussa Ayyash. Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE communications surveys & tutorials*, 17(4):2347–2376, 2015.

[11] F.Bouchebbah Y.ait mouhoub. Propotion d'un modéle de confaince pour l'internet des objets. 2015.

[12] Daniele Puccinelli and Martin Haenggi. Wireless sensor networks: applications and challenges of ubiquitous sensing. *IEEE Circuits and systems magazine*, 5(3):19–31, 2005.

[13] MARINA RUGGIERI University of Roma Tor Vergata itali HOMAYOUN NIKOOKAR Delft University of Technology.

[14] https://oer.avu.org/bitstream/handle/123456789/619/CSI

[15] Mlle MAHI Sarah Mlle MEDJAHDI Nawel. Etude et implémentation des codes ldpc pour la technologie wimax ieee 802.16. *Projet de Fin d'Etudes*.

[16] https://eduscol.education.fr/?fbclid=IwAR3AbftSk_HjWRtEpCxlSCOuir-1nHl2CgppDc2pfJifZcBTFSLUxWHGPqI.

[17] Jetmir Haxhibeqiri, Eli De Poorter, Ingrid Moerman, and Jeroen Hoebeke. A survey of lorawan for iot: From technology to application. *Sensors*, 18(11):3995, 2018.

[18] San Ramon Camino Ramon. Lora alliance technical marketing workgroup, technical overview of lora and lorawan. page 2400.

[19] T.Eirich (IBM) T.Kramp (IBM) O.Hersent (Actility) N.Sornin (Semtech), M.Luis (Semtech). Lorawan specification. lora alliance,. 2015.

[20] Brian Gladman. A specification for rijndael, the aes algorithm. at fp. gladman. plus. com/cryptography-technology/rijndael/aes. *spec*, 18(19):311, 2001.

[21] Phillip Rogaway Helger Lipmaa and David Wagner. Ctr-mode encryption. in first nist workshop on modes of operation. 2000.

[22] Hadjer BOUCHENTOUF and Riyad BOUDGHENE STAMBOULI. *Etude des performances des réseaux 4G (LTE)*. PhD thesis, 2013.

[23] MrDIALLO MamadouLamine. Sécurité des réseaux 4g/lte. *Université Mouloud Mammeri de Tizi-Ouzou (UMMTO)*, 2017/2018.

[24] http://www.univ-bejaia.dz/jspui/bitstream/123456789/8070/1/Planification

[25] Hyung G Myung. Technical overview of 3gpp lte. *Polytechnic University of New York*, 2008.

[26] F.Bouchebbah Y.ait mouhoub. Propotion d'un modéle de confaince pour l'internet des objets. *Université A/MIRA de Bejaia*.

[27] Mohamed Tahar Hammi. *Sécurisation de l'Internet des objets*. PhD thesis, 2018.

[28] Imad Saleh. Internet des objets (ido): Concepts, enjeux, défis et perspectives. *Revue Internet des objets*, 2(10.21494), 2018.

[29] https://www.sfrbusiness.fr/room/internet-des-objets/les-etapes-projet-iot.html?fbclid=IwAR0nLWsPDGiJKCaBssC94wU5YtkcdKifb9VX0MV0FbFaLez7mm1pxOtpfwU.

[30] Hijab Ali. Implémentation d'un protocole détection d'un serveur d'authentification dans l'internet des objets. master's thesis,. 2017.

[31] ERON JOKIPII MIHIR BELLARE, ANAND DESAI and PHILLIP ROGAWAY. A concrete security treatment of symmetric encryption: Analysis of the des modes of operation. proceedings of 38th annual symposium on foundations of computer science. 1997.

[32] Alf Zugenmaier and Hiroshi Aono. Security technology for sae/lte. ntt docomo technical journals. 2, 2009.

[33] Pascal Berthou. *Vers la Dématérialisation des Réseaux Hybrides Satellites et Terrestres.* PhD thesis, Université Toulouse 3 Paul Sabatier (UT3 Paul Sabatier), 2018.

[34] Chao-Chen Yang Min-Shiang Hwang and Cheng-Yeh Shiu. *An authentication scheme for mobile satellite communication systems. ACM SIGOPS Operating Sys- tems Review.* PhD thesis, 2003.

[35] https://www.memoireonline.com/01/12/5161/m_tude-et-mise-en-place-d-un-reseau-wimax-dans-la-region-de-Dakar4.html.

[36] Simon Mian. Wimax ou l'évolution des réseaux sans-fil. 2006.

[37] Michel Duchateau. *Analyse et simulation du déploiement d'un réseau sans fil a l'ULB MEMOIRE DE FIN d'ETUDE PRESENTE EN VUE DE L'OBTENTION DU GRADE D'INGENIEUR CIVIL ELECTRICIEN SPECIALITE EN TELECOMMUNICATION.* PhD thesis, 2004.

[38] Pascal Urien and Marc Loutrel. La carte à puce eap, un passeport pour la sécurité des réseaux émergents wi-fi. *5èmes Journées Réseaux, JRES2003, Lille, France*, 2003.

[39] Gabriel Montenegro NandakishoreKushalnagar and Christian Schumacher. overlow-power wirelesspersonal area networks (6lowpans) : overview, assumptions, problem-statement, and goals. ietf, ietf, rfc4919 ipv6. *5èmes Journées Réseaux, JRES2003, Lille, France*, 2007.

[40] Calypso Barnes. *Thése de doctorat Présentée en vue de l'obtention du grade de docteur en Sciences Discipline: Electronique de l'Université Cote d'Azur.* PhD thesis.

[41] Nancy El Rachkidy. *Cross-Layering et routage dans un réseau ad hoc: politique de relais de trame sur un réseau de capteurs sans fil organisé selon une topologie en arbre.* PhD thesis, 2011.

[42] 3GPP. Specification of the 3gpp confidentiality and integrity algorithms 128-eea3 and 128-eia3. in 128-eea3 and 128-eia3 specification. 3rd generation partnership project. 2011.

[43] Mak King and Michael J Riccio. Military satellite communications: Then and now. crosslink,. 11(1)(10.21494), 2010.

[44] Chao-Chen Yang Min-Shiang Hwang and Cheng-Yeh Shiu. An authentication scheme for mobile satellite communication systems. acm sigops operating systems review. 37(4)(10.21494), 2003.

[45] Zhen Gao Zhu Han Ashkan Kalantari, Gan Zheng and Bjorn Ottersten. Secrecy analysis on network coding in bidirectional multibeam satellite communications. ieee transactions on information forensics and security. 2015.

[46] Michael Hadjitheodosiou Ayan Roy-Chowdhury, John S Baras and Spyro Papademetriou. Security issues in hybrid networks with a satellite component. ieee wire- less communications. 2005.

[47] Philip Karlton Alan Freier and Paul Kocher. The secure sockets layer (ssl) protocol version 3.0. 2011.

[48] https://www.memoireonline.com/01/12/5161/m_tude-et-mise-en-place-d-un-reseau-wimax-dans-la-region-de-Dakar4.htm?fbclid=IwAR1Ur9C2QEM-SMahW09ecnVCtmRMqzD000oH60ZxgVSrinrexbAEtY1baaU.

[49] Michèle Germain. Wimax à l'usage des communications haut débit. In *Forum atena, lulu. com, Paris*, 2009.

[50] http://igm.univ-mlv.fr/dr/XPOSE2007/dgehanne_wimax/.

[51] Denis Dessales. *Conception d'un réseau de capteurs sans fil, faible consommation, dédié au diagnostic in-situ des performances des bâtiments en exploitation.* Poitiers, 2011.

[52] Rashed Alkhudaidy Mahmoud Khasawneh, Izadeen Kajman and Anwar Althu-byani. A survey on wi-fi protocols : Wpa and wpa2. in international conference on security in computer networks and distributed systems. springer. 2014.

[53] Melle Narimane DAOUD and Melle Delel Abir LOUATI. Acces aux données d'un réseau de capteurs sans fil supportant 6lowpan, en utilisant le protocole mqtt.

[54] Melle Delel Abir. Zigbee alliance organization. zigbee specification. 2012.

[55] Shahin Farahanir. Zigbee wireless networks and transceivers, book, printed in the united states of america. 2008.

[56] ZHEN Zhao. Ètude des protocoles de communication pour les systémes de gestion dans le contexte des réseaux intelligents, mémoire présenté á l'université du québec à trois-riviéres. 2017.

[57] Anas Abou Elkalam Aafaf Ouaddah and Abdellah Ait Ouahman. Towards a novel privacy-preserving access control model based on blockchain technology in iot. in europe and mena cooperation advances in information and communication tech- nologies. 2017.

[58] Mohamed Tahar Hammi. *Sécurisation de l'Internet des objets*. PhD thesis, 2018.

[59] https://whatis.techtarget.com/fr/definition/AES-Advanced-Encryption-Standardtext=AES

[60] https://fr.readkong.com/page/presentation-generale-de-l-algorithme-aes-3818649?p=2.

[61] wafa Birouk. Mémoire de magistére en informatique, theme sécurisation des données sensibles sur téléphone mobile / dispositif d'assistant numérique personnel (pda). 2008.

[62] Advanced encryption standard (aes). 2020. http://math.univ-lyon1.fr/roblot/masterpro.html.

[63] Michel Dubois. Conception, développement et analyse de systémes de fonction booléennes décrivant les algorithmes de chiffrement et de déchiffrement de l'advanced encryption standard. automatique / robotique. ecole nationale supérieure d'arts et métiers. 2018.

[64] Dfa on aes christophe giraud oberthurcardsystems. c.giraud@oberthurcs.com.

[65] https://fr.wikipedia.org/wiki/Advanced_Encryption_StandardAttaques.

[66] https://www.academia.edu/10292662/AES_Advanced_Encryption_Standard.

[67] Claudine Guerrier and Marie-Christine Monget. *Droit et sécurité des télécommunications*. Springer Science & Business Media, 1999.

[68] Doris M Baker HX Mel and Steve Burnett. *Cryptography decrypted. AddisonWesley Upper Saddle River*. 2001.

[69] https://www.malekal.com/man-in-the-middle/.

[70] http://ipeti.forumpro.fr/t21-definition-de-langage-java-java-script.

[71] https://fr.wikipedia.org/wiki/NetBeans.

[72] https://www.androidauthority.com/android-studio-tutorial-beginners-637572/.

[73] https://docs.oracle.com/javase/7/docs/api/javax/crypto/KeyGenerator.html.

[74] https://docs.oracle.com/javase/7/docs/api/java/security/KeyFactory.html.

Chapitre 5

annexe1

Chiffrement de AES

- **Transformation SubBytes:** transformation non linéaire appliquÃ©e indépendamment á chacun des octets de l'état en utilisant une table de substitution (Sbox).

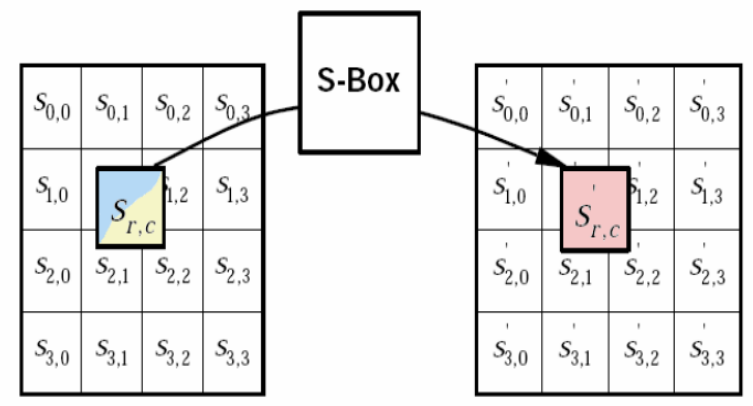

Figure 5.1: Transformation SubBytes

- **Transformation ShiftRows:** Permutation cyclique des octets sur les lignes de l'état. Le décalage des octets correspond á l'indice de la ligne considérée ($0 \leq$ r ¡ 4).

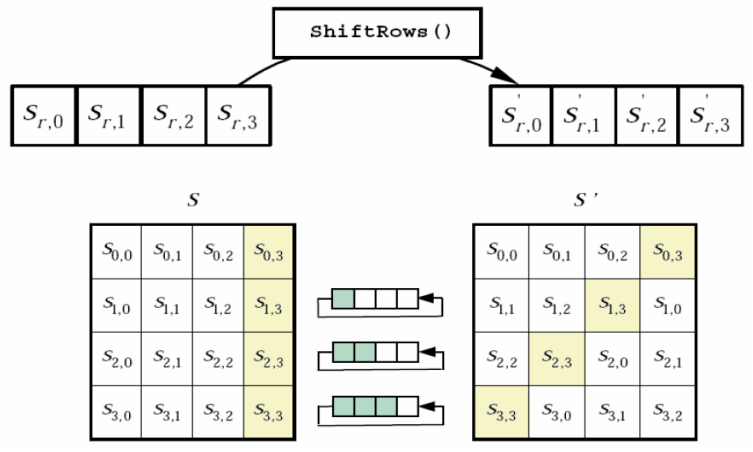

Figure 5.2: Transformation ShiftRows

✈ **Transformation MixColumns:** transformation appliquée Ã un état colonne aprés colonne.

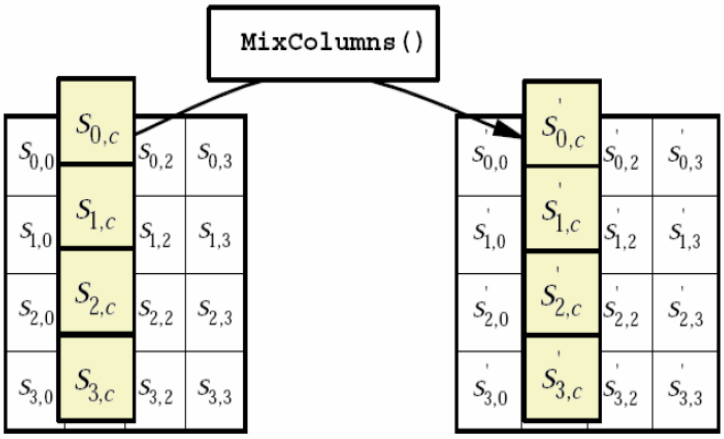

Figure 5.3: Transformation MixColumns

C'est une transformation linéaire: un produit matriciel utilisant les 4 octets d'une colonne. Les colonnes sont traitées comme des polynomes dans GF(2^8) et multipliées modulo $x^4 + 1$ avec les polynomes fixes donnés figure suivante:

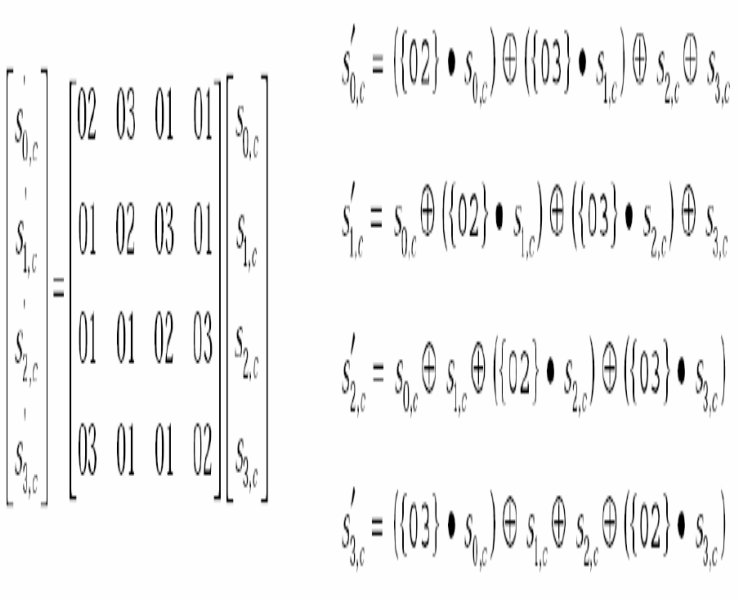

Figure 5.4: polynomes fixes

✈ **Transformation AddRoundKey:** ajout de la clef de ronde (ou de la clef lors de la ronde initiale) á l'état considéré (l'addition étant prise au sens ou exclusif). Un XOR (au niveau bit) est appliqué entre chacun des octets de l'état et de la clef de ronde.

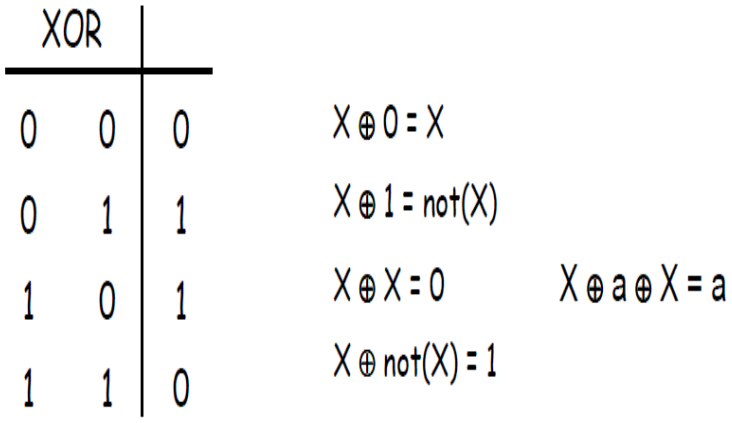

Figure 5.5: Transformation AddRoundKey

par exmple:

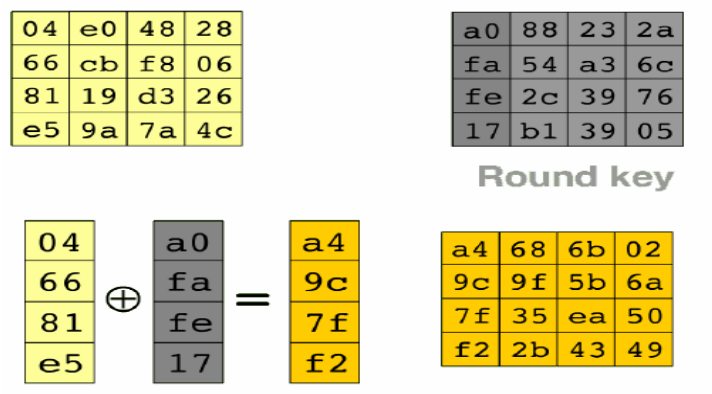

Figure 5.6: Exemple Transformation AddRoundKey

Déchiffrement de AES

✈ **InvShiftRows:**

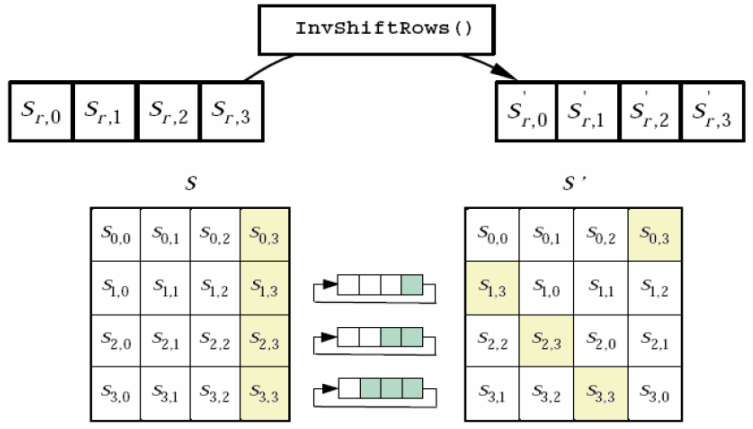

Figure 5.7: InvShiftRows

✈ **InvSubByte:** inverse de la transformation SubBytes().

x \ y	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	52	09	6a	d5	30	36	a5	38	bf	40	a3	9e	81	f3	d7	fb
1	7c	e3	39	82	9b	2f	ff	87	34	8e	43	44	c4	de	e9	cb
2	54	7b	94	32	a6	c2	23	3d	ee	4c	95	0b	42	fa	c3	4e
3	08	2e	a1	66	28	d9	24	b2	76	5b	a2	49	6d	8b	d1	25
4	72	f8	f6	64	86	68	98	16	d4	a4	5c	cc	5d	65	b6	92
5	6c	70	48	50	fd	ed	b9	da	5e	15	46	57	a7	8d	9d	84
6	90	d8	ab	00	8c	bc	d3	0a	f7	e4	58	05	b8	b3	45	06
7	d0	2c	1e	8f	ca	3f	0f	02	c1	af	bd	03	01	13	8a	6b
8	3a	91	11	41	4f	67	dc	ea	97	f2	cf	ce	f0	b4	e6	73
9	96	ac	74	22	e7	ad	35	85	e2	f9	37	e8	1c	75	df	6e
a	47	f1	1a	71	1d	29	c5	89	6f	b7	62	0e	aa	18	be	1b
b	fc	56	3e	4b	c6	d2	79	20	9a	db	c0	fe	78	cd	5a	f4
c	1f	dd	a8	33	88	07	c7	31	b1	12	10	59	27	80	ec	5f
d	60	51	7f	a9	19	b5	4a	0d	2d	e5	7a	9f	93	c9	9c	ef
e	a0	e0	3b	4d	ae	2a	f5	b0	c8	eb	bb	3c	83	53	99	61
f	17	2b	04	7e	ba	77	d6	26	e1	69	14	63	55	21	0c	7d

Figure 5.8: InvSubByte

✈ **InvMixColumns:**

$$\begin{bmatrix} s'_{0,c} \\ s'_{1,c} \\ s'_{2,c} \\ s'_{3,c} \end{bmatrix} = \begin{bmatrix} 0e & 0b & 0d & 09 \\ 09 & 0e & 0b & 0d \\ 0d & 09 & 0e & 0b \\ 0b & 0d & 09 & 0e \end{bmatrix} \begin{bmatrix} s_{0,c} \\ s_{1,c} \\ s_{2,c} \\ s_{3,c} \end{bmatrix}$$

$$s'_{0,c} = (\{0e\} \bullet s_{0,c}) \oplus (\{0b\} \bullet s_{1,c}) \oplus (\{0d\} \bullet s_{2,c}) \oplus (\{09\} \bullet s_{3,c})$$

$$s'_{1,c} = (\{09\} \bullet s_{0,c}) \oplus (\{0e\} \bullet s_{1,c}) \oplus (\{0b\} \bullet s_{2,c}) \oplus (\{0d\} \bullet s_{3,c})$$

$$s'_{2,c} = (\{0d\} \bullet s_{0,c}) \oplus (\{09\} \bullet s_{1,c}) \oplus (\{0e\} \bullet s_{2,c}) \oplus (\{0b\} \bullet s_{3,c})$$

$$s'_{3,c} = (\{0b\} \bullet s_{0,c}) \oplus (\{0d\} \bullet s_{1,c}) \oplus (\{09\} \bullet s_{2,c}) \oplus (\{0e\} \bullet s_{3,c})$$

Figure 5.9: InvSubByte

RÉSUMÉ

Dans le contexte de l'IoT (Internet of Thing) internet des objets en francais, de nombreux capteurs, actionneurs, contrÃ´leurs et dispositifs informatiques sont connectés á la plupart des infrastructures essentielles dans le monde, Il s'agit d'un paradigme avancé qui nécessite un ensemble de technologies, connaissances et infrastructures, pour apporter la confiance dans la gestion des données. La sécurisation des données devient une obligation pour les transformations de ces données pour sécuriser les systémes IoT. La sécurité des données est depuis longtemps une problématique majeure pour les transformations des données par des technologies de la communication, parmi ces technologies le WiFi. Pour cela, nous avons suggéré une assurance de la confidentialité des données transférées par un Wifi entre différents objets (tel que ordinateur, téléphone mobile, lap top, tablette) connectés par un serveur, en utilisant le cryptage symétrique basé sur l'algorithme de chiffrement AES.

Mots clé: IOT, AES, Confidantialité,Objet, AES, Wifi, Sécurité.

ABSTRACT

In the context of IoT, many sensors, actuators, controllers and computer devices are connected to most of the critical infrastructures in the world, it is an advanced paradigm that requires a set of technologies, knowledge and infrastructure, to bring confidence in the management of data. Data security becomes an obligation for the transformations of this data to secure IoT systems. Data security has long been a major issue for data transformations by communication technologies, among these technologies WiFi. For this, we suggested ensuring the confidentiality of data transferred by a Wifi between different objects (such as computer, mobile phone, lap top, tablet) connected by a server, using symmetric encryption based on the AES algorithm.

Key words: IOT,Object, AES, Confidentiality, Security .