République Algérienne Démocratique et Populaire
Université Abou Bakr Belkaid– Tlemcen
Faculté des Sciences
Département d'Informatique

Mémoire de fin d'études

Pour l'obtention du diplôme de Master en Informatique

Option : *Réseau et Système Distribué (R.S.D)*

Thème

Simulation des mécanismes de sécurité dans un réseau e-santé à base d'IoT via packet tracer

Réalisé par :

- MISSOUM Mohammed Aymen

Présenté le 25 Juin 2024 devant le jury composé de :

- *BENMAMMAR Badr* *(Président)*
- *AMRAOUI Asma* *(Encadrante)*
- *BENMOUNA Youcef* *(Examinateur)*

Année universitaire : 2023-2024

Remerciements

On remercie avant tout Dieu le tout puissant qui nous a donné la force et le courage pour réaliser ce modeste travail.

Le succès et l'accomplissement de ce mémoire découle d'effort, de confiance et de dévouement offert par notre encadrante Mme AMRAOUI Asma qui a bien accepté de superviser le travail, et nous a aidé par les discussions fructueuses et orientations bénéfiques et indispensables.

Nous tenons également à remercier les membres de jury BENMAMMAR Badr et BENMOUNA Youcef qui nous font l'honneur de présider et d'examiner notre travail.

Je n'oublie pas de remercier ma famille particulièrement ma mère, mon frère et mes sœurs et mon père Lah Yarhmah qui m'ont toujours encouragé et pour leur contribution et leur patience.

Sommaire

Listes des figures

Listes des Tables

Liste des acronymes

2FA: Two-Factor Authentication

3G: Third Generation

4G: Fourth Generation

ADSL: Asymmetric Digital Subscriber Line

AES: Advanced Encryption Standard

AWS: Amazon Web Services

BLE: Bluetooth Low Energy

CoAP: Constrained Application Protocol

CSP : Cloud Service Provider

DES : Data Encryption Standard

DNS: Domain Name System

FIDO2: Fast Identity Online 2

GSM: Global System for Mobile Communications

HTTP : HyperText Transfer Protocol

IoT : Internet des objets

ISP: Internet Service Provider

LAN: Local Area Network

LoRa: Long Range

Log4j: Logging for Java

LPWAN: Low Power Wide Area Network

LTE-M: Long Term Evolution for Machines

MFA: Multi-Factor Authentication

MOTD: Message of the Day

MQTT: Message Queuing Telemetry Transport

NB-IoT: Narrowband Internet of Things

NFC: Near Field Communication

PUF: Physically Unclonable Function

RFID: Radio-Frequency Identification

SHA-1: Secure Hash Algorithm 1

Sigfox : Non applicable (c'est un nom de marque)

SQRL: Secure Quick Reliable Login

SSO: Single Sign-On

TRNG: True Random Number Generator

Wi-Fi: Wireless Fidelity

WPA2-PSK: Wi-Fi Protected Access 2 - Pre-Shared Key

Introduction générale

L'Internet des objets représente une avancée technologique majeure qui transforme de nombreux secteurs, notamment celui de la santé. Les réseaux e-santé basés sur l'IoT permettent la collecte, la transmission et l'analyse de données médicales en temps réel améliorant ainsi la qualité des soins et facilitant la gestion des patients. Toutefois, cette transformation s'accompagne de défis considérables en matière de sécurité, car les dispositifs IoT sont souvent vulnérables aux cyberattaques.

Les dispositifs IoT dans les réseaux e-santé sont souvent exposés à diverses menaces telles que les interceptions de données, et les intrusions non autorisées. La protection des informations médicales sensibles et la garantie de la disponibilité et de l'intégrité des services de santé sont des préoccupations majeures. Par conséquent, il est crucial de développer et d'implémenter des mécanismes de sécurité efficaces pour protéger ces réseaux.

Cependant, la simulation de ces réseaux e-santé pose des défis particuliers en raison de la complexité et des exigences spécifiques de ces systèmes. Cisco Packet Tracer, un outil de simulation de réseau couramment utilisé, ne fournit pas directement les fonctionnalités spécifiques à l'e-santé, ce qui crée des obstacles pour les chercheurs et les praticiens qui souhaitent modéliser ces environnements complexes.

La contribution principale de ce mémoire réside dans le développement de solutions pratiques pour la simulation de réseaux e-santé à base d'IoT en utilisant Cisco Packet Tracer, malgré ses limitations intrinsèques. Ces solutions incluent la création de dispositifs IoT simulés spécifiques à l'e-santé ainsi que la mise en place de scénarios de simulation réalistes qui reflètent les défis et les exigences du domaine de la santé.

Ce travail est structuré en trois chapitres principaux, le premier vise à présenter les notions générales sur l’internet des objets ainsi que leur architecture et domaines d’application, ensuite le deuxième chapitre se focalise sur l’aspect sécurité de ce type de réseau en présentant les failles et les solutions existantes. Et enfin le chapitre 3 consiste à réaliser une simulation avec l’outil Cisco Packet Tracer d’un réseau IoT dans le domaine de la e-santé tout en intégrant les mécanismes de sécurité nécessaire.

Chapitre I :

Internet des objets

I.1. Introduction

Avec l'évolution rapide des différentes technologies de communication sans fil et leur intégration dans la plupart des objets intelligents, notre vie quotidienne va subir des changements dans de nombreux domaines. L'internet des objets (IoT) consiste de manière simplifiée à connecter des objets. En quelque sorte, il s'agit de l'extension de l'Internet au monde réel des objets qui nous entourent. Ces objets intelligents sont souvent des capteurs dotés de capacités de mesures (température, pression, vibration, luminosité, humidité, tension, etc.) ou des actionneurs capables d'agir. Ils peuvent s'interconnecter pour anticiper et interagir en temps réel, c'est-à-dire pour réaliser un objectif commun (surveillance de l'environnement, contrôle du trafic routier urbain, etc.).

I.2. Evolution de l'internet

Le graphe de Figure I.1 représente l'évolution de l'Internet, depuis son apparition jusqu'à aujourd'hui. Il est divisé en quatre grandes phases :

- **La phase pré-Internet (avant 1980)** : à cette époque, l'Internet n'existait pas encore. Les communications électroniques se faisaient par des moyens analogiques, tels que le téléphone, la télécopie ou le télex.
- **La phase Internet des contenus (1980-2000)** : à cette époque, l'Internet a commencé à se développer, mais il était encore principalement utilisé pour le partage de contenus, tels que des documents, des images ou des vidéos.
- **La phase Internet des services (2000-2010)** : à cette époque, l'Internet a commencé à être utilisé pour fournir des services, tels que le commerce électronique, les réseaux sociaux ou les e-mails.
- **La phase Internet des objets (2010-aujourd'hui)** : à cette époque, l'Internet a commencé à être utilisé pour connecter des objets entre eux. Ces objets, appelés objets connectés, sont capables d'échanger des données entre eux et avec des systèmes informatiques.

Le graphe montre également comment l'Internet est devenu de plus en plus intelligent. En effet, les phases Internet des services et Internet des objets ont permis de collecter et d'analyser des données de manière plus sophistiquée. Cela a conduit au développement de

nouveaux services et applications, tels que l'analyse prédictive ou la prise de décision automatisée.

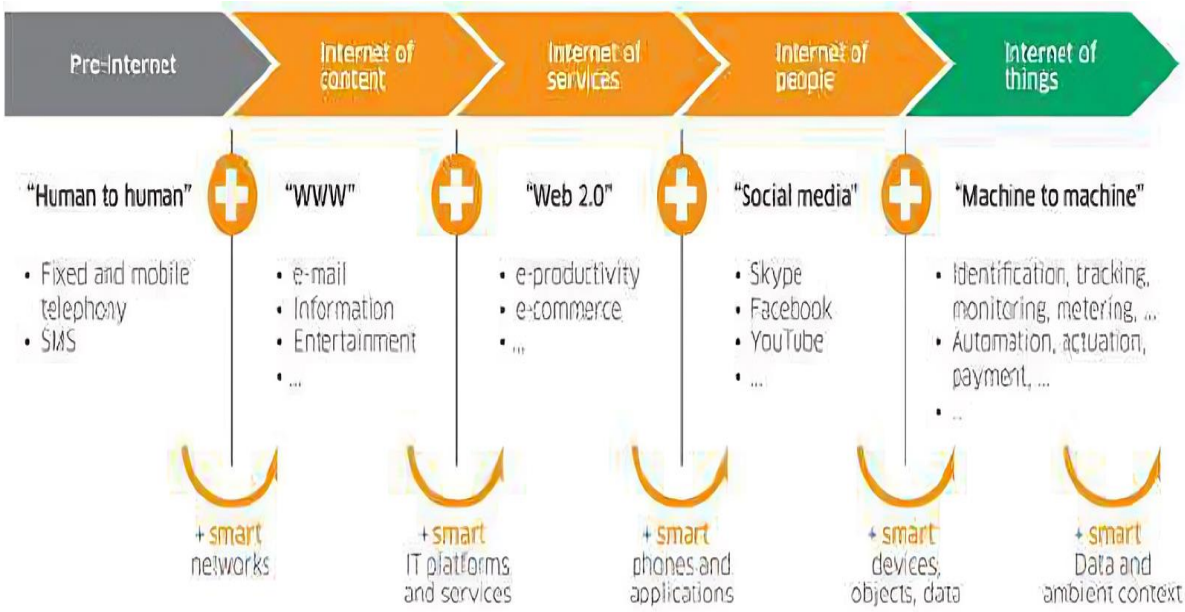

Figure I.1 : Evolution de l'internet [1]

I.3. Historique

En 1989, *Mark Weiser* professeur à Berkeley, avait une vision d'un monde où la technologie s'intègre dans les objets de la vie quotidienne. Aujourd'hui, sa vision prend forme avec l'avancé de l'informatique et électronique, tout se miniaturise et se connecte à Internet : du téléphone, montres connectées, aux capteurs. On parle désormais de l'Internet des objets. Le terme IoT a été utilisé pour la première fois au laboratoire Auto-ID center au MIT en 1999 par le professeur *Kevin Ashton*, où ils travaillaient sur l'identification de la fréquence radio (RFID) en réseau et sur les technologies de détection émergentes. Et Selon le groupe Cisco Internet Business Solutions (IBSG), l'Internet des objets est né entre 2008 et 2009, au moment où plus de « choses ou d'objets » étaient connectés à l'internet que de personnes **[1].**

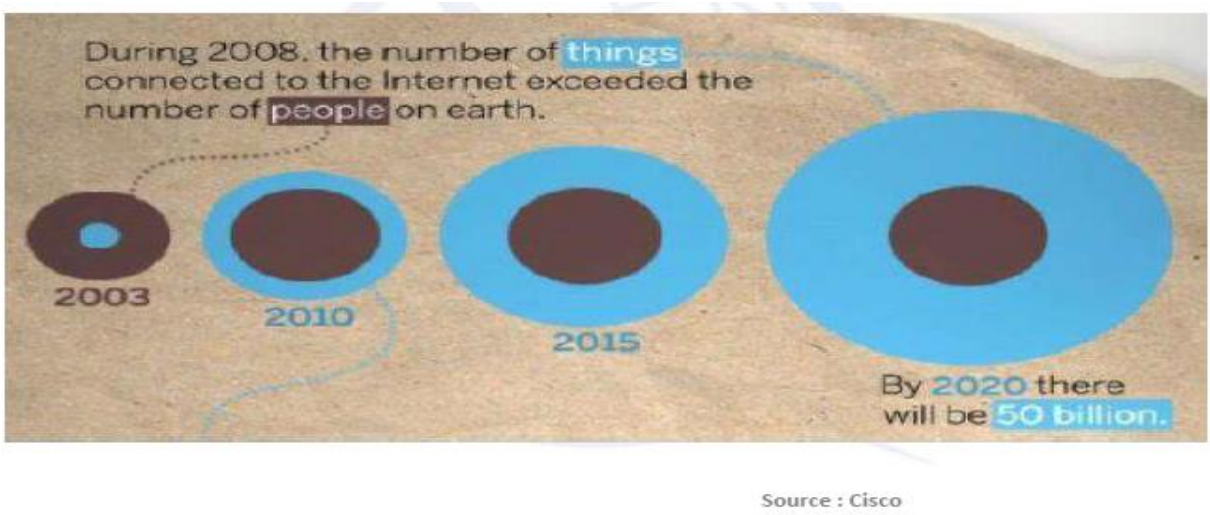

Figure I.2 : Croissance exponentielle des objets connectés jusqu'en 2020 [1]

Le figure I.2 montre l'évolution de l'utilisation des objets connectés à travers les années où on voit que le nombre d''objets connectés va dépasser le nombre de personnes sur la terre.

La première application IoT est née à l'université de Cambridge en 1991. Il s'agissait d'une caméra pointée sur une cafetière et connectée au réseau local de l'université (Chaque informaticien pouvait connaitre la disponibilité de café depuis son écran).

I.4. Le marché de l'IoT

Selon l'IHS, le figure I.3 représente l'évolution de la taille du marché mondial de l'IoT de 2015 à 2025. Elle montre que le marché de l'IoT est en forte croissance.

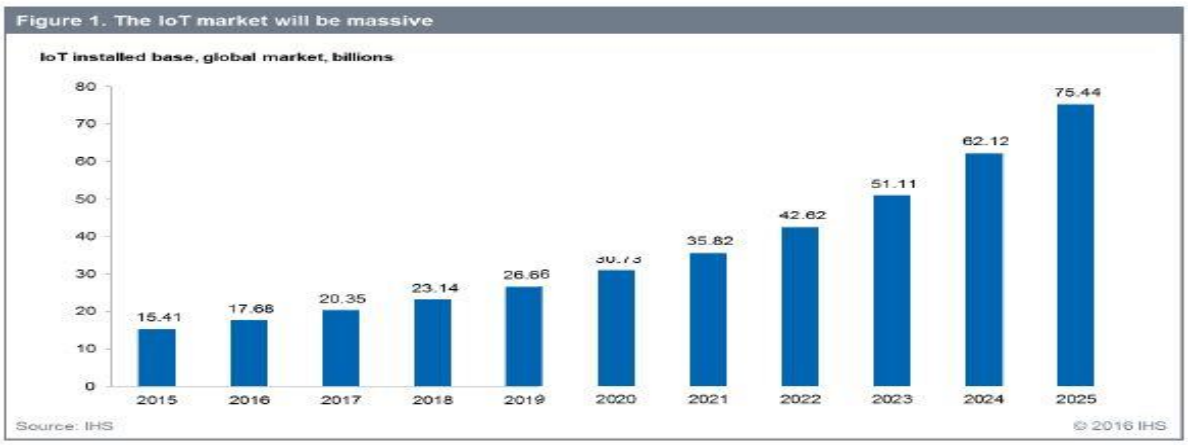

Figure I.3 : Croissance du marché de l'IoT [1]

I.5. Définition de l'IoT

Il s'agit d'une infrastructure d'objets, de personnes, de systèmes et de ressources d'information interconnectés ainsi que de services intelligents qui leur permettent de traiter les informations du monde physique et virtuel et de réagir, et même offrir à un utilisateur distants le contrôle de ses objets qui a pour but de fournir des services pour divers secteurs **[2].**

Le figure I.4 illustre un modèle de connectivité intégrant trois dimensions : le temps (Any TIME connection), le lieu (Any PLACE connection), et les objets (Any THING connection). Chaque dimension englobe diverses situations de connexion : en mouvement, à l'extérieur, à l'intérieur, le jour, la nuit, entre humains et/ou objets, avec ou sans utilisation d'un PC. Le modèle met en évidence la flexibilité et l'ubiquité des interactions numériques modernes, montrant comment elles peuvent se produire n'importe quand, n'importe où et entre n'importe quels appareils ou entités.

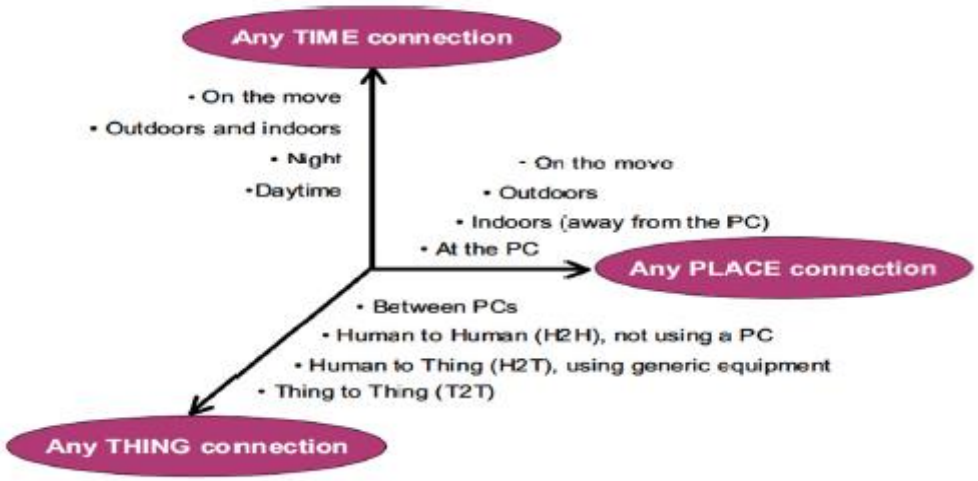

Figure I.4 : Nouvelle dimension de l'IoT [23]

I.6. Fonctionnalités de l'IoT

L'écosystème internet des objets intègre divers technologies et domaines de compétences. Un système IoT constitué généralement, de hardware, de software, des protocoles de communication, de Cloud et de mobile.

Un système IoT se décompose en 4 fonctionnalités comme la montre la figure ci-dessous :

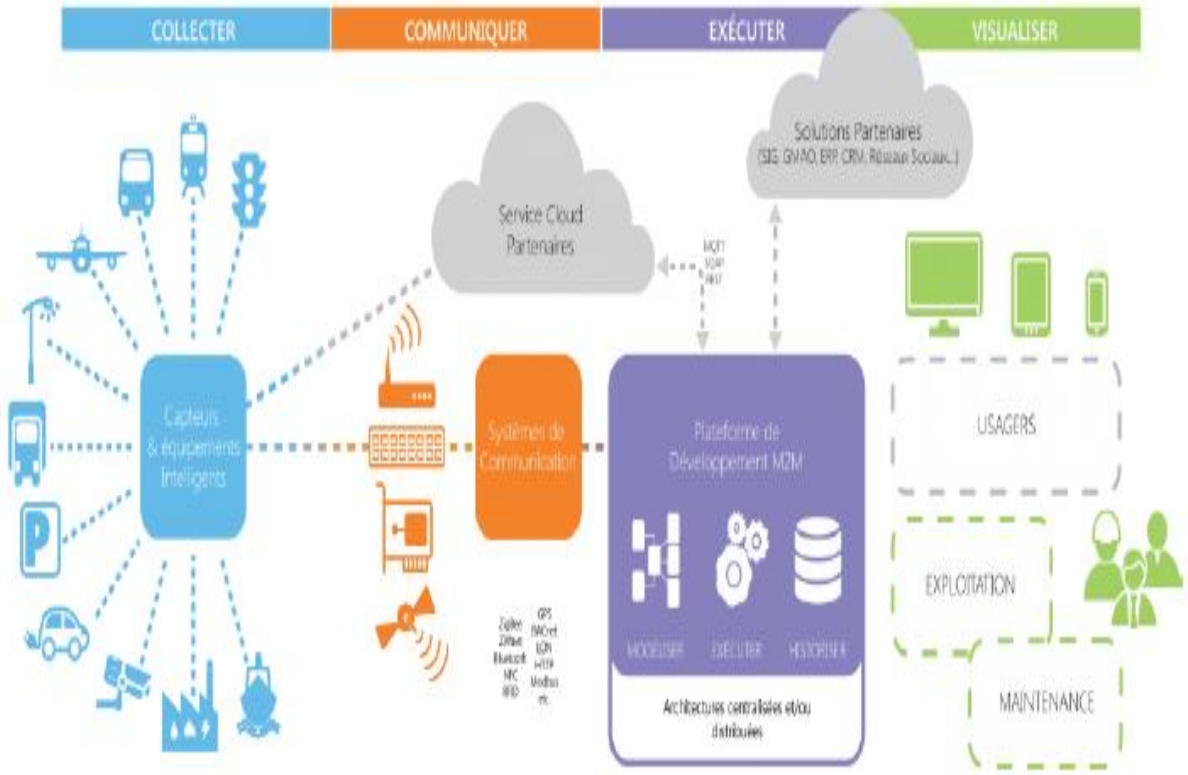

Figure I.5 : Ecosystème IoT [1]

- **Collecter / Actionner**

C'est la première couche au niveau des objets connectés. Elle est constituée de capteurs qui captent des mesures de l'environnement physique (température, humidité, etc..) et des actionneurs qui ont le pouvoir d'agir sur l'environnement (des moteurs pour fermer ou ouvrir le volet de la chambre). Certains objets sont dotés de capacités et de ressources matérielles nécessaires qui leur permettent de se connecter directement à Internet. Mais généralement, ayant des contraintes matérielles, les objets connectés implémentent des protocoles de communication à basse énergie / bas débit et utilisent une Gateway pour pouvoir se connecter à internet, cette Gateway peut être un Smartphone, un Arduino ou une Raspberry pi... **[3]**

Les protocoles de communication basse énergie / bas débit sont classés selon leur portée : courte (ex : *BLE*, *NFC*), moyenne (ex : *Zigbee*) ou longue (ex. : *Sigfox* et *LoRa*).

- **Communiquer**

Pendant cette étape, l'envoi des données du *LAN* vers le Cloud se fait, on peut distinguer deux modèles de protocoles pour transporter la donnée : Le ***modèle Publish / Subscribe*** avec des protocoles de type *MQTT* et le ***modèle REST*** avec des protocoles comme *HTTP* ou encore *CoAP*. **[3]**

- **Exécuter**

Cette étape s'occupe du stockage et du traitement des données. Lors de cette étape, la Plateforme IoT entre en jeux qui est une solution Cloud qui permet de connecter plusieurs objets connectés, de traiter et de stocker leurs données, les analyser et les exposer à travers les différentes applications. Les plateformes IoT permettent aussi de faire communiquer des objets qui utilisent des protocoles différents. **[3]**

- **Visualiser**

Cette étape a pour tâche d'afficher les services des objets connectés à travers différentes applications dédiées. Un utilisateur, à travers une application mobile, peut communiquer avec ses objets en consultant leurs données ou bien en envoyant des actions vers ses objets. **[3]**

I.7. Architecture de l'IoT

L'architecture d'une solution IoT varie d'un système à l'autre en se basant sur le type de la solution à mettre en place.

Il n'existe pas d'architecture de référence standard unique pour l'IoT car elle englobe une variété de technologies. Cela signifie qu'il n'y a pas un modèle simple qui peut être suivi pour toutes les implémentations possibles. Mais la plus général est l'architecture à 5 couches comme illustré dans la figure ci-dessous.

- **La couche perception** possède des capteurs et actionneurs qui détectent et recueillent des informations sur l'environnement.
- **La couche réseau** est responsable de la connexion, du transport et du traitement des données issues des capteurs et actionneurs.
- **La couche application** est chargée de fournir à l'utilisateur des services spécifiques et applications intelligentes.
- **Couche de traitement de données** La couche de traitement accumule, stocke et traite les données provenant de la couche précédente. Toutes ces tâches sont généralement traitées via des plateformes IoT et comprennent deux étapes principales.
- **Couche de sécurité** Cette couche est transverse à toutes les couches précédentes. La sécurité de l'IoT est primordiale, nous avons observé certaines vulnérabilités comme celle du Log4j. **[4]**

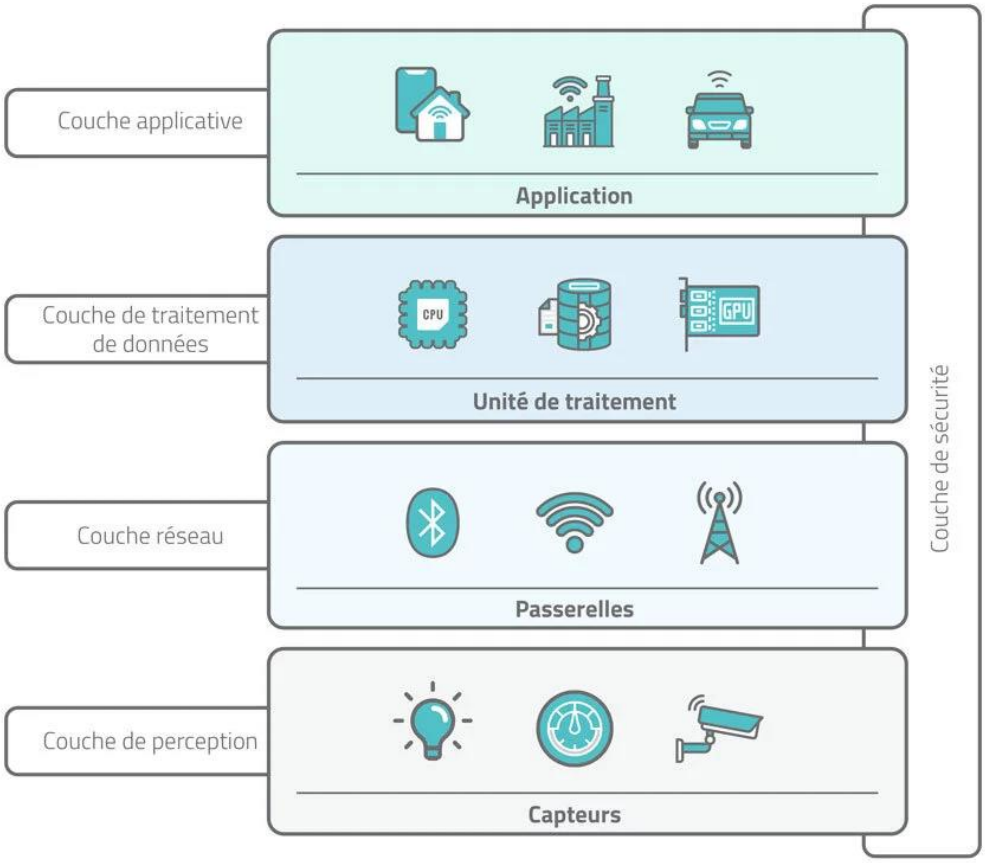

Figure I.6 : Architecture IoT à 5 couches [4]

Le figure I.7 illustre une architecture IoT en trois niveaux la plus élémentaire : Perception (capteurs et actionneurs collectant des données), Réseau (routeurs et portails transmettant les données), et Application (cloud et serveurs traitant et analysant les données). Elle montre le flux de données de leur collecte à leur exploitation pour fournir des services et applications utiles.

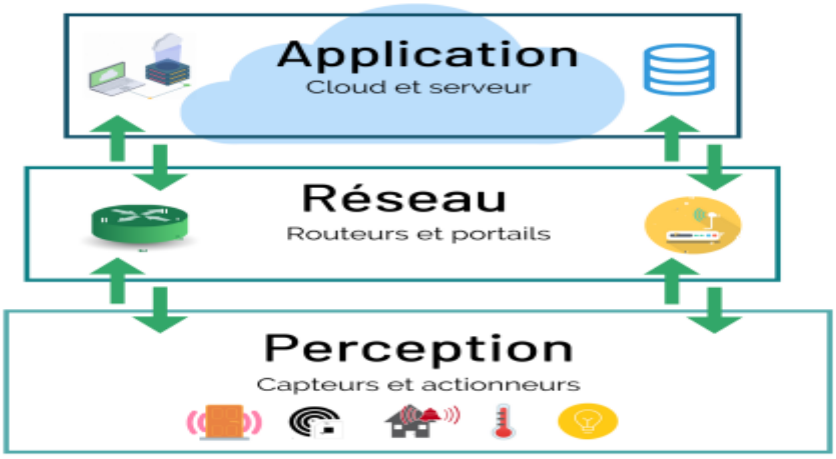

Figure I.7: Architecure IoT à 3 couches [1]

I.8. Acteurs de l'IoT

Le figure I.8 présente les différents acteurs impliqués dans l'écosystème de l'Internet des Objets (IoT). Voici une explication des rôles de chaque acteur mentionné :

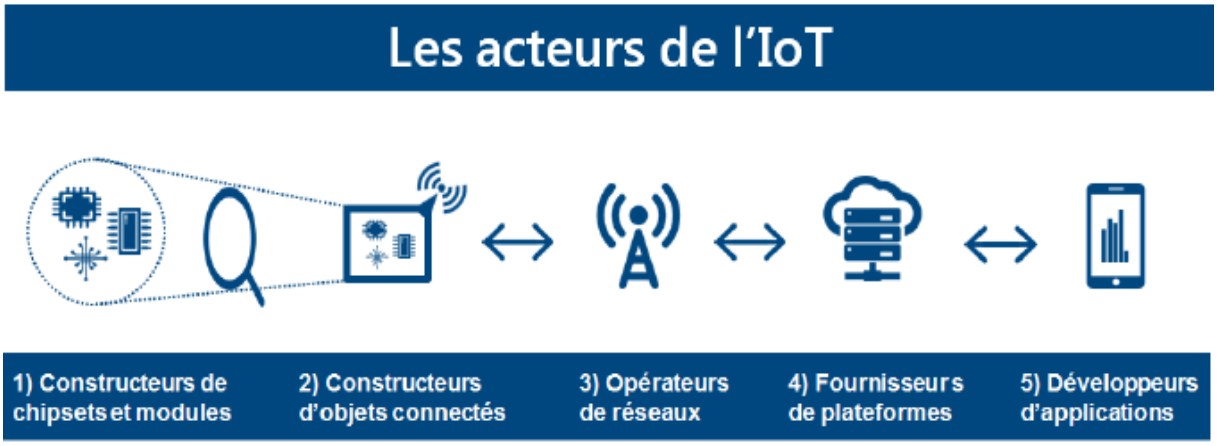

Figure I.8 : Acteurs de l'écosystème IoT [1]

- **Constructeur de chipsets et modules :** ce sont eux qui produisent les capteurs et les transmetteurs électroniques qui, une fois assemblés, composeront les objets connectés. **[5]**

- **Constructeur d'objets connectés :** il s'agit de l'objet final constitué des capteurs et transmetteurs issus des constructeurs de chipsets et modules**.** Il y a aussi une valeur

ajouté importante qui peut être apportée à ce niveau, comme l'ajout d'une « intelligence embarquée ».

Comme il se peut aussi que l'objet disposera d'un système d'exploitation plus ou moins avancé qui permettra par exemple de gérer au mieux la collecte des données, les périodes de transmissions, la sécurité…. Ce qui peut permettre à l'objet d'embarquer directement des composantes applicatives (client ou agent applicatif). **[5]**

- **Opérateur de réseaux** : « **la connectivité** » : il s'agit du réseau (*ADSL*, *3G*, *4G*, *LPWAN*) qui va permettre de relier l'objet pour qu'il puisse échanger ses informations, et de transmettre les données qu'il produit ou mesure au destinataire final **[5].**

- **Fournisseur de plateforme :** ces plateformes ont pour rôle de stocker les données émises par les objets et de les traiter afin de les rendre exploitables par les applications métiers du client final exemple de plateforme (*bluemix*, *AWS*) **[5].**

- **Développeur d'application :** l'application utilise les données récupérées par les objets connectés.et traduit les données en informations exploitables directement (mesure de température...). Il s'agit aussi des applications qui pourront mettre en valeur les données, il reste possible d'héberger ces applications dans le cloud de manière couplée avec la plateforme IoT.

Les fournisseurs de plateformes IoT proposent déjà des applications pour traiter des besoins « standards » de certains secteurs **[5].**

I.9. Protocoles de communication pour l'IoT

Un protocole de communication définit les règles standards pour communiquer entre plusieurs dispositifs numériques. Il permet de connecter un objet à un réseau, filaire ou sans-fil. Le réseau est constitué d'un ensemble d'équipements (passerelles, proxies, serveurs…) connectés entre eux et à Internet, la communication varie en fonction du type de réseau IoT.

I.9.1 Réseaux courts

- **Wi-Fi** : le *Wi-Fi* est l'un des protocoles réseau les plus utilisés pour l'internet des objets. d'une portée de 40m environ, c'est une technologie dont le succès repose essentiellement sur le haut débit qu'il offre. Le Wi-Fi est opérable avec plusieurs objets connectés. Ainsi, il est possible d'opter pour ce protocole IOT dans le cadre de l'installation d'une clé connectée par exemple. **[6]**
- **Bluetooth** : le Bluetooth est un réseau de courte portée (il fonctionne sur quelques mètres seulement), très présent pour connecter des équipements informatiques, électroniques entre eux. **[6]**
- **Near Field Communication** : la technologie *NFC* est utilisée pour le transfert sécurisé des informations sur des distances relativement courtes. Son efficacité est due à la limitation de son champ magnétique. Les cas d'usage les plus connus pour ce protocole IOT sont le paiement sans contact ou l'ouverture de portes à l'aide d'une carte magnétique. **[6]**
- **Radio Frequency Identification *:*** est une méthode permettant de mémoriser et récupérer des données à distance. Le système est activé par un transfert d'énergie électromagnétique entre une étiquette radio et un émetteur RFID**.** L'étiquette radio composée d'une puce électronique et d'une antenne reçoit le signal radio émis par le lecteur lui aussi équipé d'une technologie RFID. Les composants permettent à la fois de lire et de répondre aux signaux**.** Elle permet par exemple de faciliter la gestion logistique dans les entrepôts. **[7]**
- **Z-wave & Zigbee** : ces réseaux sont utilisés pour créer un maillage entre plusieurs équipements connectés d'un bâtiment. Ce sont des technologies qui consomment peu d'énergie. C'est le protocole IoT à sélectionner pour le remplacement du câblage électrique au sein d'une entreprise ou d'un logement domotisé. **[6]**
- **Wirepas** : ce réseau est indépendant des infrastructures réseau, car il fonctionne principalement grâce à une batterie. Cette technologie est efficace pour la gestion d'un nombre conséquent d'objets connectés. Wirepas est le protocole de communication le plus utilisé dans le secteur de l'énergie, du mobilier urbain et de l'industrie. **[6]**

I.9.2 Réseaux longs

- **Réseaux cellulaires** (GSM, 2G, 3G, 4G, 5G) : depuis des décennies, les réseaux cellulaires se succèdent. Après le GSM qui prenait uniquement en charge les SMS et les appels, les utilisateurs bénéficient aujourd'hui de la 5G. Ce protocole IoT peut relier plusieurs équipements connectés sur une longue distance à travers les cartes Sim M2M. Les réseaux cellulaires sont plus indiqués pour les sociétés qui désirent se développer dans une autre ville ou dans un autre pays. **[6]**

- **LoRaWan** : le réseau LoRa signifie Long Range ou « longue portée ». Il s'agit d'une technologie qui permet aux objets connectés d'échanger des données de faible taille en bas débit. Peu gourmande en débit et en énergie, elle a l'avantage d'être très économique pour l'utilisateur final et présente, de plus, une excellente capacité de pénétration des bâtiments, caves et sous-sols. Cette technologie utilise à la fois les fréquences radio libre 868 MHz et Internet. **[8]**

Le figure I.9 illustre les divers protocoles de communication sans fil en fonction de leur portée et de leur débit de données. Les communications sans fil à courte portée, telles que Bluetooth, Wi-Fi, Zigbee et NFC, offrent des débits de données élevés mais avec une portée limitée. Les communications cellulaires, englobant les technologies 2G, 3G, 4G et 5G, fournissent une couverture plus étendue avec des débits de données variables. Enfin, les réseaux LPWAN, incluant LTE-M, NB-IoT, LoRa et Sigfox, sont conçus pour des communications à longue portée avec des débits de données plus faibles, optimisés pour les appareils IoT à faible consommation énergétique.

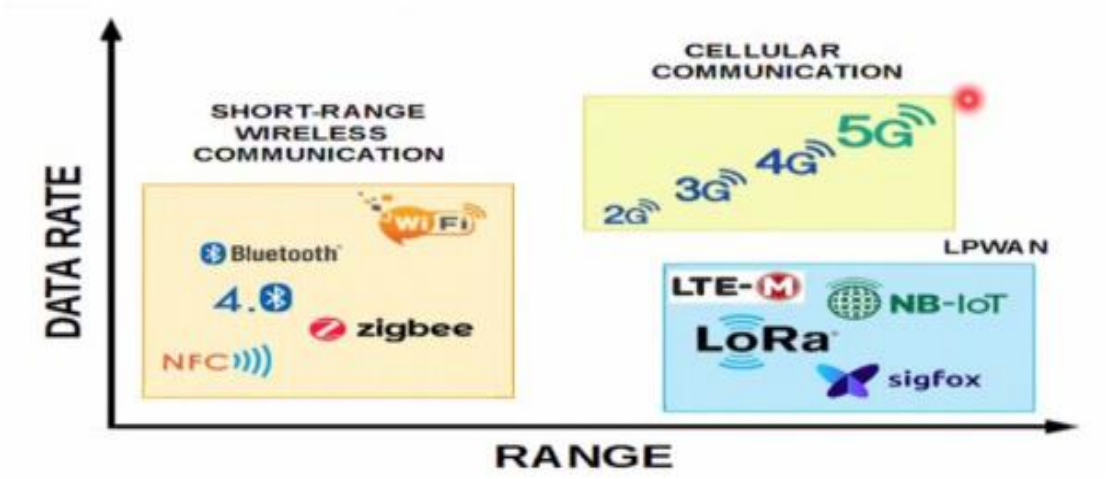

Figure I.9 : *D*ifférents types des réseaux sans fils [1]

I.10. Composantes d'une solution IoT

Généralement, une solution IoT est formée du composant suivant :

Objets physiques : des capteurs, technologie de connectivité et intelligence. **[1]**

Une passerelle (Gateway) : est une combinaison de composants matériels et logiciels utilisés pour connecter un réseau à un autre, utilisées aussi pour la communication de données en collectant les mesures effectuées par les nœuds de capteurs et en les transmettant à l'infrastructure Internet, et il peut faire des traitements locaux sur les données avant de les relayer au Cloud. **[1]**

Cloud computing : est un choix technologique (optionnel) qui permet d'alléger la charge du travail vers le Cloud et de faire des traitements locaux on the Edge, il y a trois solutions techniques sont possibles pour l'implémentation du 3ème niveau :

- Fog Computing : permet un calcul décentralisé en traitant les données IoT au niveau des nœuds locaux ―Fog‖ avant de relayer l'information vers le cloud.
- Edge Computing : le traitement des données IoT se fait à l'extrémité du réseau (Gateway ou des nœuds intermédiaires entre objets et Gateway).
- Mist Computing : le traitement des données se fait localement dans le nœud capteur. **[1]**

I.11. Domaines d'applications

L'internet des objets offre de nombreuses applications à ses utilisateurs. Parmi ces applications nous citons:

- **Villes intelligentes (Smart Cities)**

L'IoT permettra une meilleure gestion des réseaux divers qui alimentent nos villes (eaux, électricité, gaz, etc.) en permettant un contrôle continu en temps réel et précis. Des capteurs peuvent être utilisés pour l'économie de l'eau et pour améliorer la gestion des parkings et du trafic urbain et diminuer les embouteillages et les émissions en CO2. **[1]**

- **Industrie 4.0**

L'IoT permettra un suivi total des produits, de la chaîne de production, jusqu'à la chaîne logistique et de distribution en supervisant les conditions d'approvisionnements. Cette traçabilité de bout en bout permet aux usines d'améliorer l'efficacité de ses opérations, d'optimiser la production et d'améliorer la sécurité des employés. **[9]**

- **E-Santé :**

L'adoption étendue de l'Internet des objets (IoT) et ses nombreuses applications, telles que la surveillance à distance et l'intégration des dispositifs médicaux, ont transformé le secteur de la santé. Aujourd'hui, de nombreuses applications IoT sont employées, y compris les capteurs portables, les systèmes de sécurité et les appareils médicaux connectés au cloud. L'utilisation de l'IoT dans le domaine de la santé permet d'améliorer les résultats des patients et d'augmenter la qualité des soins tout au long de leur parcours médical.

I.12. Avantages et limitations de l'IoT

- **Avantages**

- Amélioration de la qualité de vie et de la sécurité (ex. : domotique et smart city).
- Automatisation et efficacité renforcée des systèmes
- Prise de décision basée sur des données en temps réel, Amélioration de la productivité et des processus opérationnels (ex. : diminution du nombre d'opérateurs humains et optimisation des chaînes de production ou de la logistique) **[10].**

- **Limitations**

- L'IoT peut dans certains domaines poser des problèmes quant à la confidentialité des données collectées pour son fonctionnement.

- Les informations personnelles relatives à une autorisation d'accès doivent, par exemple, répondre aux exigences du Règlement Général de Protection des Données (RGPD).
- Si la collecte d'informations relatives aux habitudes des occupants d'un smart building est utile à la gestion des réseaux d'énergie, elle peut porter atteinte à leur vie privée.
- Interopérabilité entre les différents appareils et leur protocole de connexion à assurer.
- Dépendance à une connectivité Internet fiable.
- Coût élevé de mise en œuvre et de maintenance dans certains secteurs **[10].**

I.13. Conclusion

Ce chapitre nous a permis d'avoir un aperçu de l'internet des objets, leur origine et puis son architecture et ses fonctionnalités et des domaines d'application ainsi de comprendre ses acteurs, en citant les avantages et la limitation de l'internet des objets et le futur de cette technologie.

Dans le chapitre suivant nous allons parler sur les risks qui peuvent survenir dans les réseaux à base d'IoT et des mesures de sécurité qu'on peut prendre pour les éviter.

Chapitre II :

Sécurité des réseaux IoT

II.1 Introduction

L'Internet des objets représente une révolution de l'Internet qui peut connecter presque tous les périphériques d'environnement sur Internet et partager leurs données pour créer de nouveaux services et applications et améliorer la qualité de vie. Néanmoins, malgré les nombreux avantages qu'ils apportent, les objets de l'IoT présentent également un certain nombre des menaces qui ralentissent leurs essors. En effet, les données collectées par ces dispositifs étant des données personnelles importantes, leur protection est obligatoire. Aussi, il est essentiel que les dispositifs connectés mettent en œuvre au minimum des mécanismes de sécurité afin de convaincre les utilisateurs d'adopter largement des solutions basées sur l'IoT.
Ce chapitre fait le tour de la question de la sécurité dans les systèmes IoT.

II.2 Sécurité de l'information

La sécurité de l'information regroupe l'ensemble des moyens organisationnels, technologiques, humains et juridiques permettant de gérer les risques et leurs impacts à l'égard de la disponibilité de l'information, de sa disponibilité et de son intégrité.
De nombreux défis de l'IoT pourrait s'inscrire dans le cadre de la triade originale de la sécurité de l'information**.**

Menaces : évènement potentiel et appréhendé, de probabilité non nulle, susceptible de porter attinte à la sécurité informatique. Une menace exploite une ou plusieurs vulnérabilités afin d'atteindre une cible grâce à une action. Lors que l'attaque est réussie, le résultat permet de produire un impact sur la cible **[1].**

Mesures de sécurité : sont mises en œuvre pour contrer une ou plusieurs menaces afin de contrôler, mitiger ou éliminer les risques.
Si malgré la mesure de sécurité, la menace réussit à atteindre un actif informationnel vulnérable, alors cette attaque est réussie.
Pour pouvoir mesurer, un système IoT nécessite l'authentification et l'autorisation des utilisateurs et des périphériques.

- L'authentification vérifie l'identité des utilisateurs ou des périphériques dans un système IoT
- L'autorisation fournit les privilèges nécessaires à l'entité autorisée **[1].**

II.3 Défis de la sécurité de l'IoT

- L'économie favorise la sécurité faible car Il n'y a pas de moyens crédibles permettant aux fournisseurs de signaler leur niveau de sécurité aux consommateurs.
- La sécurité est difficile, en particulier pour les nouvelles entreprises.
- Les systèmes IoT sont complexes et chaque partie doit être sécurisée tel que les périphériques, applications et services IoT nécessitent des correctifs de sécurité et des mises à jour pour se protéger contre les vulnérabilités connues.
- Le support de sécurité n'est pas toujours maintenu.
- La connaissance du consommateur de la sécurité IoT faible.
- Les incidents de sécurité peuvent être difficiles à détecter ou à résoudre pour les utilisateurs **[1].**

II.4 Propriétés de sécurité

- **Confidentialité**

La confidentialité est le mécanisme qui permet de cacher une donnée, et de cacher même l'information de son existence. Elle permet aussi d'empêcher toute entité non autorisée d'avoir accès à ces données. En général, ce service repose sur des algorithmes mathématiques qui permettent de déformer un texte brut et de lui redonner sa forme initiale grâce à une ou plusieurs clés de chiffrement et de cryptages.

Dans l'Internet des objets, en particulier dans le contexte de la communication, la confidentialité signifie assurer la protection des données échangées entre les appareils intelligents contre l'interception de personnes non autorisées et cela en utilisant des mécanismes dédiés **[11].**

- **Intégrité**

L'intégrité garantit que les données ne sont ni falsifiées ni modifiées ou altérées ni supprimées par une entité non autorisée. Cela est assuré grâce aux points suivants :

- Empêcher la modification des informations par des utilisateurs non autorisés.
- Empêcher la modification non autorisée ou involontaire des informations par des utilisateurs autorisés.
- Préserver une cohérence interne et externe :

  Cohérence interne : Elle garantit que les données sont cohérentes sur le plan interne.

Cohérence externe : Elle garantit que les données stockées dans la base de données sont cohérentes avec le monde réel **[11].**

- **Disponibilité**

C'est la garantie d'accès à un service ou à des ressources afin de maintenir le bon fonctionnement du système Internet des Objets. Ainsi, assurer la disponibilité signifie construire le système pour réduire l'impact d'un déni de service (DoS), pour un service auquel un attaquant pourrait essayer de bloquer l'accès **[11].**

- **Authentification**

L'authentification permet de prouver l'identité d'une entité. Dans un système IoT, l'authentification représente la première barrière de sécurité pour empêcher une personne tierce et non autorisée d'accéder aux données des dispositifs intelligents **[11].**

- **Non-répudiation**

La non-répudiation est un mécanisme garantissant qu'une opération ne peut être niée par celui qui l'avait établie. La non-répudiation assure que l'émetteur du message ne pourra pas nier dans le futur avoir émis le message **[11].**

- **Contrôle d'accès**

L'utilisation non autorisée d'une ressource IoT est permise par le contrôle d'accès. Conformément à une politique de sécurité, une liste des entités dont l'accès à une ressource est autorisé ainsi que leur niveau d'accès sont définis afin de réaliser ce contrôle **[11].**

II.5 Mécanismes de sécurité

Dans cette section, nous proposerons les principaux types de mécanismes de sécurité. En général, les mécanismes de sécurité visent à protéger l'accès aux actifs (c'est-à-dire les données et les ressources) du système contre les diverses menaces. Ainsi, l'utilisation de mécanismes de sécurité permet de mettre en œuvre des services de sécurité pour empêcher la détection et/ou la modification non autorisée des données et/ou l'accès non autorisé aux ressources. Par exemple, pour assurer l'accès aux ressources, seuls les utilisateurs autorisés peuvent configurer un service d'authentification. Cela peut être obtenu grâce à l'utilisation de divers mécanismes de sécurité : affichage du nom d'utilisateur et du mot de passe, technologie de défi-réponse utilisant le cryptage symétrique ou signature numérique, etc.

II.6 Mécanismes de chiffrement

Pour réaliser le cryptage, le processus de conversion du texte clair en un message crypté, il est possible d'utiliser un chiffrement symétrique ou un chiffrement asymétrique. L'objectif du chiffrement est de protéger la confidentialité des informations échangées entre les entités communicantes

II.6.1 Chiffrement symétrique

Afin d'échanger des données en toute sécurité, à l'aide d'un algorithme de chiffrement symétrique, l'expéditeur et le destinataire (ou les destinataires) doivent utiliser un secret partagé (c'est-à-dire clé). La notion de symétrie vient du fait que c'est la même clé, qualifiée de secrète, que les entités connectées utilisent à la fois pour le cryptage et le décryptage. La clé doit rester secrète et ne pas être dévoilée aux entités du système qui n'y ont pas droits. Le problème principal du chiffrement symétrique est qu'il nécessite un partage de clé avant que des données secrètes et chiffrées ne soient échangées. Le partage de la clé se fait via un canal sécurisé ce qui est difficile à réaliser concrètement.
Les méthodes les plus connues pour le chiffrement symétrique sont le DES le 3 *DES* (*Triple DES*) et l'*AES* **[12].**

II.6.2 Chiffrement asymétrique

Pour effectuer un chiffrement asymétrique, chaque entité doit posséder deux clés cryptographiques : une clé privée (connue uniquement de l'entité qui la possède) et une clé publique (tout le monde peut y accéder). La taille des clés est plus importante et elle peut aller jusqu'à 4 096 bits, rendant ce type d'algorithme ou ce type de chiffrement extrêmement fiable, voire même totalement sécurisé à 99% jusqu'à preuve du contraire. Le *RSA* est le plus connue pour le chiffrement asymétrique, aussi appelé chiffrement à clé publique **[12].**

II.6.3 Fonctions de hachage

Une fonction de hachage est une fonction qui mappe les données de taille arbitraire à des valeurs de taille fixe (plus petites), par exemple : 64 octets. Dans un contexte de sécurité, les fonctions de hachage sont souvent utilisées pour fournir une fonction unidirectionnelle déterministe et facile à calculer pour n'importe quelle entrée, mais difficile (informatiquement infaisable) à inverser compte tenu du condensé de l'entrée arbitraire **[13].**

Les fonctions de hachage sont largement utilisées dans différents protocoles cryptographiques, dans l'authentification, les signatures, etc.

Les principales propriétés que doit avoir une fonction de hachage cryptographique sont **[14]** :

- L'empreinte d'un message doit dépendre de tous les bits du message, si un seul bit change, le haché ou l'empreinte ne doit avoir aucune relation avec le haché du texte d'origine.
- Une fonction de hachage cryptographique doit être résistante aux préimage, à la seconde pré-image et aux collisions. Les trois problèmes suivants doivent être très difficiles :

- Pré-image : étant donné un haché h choisi aléatoirement. Trouver un message m tel que H(m)=h.
- Seconde pré image : étant donné un haché h choisi aléatoirement. Trouver un message m′ tel que H(m)=H(m′).
- Collision : trouver deux messages m et m′, tels que m≠m′ et H(m)=H(m′). **[14]**

On définit la résistance d'une fonction aux collisions, aux pré images et aux deuxièmes pré images par rapport à la difficulté de résoudre ces problèmes en pratique. Cette difficulté est évaluée par rapport aux nombres d'opérations nécessaires pour que la meilleure attaque générique contre une fonction de hachage idéale réussisse.

Il existe plusieurs fonctions de hachage ayant différents algorithmes, les plus usuelles sont : MD5, SHA-1, …etc.

II.6.4 Signature numérique

Une signature numérique a la même utilité qu'une signature manuscrite. Cependant, une signature manuscrite peut être facilement imitée, alors qu'une signature numérique est pratiquement infalsifiable. Les procédures de signature précédentes ont un coût élevé pour signer de longs messages car la signature est aussi longue que le message. On double donc la longueur du texte à crypter. Pour réduire la longueur de la signature, on peut utiliser une fonction de hachage cryptographique.

Prenons l'exemple de la signature de Schnorr. C'est une solution de signature numérique qui utilise l'algorithme d'authentification décrit par Claus Peter Schnorr**.** La Sécurité de cet algorithme est basée sur la difficulté de calculer le logarithme discret **[14].**

II.7 Technologies de communication de l'IoT et leurs mécanismes de sécurité

Sécurité dans LoRaWAN : la politique de sécurité de LoRaWAN assure les objectifs de base de la cryptographie qui sont l'authentification des objets, la confidentialité et l'intégrité des données. Cette politique définie également des techniques de partage de clés **[15].**

Sécurité dans ZigBee : pour des raisons de sécurité, il est requis au niveau de la couche application et de la couche réseau. Chaque couche est responsable de la sécurisation de son volume de données **[15].**

II.8 Authentification dans l'IoT

Avec le développement du domaine de l'Internet des objets et le besoin illimité du monde pour celui-ci. Nous devons prendre soin de la sécurité dans tous ses aspects, en utilisant plusieurs phases comme l'authentification, dont nous parlerons en profondeur dans ce qui suit.

En termes simples, l'authentification constitue la procédure de reconnaissance de l'identité d'un utilisateur. Elle s'exécute au début d'une application et valide les utilisateurs pour s'assurer qu'ils remplissent toutes les conditions de sécurité **[16]**. L'authentification de l'objet est le processus d'authentification générale d'un objet ou d'un appareil sur des réseaux câblés ou sans fil lorsque l'objet est un demandeur cherchant à accéder à des informations ou à les partager ou à réaliser un autre type d'interaction numérique. L'authentification de l'objet se produit de différentes manières dans diverses configurations informatiques, mais implique généralement un certificat numérique comme dans le protocole SSL utilisé sur Internet **[17].**

II.8.1 Authentification primaire/ Facteur unique

Cette méthode simplifie l'accès sécurisé à un système. Dans ce cas, un seul justificatif d'identité est nécessaire pour la vérification en ligne. Le mot de passe est la forme d'authentification la plus populaire.**[18]**

II.8.2 Authentification à deux facteurs

Une couche supplémentaire de sécurité qui protège les utilisateurs d'un système. En fait, l'utilisateur doit passer une étape supplémentaire après avoir saisi son identifiant et son mot de passe. Il fournit des informations supplémentaires, telles qu'un code PIN, une réponse à une " question secrète " ou un numéro envoyé par SMS ou par e-mail. Même ses caractéristiques biométriques peuvent être utilisées avec Face ID ou Touch ID. **[18]**

II.8.3 Authentification unique

En utilisant un seul ensemble d'informations d'identification, SSO permet de s'authentifier en toute sécurité auprès de plusieurs comptes en ligne. En fait, ce système est utilisé chaque fois qu'il est possible de se connecter à l'aide de Google, Apple, Facebook ou d'un autre fournisseur. Le principe repose sur un certificat échangé entre le fournisseur d'identité et le fournisseur de services. Par le biais de ce certificat, il envoie les informations d'identité à un fournisseur de services afin de s'assurer qu'elles proviennent d'une source fiable. **[18]**

II.8.4 Authentification multi-facteurs

Pour accéder au système MFA, il faut fournir deux facteurs de vérification ou plus. Une application, un compte en ligne ou un VPN constituent le système. La principale composante d'une politique de gestion des identités et des accès est cette méthode d'authentification. Les chances de réussite d'une cyberattaque sont réduites lorsque le MFA est utilisé dans les systèmes. **[18]**

II.9 Solutions d'authentification IoT

L'authentification est une sécurité dans les IoT. En effet, elle joue un rôle central dans la sécurité globale des systèmes IoT. Le schéma d'authentification des appareils IoT garantit que ces appareils peuvent être fiables ce qu'ils prétendent être. Un tel schéma fournit à chaque appareil IoT une identité unique (peut être dynamique dans le temps) qui peut être vérifié lorsque cet appareil tente de se connecter au réseau IoT. Cela donne la possibilité, entre autres, de suivre chaque dispositif tout au long de son cycle de vie (le cas échéant), pour échanger en toute sécurité avec lui, pour l'empêcher d'exécuter du code malveillant, et même s'il arrivait qu'un appareil IoT a présenté un comportement inattendu suspect, ses privilèges peuvent simplement être révoqué **[17].**

- **Authentification basée sur le matériel**

Utilise les caractéristiques physiques du matériel pour traiter l'authentification. Sur la base de ce critère, on peut distinguer les solutions matérielles implicites qui utilisent le matériel existant lors de l'authentification par exemple :

Physical Unclonable Fonction

Les Physical Unclonable Functions (PUF) sont des dispositifs matériels exploitant les variations microscopiques dues aux imperfections de fabrication pour créer des réponses uniques et impossibles à cloner. Un signal envoyé à la PUF génère une réponse unique, transformée en une clé cryptographique par un algorithme intégré. Cette clé sert à authentifier les appareils, assurant ainsi la sécurité des communications et du stockage des données, notamment dans les applications IoT**.**

True Random Number Generator

Un True Random Number Generator (TRNG) est un appareil ou algorithme qui utilise des phénomènes physiques imprévisibles pour générer des nombres véritablement aléatoires. Il est essentiel pour des applications de sécurité comme la génération de clés cryptographiques, les jeux en ligne et les loteries, car il garantit un hasard robuste et imprévisible. La fiabilité des TRNG est cruciale, car des nombres aléatoires prévisibles ou biaisés peuvent compromettre la sécurité des systèmes.

II.10 Architecture d'authentification

Il y a deux architectures d'authentification sont :

- **Architecture distribuée :** une authentification directe est utilisée pour authentifier les deux entités communicantes.
- **Architecture centralisée :** un tiers de confiance, également appelé entité centralisée, partage et gère les identifiants des entités pour la procédure d'authentification des entités communicantes.

La structure peut être plate ou hiérarchique dans les deux architectures. La structure plate n'a pas de niveau structure, tandis que la structure hiérarchique utilise plusieurs niveaux **[18].**

II.11 Menaces à différents niveaux

L'Internet des objets (IoT) connecte des appareils et des systèmes pour améliorer l'efficacité et la commodité dans divers secteurs. Cependant, cette interconnectivité apporte aussi de nouvelles menaces à différents niveaux. Comprendre ces menaces est essentiel pour protéger les réseaux IoT contre les attaques potentielles.

II.11.1 Capteurs / actionneurs

ATTAQUE	DESCRIPTION
Attaque du puits (sinkhole)	Une attaque dans laquelle un dispositif compromis capte le trafic de communication pour créer un trou noir ou activer une retransmission sélective.
Attaque Sybil	Une attaque dans laquelle un appareil malveillant assume plusieurs identités de manière illégitime.
Attaque par trou de ver	Une attaque par trou de vers se produit lorsque deux nœuds malveillants/compromis donnent l'impression que le trajet qui les relie est extrêmement court.
Détournement du dispositif	S'applique à un appareil physiquement compromis ou où les clés sont perdues.

Tableau II.1 : Les attaques sur les dispositifs

II.11.2 Communications

ATTAQUE	DESCRIPTION
Bluejacking	Une attaque qui vise les dispositifs mobiles Bluetooth, tels que les téléphones portables. Bien que les messages envoyés n'endommagent pas le dispositif visé, ils peuvent amener l'utilisateur à répondre d'une manière spécifique ou à ajouter de nouveaux contacts dans son répertoire.
Accès non	L'accès non autorisé à un réseau de capteurs sans fil peut entraîner la

autorisé	divulgation d'informations sensibles, la modification de données, le déni de service et l'utilisation illicite de ressources.

Tableau II.2 : Les attaques au niveau de communication

II.12 Autres mécanismes de sécurisé le réseaux IoT

La sécurisation des réseaux IoT repose sur divers mécanismes, notamment les pares-feux pour contrôler le trafic réseau, et le chiffrement des communications pour garantir la confidentialité des données. L'authentification et la gestion des identités assurent que seuls les utilisateurs et appareils autorisés accèdent au réseau. Tandis que les mises à jour régulières des logiciels et la surveillance continue détectent et corrigent les failles de sécurité. Enfin, les messages de bannière et le contrôle d'accès basé sur les rôles (RBAC) renforcent la sécurité en restreignant les accès non autorisés.

II.13 Conclusion

La sécurité et l'authentification sont importantes dans notre monde, en particulier dans un monde où l'Internet des objets s'est répandu, et c'est ce que nous avons expliqué ci-dessus. Nous avons commencé par un aperçu des propriétés et des mécanismes de sécurité. Ensuite, nous avons représenté le concept d'authentification dans l'Internet des objets. Après, nous avons accordé une attention particulière à l'authentification telle que ses types et ses protocoles, et cité les défis et les problèmes ouverts de l'authentification. Et enfin les attaque qui viser les system IoT.

Dans ce chapitre, nous avons parlé sur la sécurité des réseaux IoT et les diffèrent risque contre ces réseaux, ainsi les propriétés et les différents mécanismes de sécurité de ces réseaux dans les différents niveaux (les dispositifs, la communication), puis en visée sur l'authentification avec détaille et enfin en parle sur les attaques qui fait en passé sur les réseaux basé sur l'IoT.

Dans le prochain chapitre, nous allons implémenter notre réseaux IoT sur un simulateur très connu dans le domaine de e-santé avec les mécanismes de sécurité disponibles sur ce simulateur.

Chapitre III :
Simulation d’un réseau e-santé basé sur l’IoT

III.1 Introduction

Les avancées technologiques sont essentielles pour développer des nouvelles technologies. Elles relient ce qui est réel et ce qui semblait autrefois impossible. Aujourd'hui, nous vivons une période de grandes découvertes scientifiques et techniques. Ces innovations ont simplifié notre quotidien et sont particulièrement utiles en médecine et en santé. On parle d'objets connectés portatifs pour décrire ces outils. Leur avantage réside dans leur petite taille et leur capacité à s'adapter au corps humain.

Le fonctionnement de ces outils est globalement le même, bien que le niveau de sophistication
varie. Il y a en général deux parties :

- **Le capteur médical** : c'est la partie qui va, comme son nom l'indique, capter des données et des informations médicales, puis les transmettre.

- **L'appareil connecté :** c'est la partie qui va recevoir l'information transmise, puis l'analyser ou l'envoyer à une base de données plus importante.

Les hôpitaux d'aujourd'hui sont équipés de technologies de pointe pour sauver autant de vies que possible. Cependant, une lacune demeure : l'absence de connectivité basée sur l'Internet des Objets (IoT) entre les véhicules, comme les ambulances, et les hôpitaux environnants. Pour pallier ce manque, une connexion à Internet via Wi-Fi ou données cellulaires sera utilisée.

Nous avons utilisé Packet Tracer pour la simulation des IoT et IoE dans le domaine de la santé. En effet, nous avons conçu un scénario réaliste mettant en place un hôpital avec un médecin, une ambulance et plusieurs patients, chacun équipé de capteurs de température, de tension artérielle et de diabète. Ces capteurs intelligents, connectés à un réseau centralisé, permettent de surveiller en temps réel l'état de santé des patients et d'optimiser les interventions médicales.

Ce chapitre est structuré en plusieurs sections. Tout d'abord, nous présenterons le scénario en détail, décrivant les différents acteurs et équipements impliqués. Ensuite, nous expliquerons la configuration du réseau dans Packet Tracer, incluant la mise en place des

capteurs et leur intégration dans le système hospitalier. La simulation sera ensuite déroulée, montrant les interactions entre les dispositifs et les réactions aux différentes situations médicales simulées. Enfin, nous analyserons les résultats et discuterons des implications de l'utilisation des technologies IoT et IoE dans le domaine de la santé.

III.2 Cisco Packet Tracer

Cisco Packet Tracer **[19]** est un logiciel gratuit de simulation et de visualisation de réseaux développé par Cisco. Il permet de créer un réseau virtuel en utilisant divers équipements tels que des routeurs, des commutateurs, des ordinateurs et des dispositifs IoT, connectés via des câbles ou sans fil. Les utilisateurs peuvent configurer les adresses IP, les services disponibles et les paramètres de sécurité des réseaux IoT.

La version 8.1, disponible pour Windows et Linux, inclut de nouvelles fonctionnalités pour simuler les produits Cisco récents et les applications IoT. Cette version est idéale pour pratiquer la configuration et le dépannage des réseaux, ainsi que pour explorer les mesures de sécurité spécifiques aux réseaux IoT.

Nous utiliserons Packet Tracer pour simuler les objets connectés, expliquant ainsi leur fonctionnement et les aspects de sécurité de manière pratique.

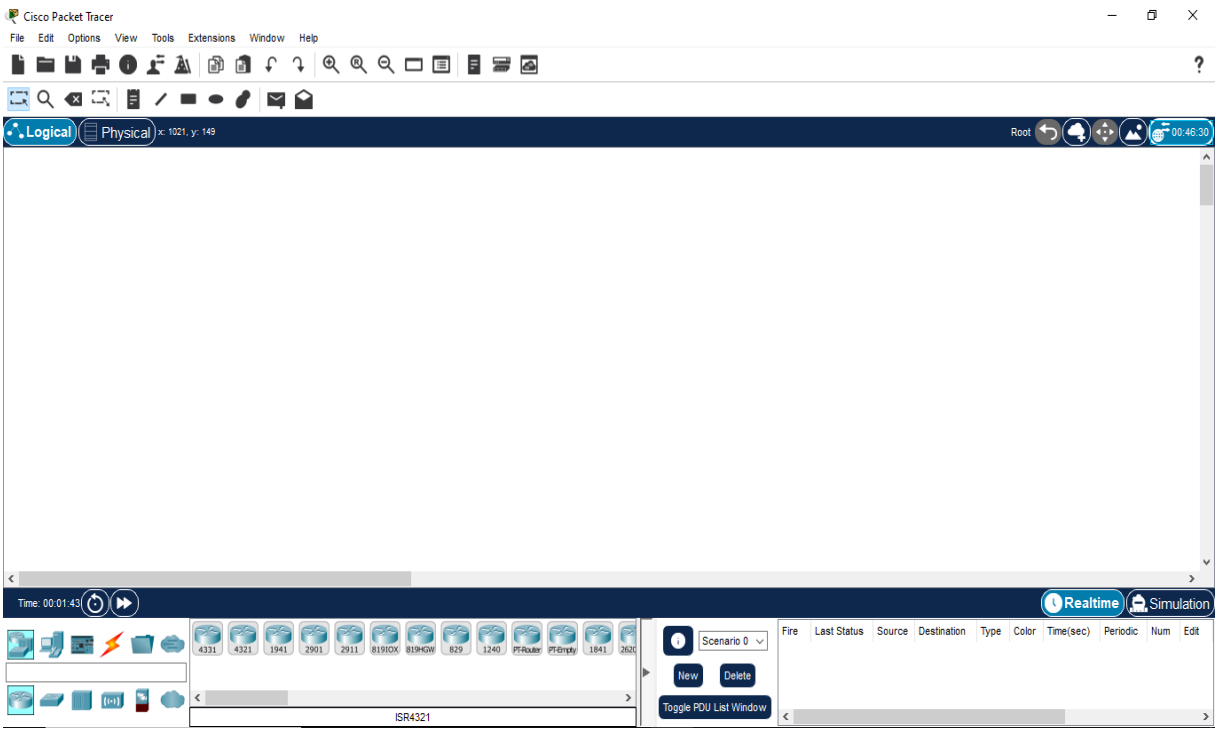

Figure III.1 : La fenêtre de Packet Tracer

III.3 Travaux relatifs

Dans cette section, nous allons parler des travaux relatifs à l'utilisation de packet tracer pour simuler des applications IoT. Ceci dit, il y a peu de travaux ayant utilisé cet outil dans le domaine de la santé car ce dernier n'inclut toujours pas les périphériques nécessaires.

Dans **[20],** les auteurs proposent une architecture pour les patients asthmatiques basée sur le Cloud en utilisant Cisco Packet Trace où ils intègrent un capteur de température pour recueillir les valeurs de température des patients et les envoyer au Cloud via un routeur sans fil. Cependant, leur proposition ne prend pas en compte l'utilisation simultanée de multiples capteurs ni la surveillance en temps réel dans Cisco Packet Tracer.

Dans **[21],** les auteurs proposent une architecture IoT basée sur le Cloud pour un réseau de santé, permettant aux patients d'être surveillés à distance par leur famille et leurs médecins. L'architecture proposée est conçue et configurée en utilisant Cisco Packet Tracer version 7.0 sur deux sites : le site 'A' situé à la maison intelligente et le site 'B' situé à l'hôpital intelligent. Les résultats de test ont montré que cette configuration permet aux médecins de surveiller les données en temps réel à distance, offrant ainsi une surveillance continue et efficace des patients.

Dans **[22],** un Arduino MKR1000 sera employé, avec des capteurs connectés au connecteur OBD II. Ces capteurs permettront à l'hôpital intelligent de communiquer en temps réel les données collectées des patients à bord de l'ambulance vers plusieurs hôpitaux simultanément ainsi les techniciens médicaux pourront ainsi examiner les dommages et accélérer le temps nécessaire aux médecins pour commencer à traiter les patients dès leur arrivée.

Les travaux présentés montrent diverses utilisations de Cisco Packet Tracer pour la simulation d'environnements IoT dans la santé, mais montrent également des limitations en termes de surveillance en temps réel et d'intégration de multiples capteurs, ouvrant la voie à des améliorations et des innovations dans ce domaine.

III.4 Architecture générale

L'Internet des objets révolutionne le fonctionnement des hôpitaux modernes en connectant divers appareils et capteurs pour collecter des données en temps réel et surveiller les patients à distance.

La figure III.2 représente une architecture réseau intégrant l'IoT, composée de plusieurs couches : des dispositifs de surveillance des patients et des appareils médicaux connectés, des réseaux de communication locaux et des passerelles IoT, des serveurs locaux et des services de cloud computing pour le traitement des données, des applications de suivi des patients, ainsi que des protocoles de sécurité et de confidentialité.

Cette intégration améliore la surveillance continue des patients, permet une réactivité accrue grâce aux alertes en temps réel et personnalise les soins grâce à l'analyse des données.

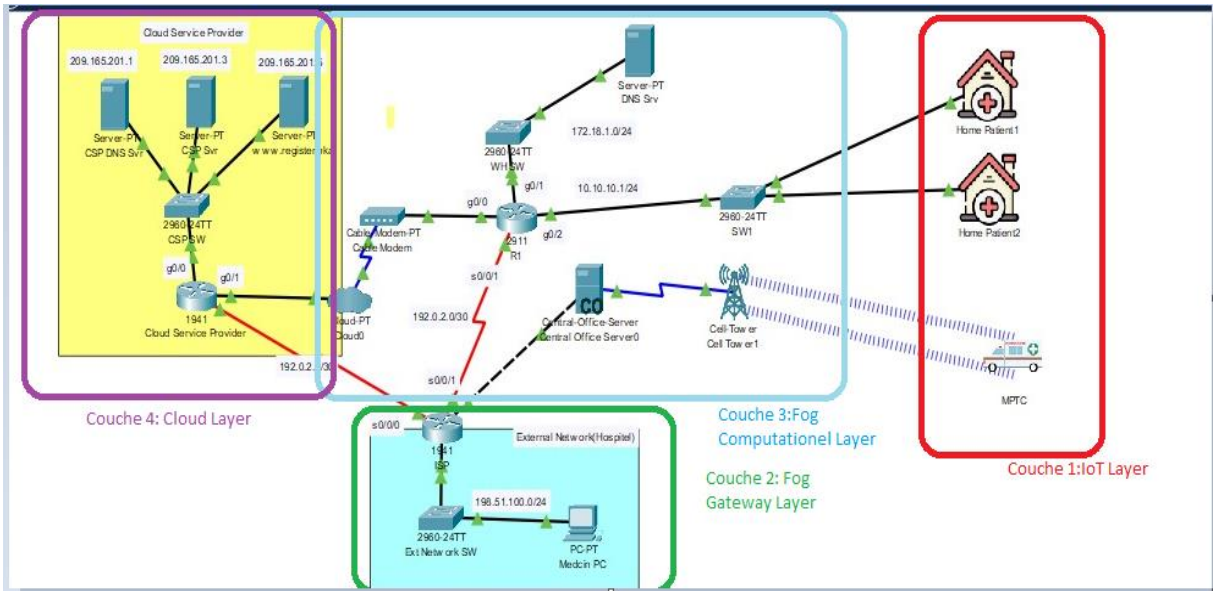

Figure III.2 : Architecture proposée

En utilisant cette architecture, nous avons conçu une simulation pour notre réseau IoT en e-santé, composée de trois couches :

- **Couche Cloud**

La couche Cloud fournit des services d'infrastructure et de plateforme aux applications. Ces services incluent le stockage de données, la gestion des bases de données, le serveur d'enregistrement, serveur DNS et serveur Mail.

- **Couche Fog**

La couche Fog est divisée en 2 sous couches :

- Fog Gateway layer : sépare le réseau interne de maison du réseau externe, tel qu'Internet. Elle fournit des fonctions de sécurité et de filtrage du trafic pour protéger le réseau interne contre les accès non autoriser.
- Fog Computationnel layer : responsable du routage du trafic entre les différentes couches du réseau. Elle comprend des routeurs (R1, ISP, CSP) et des commutateurs qui connectent les différents segments du réseau.

- **Couche IoT**

La couche des objets est la couche inférieure du réseau et comprend les appareils IoT déployés comme les smartphones, tablettes des médecins ainsi que des patients sans oublier les périphériques utilisés dans les ambulances.

III.5 Étapes de l'implémentation

III.5.1 Etape 1 : Ajout des éléments

1. Passerelles (Home Gateway)

Installer des passerelles pour collecter les données des capteurs et les transmettre aux serveurs ou au cloud, en suivant ces étapes :

- Dans Home Gateway, cliquer sur Wireless.
- Changer le SSID vers Home Gateway. Changer l'authentification en WPA2-PSK. et entrer IotWh001 en tant que Phrase de passage PSK.

- Cliquer sur Ordinateur portable puis sur Bureau. Cliquer sur PC sans fil.
- Cliquer sur l'onglet Connexion. Sélectionner le réseau Home Gateway. Si le nom du réseau sans fil n'est pas affiché, cliquer sur Actualiser.

- Pour le Smartphone et le Tablet de notre Home_Patient changer le SSID vers Home Gateway. Changer l'authentification en WPA2-PSK et entrer IotWh001 en tant que Phrase de passage PSK.

2. Capteurs et dispositifs IoT

Le capteur	Description
Capteurs de glucose	Mesurent les niveaux de glucose dans le sang pour les patients diabétiques, Le capteur est généralement inséré sous la peau et mesure en continu les niveaux de glucose
Capteurs de température corporelle	Mesurent la température corporelle pour surveiller la fièvre et les infections
Capteurs de pression artérielle	Mesurent la pression artérielle pour surveiller l'hypertension.

Tableaux III.1 : Capteurs médicaux et leurs fonctions

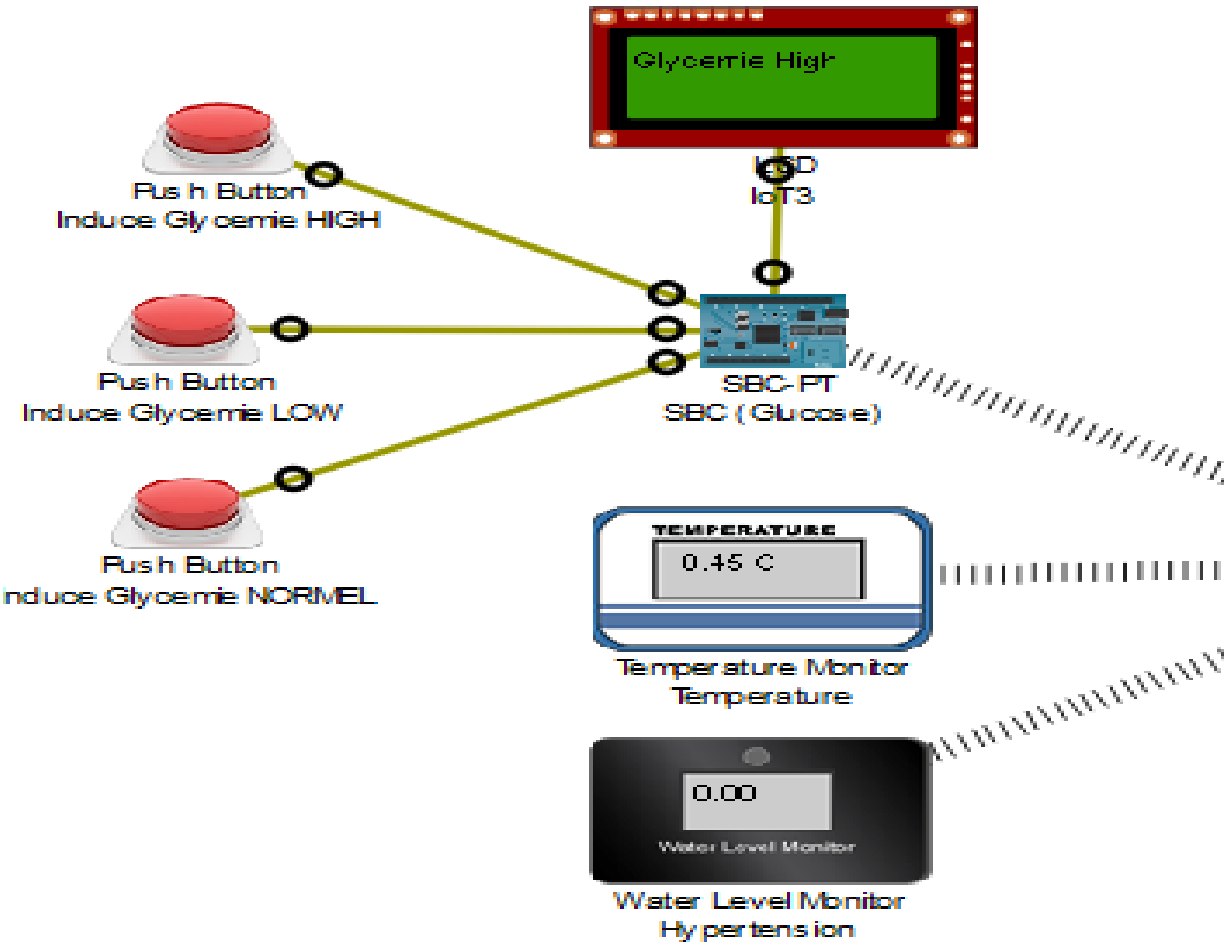

Figure III.4 : Système de surveillance médicale

Nous précisons que la dernière version 8.1 de Packet tracer ne supporte toujours pas le domaine de la e-santé, c'est pour cela qu'on va régénérer le code de certains IoT utilisés pour faire notre simulation.

- Pour le capteur de pression artérielle, on fait un changement aléatoire selon un intervalle de :
  - **Pression systolique** : 0 mmHg a 180 mmHg (normal rang est moins de 120 mmHg)
  - **Pression diastolique** : 0 mmHg a 180 mmHg (normal rang est moins de 80 mmHg)
- Pour le capteur de température, on fait un changement aléatoire selon un intervalle de :
  - **Température** : 32°C à 41°C (le rang normal environ 36,1°C à 37,2°C)
- Pour le capteur de glucose, on fait 3 boutons pour simuler le changement de glucose (HIGH/ LOW/ NORMAL) et un afficheur LCD pour représenter l'affichage de cet appareil.

3. Implémentation des capteurs

Les périphériques IoE (capteur de pression, capteur de température et le capteur de glucose) peuvent être connectés à l'aide de fils ou sans fil. La maison du patient sera connectée au réseau en mode sans fil.

- Cliquer sur 'Advanced' et sur 'I/O Config 'et dans la fenêtre qui apparaît changer le Network adapté au 'PT-IOTNM-1W' et fermer la fenêtre.
- Cliquer sur 'Advanced' et sur 'Programming' et dans la fenêtre qui apparait, on crée un nouveau python file et on insère notre code de Capteur de Température.
- On fait le même chose pour le capteur de pression.
- On crée le capteur de glucose et on insère notre code dans le SBC board.

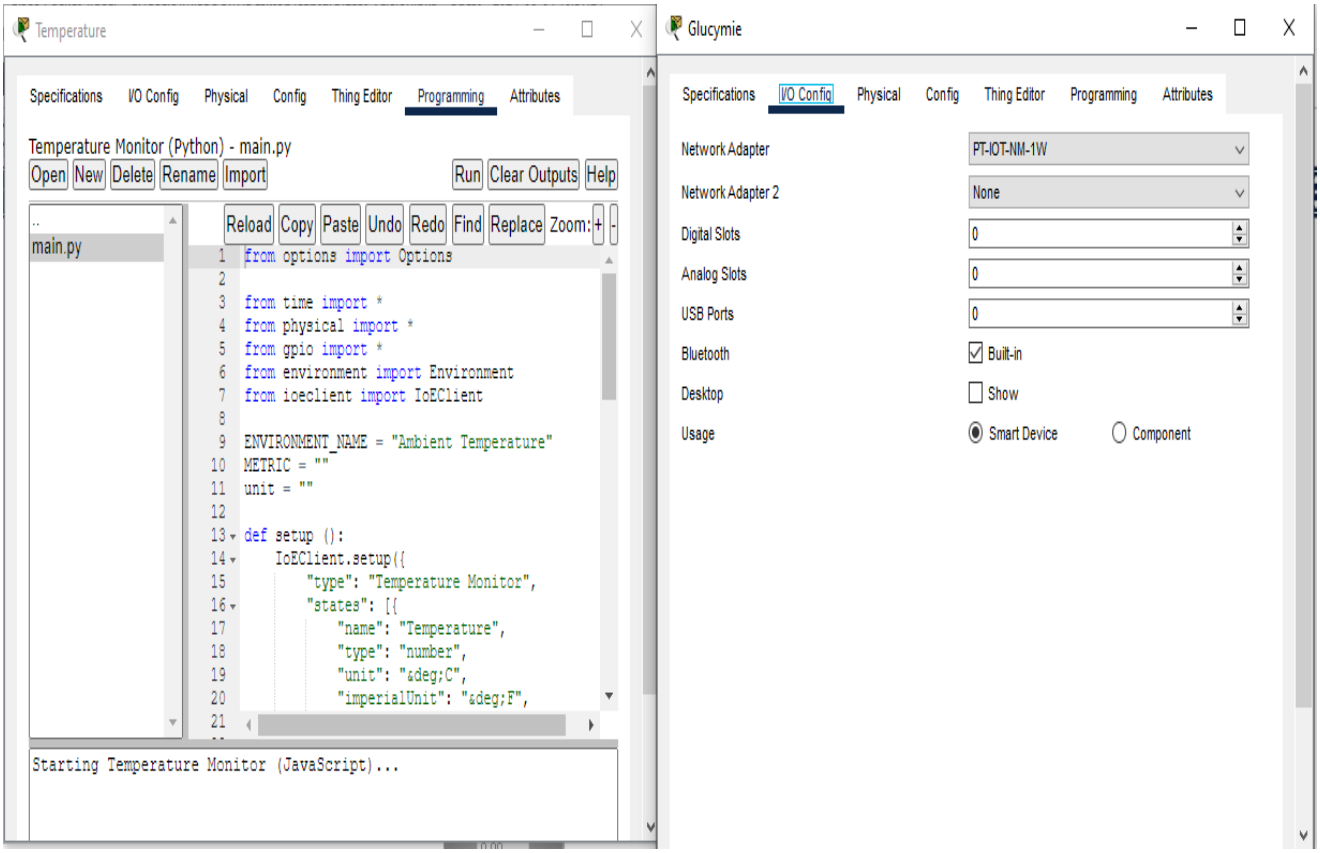

Figure III.5 : Configuration et programmation des capteurs

4. Connecter les IoT devices (capteurs)

- Dans les captures, cliquer sur Wireless.
- Changer le SSID vers Home Gateway. Changer l'authentification en WPA2-PSK. et entrer IotWh001 en tant que Phrase de passage PSK.

5. Serveurs

- **DNS** : le DNS (Domain Name System) est un système essentiel pour le fonctionnement d'Internet, servant de traducteur entre les noms de domaine lisibles par l'homme et les adresses IP numériques utilisées par les ordinateurs pour localiser et identifier des dispositifs sur des réseaux.

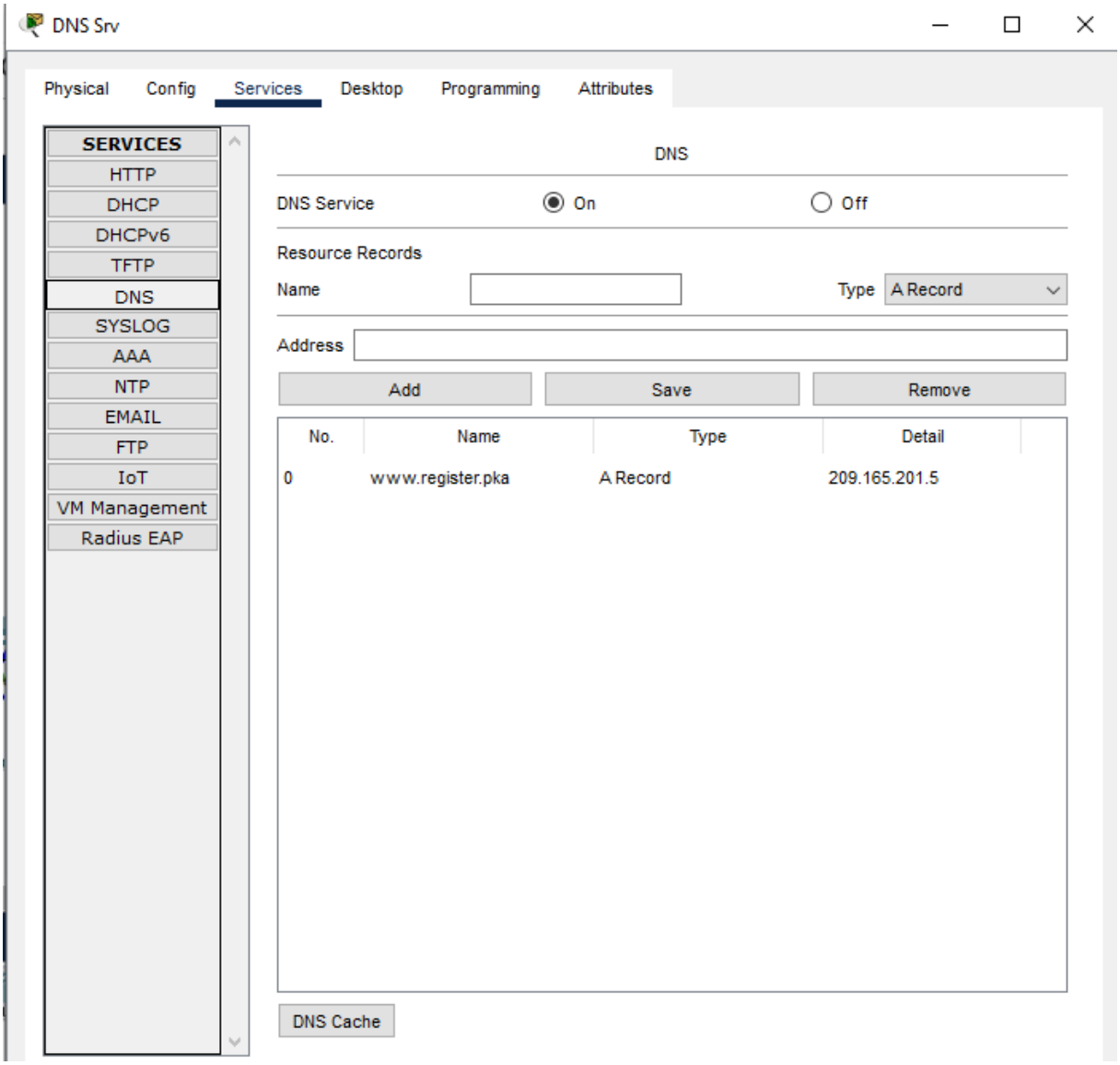

Figure III.6 : Configuration de serveur DNS

La figure III.6 montre une interface de configuration d'un serveur DNS où le service DNS est activé, permettant la gestion des enregistrements de ressources. Un enregistrement DNS est présent, liant le nom de domaine www.register.pka à l'adresse IP 209.165.201.5.

- **MAIL** : pour faire une notification par email en cas d’alerte en va créer une serveur mail pour puis connecter avec trois utilisateur la maladie dans l’appareil de glycémie, le médecin et l’ambulance.

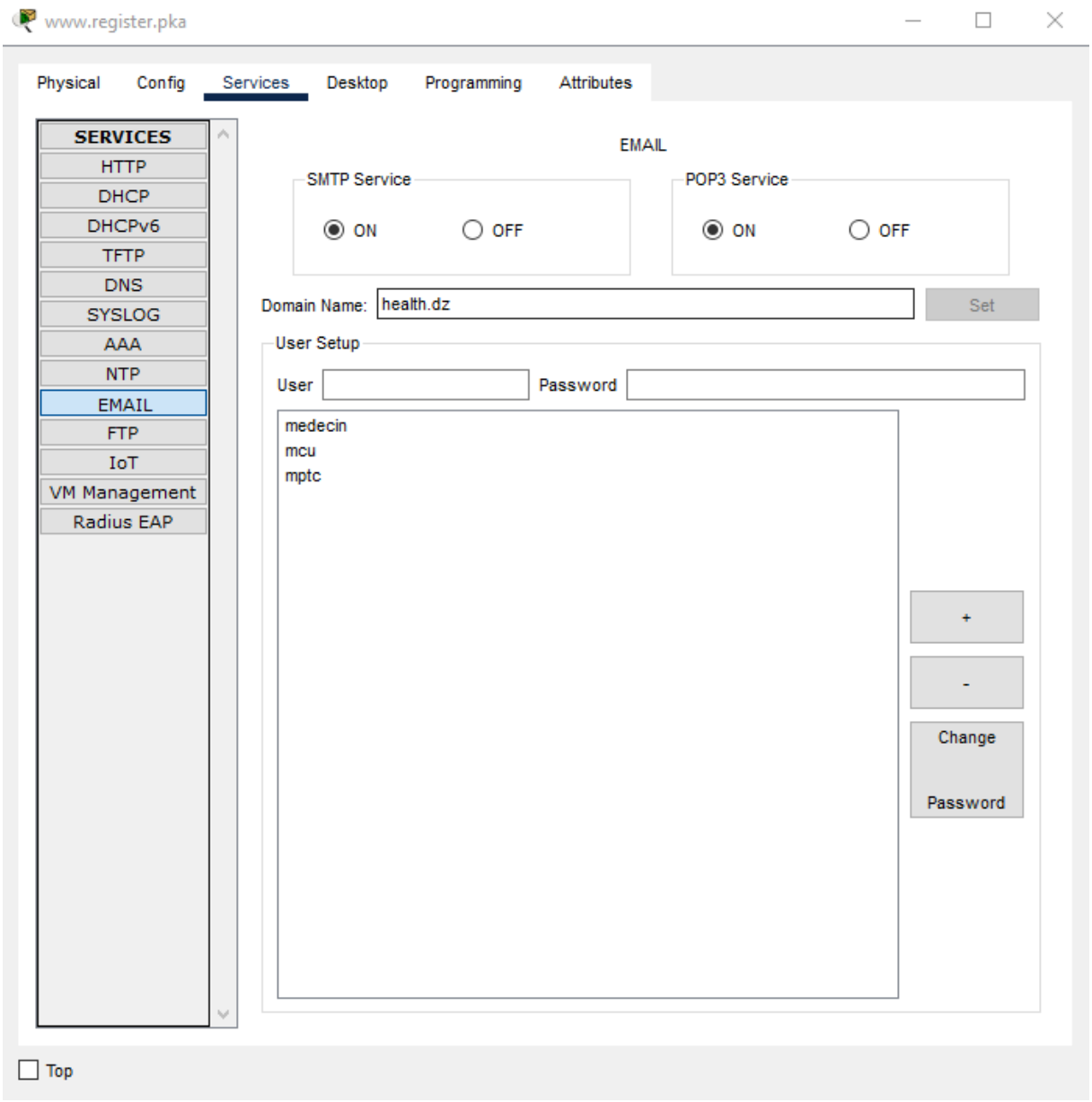

Figure III.7 : La configuration de Mail server

III.5.2 Etape 2 : Ajout des mécanismes de sécurité

Pour améliorer la sécurité dans notre réseau contre les utilisateurs non autorisés et malveillants, en utilisant plusieurs mécanismes de sécurité sur plusieurs niveaux.

1. WPA2-PSK

Les dispositifs IoT peuvent bénéficier d'une connexion réseau sécurisée qui utilise un cryptage fort pour protéger les données transitant entre les périphériques et le point d'accès. Cette méthode nécessite l'utilisation d'une clé pré-partagée, garantissant ainsi que seuls les utilisateurs autorisés disposant de cette clé peuvent accéder au réseau, réduisant ainsi le risque d'accès non autorisé et de compromission des données sensibles transmises par les dispositifs IoT. En conséquence, cela renforce la confidentialité et l'intégrité des données dans un environnement IoT, assurant ainsi un fonctionnement sûr et fiable des appareils connectés.

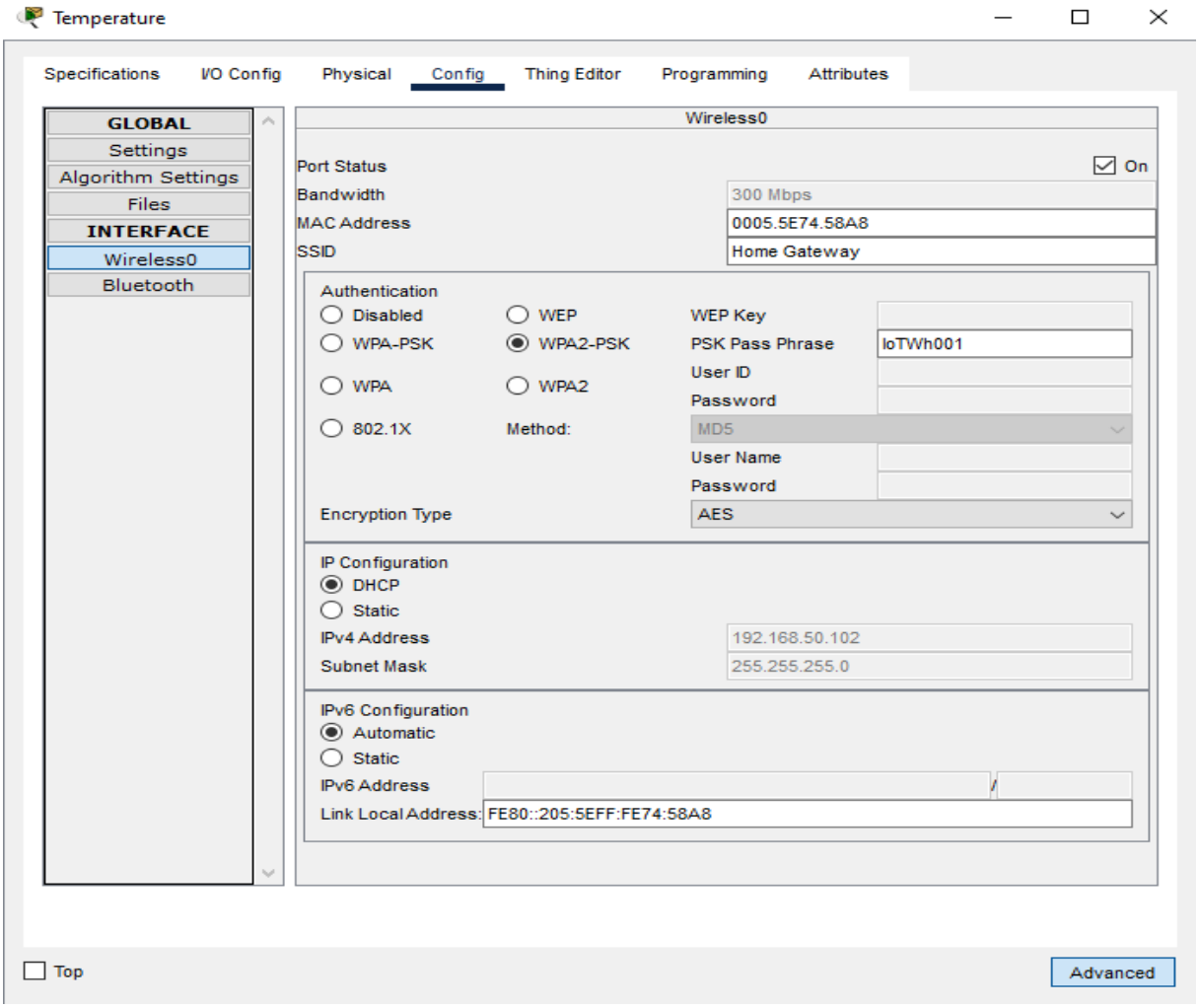

Figure III.8 : Configuration de l'authentification WPA2-PSK

2. Bannières de connexion et de message du jour (MOTD)

Les bannières de connexion et de message du jour sont des messages qui s'affichent aux utilisateurs lorsqu'ils se connectent au routeur. La bannière de connexion informe les utilisateurs qu'ils doivent saisir un mot de passe valide pour se connecter, tandis que la bannière MOTD affiche un message d'avertissement.

```
R1#en
R1#config ter
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#banner login %Login with valid password%
R1(config)#banner motd %Authorized Access Only! Unauthorized access is subject to Federal
Prosecution.%
R1(config)#
R1(config)#enable secret AbcWh001
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console
```

Figure III.9 : La configuration des bannières et le MOTD

Le mot de passe secret pour le mode d'activation est utilisé pour accéder au mode d'activation du routeur. Le mode d'activation est un mode de configuration avancé qui permet aux utilisateurs de configurer des paramètres plus avancés du routeur.

3. Utilisateurs et lignes de console

```
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#username WhAdmin secret AbcLine001
R1(config)#line console 0
R1(config-line)#login local
R1(config-line)#exit
R1(config)#line vty 0 4
R1(config-line)#login local
R1(config-line)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#
```

Figure III.10 : La configuration des utilisateurs et les lignes de console

Les utilisateurs et les lignes de console sont utilisés pour définir les utilisateurs autorisés à se connecter au routeur et les lignes de console sur lesquelles ils peuvent se connecter. La ligne de console 0 est la ligne de console par défaut, tandis que les lignes de console 1 à 4 sont des lignes de console supplémentaires.

4. Les listes de contrôle d'accès (ACL)

Les ACL, ou listes de contrôle d'accès, sont des outils de sécurité utilisés pour gérer les autorisations et contrôler l'accès aux ressources informatiques.

Dans notre architecture, nous avons associé le router R1 et CSP pour déterminer quels utilisateurs ou groupes sont autorisés à accéder.

Les commandes dans la figure ci-dessous configurent une liste de contrôle d'accès pour permettre le trafic de deux hôtes spécifiques (172.18.1.5 et 209.165.201.5) et appliquent cette liste à l'interface gigabit-ethernet 0/2 pour le trafic sortant.

R1(config)#access-list 10 permit host 172.18.1.5 : Cette commande crée ou modifie une liste de contrôle d'accès numérotée (ACL) avec le numéro 10. Elle ajoute une règle à cette ACL qui permet le trafic provenant de l'hôte ayant l'adresse IP 172.18.1.5.

R1(config)# access-list 10 permit host 209.165.201.5 : Cette commande ajoute une deuxième règle à la même ACL (numéro 10), permettant le trafic provenant de l'hôte avec l'adresse IP 209.165.201.5.

R1(config)# interface g0/2 : Cette commande entre en mode de configuration pour l'interface gigabit-ethernet 0/2 du routeur.

R1(config-if) # ip access-group 10 out : Cette commande applique l'ACL numéro 10 à l'interface g0/2, mais dans le sens sortant (out). Cela signifie que le routeur utilisera les règles définies dans l'ACL 10 pour filtrer le trafic sortant de cette interface.

```
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#access-list 10 permit host 172.18.1.5
R1(config)# access-list 10 permit host 209.165.201.5
R1(config)# interface g0/2
R1(config-if)# ip access-group 10 out
R1(config-if)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#
```

Figure III.11 : Les ACLs commandes sur R1

Les ACL sont largement utilisées dans les équipements réseau pour mettre en œuvre des politiques de sécurité et protéger les données sensibles contre les accès non autorisés.

5. Serveur de Registration (IoT Server)

Est pour configurer un serveur d'enregistrement qui fonctionne sur les services HTTP ou HTTPS. Cela pourrait être utilisé pour des fonctionnalités comme l'authentification des utilisateurs.

Le Registration Server permet de configurer des noms d'utilisateur et des mots de passe, fournissant une couche de sécurité par authentification pour accéder au monitoring de notre appareil IoT de e-santé et aussi elle peut gérer plusieurs comptes utilisateurs simultanément, ce qui est essentiel pour les environnements réseau où plusieurs administrateurs ou utilisateurs doivent accéder aux services réseau.

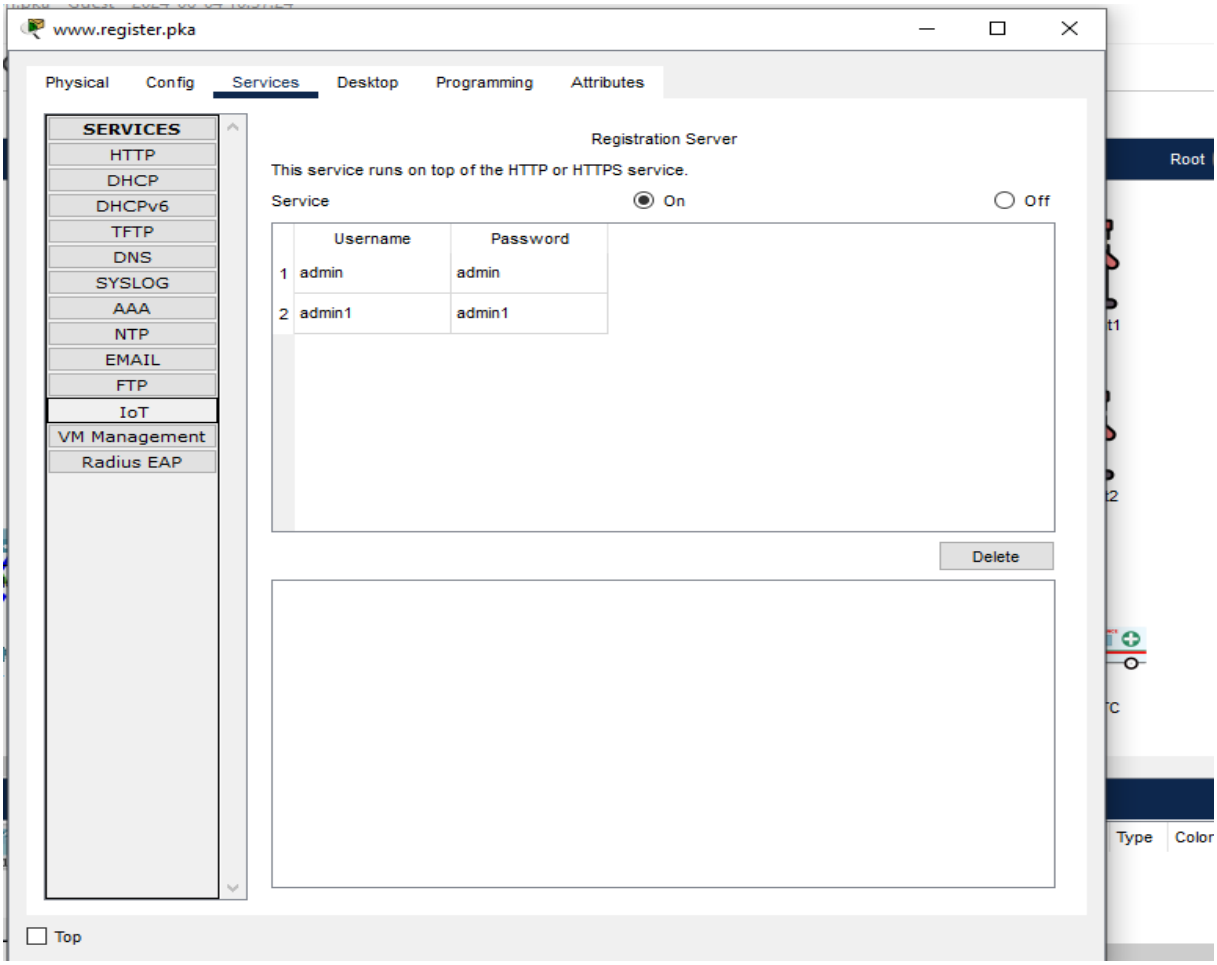

Figure III.12 : La configuration de Registration Server

Pour relier nos périphériques avec le serveur d'enregistrement :

- Dans la section de IoT server on modifie vers Remote server.

- Indiquer l'adresse IP 209.165.201.5 de registration server.
- Enter le nom d'utilisateur et le mot de passe requis pour l'authentification avec le serveur IoT distant.

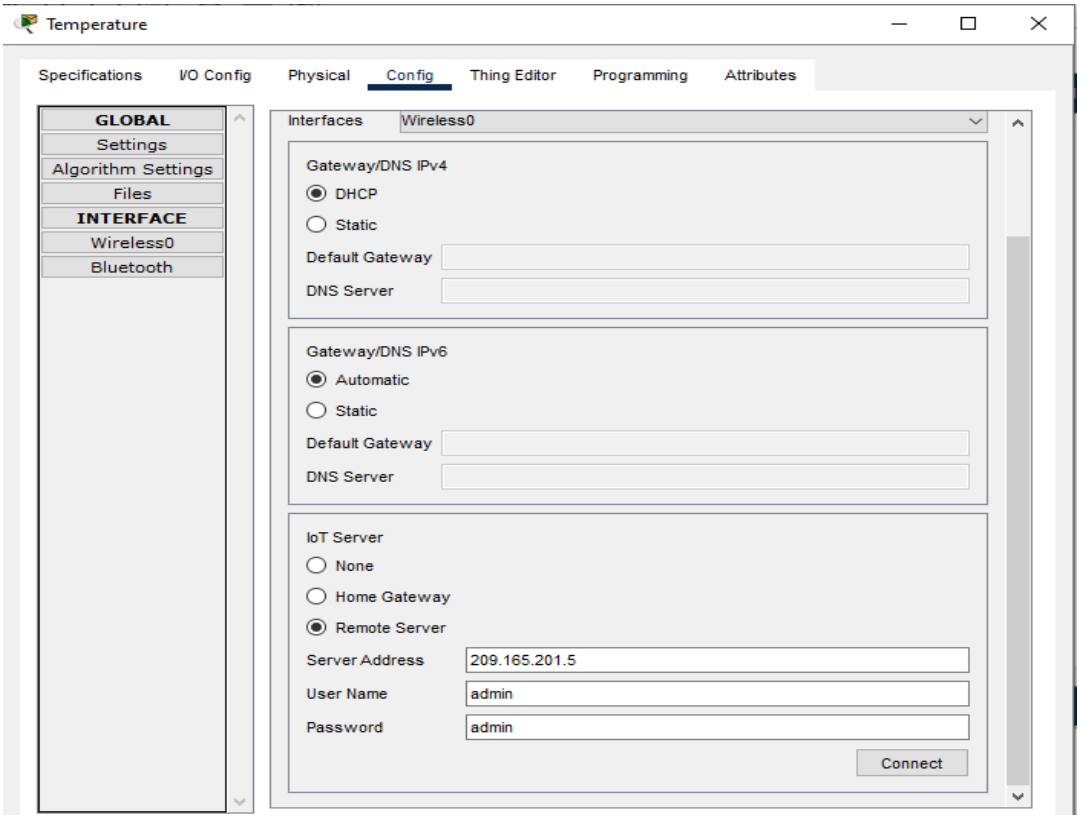

Figure III.13 : Relie les IoT devices ave le registration server

III.5.3 Etape 3 : Test

- **WPA2-PSK**

Si on saisit un mot de passe correcte, il y a une connexion avec le Home Gateway et le contraire.

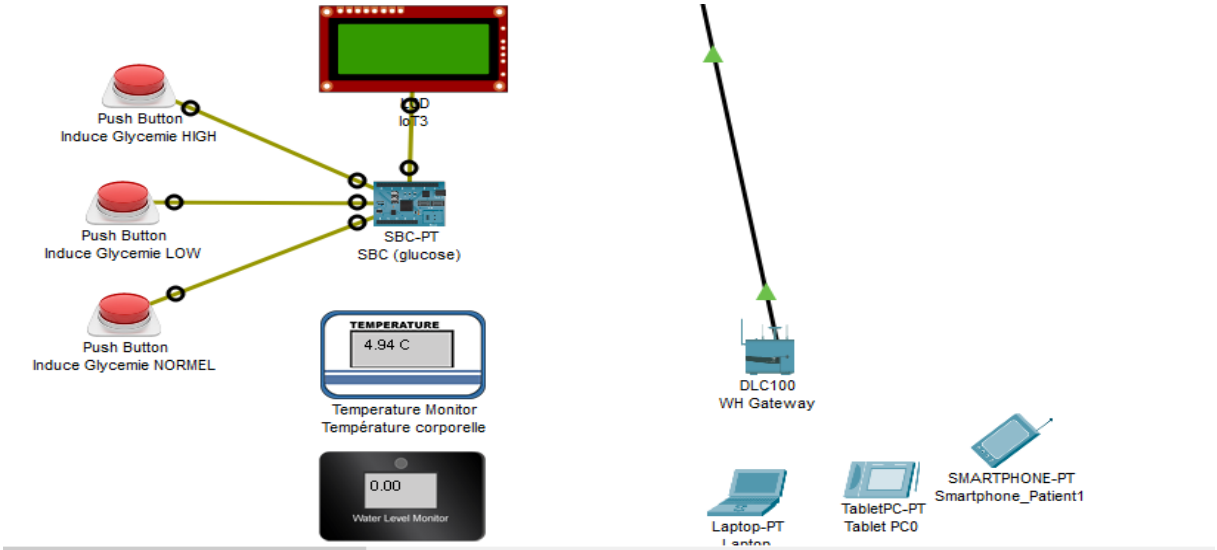

Figure III.14 : WPA2-PSK mot de passe incorrecte

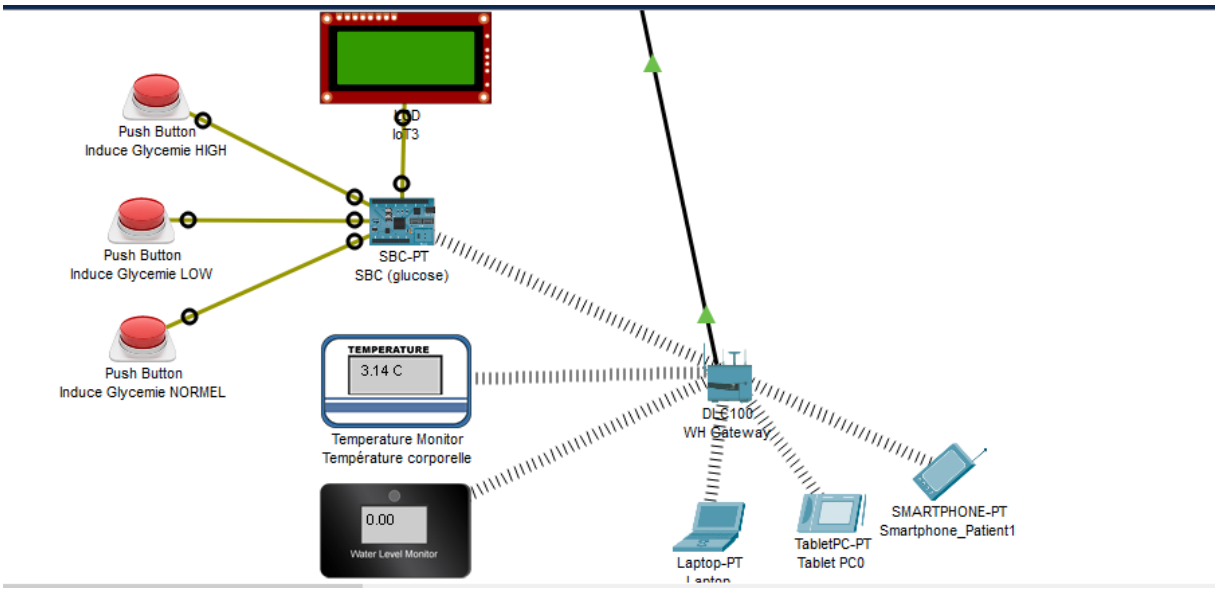

Figure III.15 : WPA2-PSK mot de passe correcte

- **Registration Server**

Pour aller à home page pour voir les valeurs de chaque IoT périphérique, il faut passer par le serveur d'enregistrement et saisir notre Username et Password, si les coordonnées ne sont pas correctes on ne peut pas accéder aux données.

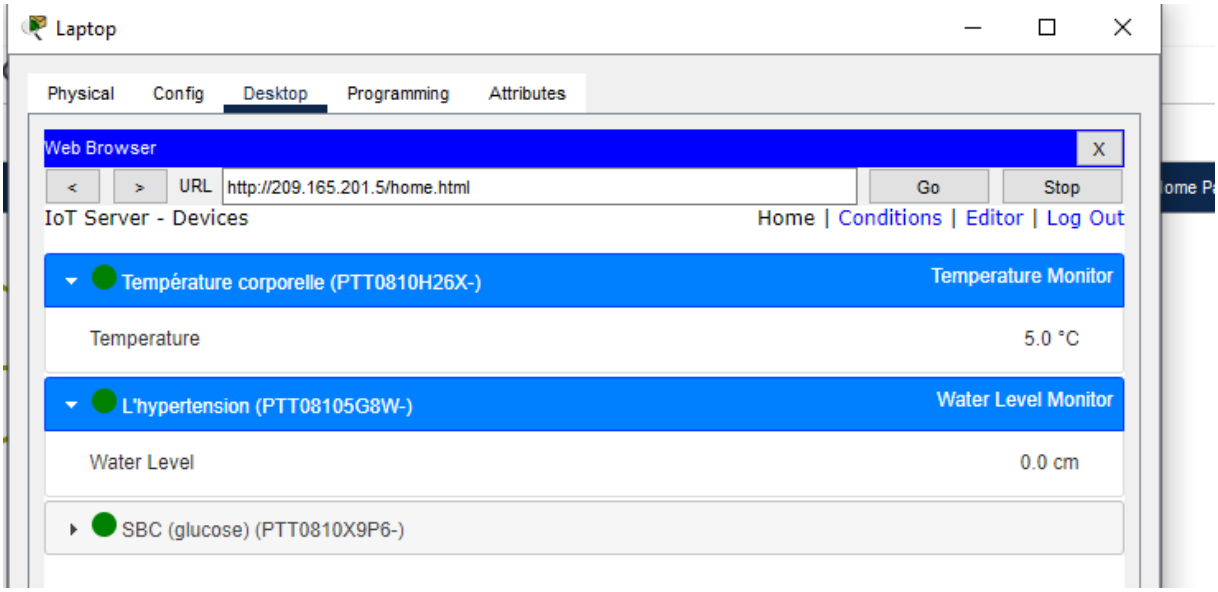

Figure III.16 : Coordonnées correctes et accès autorisé

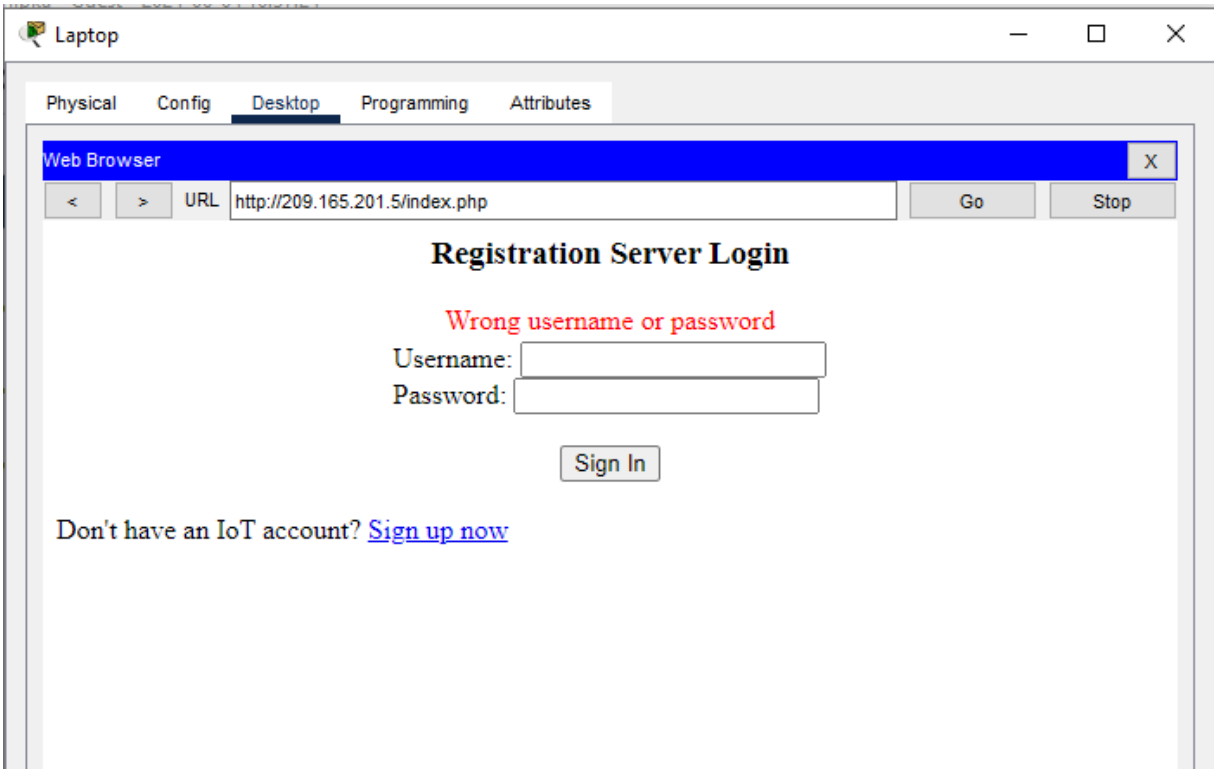

Figure III.17 : Coordonnées incorrectes et accès non autorisé

III.6 Scenario proposé

Voici notre scénario détaillé d'un réseau IoT pour la surveillance d'un patient à domicile, comprenant trois appareils intelligents pour mesurer le glucose, la tension artérielle et la température corporelle :

Dispositifs Intelligents

- Moniteur de Glucose : Un appareil intelligent fixé sur le patient qui mesure en continu le niveau de glucose dans le sang.
- Moniteur de Tension Artérielle : Un brassard connecté qui mesure la pression artérielle du patient à intervalles réguliers.
- Thermomètre Connecté : Un dispositif qui mesure et enregistre en continu la température corporelle du patient.

Collecte et Transmission des Données

- Moniteur de Glucose : Mesure en continu les niveaux de glucose et transmet les données en temps réel à une plateforme cloud sécurisée.
- Moniteur de Tension Artérielle : Enregistre les valeurs systolique et diastolique et les envoie périodiquement au même cloud.
- Thermomètre Connecté : Capture la température corporelle et transmet les données de manière continue.

Détection des Alertes

- Si le moniteur de glucose détecte une valeur de glucose supérieure (en taper sur High) ou inferieur (en taper sur Low) une alerte est automatiquement générée.
- Le système IoT envoie alors un email automatisé au médecin traitant du patient, contenant un résumé des données de glucose.

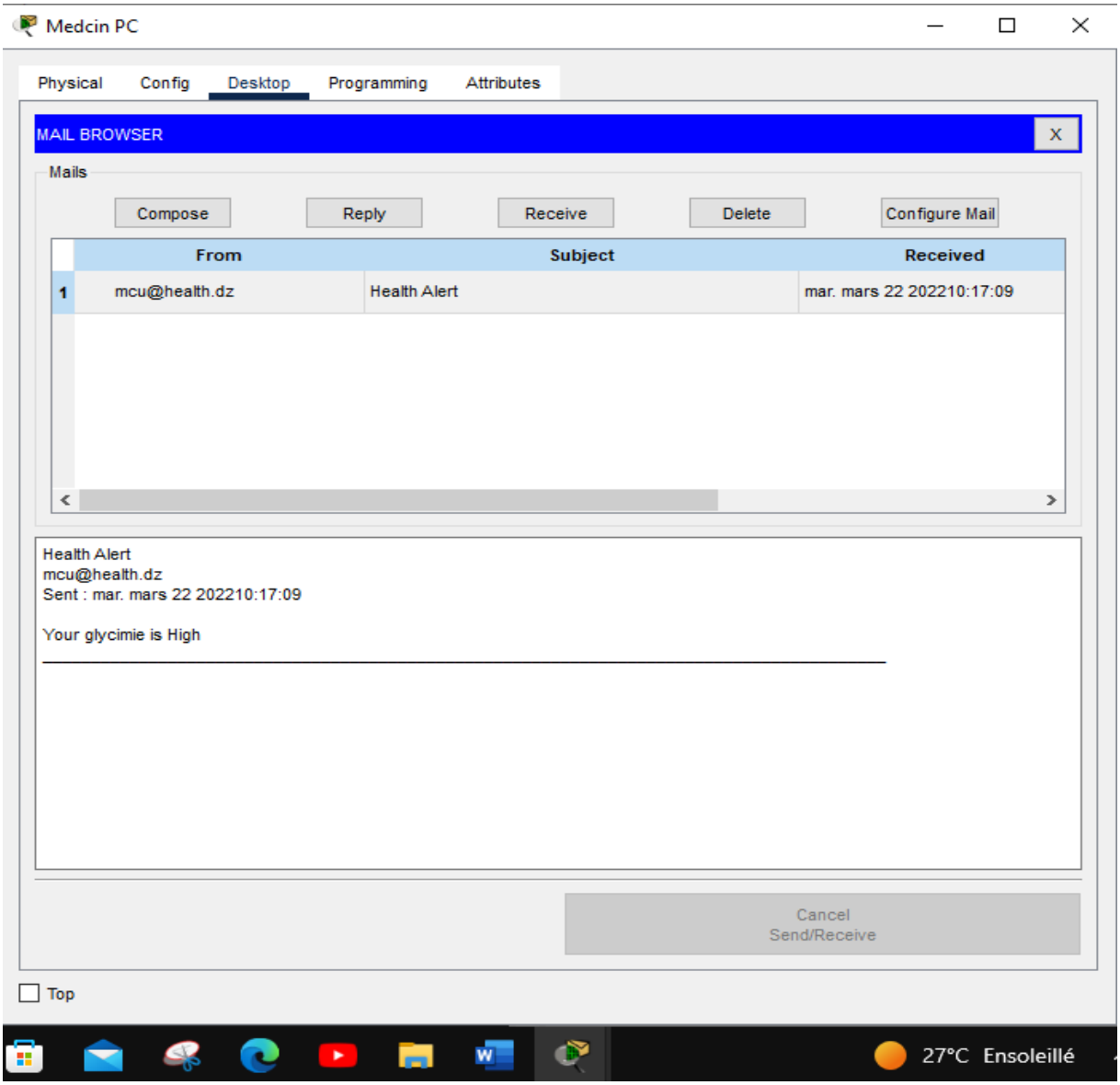

Figure III.18 : La réception d’email

Intervention Médecin

- Le médecin reçoit l'email d'alerte et se connecte à l'application de surveillance médicale via un navigateur web.

- **Authentification** : Le médecin utilise un nom d'utilisateur et un mot de passe pour accéder à l'application sécurisée.

- Une fois connecté, le médecin accède aux données complètes du patient : niveau de glucose, tension artérielle et température corporelle.

- Le médecin évalue les données et, si la situation est jugée urgente (par exemple, hyperglycémie sévère avec hypertension et fièvre), décide d'intervenir rapidement

Notification d'Urgence

- Le médecin envoyer une notification urgente à l'ambulance via un email.
- L'ambulance reçoit la notification sur un dispositif mobile (smartphone ou tablette) et se prépare pour l'intervention

La séquence d'événement :

Mesure et Surveillance : Les appareils intelligents mesurent en continu les paramètres vitaux du patient.

Détection d'Anomalie : Une valeur critique de glucose est détectée.

Notification au Médecin : Un email est envoyé au médecin.

Diagnostic du Médecin : Le médecin se connecte à l'application, évalue la situation et décide de la gravité du cas.

Notification d'Urgence : Si urgent, le médecin envoie une alerte à l'ambulance.

Intervention de l'Ambulance : L'ambulance est informée et se rend au domicile du patient pour le transporter à l'hôpital.

III.7 Implémentation de réseaux

Pour réaliser notre installation de réseau sur Packet tracer, nous composé notre travail au trois niveaux suivants :

III.7.1 Couche cloud

- **Equipements utilisés**

Equipements	**Localisation dans Packet tracer**
Routeur 1941	Network devices > router>1941
Switch-PT	Network Devices>Wireless Devices> Switch-PT
Serveur-PT (DNS/Registrations /CSP)	End devices>End Devices> Serveur-PT

Tableau III.2 : Tableau d'équipement à utilisés

- **Interconnexion des Équipements**

Pour que l'équipement communique entre elle il faut avoir une connexion spécifique dédie à chaque équipent selon son installation interne voir tableau suivant :

Equipement	**Connexion**	**Interface de connexion**
Server DNS	Switch-CSP	Fa 0/2
Server Registration	Switch-CSP	Fa 0/1

Tableau III.3 : Tableau des interconnexions des équipements

III.7.2 Couche Fog

- **Equipements utilisés**

Equipements	**Localisation dans Packet tracer**
Routeur 2911	Network devices > router>2911
Cell Tower	Network devices > Wireless Devices>Cell-Tower
Switch-PT	Network Devices>Wireless Devices> Switch-PT
Serveur-PT (serveur DNS)	End devices>End Devices> Serveur-PT
Cloud-PT	Network Devices>WAN Emulation>Cloud-PT
Cable-Modem	Network Devices>WAN Emulation> Cable-Modem

Tableau III.4 : Tableau d'équipement à utilisés

- **Interconnexion des Équipements**

Equipement	**Connexion**	**Interface de connexion**
Cell Tower	Central office server	Coax0 – Coax 0/0
Central office server	Router -ISP	Fa 0/0 – Gig 0/1
Server Registration	Switch-CSP	Fa 0 – Fa 0/2
Cloud	Router-CSP	Gig 8 – g 0/1

Cable Modem	Cloud	Coax 7 – Gig 8

Tableau III.5 : Tableau des interconnexions des équipements

III.7.3 Couche IoT

- **Equipements utilisés**

Equipements	**Localisation dans Packet tracer**
Sbc(Glucose)	Implémenter (n'exister pas sur packet tracer)
Température	Implémenter (n'exister pas sur packet tracer)
L'hypertension	Implémenter (n'exister pas sur packet tracer)
Home Gateway	Network devices > Wireless Devices> Home Gateway
Laptop Smartphone Tablet	End devices>End Devices>

Tableau III.6 : Tableau d'équipement à utilisés

- **Interconnexion des Équipements**

Equipements	**Connexion**	**Interface de connexion**
Cable Modem	Home Gateway (DL100)	Port1-internet
Laptop	Home Gateway (DL100)	Wireless-wireless
SBC(Glucose)	Home Gateway (DL100)	Wireless-wireless
Température	Home Gateway (DL100)	Wireless-wireless
L'hypertension	Home Gateway (DL100)	Wireless-wireless

Tableau III.7 : Tableau des interconnexions des équipements

III.8 Diagramme de flux

Un diagramme de flux est une représentation graphique d'un processus ou d'un système qui montre les étapes séquentielles de ce processus ou de ce système. Il utilise des symboles standard pour illustrer les différentes étapes, actions, décisions, et connexions entre elles, facilitant ainsi la compréhension des opérations et des flux d'information ou de travail.

La figure III.18 montre l'organigramme du processus de simulation du capteur de glucose. Lorsqu'un incendie est détecté, l'appareil de glucose affiche cette information sur un afficheur LCD et envoie automatiquement un email au médecin. Toutes ces fonctions sont programmées et contrôlées via le microcontrôleur MCU.

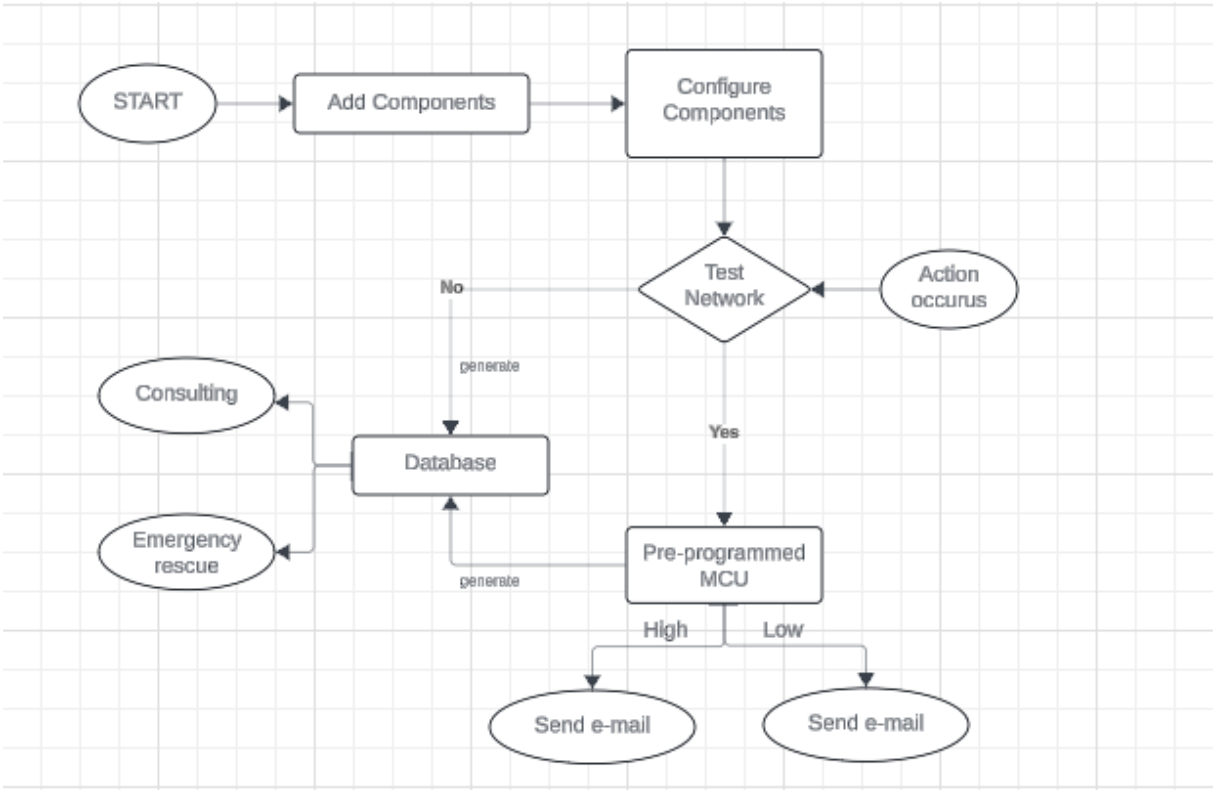

Figure III.19 : Le diagramme de flux de capteur glucose processus

Le graphe de figure III.19 illustre le processus optimisé par les dispositifs intelligents commence par la détection d'une situation urgente, qui peut être identifiée par des dispositifs intelligents de surveillance continue ou par notification d'urgence.

En cas de situation urgente, le système envoie automatiquement un email vers une médecin.

Parallèlement, le système collecte et transmet les données du patient à l'ambulance. Ces données peuvent inclure des informations sur l'état de santé du patient

Une fois le patient pris en charge par l'ambulance, le système continue de surveiller son état de santé et de transmettre les données à l'hôpital.

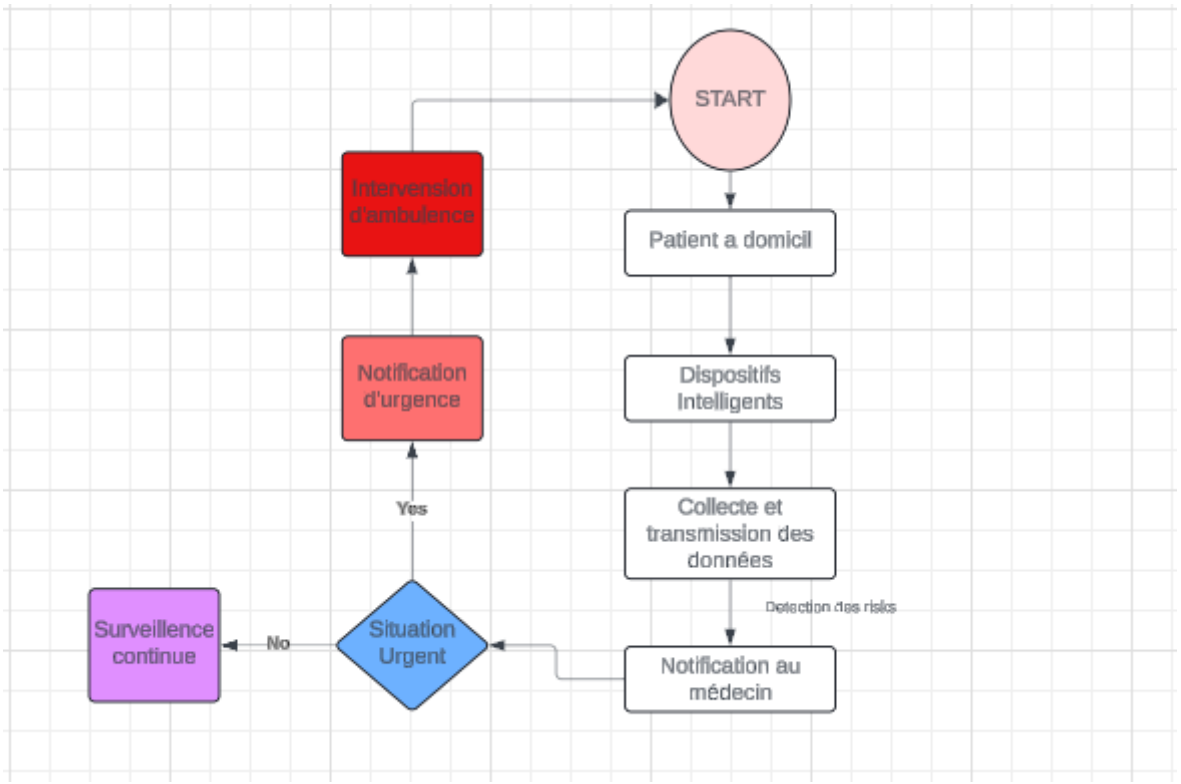

Figure III.20 : Diagramme de flux de données et de control d'un processus optimisé par les dispositifs intelligents

III.9 Conclusion

Ce chapitre a été consacré à la simulation d'un système de e-santé avec différents utilisateurs (patients, médecins et ambulances) ainsi que des capteurs IoT pour collecter les données des patients. Nous avons également présenté l'architecture proposée, en détaillant les mécanismes de sécurité utilisés. De plus, nous avons décrit le scénario et la configuration mise en place pour l'interconnexion de réseau.

Conclusion générale

Ce projet de fin d'études (PFE) s'est concentré sur la simulation des mécanismes de sécurité dans les réseaux e-santé IoT en utilisant Cisco Packet Tracer. L'objectif principal était de concevoir, implémenter et évaluer des solutions de sécurité pour protéger les dispositifs et les données médicales sensibles dans un environnement IoT.

Le projet a commencé par une analyse approfondie de l'Internet des objets (IoT), mettant en lumière ses applications spécifiques dans le domaine de la santé. Les différents composants, architectures, et protocoles de communication IoT ont été étudiés, fournissant une base solide pour la compréhension des défis et des opportunités associés aux réseaux e-santé.

Ensuite, une exploration détaillée des menaces et des vulnérabilités propres aux réseaux IoT a été menée. Les mécanismes de sécurité, tels que le chiffrement des données, l'authentification des dispositifs, et les systèmes de détection et de prévention des intrusions, ont été analysés pour déterminer leurs capacités à sécuriser les réseaux e-santé.

Le cœur du projet a consisté en la conception et la simulation d'un réseau e-santé IoT sécurisé en utilisant Cisco Packet Tracer, divers mécanismes de sécurité ont été implémentés et testés. Les scénarios de simulation ont permis d'évaluer l'efficacité de ces mécanismes en conditions réelles, révélant leur impact sur la performance réseau et leur capacité à prévenir les accès des gens non autoriser.

Ce projet a démontré l'importance cruciale de la sécurité dans les réseaux e-santé IoT, montrant que des mesures de sécurité bien conçues et implémentées améliorent grandement la protection des dispositifs et des données médicales, tout en assurant la continuité et la fiabilité des services de santé. La sécurisation des réseaux e-santé IoT est essentielle pour le futur de la santé connectée. Ce PFE apporte une contribution significative en proposant des solutions pratiques et des recommandations pour renforcer la sécurité des infrastructures IoT médicales.

Références bibliographiques

[1] Hend Ben Hadji, « Les fondamentaux de l'iot », Prida Workshop, 2020 (disponible sur : https://www.itu.int/en/ITU-D/Regional-Presence/Africa/Documents/PRIDA%202020%20-%20ONLINE%20Capacity%20building%20%26%20digital%20services/FR_Workshop_Slides.pdf). Consulté le : 22/02/2024.

[2] Internet of Things (IoT), ISO/IEC JTC 1 Information Technology, 2014 (disponible sur : https://www.iso.org/files/live/sites/isoorg/files/developing_standards/docs/en/internet_of_things_report-jtc1.pdf). Consulté le : 22/02/2024.

[3] Sameh BEN FREDJ, « bien choisir sa plate-forme pour faire communiquer ses objets connectés », 2015. (disponible sur : https://www.usine-digitale.fr/article/bien-choisir-sa-plate-forme-pour-faire-communiquer-ses-objets-connectes.N342721). Consulté le : 23/02/2024.

[4] Faker Skandrani, « Architecture IoT : L'essentiel à savoir »**,** 2022 (disponible sur : https://iotindustriel.com/iot-iiot/architecture-iot-lessentiel-a-savoir/). Consulté le : 23/02/2024.

[5] Michael millot et Arnaud paoletti. « Decryptage de l'ecosystème de l'iot ». Salon iot world. 2018. (disponible sur : https://www.digitalcorner-wavestone.com/2016/04/salon-iot-world-decryptage-de-lecosysteme-de-liot-2/). Consulté le : 22/05/2024.

[6] Lexhan, « Quel protocoles Iot choisi pour ses objets connectés », 2022 (disponible sur : https://www.lexhan-group.fr/blog/connectivite/protocoles-iot-pour-objets-connectes/). Consulté le : 22/05/2024.

[7] Deborah Dos Santos, « Comprendre la RFID en 10 points **»,** (disponible sur : https://sbedirect.com/fr/blog/article/comprendre-la-rfid-en-10-points.html). Consulté le : 22/05/2024.

[8] LoRAWAN Public – Le protocole radio bas débit opéré. (disponible sur : http://telereleve-energies.fr/technologie-lorawan-public). Consulté le : 30/04/2024.

[9] **M**obility work, « Tout savoir sur l'industrie 4.0 ». 2022. (disponible sur : https://mobility-work.com/fr/blog/industrie-4-0/). Consulté le : 30/04/2024.

[10] Laura MILLET JIMÉNEZ, « IoT : Technologies, Cas d'usages, avantages et limites - Guide complet », 2023. (disponible sur : https://blog.ubisolutions.net/iot-technologies-cas-dusages-avantages-et-limites-guide-complet). Consulté le 30/04/2024.

[11] Fatma Merabet. « Solutions de sécurité pour l'internet des objets dans le cadre de l'assistance à l'autonomie à domicile. ». Thèse de Doctorat : Université de Limoges; Université Mouloud Mammeri (Tizi-Ouzou, Algérie), 2021.

[12] Simmons, Gustavus J. "Symmetric and asymmetric encryption." ACM Computing Surveys (CSUR) 11.4 (1979): 305-330.

[13] G. Van Assche, "Permutation-based cryptography for the Internet of Things". RIOT Summit 2017.

[14] TALEB, F. Support de cours "Cryptologie", département d'informatique, Université Dr Moulay TAHAR, Saida, Algérie, 2019.

[15] Hartwig Mayer. "Ecdsa security in bitcoin and ethereum: a research survey. CoinFaabrik, June, 28.

[16] kevunie, « Authentification : guide complet sur ce mode de sécurisation en ligne », 2021. (disponible sur : https://www.objetconnecte.com/authentification-guide-complet/). Consulté le : 30/05/2024.

[17] Achraf Fayad. « Secure authentication protocol for Internet of Things. Networking and Internet Architecture ». Thèse de Doctorat Institut Polytechnique de Paris, 2020.

[18] TALEB Fadia, « Système d'authentification dans l'internet des objets : Étude et sécurisation ». Thèse de doctorat Université Moulay Tahar de Saida, 2022.

[19] Cisco Networking Academy. https://www.netacad.com/courses/packet-tracer

[**20**] T. G. AL-Jaf and E. H. Al-Hemiary, "Internet of Things Based Cloud Smart Monitoring for Asthma Patient," Qalaai Zanist Scientific Journal, vol. 2, no. 2, pp. 359 - 364, 2017.

[**21**] AL-JOBOURY, Istabraq M. et HEMIARY, Emad H. Internet of things architecture-based cloud for healthcare. Iraqi Journal of Information and Communication Technology, 2018, vol. 1, no 1, p. 18-26.

[**22**] ALSBOU, Nesreen, PRICE, Dakota, et ALI, Imad. IoT-based smart hospital using cisco packet tracer analysis. In : 2022 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS). IEEE, 2022. p. 1-6.

[23] Une nouvelle dimension pour l'IdO (Source ITU 2005 [INT 2005] tirée de [CHA 2012])

Résumé

Ce projet de fin d'études se concentre sur la simulation des mécanismes de sécurité dans les réseaux e-santé IoT à l'aide de Cisco Packet Tracer. Le projet comprend trois étapes principales : une analyse des concepts IoT, une étude des mécanismes de sécurité appropriés, et la conception et simulation d'un réseau e-santé sécurisé. Les résultats montrent que les mécanismes de sécurité implémentés, tels que le chiffrement des données, l'authentification des dispositifs, et les systèmes de détection et de prévention des intrusions, peuvent efficacement protéger les données médicales et assurer la fiabilité des services e-santé.

Mots clés : internet des objets, e-santé, sécurité des réseaux, simulation, cisco packet tracer.

Abstract

This final year project focuses on simulating security mechanisms in IoT e-health networks using Cisco Packet Tracer. The project involves three main stages: analyzing IoT concepts, studying appropriate security mechanisms, and designing and simulating a secure e-health network. The results demonstrate that the implemented security mechanisms, such as data encryption, device authentication, and intrusion detection and prevention systems, can effectively protect medical data and ensure the reliability of e-health services.

Keywords: internet of things, healthcare, network security, simulation, cisco packet tracer.

ملخص

يُركِّز هذا المشروع النهائي على محاكاة آليات الأمان في شبكات الصحة الإلكترونية المتصلة بإنترنت الأشياء باستخدام Cisco Packet Tracer. يتضمن المشروع ثلاث مراحل رئيسية: تحليل مفاهيم إنترنت الأشياء، دراسة آليات الأمان المناسبة، وتصميم ومحاكاة شبكة صحية إلكترونية آمنة. تُظهِر النتائج أن آليات الأمان المطبَّقة، مثل تشفير البيانات، مصادقة الأجهزة، وأنظمة كشف ومنع التطفل، يمكنها حماية البيانات الطبية بفعالية وضمان موثوقية خدمات الصحة الإلكترونية.

الكلمات المفتاحية: انترنت الأشياء، الصحة الالكترونية، أمن الشبكات، محاكاة، Cisco packet tracer .