Ecole Nationale
Supérieure
d'Ingénieurs
de Tunis

الجمهورية التونسية
وزارة التعليم العالي والبحث العلمي
جامعة تونس
المدرسة الوطنية العليا للمهندسين بتونس

Rapport de Matière Internet Of Things

En vue de l'obtention

Validation de la projet internet of things

Option :

Projet internet of things : Smart Office

Elaboré par :
Ben Jaafer Amen

Ecole nationale supérieure d'Ingénieurs de Tunis (ENSIT) **Année universitaire :2022/2023**
Avenue Taha Hussein, 1008 Tunis B.P 56 Bab Menara
Tél : (+216)71 49 60 66/71 49 40 20/71 39 95 25
Fax : (+216)71 39 11 66

Notre Solution :

1. Justification par rapport à l'environnement tunisien :

Tunisie Telecom vient de lancer avec son partenaire technologique Chifco les solutions domotiques Smart Office
L'offre Smart Office est une offre à la carte permettant au client entreprise de superviser ses bâtiments, et d'être alerté en temps réel en cas d'intrusion ou d'incidents durant son absence tout en optimisant la consommation d'énergie.
Ce pack est composé d'une Box ou Centrale domotique avec une télécommande et 8 capteurs au choix du client parmi une gamme de capteurs qui gèrent la sécurité et l'énergie.

2. Etude et justification des technologies de communication utiliser :

En informatique et, particulièrement dans l'univers de l'IoT, il se passe exactement la même chose. Tout est affaire de protocole lorsqu'il s'agit d'échanger des informations. Les protocoles sont différents selon le réseau auquel l'objet IoT appartient. Les différences se portent sur le langage utilisé, la distance, le délai, la fréquence, la qualité des connexions et le volume des messages à transmettre…

Le Wi-Fi :

Figure 1: Logo Wifi

Les réseaux IoT à courte portée sont souvent synonymes de Wifi. « Vieille » technologie, universelle et en perpétuelle évolution, le Wi-Fi permet de transporter beaucoup d'informations très rapidement (600Mbits/s au maximum). Protocole bidirectionnel, il permet de mettre à jour les micrologiciels des appareils IoT à distance et de prendre la main sur leur OS à travers le réseau.

Bluetooth et Bluetooth Low Energy :

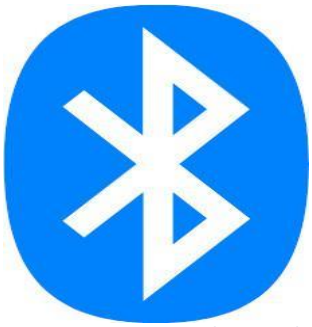

Figure 2: Logo Bluetooth

Le Bluetooth Low Energy est le protocole de communication sans-fil le plus utilisé dans le monde, puisque présent dans tous les smartphones et tous les PC portables (laptops) modernes. Il équipe également toutes les montres connectées et autres capteurs d'activité (wearables).

RFID et NFC :

Figure 3: Logo RFID

La Radio Frequency Identification n'a besoin d'aucune source énergétique pour fonctionner. C'est là son grand atout. La RFID sert à identifier des biens, des machines, des personnes, des animaux… On utilise le protocole pour de la gestion de stocks et la traçabilité des produits. On compte aujourd'hui plus de 20 milliards de tags (badges) RFID dans le monde.

Les protocoles de réseaux GSM :

Figure 4 : Réseaux GSM

2G, 3G, 4G, 5G : les **réseaux GSM** sont des réseaux cellulaires. Le signal est capté par une antenne couvrant un certain volume de captation et est relayé au sein d'un réseau propriétaire puis à Internet.

3. Description de votre architecture et de son implémentation :

Figure 5:Architecture du projet

1. **Serrure de porte basée sur RFID :**

La porte ne peut être déverrouillée qu'en utilisant une carte RFID valide. Si quelqu'un veut entrer dans le bureau, il ou elle doit montrer la RFID. Si le RFID est valide, la porte sera ouverte, sinon non.

2. **Smart Windows, basé sur la lumière et la pluie :**

Fenêtre intelligente qui s'ouvrira automatiquement le matin et qu'il n'y a pas de pluie à l'aide d'un capteur de pluie, d'un capteur photo. S'il fait nuit, la fenêtre sera fermée pour éviter les moustiques même s'il pleut.

3. **Solar Power battery charging :**

Basé sur l'énergie solaire, le ventilateur et la lumière fonctionneront automatiquement. Mais, si l'alimentation de la batterie se termine, ils ne fonctionneront pas. La batterie ne se charge que lorsqu'il y a suffisamment de lumière.

4. **Protection antivol :**

Pour fournir une protection antivol, un capteur de déclenchement est utilisé, si quelqu'un brise la fenêtre et entre, le capteur de déclenchement émettra une sirène d'alerte.

5. **Auto fan & coffee maker :**

Lorsque quelqu'un entre dans la cantine, le ventilateur et la cafetière s'allument en détectant le mouvement.

6. **Music Player :**

La musique peut être lue à l'aide d'un lecteur de musique via Bluetooth sur un haut-parleur portable. But de divertissement.

7. **Smart street lamp :**

S'allume quand il fait nuit grâce au capteur photo. Économie d'énergie.

8. **Smart garage :**

S'ouvre lorsqu'il détecte de la fumée, cela signifie que la voiture est allumée. Soit il entrera, soit il sortira. La porte de garage se ferme lorsqu'il n'y a pas de fumée, ce qui signifie que la voiture est loin ou qu'elle est éteinte à l'intérieur du garage.

9. **Fire alarm & smoke alarm :**

Si quelque chose prend feu, le détecteur d'incendie émettra une sirène pour alerter tout le monde. Si une quantité ridicule de fumée est générée par le véhicule, le détecteur de fumée déclenchera une alerte sirène.

Appareils IOT :

Fan, light, Windows, Garage, Door, Battery, Siren, Solar panel, Appliance, Portable music player, Motion Detector, Street lamp, Old car, Fire monitor, RFID card, RFID reader, Trip sensor, Fire sprinkler, Smoke detector.

Sensors :

Custom made Rain sensor, Photo sensor, Smoke sensor.

Actuators :

Led, speaker, alarm

4. Etude des attaques possibles sur votre système :

Attaques par déni de service (DoS) :

Le nœud fonctionnant sur batterie peut recevoir un très grand nombre de demandes, qui semblent légitimes, envoyées par un attaquant. Les attaques peuvent entraîner des effets indésirables (exemple panne de courant).

Réplication de nœuds :

L'objectif principal d'une telle attaque est d'ajouter un objet en dupliquant le numéro d'identification à un ensemble actuel d'objets. Une baisse remarquable des performances du réseau peut se produire à cause de cette attaque.

De plus, à l'arrivée des paquets sur une réplique, elle peut non seulement corrompre les paquets, mais aussi les détourner, causant ainsi de graves dommages aux systèmes IoT. Il est également capable d'exécuter un protocole de révocation d'objet.

Nœud malveillant :

Dans l'environnement IoT, certains nœuds peuvent obtenir un accès non autorisé à un réseau IoT et à d'autres objets. Ceci conduit à la perturbation des fonctionnalités et de la cybersécurité de l'environnement.

Attaque par canal auxiliaire :

C'est une attaque contre les techniques de cryptage, qui peut affecter leur sécurité et leur fiabilité. Dans l'attaque par canal latéral, les objets effectuent leurs opérations normalement en divulguant des informations critiques.

Attaque de collisions :

Ce type d'attaques peut être lancé sur la couche de liaison. Elles consistent à ajouter du bruit dans le canal de communication, ce qui entraîne la retransmission de paquets et la consommation de ressources énergétiques limitées.